

Security Guide for Cisco Unified Communications Manager Release 14 and SUs

First Published: 2022-06-16

Last Modified: 2026-04-08

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface xv

About this Manual xv

Audience xvii

Document Conventions xviii

Legal Compliance xviii

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

PART I

An Introduction to Unified CM Security 5

CHAPTER 2

An Overview 7

System Requirements 7

Best Practices 7

Device Resets, Server and Cluster Reboots, and Service Restarts 8

Reset Devices, Servers, Clusters, and Services 9

Media Encryption with Barge Setup 9

Common Icons 9

CHAPTER 3

Configurations 11

Security Configurations 11

CHAPTER 4

Default Security 13

Default Security Overview 13

Initial Trust List 13

Certificate Management Changes for ITLRecovery Certificate 15

ITLRecovery Certificate 15
Interactions and Restrictions 16
Trust Verification Service 16
Authentication, Integrity, and Authorization 16
Image Authentication 17
Device Authentication 17
File Authentication 17
Signaling Authentication 18
Digest Authentication 18
Authorization 20
NMAP Scan Operation 21
Autoregistration 21
Migrate IP Phones Between Clusters with Cisco Unified Communications Manager and ITL Files 21
Encryption 22
Secure End Users Login Credentials 22
Signaling Encryption 23
Media Encryption 23
SCCP Gateway and Hardware Conference Bridge Support for Secure Hash Algorithm (SHA-2) 25
AES 256 Encryption Support for TLS and SIP SRTP 26
AES 256 and SHA-2 Support in TLS 27
AES 256 Support in SRTP SIP Call Signaling 28
Cisco Unified Communications Manager Requirements 28
Interactions and Restrictions 29
AES 80-Bit Authentication Support 29
SRTP Cipher Mismatch with Media Streaming Devices 30
Self-encrypting Drive 30
Configuration File Encryption 30
Default Security Administration Tasks 31
Update ITL File for Cisco Unified IP Phones 31
Obtain ITL File Status 32
Obtain Cisco Unified IP Phone Support List 32
Roll Back Cluster to a Pre-8.0 Release 33
Switch Back to Release 8.6 or Later After Revert 34
Perform Bulk Reset of ITL File 35

Reset CTL Localkey 36
View the Validity Period of ITLRecovery Certificate 36
Set Up Authentication and Encryption 37

PART II **Basic System Security** 39

CHAPTER 5 **Certificates** 41
Certificate Management 41
Certificate Overview 41
Certificate Types 42
Phone Certificate Types 43
Server Certificate Types 44
Third-Party CA-Signed Certificates 45
Support for Certificates from External CAs 46
Certificate Signing Request Key Usage Extensions 47
Certificate Tasks 47
Bulk Certificate Export 48
Show Certificates 48
Download Certificates 49
Install Intermediate Certificates 49
Delete a Trust Certificate 50
Generate a Certificate Signing Request 51
Generate Self-Signed Certificate 54
Regenerate a Certificate 58
Add Certificate Authority-Signed CAPF Root Certificate to the Trust Store 66
Update the CTL File 66
Interactions and Restrictions 66
Certificate Monitoring and Revocation 67
Certificate Monitoring Overview 67
Certificate Monitoring Configuration 67
Certificate Revocation Overview 68
Certificate Revocation Configuration 68
Simplified Certificate Management 70
Simplified Certificate Management Overview 70

Simplified Certificate Management User Interface Updates 71
Reuse Multi-Server Tomcat Certificate for CallManager 71

CHAPTER 6 **Certificate Authority Proxy Function 73**
Certificates Authority Proxy Function Overview 73
Certificates Authority Proxy Function Configuration Task Flow 75
Upload Root Certificate for Third-Party CAs 76
Upload Certificate Authority (CA) Root Certificate 77
Configure Online Certificate Authority Settings 78
Configure Offline Certificate Authority Settings 79
Activate or Restart CAPF Services 80
Configure CAPF Settings in a Universal Device Template 80
Update CAPF Settings via Bulk Admin 81
Configure CAPF Settings for a Phone 83
Set KeepAlive Timer 83
Certificates Authority Proxy Function Administration Task Flow 84
Run Stale LSC Report 84
LSC Generation via CAPF 85
View Pending CSR List 85
Delete Stale LSC Certificates 85
CAPF System Interactions 86
CAPF Examples with 7942 and 7962 Phones 87
CAPF Interaction with IPv6 Addressing 88

CHAPTER 7 **Security Modes 91**
Security Modes Overview 91
Non Secure Mode (Default Mode) 91
Configure Secure Mode 91
Mixed Mode 92
Verify Security Mode 93
SAST Roles of CTL File 93
SIP OAuth Mode 94
SIP OAuth Configuration Through CLI 94

CHAPTER 8 SIP OAuth Mode 97

SIP OAuth Mode Overview 97

SIP OAuth Mode Prerequisites 98

SIP OAuth Mode Configuration Task Flow 99

Upload CA Certificate to the Phone Edge Trust 100

Enable OAuth Access Token for Devices 100

Configure Refresh Logins 101

Configure OAuth Ports 101

Configure OAuth Connection to Expressway-C 102

Enable SIP OAuth Mode 103

Restart Cisco CallManager Service 103

Configure Device Security Mode in Phone Security Profile 103

Configure SIP Oauth Registered Phones for MRA Mode 104

CHAPTER 9 TFTP Encryption 107

TFTP Encrypted Configuration Files Overview 107

TFTP Encrypted Configuration Files Tips 108

Encryption for Phone Configuration File Task Flow 109

Enable TFTP Encryption 109

Configure SHA-512 Signing Algorithm 110

Verify LSC or MIC Certificate Installation 110

Update CTL File 111

Restart Services 111

Reset Phones 112

Disable TFTP Encrypted Configuration Files 112

CHAPTER 10 Cipher Management 115

Cipher Management 115

Recommended Ciphers 116

Configure Cipher String 117

Cipher Limitations 120

Cipher Restrictions 128

CHAPTER 11 **Phone Security** 131

Phone Security Overview 131

Phone Hardening Overview 132

Set Up Phone Hardening 135

Trusted Devices 136

Cisco Unified Communications Manager Administration 136

Phone Model Support 137

View Phone Security Settings 137

Set Up Phone Security 138

Preferred Vendor SIP Phone Security Set Up 138

Set Up Preferred Vendor SIP Phone Security Profile Per-Device Certificates 138

Set Up Preferred Vendor SIP Phone Security Profile Shared Certificates 139

Migrate Phones from One Cluster to Another Cluster 140

Phone Security Interactions and Restrictions 140

Phone Security Profiles 141

Phone Security Profile Settings 142

Phone Security Configuration Task Flow 151

Find Phone Security Profile 152

Set Up Phone Security Profile 152

Apply Security Profiles to Phone 153

Synchronize Phone Security Profile with Phones 153

Delete Phone Security Profile 154

Find Phones with Phone Security Profiles 154

SIP Trunk Security Profile Interactions and Restrictions 155

Digest Authentication for SIP Phones Overview 155

Digest Authentication for SIP Phones Prerequisite 156

Digest Authentication for SIP Phones Configuration Task Flow 156

Assign Digest Credentials to Phone User 157

Enable Digest Authentication in Phone Security Profile 157

Assign Digest Authentication to the Phone 157

Configure SIP Station Realm 158

End User Digest Credential Settings 158

CHAPTER 12 **Secure Conference Resources Setup** 159

Secure Conference 159
Conference Bridge Requirements 160
Secure Conference Icons 161
Secure Conference Status 161
Ad Hoc Conference Lists 162
Meet-Me Conference with Minimum Security Level 163
Cisco Unified IP Phone Secure Conference and Icon Support 164
Secure Conference CTI Support 164
Secure Conference Over Trunks and Gateways 164
CDR Data 165
Interactions and Restrictions 165
Cisco Unified Communications Manager Interactions with Secure Conference 165
Cisco Unified Communications Manager Restrictions with Secure Conference 166
Securing Conference Resources Tips 166
Set Up Secure Conference Bridge 168
Set Up Secure Conference Bridge in Cisco Unified Communications Manager Administration 169
Set Up Minimum Security Level for Meet-Me Conferences 169
Set Up Packet Capturing for Secure Conference Bridge 170

CHAPTER 13 **Voice-Messaging Ports Security Setup** 171

Voice-Messaging Security 171
Voice-Messaging Security Setup Tips 171
Set Up Secure Voice-Messaging Port 172
Apply Security Profile to Single Voice-Messaging Port 173
Apply Security Profile Using Voice Mail Port Wizard 174

CHAPTER 14 **Secure Tones and Icons** 175

Secure Tones and Icons Overview 175
Secure Phone Call Identification 177
Secure Icons and Tones Tips 177
Supported Devices Secure Tones 178
Protected Devices Secure Tones 178

Secure Icons and Tones Configuration Tasks 179
Set Up Secure Icon Policy 179
Enable Secure Indication Tone for Cluster 180
Configure Phone As a Protected Device 180
Secure Calls and Tones Limitations and Restrictions 181

CHAPTER 15 **Trunk and Gateway SIP Security** 183
Trunk and Gateway SIP Security Overview 183
SIP Trunk Encryption 183
Cisco IOS MGCP Gateway Encryption 184
H.323 Gateway and H.323/H.225/H.245 Trunk Encryption 185
About SIP Trunk Security Profile Setup 186
SIP Trunk Security Profile Setup Tips 186
Configure Trunk and Gateway SIP Security Task Flow 187
Set Up Secure Gateways and Trunks 187
Set Up SIP Trunk Security Profile 188
SIP Trunk Security Profile Settings 189
Apply SIP Trunk Security Profile 194
Synchronize SIP Trunk Security Profile with SIP Trunks 195
Allow SRTP Using Unified Communications Manager Administration 195

CHAPTER 16 **TLS Setup** 197
TLS Overview 197
TLS Prerequisites 197
TLS Configuration Task Flow 198
Set Minimum TLS Version 199
Set TLS Ciphers 199
Configure TLS in a SIP Trunk Security Profile 200
Add Secure Profile to a SIP Trunk 200
Configure TLS in a Phone Security Profile 201
Add Secure Phone Profile to a Phone 201
Add Secure Phone Profile to a Universal Device Template 202
TLS Interactions and Restrictions 203
TLS Interactions 203

TLS Restrictions 203

PART III User Security 209

CHAPTER 17 Identity Management 211

User Security Overview 211

Identity Management Overview 212

SAML SSO Deployment 212

LDAP Authentication 213

Configure LDAP Authentication 214

Local Database Authentication 214

OAuth Framework 215

Configure SIP OAuth Mode 216

Revoke Existing OAuth Refresh Tokens 216

CHAPTER 18 Credential Policies 217

Credential Policy Overview 217

JTAPI and TAPI Support for Credential Policies 218

Configure Default Credential Policy 219

Edit User Credentials or Credential Policy 220

Enable PIN Synchronization 220

Monitor Authentication Activity 221

Configuring Credential Caching 222

Manage Session Termination 223

CHAPTER 19 Contact Search Authentication 225

Contact Search Authentication Overview 225

Contact Search Authentication Task Flow 225

Confirm Phone Support for Contact Search Authentication 226

Enable Contact Search Authentication 226

Configure Secure Directory Server for Contact Search 226

PART IV Advanced System Security 229

CHAPTER 20 **FIPS Mode Setup** 231

FIPS Setup 231

Enable FIPS 140-2 Mode 233

CiscoSSH Support 236

Disable FIPS 140-2 Mode 236

Check FIPS 140-2 Mode Status 236

FIPS 140-2 Mode Server Reboot 237

FIPS Mode Restrictions 238

Enhanced Security Mode 239

Configure Enhanced Security Mode 240

Common Criteria Mode 241

Common Criteria Configuration Task Flow 241

Enable TLS 242

Configure Common Criteria Mode 243

CHAPTER 21 **V.150 Minimum Essential Requirements** 245

V.150 Overview 245

Configure V.150 Task Flow 245

Configure Media Resource Group Task Flow 247

Configure Media Resource Group for Non-V.150 Endpoints 247

Configure a Media Resource Group List for Non-V.150 Endpoints 248

Configure Media Resource Group for V.150 Endpoints 248

Configure a Media Resource Group List for V.150 Endpoints 248

Configure the Gateway for Cisco V.150 (MER) 249

Configure V.150 MGCP Gateway Port Interface 250

Configure V.150 SCCP Gateway Port Interface 250

Configure V.150 Support for Phone 251

Configure SIP Trunk Task Flow 251

Configure SIP Profile for V.150 252

Set the Clusterwide V.150 Filter 252

Add V.150 Filter to SIP Trunk Security Profile 253

Configure SIP Trunk for V.150 254

CHAPTER 22 **IPSec Setup** 255

IPSec Overview 255

CHAPTER 23 **Authentication and Encryption Setup for CTI, JTAPI, and TAPI** 257

Authentication for CTI, JTAPI, and TAPI Applications 257

Encryption for CTI, JTAPI, and TAPI Applications 259

Stronger Cipher Suites on CTI Ports 260

CAPF Functions for CTI, JTAPI, and TAPI Applications 260

CAPF System Interactions and Requirements for CTI, JTAPI, and TAPI Applications 261

Certificate Authority Proxy Function Service Activation 262

Set Up Application User or End User CAPF Profile 262

CAPF Settings 262

Update CAPF Service Parameters 264

Delete Application User CAPF or End User CAPF Profile 265

Securing CTI, JTAPI, and TAPI 266

Add Application and End Users to Security-Related Access Control Groups 267

Set Up JTAPI/TAPI Security-Related Service Parameters 268

View Certificate Operation Status for Application or End User 269

CHAPTER 24 **Secure Recording and Monitoring** 271

About Secure Call Monitoring and Recording Setup 271

Set Up Secure Call Monitoring and Recording 272

CHAPTER 25 **VPN Client** 273

VPN Client Overview 273

VPN Client Configuration Task Flow 273

Complete Cisco IOS Prerequisites 274

Configure Cisco IOS SSL VPN to Support IP Phones 275

Complete ASA Prerequisites for AnyConnect 277

Configure ASA for VPN Client on IP Phone 277

Upload VPN Concentrator Certificates 279

Configure VPN Gateway 280

VPN Gateway Fields for VPN Client 281

Configure VPN Group 281
VPN Group Fields for VPN Client 282
Configure VPN Profile 282
VPN Profile Fields for VPN Client 282
Configure VPN Feature Parameters 283
VPN Feature Parameters 284
Add VPN Details to Common Phone Profile 285

CHAPTER 26 **Operating System and Security Hardening** 287
Security Hardening 287

PART V **Troubleshooting** 291

CHAPTER 27 **Security Troubleshooting Overview** 293
Remote Access 293
Cisco Secure Telnet 294
Firewall Protection 294
Cisco Secure Telnet Design 294
Cisco Secure Telnet Structure 295
Set up a Remote Account 295



Preface

Implementing security mechanisms in the Cisco Unified Communications Manager system prevents identity theft of the phones and the Unified Communications Manager server, data tampering, and call-signaling/media-stream tampering.

The CiscoIP telephony network establishes and maintains authenticated communication streams, digitally signs files before transferring the file to the phone, and encrypts media streams and call signaling between Cisco Unified IP Phones.

- About this Manual, on page xv
- Audience, on page xvii
- Document Conventions, on page xviii
- Legal Compliance, on page xviii

About this Manual

The Security Guide includes the following Parts with short Descriptions:

Table 1: Parts and Descriptions

Part	Description
An Introduction to CUCM Security	Provides information on following topics about security overview. • System Requirements • Common Icons • Best Practices It also provides an overview to configure Security in your systems.

Part	Description
Basic System Security	Provides information on following topics to configure basic security in your systems. • Certificates • Security Modes • Cipher Management • Secure Tones and Icons • TFTP Encryption • Phone Security • Trunk and Gateway SIP Security • TLS Setup

User Security	Provides information on following topics to configure user security in your systems.
	• Identity Management
	  • User Access Control
	  • Credential Policies
	• Directory Access
	  • Contact Search Authentication Configuration
	  • Configure Secure Directory Server for Contact Search

Part	Description
Advanced System Security	Provides information on following topics to configure advanced system security in your systems. • FIPS Mode • Enhanced Security Mode • Common Criteria Mode • Cisco V.150 Minimum Essential Requirements • ECDSA and RSA • IPsec Policies • Authentication and Encryption Set up for CTI • JTAPI, and TAPI • Secure Call Monitoring and Recording • VPN Client
Appendix	Provides information on following topics to secure your systems. • Additional Security Configurations • Terms and Acronyms • Interactions and Restrictions • Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS) • Troubleshooting Information • Remote Account • Log Details • Common Vulnerabilities and PSIRT • OS Hardening

Audience

The intended audiences for this guide are:

- System Administrators
- Phone Administrators

They configure call security features for Unified Communications Manager.

Document Conventions

This section provides information on the document conventions followed in the guide.

Notes use the following convention:



Note Means *reader take note* of the important or additional information.

Tips use the following convention:



Tip Means *the following are useful tips*.

Cautions use the following convention:



Caution Means that *the reader should be careful*. In this situation, read the instructions carefully else, you can damage the equipment or lose data.

Attentions use the following convention:



Attention Means that *the reader should pay attention*. In this situation, read the instructions carefully else, you can damage the equipment or lose data.

Warning

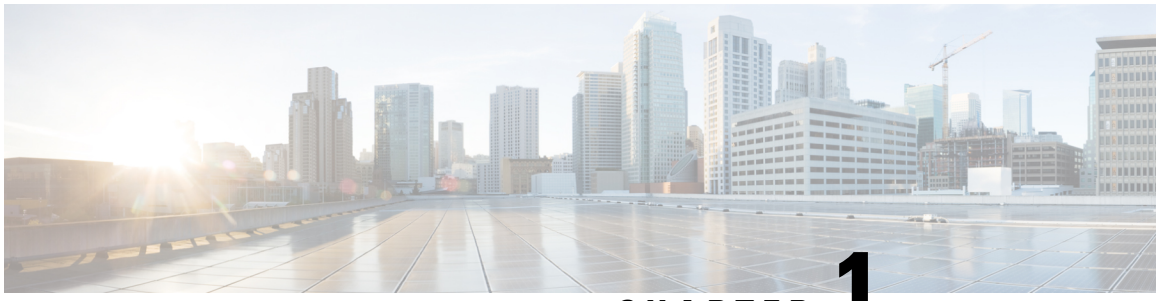


Warning Means that *the reader **must** follow instructions*. In this situation, read the instructions carefully else, you can damage the equipment or lose data.

Legal Compliance

The Unified Communications Manager (Security) product contains cryptographic features and its import, export information. Transfer and use of information is subject to the laws governing United States and the local country. Delivery of Cisco cryptographic products doesn't imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors, and users are responsible for compliance with the U.S. and local country laws. By using this product, you agree to comply with applicable laws and regulations. If you're unable to comply with the U.S. and local laws, return this product immediately.

Find further information regarding U.S. export regulations at http://www.access.gpo.gov/bis/ear/ear_data.html.



CHAPTER 1

New and Changed Information

• New and Changed Information, on page 1

New and Changed Information

The following table provides an overview of the significant changes to the features in this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 2: New Features and Changed Behavior in Unified Communications Manager and IM and Presence Service

Feature or Change	Description	See	Date
FIPS Requirements	In Release 14SU5, the CiscoSSL version is updated.	FIPS Setup, on page 231	October 09, 2025
Support to renew refresh token automatically	Unified Communications Manager supports the automatic renewal of refresh token for Webex clients in Release 14SU4.	OAuth Framework, on page 215	May 30, 2024
Oauth—Eliminate Refresh token dependency on CUCM publisher	In Release 14SU4, this feature introduces a new enterprise parameter '**Auto Renew Refresh Token**' that is enabled by default.	Refer to the 'Common Enterprise Parameters and Services' section of the System Configuration Guide for Cisco Unified Communications Manager	May 30, 2024
ECDHE cipher support on CAPF and TVS	Updated cipher list to include ECDHE cipher support on CAPF and TVS	Cipher Limitations, on page 120	May 30, 2024

New and Changed Information

Feature or Change	Description	See	Date
Certificate Revocation List Support	In Release 14SU3, this feature introduces certificate revocation list, where the CA will have a list of digital certificates that have been revoked before their actual or assigned expiration date.	Certificate Revocation Configuration, on page 68	May 18, 2023
Cisco SSL7 upgrade	In Release 14SU2, CiscoSSL and Ciscofom is upgraded from version 6 to 7 in Unified Communication Manager.	FIPS Setup, on page 231 FIPS Mode Restrictions, on page 238 Web Requests From CCMAdmin or CCMUser to Cisco Unified Communications Manager	June 16, 2022
CiscoSSL6x to CiscoSSL7x upgrade (VOS modules, being done by Adaptation team)	In Release 14SU2, CiscoSSL and Ciscofom is upgraded from version 6 to 7 in Unified Communication Manager.	FIPS Setup, on page 231 FIPS Mode Restrictions, on page 238	June 16, 2022
Enrollment over Secure Transport Support	In Release 14SU2, this feature supports the automatic enrollment of certificates with CAs having inbuilt EST server mode.	Configure Online Certificate Authority Settings, on page 78	June 16, 2022
EPNM multi line enhancement (TFTP work)	Unified Communications Manager supports masking of External Phone Number for all configured line numbers for the latest phone models in Release 14SU2.	External Phone Number Mask	June 16, 2022
Making OU not mandatory as part of CSR generation	In Release 14SU2, this feature introduces an option to include the Organization Unit field in the Certificate Signing Request.	Certificate Signing Request Fields, on page 52	June 16, 2022

Feature or Change	Description	See	Date
Spectralink/Saturn and Mars (Support download of large files from CUCM TFTP)	Unified Communications Manager supports HTTP range requests (RFC7233) support on TFTP and Proxy TFTP (if the download file is at least 100MB) in Release 14SU1.	Potential Issues with Firmware Installs	October 27, 2021
SSO Redirect URI for Webex Apps	This feature enhances the security of Cisco Jabber/Webex Client that uses the external browser to perform SSO to be cross launched by the browser using SSO Redirect URI.	SSO Redirect URI for Webex Apps	October 27, 2021
TFTP proxy support for Oauth	Unified Communications Manager supports TFTP Proxy in SIP OAuth deployments.	Configure TFTP Server Dynamically Configure TFTP Server Manually Enable SIP OAuth Mode Certificate Signing Request Fields, on page 52	October 27, 2021
CSCvu05478 : Unable to upload multiple certificates from same certificate authority	As part of this CDET we will be able to upload multiple certificates from a single certificate authority using the certificate name convention Common Name_SerialNumber.	Certificate Signing Request Fields, on page 52	October 27, 2021
CSCvz05710 - CiscoJ upgrade to 5.3.6 version backport to 12.5 SU6	As part of this feature we will upgrade to CiscoJ 5.3.7 version in 12.5 SU6 and 14 SU1.	FIPS Setup, on page 231	October 27, 2021

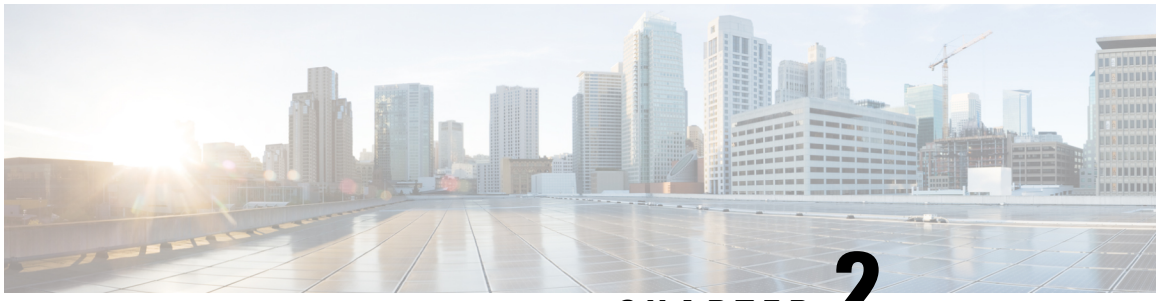
New and Changed Information



PART I

An Introduction to Unified CM Security

- An Overview, on page 7
- Configurations, on page 11
- Default Security, on page 13



CHAPTER 2

An Overview

- System Requirements, on page 7
- Best Practices, on page 7
- Common Icons, on page 9

System Requirements

The following are the system requirements to authenticate or encrypt the Unified Communications Manager:

- Login to Cisco Unified Communications Manager Administration CLI of the Unified Communications Manager publisher and run **util ctl** command to set the cluster to mixed mode (Secure Mode).
- Locally Significant Certificates (LSC) exist in all phones to authenticate the TLS connection with Unified Communications Manager.

Note A few Endpoints also use MICs if the LSC is not present but we always recommend you to use LSCs.

Best Practices

Cisco strongly recommends the following best practices:

- Always perform installation and configuration tasks in a secure lab environment before you deploy to a wide-scale network.
- Use IPSec for gateways and other application servers at remote locations.

Warning Failure to use IPSec in these instances results in session encryption keys getting transmitted in the clear.

- To prevent toll fraud, configure conference enhancements that are described in the System Configuration Guide for Cisco Unified Communications Manager. Likewise, you can perform configuration tasks to

restrict external transferring of calls. For more information on how to perform this task, see Feature Configuration Guide for Cisco Unified Communications Manager.

Device Resets, Server and Cluster Reboots, and Service Restarts

The following table lists the security actions with reset, restart, and reboot details:

Table 3: Security Actions with Reset, Restart, and Reboot details:

Sl No	Action	Reset (Yes / No)	Restart (Yes / No)
1	Apply Security Profile	Yes	No
2	Apply Phone Hardening	—	—
3	Security Mode Changes	Yes. All devices	Yes. Restart CallManager service.
4	CTL File Update	—	Yes.All encrypted and authenticated phones need to be reset to ensure they get an updated CTL file.
5	Update Ports for TLS Connection	—	Yes. Restart the CTL Provider Service.
6	Update /Configure CAPF service parameters	—	Yes. Restart the Cisco Certificate Authority Proxy Function service
7	Start or Stop the CTL Provider service	—	Yes. Restart all Cisco CallManager and Cisco TFTP services
7	Configure secure SRST references	Yes. Reset dependent devices	—
8	Change the Smart Card service to Started and Automatic	—	Yes
9	Configure security-related service parameters that are associated with the application User CAPF Profile.	—	Yes. Restart the Cisco IP Manager Assistant service, Cisco Web Dialer Web Service, and the Cisco Extended Functions service after

To restart the Unified Communications Manager service, see Administration Guide for Cisco Unified Communications Manager.

To reset a single device after you update the phone configuration, see topics related to applying the phone security profile.

Reset Devices, Servers, Clusters, and Services

This section provides information on when to reset devices, servers, clusters, and services in Cisco Unified Serviceability.

To reset all devices in a cluster, perform the following procedure:

Procedure

Step 1 From Unified Communications Manager, choose **System** > **CiscoUnifiedCM**.

Step 2 Click **Find**.

A list of configured Unified Communications Manager servers appears.

Step 3 Choose the Unified Communications Manager on which you want to reset devices.

Step 4 Click **Reset**.

Step 5 Perform Step 2 and Step 4 for each server in the cluster.

Media Encryption with Barge Setup

Configure barge for Cisco Unified IP Phones 7962 and 7942 for encryption and perform the following tasks in Cisco Unified Communications Manager Administration.

- Update the Cluster Security Mode using CLI commands (utils ctl set cluster mixed-mode).
- Update the Builtin Bridge Enable parameter in the **Service Parameter** window.

On completion of the tasks, the following message appears.

Attention If you configure encryption for Cisco Unified IP Phone models 7962 and 7942, the encrypted devices can't accept a barge request when they are participating in an encrypted call. The barge attempt fails when the call is encrypted.

Cisco Unified IP Phones 7962 and 7942 configured with an encrypted security profile doesn't display the message in the **Phone Configuration** window. You choose **Default** for the Built In Bridge setting or the default setting equals Default. The same restriction applies for either selection.

Tip Reset the dependent CiscoIP devices for changes to take effect.

Common Icons

Unified Communications Manager provides a security status for calls based on security levels configured for all servers and devices participating in the call.

All phones that support security icons display call security level.

- A shield icon appears for calls with authenticated level of signaling security. A shield identifies a secured connection between Cisco IP devices, which means that the devices are authenticated and are using encrypted signaling.
- A lock icon appears for calls with encrypted media, which means that the devices are using encrypted signaling and encrypted media.



Note Some phone models only display the lock icon. See the respective Cisco IP Phones documentation you are using for more information.

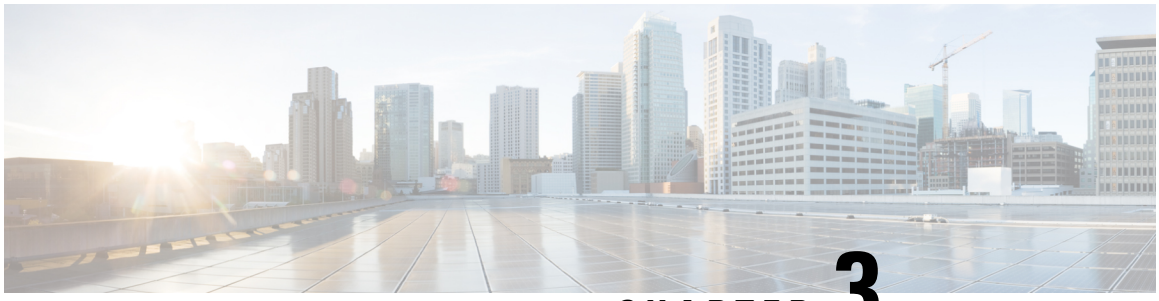
The security status of a call can change for point-to-point, intracluster, intercluster, and multihop calls. SCCP line, SIP line, and H.323 signaling support notification of call security status changes to participating endpoints.

The audio and video call provide basis for the call security status. The call is secure only if both the audio and video are secure.



Note The "Override BFCP Application Encryption Status When Designating Call Security Status" service parameter displays a lock icon when the parameter value is True and audio is secure. This condition ignores the security statuses of all other media channels. The default parameter value is False.

For conference and barge calls, the security icon displays the security status for the conference.



CHAPTER 3

Configurations

- Security Configurations, on page 11

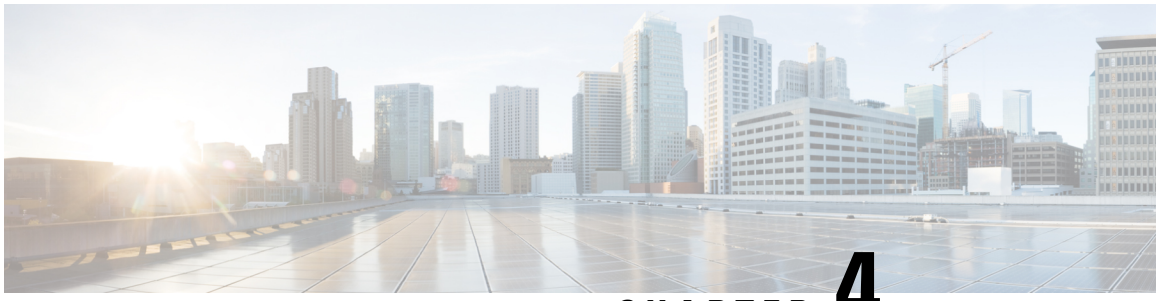
Security Configurations

This chapter provides end to end security solutions and references to various security task flows and their brief descriptions.

Table 4: Security Configurations

Steps	Procedure	Description
Step 1	Generate Certificates	Configure and exchange certificates for your system.
Step 2	Configure Certificate Monitoring and Revocation	Configure the system to monitor certificate expiry and to revoke certificates automatically through the Online Certificate Status Protocol (OCSP).
Step 3	Enable Mixed Mode	When mixed mode is enabled, your system uses the Certificate Trust List (CTL) file for security if you're deploying Cisco Unified IP Phone, TelePresence Endpoints, or Jabber without OAuth.
Step 4	Configure Certificate Authority Proxy Function (CAPF)	Configure CAPF to generate LSC certificates for phones.
Step 5	Configure Encrypted TFTP	Configure encrypted TFTP so that the initial phone configuration file sent to the phone is encrypted.
Step 6	Configure Phone Security	Configure Phone Security profiles to include items like TFTP encryption and TLS signaling for your phones.
Step 7	Configure Phone Hardening	Configure optional product-specific configurations to harden the connection to the phone.
Step 8	Configure Secure Trunks	Configure secure trunks to enable TLS and digest authentication on trunks.

Steps	Procedure	Description
Step 9	Enable SIP on Trunks	Configure SIP Trunk for SRTP.
Step 10	Enable SAML SSO	Configure your Identity Management Framework. SAML SSO is recommended for Identity Management. However, you can also use LDAP Authentication or Local authentication.
Step 11	Configure User Access	Assign end users to access control groups to contain roles and access privileges that they need.
Step 12	Configure Credential Policies	Configure default credential policies for user passwords, user PINs, and application user passwords.
Step 13	Configure Contact Search Authentication	Ensure authentication of all directory searches to secure the company directory.
Step 14	Enable TLS	Configure TLS signaling through Phone Security and Trunk Security Profiles.
Step 15	Configure Cipher Management	Customize the list of encryption ciphers that are supported on your system.
Step 16	Configure IPSec Policies	Configure IPSec Policies for your system.
Step 17	Configure Gateway Security	Configure secure gateway for your system.
Step 18	Configure OS Hardening	Configure OS Hardening.
Step 19	Configure FIPS	Configure FIPS mode, Enhanced Security Mode, and Common Criteria Mode to meet compliance guidelines around encryption and data security.
Step 20	Configure Security Features	Configure optional security features, such as: • Secure Monitoring and Recording • Secure Conferencing • Secure Tones and Icons • V.150 • Mobile and Remote Access • AS-SIP



CHAPTER 4

Default Security

- Default Security Overview, on page 13
- Encryption, on page 22
- Default Security Administration Tasks, on page 31

Default Security Overview

The Default Security features provides a basic level of security for supported Cisco Unified IP Phone without any extra configuration requirement.

This feature provides the following default security for supported IP Phones:

- Default Authentication of TFTP
- Optional Encryption
- Certificate Verifications

Default Security uses the following components to provide basic security in non secure environments:

- Identity Trust List (ITL)—this file is created only after TFTP service is activated at cluster installation and is used by Cisco Unified IP Phone to establish trust.
- Trust Verification Service—This service runs on all Unified Communications Manager nodes and authenticates certificates for Cisco Unified IP Phone. The TVS certificate, along with a few other key certificates, is bundled in the ITL file.

Initial Trust List

The Initial Trust List (ITL) file is used for the initial security, so that the endpoints can trust Unified Communications Manager. ITL does not need any security features to be enabled explicitly. The ITL file is automatically created when the TFTP service is activated and the cluster is installed. The Unified Communications Manager's TFTP server’s private key is used to sign the ITL file.

When the Unified Communications Manager cluster or server is in non-secure mode, the ITL file is downloaded on every supported Cisco Unified IP Phone. You can view the contents of an ITL file using the CLI command **admin:show itl**.

Cisco Unified IP Phone need the ITL file to perform the following tasks:

- Communicate securely to CAPF, a prerequisite to support the configuration file encryption.
- Authenticate the configuration file signature
- Authenticate application servers, such as EM services, directory, and MIDlet during HTTPS establishment using TVS.

If the Cisco IP Phone does not have an existing CTL file, it trusts the first ITL file automatically. The TVS must be able to return the certificate corresponding to the signer.

If the Cisco IP Phone has an existing CTL file, it uses the CTL file to authenticate the ITL file signature.



Note The SHA-1or MD5 algorithm value changes only when there is a change in the Initial Trust List (ITL) file value. You can use the checksum value of the ITL files to identify the difference between the ITL file of Cisco IP Phone and Unified Communications Manager cluster. The checksum value of the ITL file changes only when you modify the ITL file.

The Initial Trust List (ITL) file has the same format as the CTL file. However, it is a smaller and leaner version.

The following attributes apply to the ITL file:

- The system builds the ITL file automatically when the TFTP service is activated and you install the cluster. The ITL file is updated automatically if the content is modified.
- The ITL file does not require eTokens. It uses a soft eToken (the private key associated with TFTP server's CallManager certificate).
- The Cisco Unified IP Phone download the ITL file during a reset, restart, or after downloading the CTL file.

The ITL file contains the following certificates:

- ITLRecovery Certificate—This certificate signs the ITL File.
- The CallManager certificate of the TFTP server—This certificate allows you to authenticate the ITL file signature and the phone configuration file signature.
- All the TVS certificates available on the cluster—These certificates allow the phone to communicate to TVS securely and to request certificates authentication.
- The CAPF certificate—These certificates support configuration file encryption. The CAPF certificate isn't required in the ITL File (TVS can authenticate it), however, it simplifies the connection to CAPF.

The ITL file contains a record for each certificate. Each record contains:

- A certificate
- Pre-extracted certificate fields for easy lookup by the Cisco IP Phone
- Certificate role (TFTP, CUCM, TFTP+CCM, CAPF, TVS, SAST)

The TFTP server's CallManager certificate is present in two ITL records with two different roles:

- TFTP or the TFTP and CCM role—To authenticate configuration file signature.
- SAST role—To authenticate the ITL file signature.

Certificate Management Changes for ITLRecovery Certificate

- The validity of ITLRecovery has been extended from 5 years to 20 years to ensure that the ITLRecovery certificate remains same for a longer period.

Note The default validity period of ITLRecovery certificate is 5 years. However, you can also configure the validity period of ITLRecovery certificate to 5, 10, 15, or 20 years. While upgrading Unified Communications Manager, the ITLRecovery certificate gets copied to the later release.

- Before you regenerate an ITLRecovery certificate, a warning message appears on both the CLI and the GUI. This warning message displays that if you use a tokenless CTL and if you regenerate the CallManager certificate, ensure that the CTL file has the updated CallManager certificate and that certificate is updated to endpoints.

ITLRecovery Certificate

The ITLRecovery Certificate feature introduces a new drop-down list **ITL File Status** to allow administrators to identify phones that have older ITL so that they can take necessary action for these phones.

Some phones do not get the latest ITL file and retain the old ones when the ITL files are updated (like the renewal of CM certificates). The system displays the centralized report of phones with mismatched ITL files in the user interface .

Following are the different ITLRecovery scenarios:

TFTP Service Activaton:

- When the TFTP Service is activated, the hash of the generated ITL file along with the server hostname is stored in the DB. It is updated every time an ITL update happens in TFTP code.
- If TFTP hostname is already present in the table, the generated ITL hash is compared against the stored value.
  - If the ITL hash is not the same, the new ITL hash is updated in the DB.
  - If the ITL hash is the same, the TFTP log shows "Tftp Itl hash not changed".

Device Registration and download of ITLFile

- When a phone registers with Unified Communications Manager, if the details of ITLFile (Server hostname, hash, timestamp) present in the server does not exist in the DB, it is inserted.
- When a phone registers with Unified Communications Manager, it sends a SIP alarm which contains the details of the ITL file applied on the phone. This is compared against the hash of the ITL file stored in DB.
  - If the ITL hash is the same, the device hash information is updated with the new timestamp.
  - If the ITL hash is not the same, the reported ITL hash and timestamp are updated against the device.
- When the phone unregisters, the trust hash information of that device is deleted.

Interactions and Restrictions

If a Unified Communications Manager cluster has more than 39 certificates, then the ITL file size on Cisco IP Phone exceeds 64 kilobytes. Increase in the ITL file size affects the ITL to load properly on the phone causing the phone registration to fail with Unified Communications Manager.

Trust Verification Service

There are large number of phones in a network and Cisco Unified IP Phone have limited memory. Hence, Unified Communications Manager acts as a remote trust store through TVS and so that a certificate trust store doesn't have to be placed on each phone. The Cisco Unified IP Phones contact TVS server for verification, because it cannot verify a signature or certificate through CTL or ITL files. Thus, having a central trust store is easier to manage than having the trust store on all the Cisco Unified IP Phones.

TVS enables Cisco Unified IP Phone to authenticate application servers, such as EM services, directory, and MIDlet, during HTTPS establishment.

TVS provides the following features:

- Scalability—Cisco Unified IP Phone resources are not impacted by the number of certificates to trust.
- Flexibility—Addition or removal of trust certificates are automatically reflected in the system.
- Security by Default—Non-media and signaling security features are part of the default installation and don't require user intervention.



Note When you enable secure signaling and media, create a CTL file and then set the cluster to mixed mode. To create a CTL file and set the cluster to mixed mode, use the CLI command **utils ctl set-cluster mixed-mode**.

The following are the basic concepts that describe TVS:

- TVS runs on the Unified Communications Manager server and authenticates certificates on behalf of the Cisco IP Phone.
- Cisco Unified IP Phone only needs to trust TVS, instead of downloading all the trusted certificates.
- The ITL file is generated automatically without user intervention. The ITL file is downloaded by Cisco Unified IP Phone and trust flows from there.

Authentication, Integrity, and Authorization

Integrity and authentication protect against the following threats:

- TFTP file manipulation (integrity)
- Modification of call-processing signaling between the phone and Unified Communications Manager (authentication)
- Man-in-the-middle attacks (authentication), as defined in *Acronyms* section.
- Phone and server identity theft (authentication)
- Replay attack (digest authentication)

Authorization specifies what an authenticated user, service, or application can do. You can implement multiple authentication and authorization methods in a single session.

Image Authentication

This process prevents tampering with the binary image, the firmware load, prior to loading it on the phone. Tampering with the image causes the phone to fail the authentication process and reject the image. Image authentication occurs through signed binary files that automatically install when you install Unified Communications Manager. Likewise, firmware updates that you download from the web also provide signed binary images.

Device Authentication

This process validates the identity of the communicating device and ensures that the entity is who it claims to be.

Device authentication occurs between the Unified Communications Manager server and supported Cisco Unified IP Phones, SIP trunks, or JTAPI/TAPI/CTI applications (when supported). An authenticated connection occurs between these entities only when each entity accepts the certificate of the other entity. Mutual authentication describes this process of mutual certificate exchange.

Device authentication relies on the creation of the CiscoCTL file (for authenticating Unified Communications Manager server node and applications), and the Certificate Authority Proxy Function (for authenticating phones and JTAPI/TAPI/CTI applications).



Tip A SIP user agent that connects via a SIP trunk authenticates to Unified Communications Manager if the CallManager trust store contains the SIP user agent certificate and if the SIP user agent contains the Unified Communications Manager certificate in its trust store. For information on updating the CallManager trust store, refer to the *Administration Guide for Cisco Unified Communications Manager* that supports this Unified Communications Manager release.

File Authentication

This process validates digitally signed files that the phone downloads; for example, the configuration, ring list, locale, and CTL files. The phone validates the signature to verify that file tampering did not occur after the file creation. For a list of devices that are supported, see “Phone Model Support”.

If you configure the cluster for mixed mode, the TFTP server signs static files, such as ring list, localized, default.cnf.xml, and ring list wav files, in.sgn format. The TFTP server signs files in <device name>.cnf.xml format every time that the TFTP server verifies that a data change occurred for the file.

The TFTP server writes the signed files to disk if caching is disabled. If the TFTP server verifies that a saved file has changed, the TFTP server re-signs the file. The new file on the disk overwrites the saved file that gets deleted. Before the phone can download the new file, the administrator must restart affected devices in Unified Communications Manager.

After the phone receives the files from the TFTP server, the phone verifies the integrity of the files by validating the signature on the file. For the phone to establish an authenticated connection, ensure that the following criteria are met:

- A certificate must exist in the phone.

- The CTL file must exist on the phone, and the Unified Communications Manager entry and certificate must exist in the file.
- You configured the device for authentication or encryption.

Signaling Authentication

This process, also known as signaling integrity, uses the TLS protocol to validate that no tampering occurred to signaling packets during transmission.

Signaling authentication relies on the creation of the Certificate Trust List (CTL)file.

Digest Authentication

This process for SIP trunks and phones allows Unified Communications Manager to challenge the identity of a device that is connecting to Unified Communications Manager. When challenged, the device presents its digest credentials, similar to a username and password, to Unified Communications Manager for verification. If the credentials that are presented match those that are configured in the database for that device, digest authentication succeeds, and Unified Communications Manager processes the SIP request.

Note Be aware that the cluster security mode has no effect on digest authentication.

Note If you enable digest authentication for a device, the device requires a unique digest user ID and password to register.

You configure SIP digest credentials in the Unified Communications Manager database for a phone user or application user.

- For applications, you specify digest credentials in the Application User Configuration window.
- For phones that are running SIP, you specify the digest authentication credentials in the End User window. To associate the credentials with the phone after you configure the user, you choose a Digest User, the end user, in the Phone Configuration window. After you reset the phone, the credentials exist in the phone configuration file that the TFTPserver offers to the phone. See topics related to encrypted phone configuration file setup to ensure digest credentials do not get sent in the clear in TFTP downloads.
- For challenges received on SIP trunks, you configure a SIP realm, which specifies the realm username (device or application user) and digest credentials.

When you enable digest authentication for an external phone or trunk that is running SIP and configure digest credentials, Unified Communications Manager calculates a credentials checksum that includes a hash of the username, password, and the realm. The system uses a nonce value, which is a random number, to calculate the MD5 hash. Unified Communications Manager encrypts the values and stores the username and the checksum in the database.

To initiate a challenge, Unified Communications Manager uses a SIP 401 (Unauthorized) message, which includes the nonce and the realm in the header. You configure the nonce validity time in the SIP device security profile for the phone or trunk. The nonce validity time specifies the number of minutes that a nonce value

stays valid. When the time interval expires, Unified Communications Manager rejects the external device and generates a new number.

Note Unified Communications Manager acts as a user agent server (UAS) for SIP calls that are originated by line-side phones or devices that are reached through the SIP trunk, as a user agent client (UAC) for SIP calls that it originates to the SIP trunk, or a back-to-back user agent (B2BUA) for line-to-line or trunk-to-trunk connections. In most environments, Unified Communications Manager acts primarily as B2BUA connecting SCCP and SIP endpoints. (A SIP user agent represents a device or application that originates a SIP message.)

Tip Digest authentication does not provide integrity or confidentiality. To ensure integrity and confidentiality for the device, configure the TLS protocol for the device, if the device supports TLS. If the device supports encryption, configure the device security mode as encrypted. If the device supports encrypted phone configuration files, configure encryption for the files.

Digest Authentication for Phones

When you enable digest authentication for a phone, Unified Communications Manager challenges all requests for phones that are running SIP except keepalive messages. Unified Communications Manager does not respond to challenges from line-side phones.

After receiving a response, Unified Communications Manager validates the checksum for the username that is stored in the database against the credentials in the response header.

Phones that are running SIP exist in the Unified Communications Manager realm, which is defined in Unified Communications Manager Administration at installation. You configure the SIP Realm for challenges to phones with the service parameter SIP Station Realm. Each digest user can have one set of digest credentials per realm.

Tip If you enable digest authentication for an end user but do not configure the digest credentials, the phone will fail registration. If the cluster mode is nonsecure and you enable digest authentication and configure digest credentials, the digest credentials get sent to the phone, and Unified Communications Manager still initiates challenges.

Digest Authentication for Trunks

When you enable digest authentication for a trunk, Unified Communications Manager challenges SIP trunk requests from SIP devices and applications that connect through a SIP trunk. The system uses the Cluster ID enterprise parameter in the challenge message. SIP user agents that connect through the SIP trunk respond with the unique digest credentials that you configured for the device or application in Unified Communications Manager.

When Unified Communications Manager initiates a SIP trunk request, a SIP user agent that connects through the SIP trunk can challenge the identity of Unified Communications Manager. For these incoming challenges, you configure a SIP Realm to provide the requested credentials for the user. When Unified Communications Manager receives a SIP 401(Unauthorized) or SIP 407 (Proxy Authentication Required) message, Unified

Communications Manager looks up the encrypted password for the realm that connects though the trunk and for the username that the challenge message specifies. Unified Communications Manager decrypts the password, calculates the digest, and presents it in the response message.

Tip The realm represents the domain that connects through the SIP trunk, such as xyz.com, which helps to identify the source of the request.

To configure the SIP Realm, see topics related to digest authentication for SIP trunks. You must configure a SIP Realm and username and password in Unified Communications Manager for each SIP trunk user agent that can challenge Unified Communications Manager. Each user agent can have one set of digest credentials per realm.

Authorization

Unified Communications Manager uses the authorization process to restrict certain categories of messages from phones that are running SIP, from SIP trunks, and from SIP application requests on SIP trunks.

- For SIP INVITE messages and in-dialog messages, and for phones that are running SIP, Unified Communications Manager provides authorization through calling search spaces and partitions.
- For SIP SUBSCRIBE requests from phones, Unified Communications Manager provides authorization for user access to presence groups.
- For SIP trunks, Unified Communications Manager provides authorization of presence subscriptions and certain non-INVITE SIP messages; for example, out-of-dial REFER, unsolicited notification, and any SIP request with the replaces header. You specify authorization in the SIP Trunk Security Profile Configuration window when you check the allowed SIP requests in the window.

To enable authorization for SIP trunk applications, check the Enable Application Level Authorization and the Digest Authentication check box in the SIP Trunk Security Profile window; then, check the allowed SIP request check boxes in the Application User Configuration window.

If you enable both SIP trunk authorization and application level authorization, authorization occurs for the SIP trunk first and then for the SIP application user. For the trunk, Unified Communications Manager downloads the trunk Access Control List (ACL) information and caches it. The ACL information gets applied to the incoming SIP request. If the ACL does not allow the SIP request, the call fails with a 403 Forbidden message.

If the ACL allows the SIP request, Unified Communications Manager checks whether digest authentication is enabled in the SIP Trunk Security Profile. If digest authentication is not enabled and application-level authorization is not enabled, Unified Communications Manager processes the request. If digest authentication is enabled, Unified Communications Manager verifies that the authentication header exists in the incoming request and then uses digest authentication to identify the source application. If the header does not exist, Unified Communications Manager challenges the device with a 401 message.

Before an application-level ACL gets applied, Unified Communications Manager authenticates the SIP trunk user agent through digest authentication. Therefore, you must enable digest authentication in the SIP Trunk Security Profile before application-level authorization can occur.

NMAP Scan Operation

You can run a Network Mapper (NMAP) scan program on any Windows or Linux platform to perform vulnerability scans. NMAP represents a free and open source utility for network exploration or security auditing.

Note NMAP DP scan can take up to 18 hours to complete.

Syntax

nmap -n -vv -sU -p <*port_range*> <*ccm_ip_address*>

where:

-*n*: No DNS resolution. Tells NMAP to never do reverse DNS resolution on the active IP addresses that it finds. Because DNS can be slow even with the NMAP built-in parallel stub resolver, this option can slash scanning times.

-*v*: Increases the verbosity level, which causes NMAP to print more information about the scan in progress. The system shows open ports as they are found and provides completion time estimates when NMAP estimates that a scan will take more than a few minutes. Use this option twice or more for even greater verbosity.

-*sU*: Specifies a UDP port scan.

-*p*: Specifies which ports to scan and overrides the default. Be aware that individual port numbers are acceptable, as are ranges that are separated by a hyphen (for example 1-1023).

ccm_ip_address: IP address of Cisco Unified Communications Manager

Autoregistration

The system supports autoregistration in both mixed mode and nonsecure mode. The default configuration file will also be signed. Cisco IP Phones that do not support Security by Default will be served a nonsigned default configuration file.

Migrate IP Phones Between Clusters with Cisco Unified Communications Manager and ITL Files

Unified Communications Manager 8.0(1) and later introduced the new Security By Default feature and the use of Initial Trust List (ITL) files. With this new feature, you must be careful when moving phones between different Unified CM clusters and ensure that you follow the proper steps for migration.

Caution Failure to follow the proper steps may lead to a situation where thousands of phones must manually have their ITL files deleted.

Cisco IP Phones that support the new ITL file must download this special file from their Unified CM TFTP server. Once an ITL file is installed on a phone, all future configuration files and ITL file updates must be signed by one of the following items:

- The TFTP server certificate that is currently installed on the phone or
- A TFTP certificate that can be validated TVS services on one of the clusters. You can find the certificates of TVS services within the cluster listed in the ITL file.

With this new security functionality in mind, three problems can occur when moving a phone from one cluster to another cluster:

1. The ITL file of the new cluster is not signed by the current ITL file signer, so the phone cannot accept the new ITL file or configuration files.
2. The TVS servers listed in the existing ITL of the phone may not be reachable when the phones are moved to the new cluster.
3. Even if the TVS servers are reachable for certificate verification, the old cluster servers may not have the new server certificates.

If one or more of these three problems are encountered, one possible solution is to delete the ITL file manually from all phones being moved between clusters. However, this is not a desirable solution since it requires massive effort as the number of phones increases.

The most preferred option is to make use of the Cisco Unified CM Enterprise Parameter Prepare Cluster for Rollback to pre-8.0. Once this parameter is set to True, the phones download a special ITL file that contains empty TVS and TFTP certificate sections.

When a phone has an empty ITL file, the phone accepts any unsigned configuration file (for migrations to Unified CM pre-8.x clusters), and also accepts any new ITL file (for migrations to different Unified CM 8.x clusters).

The empty ITL file can be verified on the phone by checking **Settings** > **Security** > **Trust List** > **ITL**. Empty entries appear where the old TVS and TFTP servers used to be.

The phones must have access to the old Unified CM servers only as long as it takes them to download the new empty ITL files.

If you plan to keep the old cluster online, disable the Prepare Cluster for Rollback to pre-8.0 Enterprise Parameter to restore Security By Default.

Encryption

Tip Encryption capability installs automatically when you install Unified Communications Manager on a server.

This section describes the types of encryption that Unified Communications Manager supports:

Secure End Users Login Credentials

From Unified Communications Manager Release 12.5(1), all end users login credentials are hashed with SHA2 to provide enhanced security. Earlier than Unified Communications Manager Release 12.5(1), all end users login credentials were hashed with SHA1 only. Unified Communications Manager Release 12.5(1) also includes the “UCM Users with the Out-Of-Date Credential Algorithm” report. This report is available in the

Cisco Unified Reporting page. This report helps the administrator to list all the end users whose passwords or PINs are hashed with SHA1.

All end users passwords or PINs that are hashed with SHA1 are migrated to SHA2 automatically upon their first successful login. The end users with SHA1 hashed (out of date) credentials can update their PINs or passwords using one of the following ways:

- Update the PIN by logging into Extension Mobility or Directory access on the phone.
- Update the password by logging into Cisco Jabber, Cisco Unified Communications Self Care Portal, or Cisco Unified CM Administration.

For more information on how to generate the report, see the *Cisco Unified CM Administration Online Help*.

Signaling Encryption

Signaling encryption ensures that all SIP and SCCP signaling messages that are sent between the device and the Unified Communications Manager server are encrypted.

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.

Cisco does not support Network Address Translation (NAT) with Unified Communications Manager if you configure the cluster for mixed mode; NAT does not work with signaling encryption.

You can enable UDP ALG in the firewall to allow media stream firewall traversal. Enabling the UDP ALG allows the media source on the trusted side of the firewall to open a bidirectional media flow through the firewall by sending the media packet through the firewall.

Tip Hardware DSP resources cannot initiate this type of connection and, therefore, must exist outside the firewall.

Signaling encryption does not support NAT traversal. Instead of using NAT, consider using LAN extension VPNs.

Media Encryption

Media encryption, which uses Secure Real-Time Protocol (SRTP), ensures that only the intended recipient can interpret the media streams between supported devices. Media encryption includes creating a media master key pair for the devices, delivering the keys to the devices, and securing the delivery of the keys while the keys are in transport. Unified Communications Manager supports SRTP primarily for IOS gateways and Unified Communications Manager H.323 trunks on gatekeeper-controlled and non-gatekeeper-controlled trunks as well as on SIP trunks.

Note Cisco Unified Communications Manager handles media encryption keys differently for different devices and protocols. All phones that are running SCCP get their media encryption keys from Unified Communications Manager, which secures the media encryption key downloads to phones with TLS encrypted signaling channels. Phones that are running SIP generate and store their own media encryption keys. Media encryption keys that are derived by Unified Communications Manager system securely get sent via encrypted signaling paths to gateways over IPSec-protected links for H.323 and MGCP or encrypted TLS links for SCCP and SIP.

Devices must state upon negotiation if it can use SRTP. CUCM does not support SRTP if the device uses cached previous negotiations SDP with different devices within the same call.

If the devices support SRTP, the system uses a SRTP connection. If at least one device does not support SRTP, the system uses an RTP connection. SRTP-to-RTP fallback may occur for transfers from a secure device to a non-secure device, transcoding, music on hold, and so on.

For most security-supported devices, 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. CiscoIOS gateways and trunks support media encryption without authentication. For CiscoIOS gateways and trunks, you must configure IPSec when you enable the SRTP capability (media encryption).

Warning Before you configure SRTP or signaling encryption for gateways and trunks, Ciscostrongly recommends that you configure IPSec because CiscoIOS MGCP gateways, H.323 gateways, and H.323/H.245/H.225 trunks rely on IPSec configuration to ensure that security-related information does not get sent in the clear. Unified Communications Manager does not verify that you configured IPSec correctly. If you do not configure IPSec correctly, security-related information may get exposed.

SIP trunks rely on TLS to ensure that security-related information does not get sent in the clear.

The following example demonstrates media encryption for SCCP and MGCP calls.

1. Device A and Device B, which support media encryption and authentication, register with Unified Communications Manager.
2. When Device A places a call to Device B, Unified Communications Manager requests two sets of media session master values from the key manager function.
3. Both devices receive the two sets: one set for the media stream, Device A—Device B, and the other set for the media stream, Device B—Device A.
4. Using the first set of master values, Device A derives the keys that encrypt and authenticate the media stream, Device A—Device B.
5. Using the second set of master values, Device A derives the keys that authenticate and decrypt the media stream, Device B—Device A.
6. Device B uses these sets in the inverse operational sequence.
7. After the devices receive the keys, the devices perform the required key derivation, and SRTP packet processing occurs.

Note Phones that are running SIP and H.323 trunks/gateways generate their own cryptographic parameters and send them to Unified Communications Manager.

For media encryption with conference calls, refer to topics related to secure conference resources.

SCCP Gateway and Hardware Conference Bridge Support for Secure Hash Algorithm (SHA-2)

The secure Skinny Client Control Protocol (SCCP) enhances Foreign Exchange Station (FXS) analog endpoints through signaling integrity and media encryption using Transport Layer Security (TLS) and Secured Real-Time Transport Protocol (SRTP) with Unified Communications Manager.

Unified Communications Manager now provides enhanced support to the SHA-2 algorithms on SCCP Gateway (Analog endpoints) and Hardware conference bridge (TLS and SRTP).

Prerequisite

SHA-2 support for SCCP Analog endpoints and Hardware Conference Bridge works with the following Unified Communications Manager and Gateway Versions.

- Unified CM Version 14 SU1 and above.
- Gateway IOS Version: IOS XE 17.6.1 and must be configured to support TLS V1.2 for secure signaling.

Note

- For Analog endpoints, enable STCAPP on the voice gateway and make sure that the FXS ports are available on the voice gateway to register secure FXS ports on the Unified Communications Manager.
- For the Hardware conference bridge, a secure DSPFARM profile for the conference is needed as it supports a combination of transcoding sessions, MTP sessions, and conferences simultaneously.

Override Functionality

Unified Communications Manager requests conferencing or transcoding services from the gateway, which either grants or denies these requests, depending on resource availability.

If you haven't configured any ciphers on the **Cipher Management** page of the Cisco Unified OS Administration user interface, the default settings from **Enterprise Parameters** > **TLS Ciphers** will be recognized and negotiated. SCCP FXS defaults to the SHA-1 TLS cipher to avoid backward compatibility with the SCCP Cisco IP phone.

If you have selected the default option **All Supported Ciphers** in the **Cisco Unified CM Administration** > **Systems** > **Enterprise Parameter** > **TLS Ciphers** field, the following ciphers will be recognized and negotiated by Unified CM for TLS connection: AEAD_AES_256_GCM, AEAD_AES_128_GCM, AES_CM_128_HMAC_SHA1_32, SHA1_80, F8_128_HMAC_SHA1_32, F8_SHA1_80. However, if **Cisco Unified OS Administration** > **Security** > **Cipher Management** is configured with "AES256-GCM-SHA384:AES256-SHA256" on **All TLS** interfaces, all SIP interfaces support only the

"AES256-GCM-SHA384:AES256-SHA256" ciphers and ignore the Enterprise Parameter value. For more information, see the "Configure Cipher String" and "Cipher Limitations" sections.

For Example:

1. In the **Cisco Unified OS Administration** > **Cipher Management** is set to **Default**, SHA-1 TLS is negotiated.
2. In the **Cisco Unified OS Administration** > **Cipher Management** is set to **ALL**, SHA-2 TLS is negotiated.

Algorithms on a Secure Call

Unified Communications Manager is enhanced to allow negotiation of the added algorithms on a secure call. As part of this enhancement, the SCCP version has been increased to version 23 in Unified Communications Manager.

Newer Open Receive Channel (ORC) and Start Media Transmission (SMT) version 23 structures are implemented with MAX_KEY_SIZE = 32 to support Key and Salt sizes for the new SHA-2 cipher suites.



Note SHA-2 isn't supported on the SCCP phones, H323, and MGCP.

To secure media for analog endpoints registered over SCCP:

- Call between two secure SCCP Analog endpoints registered to Unfied CM must negotiate with one of the SHA-2 ciphers: AEAD_AES_256_GCM OR AEAD_AES_128_GCM.
- Call between a secure SCCP Analog endpoint and a SIP endpoint that has SHA-2 support, registered to Unfied CM negotiates with one of the SHA-2 ciphers: AEAD_AES_256_GCM OR AEAD_AES_128_GCM.

To secure media when the conference is hosted on Hardware conference bridge:

- When an SCCP Analog endpoint or SIP endpoint that has SHA-2 support is connected to the SCCP Hardware conference bridge, then SHA-2 ciphers negotiate: AEAD_AES_256_GCM OR AEAD_AES_128_GCM.
- During a secure conference call, if a mix of media establishment algorithms is present in the endpoints of the secure SCCP conference, the conference bridge negotiates the corresponding algorithm in that particular call leg.

AES 256 Encryption Support for TLS and SIP SRTP

Cisco Collaboration Solutions use Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) for signaling and media encryption. Currently, Advanced Encryption Standard (AES) with a 128-bit encryption key is used as the encryption cipher. AES also uses Hash-based Message Authentication Code Secure Hash Algorithm-1 (HMAC-SHA-1) as the authentication method. These algorithms cannot effectively scale to meet the required changing security and performance needs. To meet escalating security and performance requirements, the algorithms and protocols for encryption, authentication, digital signatures, and key exchange in Next-Generation Encryption (NGE) are developed. Also, AES 256 encryption support is provided instead of AES 128 for TLS and Session Initiation Protocol (SIP) SRTP that supports NGE.

The AES 256 encryption support for TLS and SIP SRTP is enhanced to focus on AES 256 cipher support in signaling and media encryption. This feature is useful for the applications that run on Unified Communications Manager to initiate and support TLS 1.2 connections with the AES-256 based ciphers that conform to SHA-2 (Secure Hash Algorithm) standards and is Federal Information Processing Standards (FIPS) compliant.

This feature has the following requirements:

- The connection that the SIP trunk and SIP line initiates.
- The ciphers that Unified Communications Manager supports for SRTP calls over SIP line and SIP trunk.



Note With this release, TLS 1.2 is supported on some interfaces like SIP, but is not supported on all interfaces. It is recommended that you leave TLS 1.0 and 1.1 enabled in your Collaboration deployment.

AES 256 and SHA-2 Support in TLS

The Transport Layer Security (TLS) protocol provides authentication, data integrity, and confidentiality for communications between two applications. TLS 1.2 is based on Secure Sockets Layer (SSL) protocol version 3.0, although the two protocols are not compatible with each other. TLS operates in a client/server mode where one side acts as a server and the other side acts as a client. SSL is positioned as a protocol layer between the Transmission Control Protocol (TCP) layer and the application to form a secure connection between clients and servers so that they can communicate securely over a network. To operate, TLS requires TCP as the reliable transport layer protocol.

In Unified Communications Manager, AES 256 and SHA-2 (Secure Hash Algorithm-2) support in TLS 1.2 is an enhancement to handle the connection that is initiated by the SIP Trunk and the SIP line. The supported ciphers, which are AES 256 and SHA-2 compliant, are listed as follows:

- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256—The cipher string is ECDH-RSA-AES128-GCM-SHA256.
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384—The cipher string is ECDH-RSA-AES256-GCM-SHA384.

where:

- TLS is Transport Layer Security
- ECDH is Elliptic curve Diffie–Hellman, which is an algorithm
- RSA is Rivest Shamir Adleman, which is an algorithm
- AES is Advanced Encryption Standards
- GCM is Galois/Counter Mode

In addition to the newly-supported ciphers, Unified Communications Manager continues to support TLS_RSA_WITH_AES_128_CBC_SHA. The cipher string of this cipher is AES128-SHA.

Note

- The Unified Communications Manager certificates are based on RSA.
- In Unified Communications Manager, Cisco Endpoints (phones) do not support the above mentioned new ciphers for TLS 1.2.
- With AES 256 and SHA-2 (Secure Hash Algorithm-2) support in TLS 1.2 enhancement in Unified Communications Manager, the default key size for Certificate Authority Proxy Function (CAPF) is increased to 2048 bits.

AES 256 Support in SRTP SIP Call Signaling

Secure Real-time Transport Protocol (SRTP) defines the methods of providing confidentiality and data integrity for both Real-time Transport Protocol (RTP) voice and video media and their corresponding Real-time Transport Control Protocol (RTCP) streams. SRTP implements this method through the use of encryption and message authentication headers. In SRTP, encryption applies to the payload of the RTP packet only, and not to the RTP header. However, message authentication applies to both the RTP header and the RTP payload. Also, SRTP indirectly provides protection against replay attacks because message authentication applies to the RTP sequence number within the header. SRTP uses Advanced Encryption Standards (AES) with a 128-bit encryption key as the encryption cipher. It also uses Hash-based Message Authentication Code Secure Hash Algorithm-1 (HMAC-SHA-1) as the authentication method.

Unified Communications Manager supports crypto ciphers for the SRTP calls over SIP line and SIP trunk. These crypto ciphers are AEAD_AES_256_GCM and AEAD_AES_128_GCM, where AEAD is Authenticated-Encryption with Associated-Data, and GCM is Galois/Counter Mode. These ciphers are based on GCM. If these ciphers are present in the Session Description Protocol (SDP), they are treated with higher priority as compared to the AES 128 and SHA-1 based ciphers. Cisco Endpoints (phones) do not support these new ciphers that you add for Unified Communications Manager for SRTP.

In addition to the newly supported ciphers, Unified Communications Manager continues to support the following ciphers:

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- F8_128_HMAC_SHA1_80

AES 256 encryption is supported in the following calls:

- SIP line to SIP line call signaling
- SIP line to SIP trunk signaling
- SIP trunk to SIP trunk signaling

Cisco Unified Communications Manager Requirements

- Support for TLS Version 1.2 on the SIP trunk and SIP line connections is available.
- Cipher support—TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (cipher string ECDHE-RSA-AES256-GCM-SHA384) and TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

(cipher string ECDHE-RSA-AES128-GCM-SHA256)—is available when the TLS 1.2 connection is made. These ciphers are based on GCM and conform to SHA-2 category.

- Unified Communications Manager initiates TLS1.2 with the TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ciphers. If the peer does not support TLS1.2, then Unified Communications Manager will fall back to TLS 1.0 with the existing AES128-SHA cipher.
- The SRTP calls over SIP line and SIP trunk support the GCM-based AEAD_AES_256_GCM and AEAD_AES_128_GCM ciphers.

Interactions and Restrictions

- Unified Communications Manager requirements apply to SIP line and SIP trunk, and basic SIP to SIP calls only.
- The device types that are based on non-SIP protocols will continue to support the existing behavior with the TLS versions with the supported ciphers. Skinny Call Control Protocol (SCCP) also supports TLS 1.2 with the earlier supported ciphers.
- SIP to non-SIP calls will continue to use AES 128 and SHA-1 based ciphers.

AES 80-Bit Authentication Support

Unified Communications Manager supports Advanced Encryption Standard (AES) with a 128-bit encryption key and an 80-bit authentication tag used as the encryption cipher on Music On Hold (MOH), Interactive Voice Response (IVR), and Annunciator. By default, the phones that support the 80-bit authentication tag play the MOH, IVR, and Annunciator using the AES_CM_128_HMAC_SHA1_80 crypto ciphers.

When a phone securely connects with IP Voice Media Streaming (IPVMS), precedence is given to the AES_CM_128_HMAC_SHA1_80 crypto cipher. If the phone does not support 80-bit authentication, it reverts to the AES_CM_128_HMAC_SHA1_32 cipher. If a phone does not support an 80-bit or 32-bit authentication tag, the negotiation occurs over Real-Time Transport Protocol (RTP).

Note The SCCP phone supports only a 32-bit authentication tag. Hence, negotiation between the phone and IPVMS happens only over the AES_CM_128_HMAC_SHA1_32 cipher.

If Phone A supports AES_CM_128_HMAC_SHA1_80 and Phone B supports the AES_CM_128_HMAC_SHA1_32 crypto cipher, and when User A (Phone A) dials User B (Phone B) and the call is placed on hold by User B, then Phone A connects to MOH. The negotiation between Phone A and MOH occurs through AES_CM_128_HMAC_SHA1_80 cipher because Phone A supports only the 80-bit authentication tag.

If User B (Phone B) dials User A (Phone A) and the call is placed on hold by User A, the negotiation between Phone B and MOH occurs through the AES_CM_128_HMAC_SHA1_32 cipher because Phone B supports only the 32-bit authentication tag.

If a phone supports an 80-bit authentication tag, the negotiation between a phone and an IVR or Annunciator occurs through AES_CM_128_HMAC_SHA1_80.

The following table shows the supported crypto ciphers on the phones and their negotiation cipher.

Table 5: Phones Capabilities vs. Negotiated Cipher

Phones Capabilities	Negotiated Cipher
AES_CM_128_HMAC_SHA1_32 and AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32	AES_CM_128_HMAC_SHA1_32
AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_80
Other than AES_CM_128_HMAC_SHA1_32 and AES_CM_128_HMAC_SHA1_80	Revert to RTP.

SRTP Cipher Mismatch with Media Streaming Devices

When a secure call is invoking features like Hold, IVR, or Annunciator announcements, and the remote caller performs a consult transfer, the new call leg may support a different crypto capability that of MOH, IVR, or Annunciator. This results in the crypto mismatch and the call will either be dropped to the non-secure mode or completely dropped depending on the SRTP fallback option of the endpoint. The secure call is dropped even when the **Block Unencrypted Calls** service parameter is set to **True** in **Unified Communications Manager** > **System** > **Service Parameters** > **Service Parameter Configuration** window.

A new enhancement to the Unified Communications Manager platform supports all crypto ciphers when exchanging call capabilities post-Cisco IP Voice Media Streaming (IPVMS) devices (MOH, IVR, or Annunciator). The SRTP fallback configuration does not impact active calls or compromise security.

Self-encrypting Drive

Unified Communications Manager supports self-encrypting drives (SED). This is also called Full Disk Encryption (FDE). FDE is a cryptographic method that is used to encrypt all the data that is available on the hard drive. The data includes files, operating system, and software programs. The hardware available on the disk encrypts all the incoming data and decrypts all the outgoing data.

When the drive is locked, an encryption key is created and stored internally. All data that is stored on this derive is encrypted using that key and stored in the encrypted form. The FDE comprises a key ID and a security key.

For more information, see Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide.

Configuration File Encryption

Unified Communications Manager pushes confidential data such as digest credentials and administrator passwords to phones in configuration file downloads from the TFTP server.

Unified Communications Manager uses reversible encryption to secure these credentials in the database. To secure this data during the download process, Cisco recommends that you configure encrypted configuration files for all Cisco IP Phones that support this option. When this option is enabled, only the device configuration file gets encrypted for download.

Note In some circumstances, you may choose to download confidential data to phones in the clear; for example, to troubleshoot the phone.

Unified Communications Manager encodes and stores encryption keys in the database. The TFTP server encrypts and decrypts configuration files by using symmetric encryption keys:

- If the phone has PKI capabilities, Unified Communications Manager can use the phone public key to encrypt the phone configuration file.
- If the phone does not have PKI capabilities, you must configure a unique symmetric key in Unified Communications Manager and in the phone.

You enable encrypted configuration file settings in the Phone Security Profile window in Unified Communications Manager Administration, which you then apply to a phone in the Phone Configuration window.

Default Security Administration Tasks

The following are the default security administration tasks:

Procedure

	Command or Action	Purpose
Step 1	Update ITL File for Cisco Unified IP Phones	Validates TFTP configuration files.
Step 2	Obtain ITL File Status	Obtain an ITL file status of the phones.
Step 3	Get Endpoint Support for Security by Default	Obtain the Cisco Unified IP Phone Support List using Cisco Unified Reporting page.
Step 4	Roll Back Cluster to a Pre-8.0 Release	Prepare the cluster for rollback.
Step 5	Perform Bulk Reset of ITL File, on page 35	Perform the bulk reset of ITL file.
Step 6	Reset CTL Localkey	Perform a reset of the Cisco Trust List (CTL) file with the CLI command
Step 7	View the Validity Period of ITLRecovery Certificate	View the validity period of ITLRecovery Certificate.
Step 8	Set Up Authentication and Encryption	Implement authentication and encryption for a new install.

Update ITL File for Cisco Unified IP Phones

A centralized TFTP with Unified Communication Manager using Security By Default with ITL files installed on the phones does not validate TFTP configuration files.

Perform the following procedure before any phones from the remote clusters are added to the centralized TFTP deployment.

Procedure

Step 1 On the Central TFTP server, enable the Enterprise Parameter **Prepare cluster for pre CM-8.0 rollback**.

Step 2 Restart TVS and TFTP.

Step 3 Reset all phones to verify that they download the new ITL file that disables ITL signature verification.

Step 4 Configure Enterprise Parameter Secure https URLs to use HTTP instead of HTTPS.

Note
Unified Communications Manager Release 10.5 and later automatically resets phones after you enable the **Prepare cluster for pre CM-8.0 rollback** Enterprise Parameter. For Central TFTP server's Unified Communications Manager version and how to enable this parameter, see "Roll Back Cluster to a Pre-8.0 Release" section in the Security Guide for Cisco Unified Communications Manager.

Obtain ITL File Status

Use the following procedure to obtain an ITL file status of the phones.

Procedure

Step 1 From Cisco Unified Communications Manager Administration choose **Device** > **Phone**.

Step 2 Choose **ITL File Status** in **Find Phone where** drop-down list and select the criteria.

Note
The following table is applicable only until Release 15.

Field	Description
Match	ITL Hash of server and phone are the same.
MisMatch	ITL Hash of the server is not as that of the phone.
Not Installed	The phone fails to register to a new CUCM server and bounces back to its prior server.
Unknown	The ITL Hash of the phone or the server is unknown.

Step 3 Click **Find**.

Obtain Cisco Unified IP Phone Support List

Use the Cisco Unified Reporting tool to generate a list of Cisco endpoints that support Security By Default.

Procedure

Step 1 From Cisco Unified Reporting, choose **System Reports**.

Step 2 From the **System Reports** list, choose **Unified CM Phone Feature List**.

Step 3 From the **Product** drop-down list, choose **Security By Default**.

Step 4 Click **Submit**.
A report is generated with the list of supported features for the particular phone.

Roll Back Cluster to a Pre-8.0 Release

Before you roll back a cluster to a pre-8.0 release of Unified Communications Manager, you must prepare the cluster for rollback using the Prepare Cluster for Rollback to pre-8.0 enterprise parameter.

To prepare the cluster for rollback, follow this procedure on each server in the cluster.

Procedure

Step 1 From Unified Communications Manager, choose **System** > **Enterprise Parameters Configuration**.

The **Enterprise Parameters Configuration** window displays.

Set the Prepare Cluster for Rollback to pre-8.0 enterprise parameter to **True**.

Note
Enable this parameter only if you are preparing to rollback your cluster to a pre-8.0 release of Unified Communications Manager. Phone services that use https (for example, extension mobility) will not work while this parameter is enabled. However, users will be able to continue making and receiving basic phone calls while this parameter is enabled.

Step 2 Wait ten minutes for the Cisco IP Phones to automatically restart and register with Unified Communications Manager.

Step 3 Revert each server in the cluster to the previous release.

For more information about reverting a cluster to a previous version, see *Administration Guide for Cisco Unified Communications Manager* .

Step 4 Wait until the cluster finishes switching to the previous version.

Step 5 If you are running one of the following releases in mixed mode, you must run the CTL client:

- Unified Communications Manager Release 7.1(2)
  - All regular releases of 7.1(2)
  - All ES releases of 712 prior to 007.001(002.32016.001)
- Unified Communications Manager Release 7.1(3)
  - All regular releases of 713 prior to 007.001(003.21900.003) = 7.1(3a)su1a

- All ES releases of 713 prior to 007.001(003.21005.001)

Note
For more information about running the CTL client, see the "Configuring the CTL Client" chapter.

Step 6 If "Prepare Cluster for Rollback to pre 8.0" is set to True in Enterprise Parameters then the following change must be made for Corporate Directories to work:

Under **Device > Device Settings > Phone Services > Corporate Directory** you must change the Service URL from Application:Cisco/CorporateDirectory to http://<ipaddr>:8080/ccmcip/xmldirectoryinput.jsp.

Step 7 If "Prepare Cluster for Rollback to pre 8.0" is set to True in Enterprise Parameters then the following change must be made for Personal Directories to work:

Under **Device > Device Settings > Phone Services > Personal Directory** you must change the Service URL from Application:Cisco/PersonalDirectory to 'http://<ipaddr>>:8080/ccmpd/pdCheckLogin.do?name=undefined.

Switch Back to Release 8.6 or Later After Revert

If you decide to switch back to the release 8.6 or later partition after you revert the cluster to Release 7.x, follow this procedure.

Procedure

Step 1 Follow the procedure for switching the cluster back to the inactive partition. For more information, see the *Administration Guide for Cisco Unified Communications Manager* .

Step 2 If you were running one of the following releases in mixed mode, you must run the CTL client:

Unified Communications Manager Release 7.1(2)

- All regular releases of 7.1(2)
- All ES releases of 712 prior to 007.001(002.32016.001)
- Unified Communications Manager Release 7.1(3)
  - All regular releases of 713 prior to 007.001(003.21900.003) = 7.1(3a)su1a
  - All ES releases of 713 prior to 007.001(003.21005.001)

Note
For more information about running the CTL client, see the "Configuring the CTL Client" chapter.

Step 3 From Unified Communications Manager Administration, choose **System** > **Enterprise Parameters Configuration**.

The **Enterprise Parameters Configuration** window displays.

Set the Prepare Cluster for Rollback to pre-8.6 enterprise parameter to **False**.

Step 4 Wait ten minutes for the Cisco Unified IP Phones to automatically restart and register with Unified Communications Manager.

Perform Bulk Reset of ITL File

Make sure you perform this procedure only from the Unified Communications Manager publisher.

The bulk reset of the ITL file is performed, when phones no longer trust the ITL file signer and also cannot authenticate the ITL file provided by the TFTP service locally or using TVS.

To perform a bulk reset, use the CLI command **utils itl reset**. This command generates a new ITL recovery file and re-establishes the trust between phones and the TFTP service on CUCM.



Tip When you install Unified Communications Manager, use the CLI command **file get tftp** *ITLRecovery.p12*to export the ITL Recovery pair and then perform a backup through DR. You will also be prompted to enter the SFTP server (where the key is exported) and password.

Procedure

Step 1 Perform any one of the following steps:

- Run **utils itl reset localkey**.
- Run **utils itl reset remotekey**.

Note
For **utils itl reset localkey**, the local key resides on the publisher. When issuing this command, the ITL file is signed temporarily by the CallManager key while the ITL Recovery key is resetting.

Step 2 Run **show itl** to verify that the reset was successful.

Step 3 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 4 Click **Reset**.

The devices restart. They are ready to download the ITL file that is signed by the CallManager key and accept configuration files.

Step 5 Restart the TFTP service and restart all devices.

Note
Restarting the TFTP service causes the ITL File to be signed by the ITLRecovery Key and rolling back the changes in Step 1.

The devices download the ITL file that is signed with the ITLRecovery Key and register correctly to Unified Communications Manager again.

Reset CTL Localkey

When devices on a Unified Communications Manager cluster are locked and lose their trusted status, perform a reset of the Cisco Trust List (CTL) file with the CLI command **utils ctl reset localkey**. This command generates a new CTL file.

Procedure

Step 1 Run **utils ctl reset localkey**

Note
For **utils ctl reset localkey**, the local key resides on the publisher. When issuing this command, the CTL file is temporarily signed by the CallManager key.

Step 2 Run **show ctl** to verify that the reset was successful.

Step 3 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.
The **Enterprise Parameters Configuration** page appears.

Step 4 Click **Reset**.

The devices restart. They are ready to download the CTL file that is signed by the CallManager key and accept configuration files.

Step 5 Run the **utils ctl update CTLFile** and restart the necessary services rolling back the changes in Step 1.

The devices restart. They are ready to download the CTL file that is signed by the ITLRecovery key and accept configuration files.

The devices download the CTL file that is signed using the required keys and register correctly to Unified Communications Manager again.

View the Validity Period of ITLRecovery Certificate

The ITLRecovery certificate has a long validity period with phones. You can navigate to the **Certificate File Data** pane to view the validity period or any other ITLRecovery certificate details.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Enter the required search parameters to find the certificate and view its configuration details.
The list of certificates that match the criteria appears in the **Certificate List** page.

Step 3 Click the **ITLRecovery** link to view the validity period.

The ITLRecovery certificate details appear in the **Certificate File Data** pane.

The validity period is 20 years from the current year.

Set Up Authentication and Encryption



Important You can use the **utils ctl** CLI command set to set up the encryption. For more information about this option, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

The following procedure provides all the tasks that you must perform to implement authentication and encryption. See the related topics for chapter references which contain tasks that you must perform for the specified security feature.

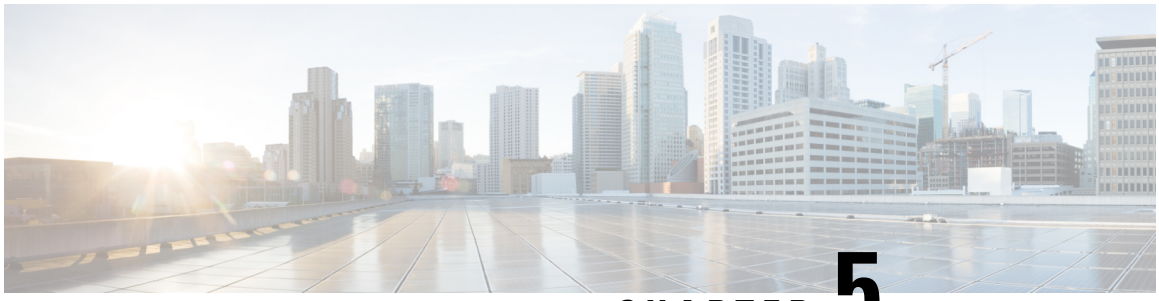
- To implement authentication and encryption for a new install, refer to the following table.
- To add a node to a secure cluster, see *Installing Cisco Unified Communications Manager*, which describes how to add a node and how to configure security for the new node.



PART II

Basic System Security

- Certificates, on page 41
- Certificate Authority Proxy Function, on page 73
- Security Modes , on page 91
- SIP OAuth Mode, on page 97
- TFTP Encryption , on page 107
- Cipher Management, on page 115
- Phone Security , on page 131
- Secure Conference Resources Setup, on page 159
- Voice-Messaging Ports Security Setup, on page 171
- Secure Tones and Icons, on page 175
- Trunk and Gateway SIP Security , on page 183
- TLS Setup, on page 197



CHAPTER 5

Certificates

- Certificate Management, on page 41
- Certificate Monitoring and Revocation, on page 67
- Simplified Certificate Management, on page 70

Certificate Management

Certificate Management feature provides an overview of the various certificate types, tasks involved to manage certificates, and how to monitor and revoke certificates.

Certificate Overview

Certificates are critical for establishing secure connections in a deployment. They authenticate individuals, computers, and other services on the network. Implementing certificate management provides a good level of protection while reducing complexity.

A Certificate is a file that proves the identity of the certificate owner and contains the following information:

- Certificate Holder Name
- Public Key
- Digital Signature of the Certificate Authority issuing the Certificate

Unified Communications Manager uses certificates that use the Public Key Infrastructure (PKI) to enable encryption and validate server - client identity. It doesn't trust other systems and denies access, unless it has a matching certificate in the appropriate trust store.

Root Certificates secure connections between users and hosts, including devices and application users. Certificates secure and add the client and server identities to the root trust stores.

Administrators can view the fingerprint of server certificates, regenerate self-signed certificates, and delete trust certificates from Unified Communications Manager interface. They can also regenerate and view self-signed certificates using CLI.

For more information on how to update the Unified Communications Manager trust store and manage certificates, see Administration Guide for Cisco Unified Communications Manager.

Note When you install Cisco Unified Communications Manager, you must enter information for the security certificate, including the country. This information is used to create the Certificate Signing Request. After you complete the installation, you cannot change the country using the **set web-security** command; ensure that you enter a valid country code during the installation.

Note Unified Communications Manager supports only PEM (.pem) and DER (.der) formatted certificates. The maximum size of certificate supported for DER or PEM is 4096 bits.

Note Unified Communications Manager does not support certificates with wildcard entry. For example, "*.cisco.com".

Note If there is an expired certificate in any of the Unified Communications Manager trust store, these certificates will not be imported during upgrade to release 12.5(1)SU6 and 14SU2 or higher.

When you upload two certificates, make sure that they have the same name and validity period but different serial numbers and signature algorithms.

For Example,

Root CA with `27:20:41:0c:5b:08:69:80:42:62:4f:13:bd:16:06:6a`serial number and SHA-1 algorithm exists in Unified Communications Manager tomcat-trust.

When you attempt to upload the certificate with `7b:35:33:71:0b:7c:08:b2:47:b3:aa:f9:5c:0d:ca:e4` serial number and SHA-256 algorithm, the certificate management:

- Verifies the incoming certificate validity.
- Searches the certificate with the same name in the Tomcat trust folder.
- Compares the serial number of the certificate existing in the Tomcat trust folder and the incoming certificate that you're uploading.

If the serial numbers are different, it verifies the validity start date of both the certificates. If the start timestamp of the new incoming certificate is the latest, then it replaces the existing certificate else it's not uploaded.

Both SHA-1 and SHA-256 algorithms have the same subject name or common name, which implies that they belong to the same entity. The Unified Communications Manager framework doesn't support both these algorithms on the Unified Communications Manager server simultaneously. It supports only one certificate that belongs to any entity in a particular trust folder, irrespective of the signature algorithm.

Certificate Types

This section provides an overview of the different types of certificates and certificate signing request key usage extensions.

Phone Certificate Types

A phone certificate is a unique identifier which authenticates phones. It's crucial for security against IP attacks.

Phone Certificates are as follows:

Table 6:

Phone Certificates	Description
Manufacture Installed Certificate (MIC)	MICs are signed by Cisco Manufacturing CA and we automatically install this certificate in supported Cisco Unified IP Phone. MICs authenticate with CiscoCertificate Authority Proxy Function (CAPF) for Locally Significant Certificates (LSC) installation or download an encrypted configuration file. Cannot use after expiry, as administrators can't modify, delete, or revoke the certificates.
Locally Significant Certificates (LSC)	Cisco Unified IP Phones require an LSC to operate in secure mode and is used for authentication and encryption. They are signed by CAPF, Online or Offline CA and takes precedence over MIC. After you perform the necessary tasks that are associated with CAPF, this certificate gets installed on supported phones. The LSC secures the connection between Unified Communications Manager and the phone after you configure the device security mode for authentication or encryption.

Tip We recommend that you use only MICs for LSC installation. We support LSCs to authenticate the TLS connection with Unified Communications Manager. When phone configurations use MICs for TLS authentication or for any other purpose, we assume no liability as MIC root certificates get easily compromised.

Upgrade Cisco Unified IP Phones 6900, 7900, 8900, and 9900 series to use LSCs for a TLS connection to Unified Communications Manager. Remove MIC root certificates from the Unified Communications Manager trust store to avoid possible future compatibility issues.

Note Phone models that use MICs for TLS connection to Unified Communications Manager may not be able to register.

Administrators should remove the following MIC root certificates from the Unified Communications Manager trust store:

- CAP-RTP-001
- CAP-RTP-002
- Cisco_Manufacturing_CA
- Cisco_Root_CA_2048
- Cisco_Manufacturing_CA_SHA2

- Cisco_Root_CA_M2
- ACT2_SUDI_CA

MIC root certificates that stay in the CAPF trust store get used for certificate upgrades. For information on updating the Unified Communications Manager trust store and managing certificates, see Administration Guide for Cisco Unified Communications Manager.

Note CAP-RTP-001 and CAP-RTP-002 certificates are removed from Unified Communications Manager.

Note In Unified Communications Manager Release 12.5.1SU2 and earlier, the Secure Onboarding feature doesn't work if you remove the Cisco Manufacturing certificates from the CallManger-trust store, because it can't validate the Manufacture Installed Certificates (MICs) from phones. However, this feature works from Unified Communications Manager Release 12.5.1SU3 onwards, because it uses the CAPF-trust store to validate the MICs from phones.

Server Certificate Types

Server Certificates are basically to identify a server. The server certificates serve the rationale of encrypting and decrypting the content.

Self-signed (own) certificate types in Unified Communications Manager servers are as follows:

Unified Communications Manager imports the following certificate types to the Unified Communications Manager trust store:

Table 7: Certificate Type and Description

Certificate Type	Description
Cisco Unity server or Cisco Unity Connection certificate	Cisco Unity and Cisco Unity Connection use this self-signed root certificate to sign the Cisco Unity SCCP and Cisco Unity Connection SCCP device certificates. For Cisco Unity, the Cisco Unity Telephony Integration Manager (UTIM) manages this certificate. For Cisco Unity Connection, Cisco Unity Connection Administration manages this certificate.
Cisco Unity and Cisco Unity Connection SCCP device certificates	Cisco Unity and Cisco Unity Connection SCCP devices use this signed certificate to establish a TLS connection with Unified Communications Manager.
SIP Proxy server certificate	A SIP user agent that connects via a SIP trunk authenticates to Unified Communications Manager if the CallManager trust store contains the SIP user agent certificate and if the SIP user agent contains the Unified Communications Manager certificate in its trust store.

Note The certificate name represents a hash of the certificate subject name, which is based on the voice-mail server name. Every device (or port) gets issued a certificate that is rooted at the root certificate.

The following additional trust store exists:

- Common trust store for Tomcat and web applications
- IPSec-trust
- CAPF-trust
- Userlicensing-trust
- TVS-trust
- Phone-SAST-trust
- Phone-CTL-trust

For more information about CA trust certificates for Cisco Unity Connection, see the Administration Guide for Cisco Unified Communications Manager. These trust-certificates secure connections to Exchange or Meeting Place Express for fetching e-mails, calendar information, or contacts.

Third-Party CA-Signed Certificates

CA-Signed certificates are trusted third party certificates which signs and issues digital certificates.

By default, Unified Communications Manager uses self-signed certificates for all connections. However, you can add security by configuring a third-party CA to sign certificates. To use a third-party CA, install the CA root certificate chain in Cisco Unified Communications Manager Administration.

To issue CA-signed certificates, submit a Certificate Signing Request (CSR) so that the CA can issue and sign a certificate. For details on how to Upload, Download, and View Certificates, see the **Self-Signed Certificates** section.

Configuration

If you want to use CA-signed certificates from another system connecting to Unified Communications Manager, do the following in Cisco Unified Communications Manager Administration:

- Upload the root certificate chain of the CA that signed the certificates.
- Upload the CA-signed certificates from the other system.

If you want to use CA-signed certificates for Unified Communications Manager:

- Complete a CSR to request CA-signed certificates in Cisco Unified Communications Manager Administration.
- Download both the CA root certificate chain and the CA-signed certificates in Cisco Unified Communications Manager Administration
- Upload both the CA root certificate chain and the CA-signed certificates.

For details on how to obtain and configure root certificates for your CA, see the Certificate Authority documentation.

Support for Certificates from External CAs

Unified Communications Manager supports integration with third-party certificate authorities (CAs) by using a PKCS#10 certificate signing request (CSR) mechanism, which is accessible at the Unified Communications Manager GUI.

Customers who currently use third-party CAs should use the CSR mechanism to issue certificates for:

- Unified Communications Manager
- CAPF
- IPSec
- Tomcat
- TVS

Note Multiserver (SAN) CA-signed certificates only applies to nodes in the cluster when the certificate gets uploaded to the Publisher. Generate a new multiserver certificate. Upload it to the cluster every time you add a new node or build it again.

If you run your system in mixed mode, some endpoints may not accept CA certificates with a key size of 4096 or longer. To use CA certificates in mixed mode, choose one of the following options:

- Use certificates with a certificate key size less than 4096.
- Use self-signed certificates.

Note Cisco's CTL client is no longer supported from Release 14. We recommend that you use the CLI command to switch the Unified Communications Manager server to Mixed Mode instead of the Cisco CTL Plugin.

Restart the appropriate services for the update after running the CTL client.

For example:

- Restart TFTP services and Unified Communications Manager services when you update the Unified Communications Manager certificate.
- Restart CAPF when you update the CAPF certificate.

After uploading the Unified Communications Manager or CAPF certificates, you might observe the phones reset automatically to update their ITL File.

For information on generating Certificate Signing Requests (CSRs) at the platform, see Administration Guide for Cisco Unified Communications Manager.

Certificate Signing Request Key Usage Extensions

The following tables display key usage extensions for Certificate Signing Requests (CSRs) for both Unified Communications Manager and the IM and Presence Service CA certificates.

Table 8: Cisco Unified Communications Manager CSR Key Usage Extensions

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
CallManager CallManager-ECDSA	Y	Y	Y		Y	N	Y		
CAPF (publisher only)	N	Y	Y		Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	N	Y		
TVS	Y	Y	Y		Y	Y	Y		

Note Ensure that 'Data Encipherment' bit is not changed or removed as part of the CA-signing certificate process.

Table 9: IM and Presence Service CSR Key Usage Extensions

	Multi server	Extended Key Usage			Key Usage				
		Server Authentication (1.3.6.1.5.5.7.3.1)	Client Authentication (1.3.6.1.5.5.7.3.2)	IP security end system (1.3.6.1.5.5.7.3.5)	Digital Signature	Key Encipherment	Data Encipherment	Key Cert Sign	Key Agreement
cup cup-ECDSA	N	Y	Y	Y	Y	N	Y		
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	N	Y		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	N	Y		
ipsec	N	Y	Y	Y	Y	N	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	N	Y		

Certificate Tasks

This section lists all the procedures to manage certificates.

Bulk Certificate Export

If both the old and new clusters are online at the same time, you can use the Bulk Certificate migration method.

Remember that the Cisco Unified IP Phones verify every downloaded file against either the ITL file, or against a TVS server that exists in the ITL file. If the phone needs to move to a new cluster, the ITL file that the new cluster presents must be trusted by the old cluster TVS certificate store.

Note The Bulk Certificate Export method only works if both clusters are online with network connectivity while the phones are being migrated.

Note During bulk certificate import, you need to import an additional ITLRecovery certificate on both the visiting cluster and the home cluster for Cisco Extension Mobility Cross Cluster (EMCC) to continue functioning. A new option to import ITL_Recovery certificate is added in Bulk Certificate Management for the **Certificate Type** drop-down list.

To use the Bulk Certificate Export method complete the following procedure:

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Security** > **Bulk Certificate Management**.

Step 2 Export certificates from new destination cluster (TFTP only) to a central SFTP server.

Step 3 Consolidate certificates (TFTP only) on the SFTP server using the Bulk Certificate interface.

Step 4 On the origination cluster use the Bulk Certificate function to import the TFTP certificates from the central SFTP server.

Step 5 Use DHCP option 150, or some other method, to point the phones to the new destination cluster.

The phones download the new destination cluster ITL file and attempt to verify it against their existing ITL file. The certificate is not in the existing ITL file so the phone requests the old TVS server to verify the signature of the new ITL file. The phone sends a TVS query to the old origination cluster on TCP port 2445 to make this request.

If the certificate export/consolidate/import process works correctly then the TVS returns success, and the phone replaces the ITL file in memory with the newly downloaded ITL file.

The phones can now download and verify the signed configuration files from the new cluster.

Show Certificates

Use the filter option on the Certificate List page, to sort and view the list of certificates, based on their common name, expiry date, key type, and usage. The filter option thus allows you to sort, view, and manage your data effectively.

From Unified Communications Manager Release 14, you can choose the usage option to sort and view the list of identity or trust certificates.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
The Certificate List page appears.

Step 2 From the **Find Certificate List where** drop-down list, choose the required filter option, enter the search item in the **Find** field, and click the **Find** button.

For example, to view only identity certificates, choose **Usage** from the **Find Certificate List where** drop-down list, enter Identity in the **Find** field, and click the **Find** button.

The Certificate display data with the BCFIPS provider has been modified for Release 14SU2 and later.

Tag Name Till 14SU1	Tag Name From 14SU2
Issuer Name	IssuerDN
Validity From	Start Date
To	Final Date
Subject Name	SubjectDN
Key	Public Key
Key Value	Modulus

Note
The x509 extensions are displayed with the OID names instead of the actual key usage names.

Download Certificates

Use the download certificates task to have a copy of your certificate or upload the certificate when you submit a CSR request.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Specify search criteria and then click **Find**.

Step 3 Choose the required file name and Click **Download**.

Install Intermediate Certificates

To install an intermediate certificate, you must install a root certificate first and then upload the signed certificate. This step is required only if the certificate authority provides a signed certificate with multiple certificates in the certificate chain.

Procedure

Step 1 From Cisco Unified OS Administration, click **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate / Certificate Chain**.

Step 3 Choose the appropriate trust store from the **Certificate Purpose** drop-down list to install the root certificate.

Step 4 Enter the description for the certificate purpose selected.

Step 5 Choose the file to upload by performing one of the following steps:

- In the **Upload File** text box, enter the path to the file.
- Click **Browse** and navigate to the file; then click **Open**.

Step 6 Click **Upload**.

Step 7 Access the Cisco Unified Intelligence Center URL using the FQDN after you install the customer certificate. If you access the Cisco Unified Intelligence Center using an IP address, you will see the message “Click here to continue”, even after you successfully install the custom certificate.

Note

- TFTP service should be restarted when a Tomcat certificate is uploaded. Else, the TFTP continues to offer the old cached self-signed tomcat certificate.
- Uploading certificates from phone edge trust should be done from publisher.

Delete a Trust Certificate

A trusted certificate is the only type of certificate that you can delete. You cannot delete a self-signed certificate that is generated by your system.



Caution Deleting a certificate can affect your system operations. It can also break a certificate chain if the certificate is part of an existing chain. Verify this relationship from the username and subject name of the relevant certificates in the **Certificate List** window. You cannot undo this action.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Use the **Find** controls to filter the certificate list.

Step 3 Choose the filename of the certificate.

Step 4 Click **Delete**.

Step 5 Click **OK**.

Note

- If you delete the “CAPF-trust”, “tomcat-trust”, “CallManager-trust”, or “Phone-SAST-trust” certificate type, the certificate is deleted across all servers in the cluster.
- Deletion of certificates from phone edge trust should be done from publisher.
- If you import a certificate into the CAPF-trust, it is enabled only on that particular node and is not replicated across the cluster.

Generate a Certificate Signing Request

Generate a Certificate Signing Request (CSR) which is a block of encrypted text that contains certificate application information, public key, organization name, common name, locality, and country. A certificate authority uses this CSR to generate a trusted certificate for your system.



Note If you generate a new CSR, you overwrite any existing CSRs.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Generate CSR**.

Step 3 Configure fields on the **Generate Certificate Signing Request** window. See the online help for more information about the fields and their configuration options.

Step 4 Click **Generate**.

Certificate Signing Request Fields

Table 10: Certificate Signing Request Fields

Field	Description
Certificate Purpose	From the drop-down list, select a value: • **tomcat** • **tomcat-ECDSA** • **tomcat-client** • **tomcat-client-ECDSA** • **ipsec** • **CallManager-ECDSA** • **CallManager** • **CallManager-client** • **CallManager-client-ECDSA** • **CAPF** • **TVS**

Distribution	Select a Unified Communications Manager server.
	When you select this field for multiserver for ECDSA, the syntax is:
	`Callmanager-ecdsa common name: <host-name>-EC-ms.<domain>`
	When you select this field for multiserver for RSA, the syntax is:
	`Callmanager common name: <host-name>-ms.<domain>`

Common Name / Common Name_SerialNumber	**Important** Supported from Release 14SU1 onwards. Displays the common name or the common name appended with the serial number of the certificate. Common Name or Common Name_SerialNumber is the file name of the certificate. Shows the name of the Unified Communications Manager application that you selected in the **Distribution** field by default.

Field	Description
Include OU in CSR	**Important** Supported from Release 14SU1 onwards. By default, the Organization Unit field is removed from the Certificate Signing Request. Choose this option to include the Organization Unit field in the Certificate Signing Request. **Note** If the Certificate Signing Request has an Organization Unit and the signed CA certificate does not, you can upload the signed CA certificate to Unified Communications Manager.
Auto-populated Domains	This field appears in Subject Alternate Names (SANs) section. It lists the host names that are to be protected by a single certificate.
Parent Domain	This field appears in Subject Alternate Names (SANs) section. It shows the default domain name. You can modify the domain name, if required.
Key Type	This field identifies the type of key used for encryption and decryption for the public-private key pair. Unified Communications Manager supports **EC** and **RSA** key types.
Key Length	From the **Key Length** drop-down list, select one of the values. Depending on the key length, the CSR request limits the hash algorithm choices. By having the limited hash algorithm choices, you can use a hash algorithm strength that is greater than or equal to the key length strength. For example, for a key length of 256, the supported hash algorithms are SHA256, SHA384, or SHA512. Similarly, for the key length of 384, the supported hash algorithms are SHA384 or SHA512. **Note** Certificates with a **key length** value of 3072 or 4096 can only be selected for RSA certificates. These options aren't available for ECDSA certificates. **Note** Some phone models may fail to register if the RSA **key length** selected for the CallManager **Certificate Purpose** is greater than 2048. From the Unified CM Phone Feature List Report on the Cisco Unified Reporting Tool (CURT), you can check the **3072/4096 RSA key size support** feature for the list of supported phone models.

Field	Description
Hash Algorithm	Select a value from the **Hash Algorithm** drop-down list to have stronger hash algorithm as the elliptical curve key length. From the **Hash Algorithm** drop-down list, select one of the values. **Note** • The values for the **Hash Algorithm** field change based on the value you select in the **Key Length** field. • If your system is running on FIPS mode, it's mandatory that you select SHA256 as the hashing algorithm.

Download a Certificate Signing Request

Download the CSR after you generate it and have it ready to submit to your certificate authority.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
Step 2 Click **Download CSR**.
Step 3 Choose the certificate name from the **Certificate Purpose** drop-down list.
Step 4 Click **Download CSR**.
Step 5 (Optional) If prompted, click **Save**.

Generate Self-Signed Certificate

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
The **Certificate List** window appears.
Step 2 Enter search parameters to find a certificate and view its configuration details.
The system displays the records that match all the criteria in the **Certificate List** window.
Step 3 Click **Generate Self-Signed Certificate** to generate a new self-signed certificate.
The **Generate New Self-Signed Certificate** window appears.
Step 4 From the **Certificate Purpose** drop-down box, select a system security certificate, such as **CallManager-ECDSA**.
Step 5 Configure the fields in the **Generate New Self-Signed Certificate** window. See the Related Topics section for more information about the fields and their configuration options.
Step 6 Click **Generate**.

Related Topics

Self-Signed Certificate Fields, on page 55

Self-Signed Certificate Fields

Table 11: Self-Signed Certificate Fields

Field	Description
Certificate Purpose	Choose the required option from the drop-down list. When you choose any of the following options, the **Key Type** field is automatically set to **RSA**. • Cisco Tomcat • ipsec • ITLRecovery • CallManager • CAPF • TVS When you choose any of the following options, the **Key Type** field is automatically set to **EC** (Elliptical Curve). • tomcat-ECDSA • CallManager-ECDSA
Distribution	Choose a Unified Communications Manager server from the drop-down list.
Common Name / Common Name_SerialNumber	Displays the common name or the common name appended with the serial number of the certificate. Common Name or Common Name_SerialNumber is the file name of the certificate.
Include OU in CSR	By default, the Organization Unit field is removed from the Certificate Signing Request. Choose this option to include the Organization Unit field in the Certificate Signing Request. **Note** If the Certificate Signing Request has an Organization Unit and the signed CA certificate does not, you can upload the signed CA certificate to Unified Communications Manager.

Field	Description
Auto-populated Domains	Appears only if you have chosen any of the following options using the **Certificate Purpose** drop-down list. • tomcat • tomcat-ECDSA • CallManager • CallManager-ECDSA • TVS This field lists the host names that are protected by a single certificate. The certificate common name is the same as the hostname. Both, **CallManager-ECDSA** and **tomcat-ECDSA**certificate has a common name that is different from the hostname. The field displays the fully qualified domain name for the **CallManager-ECDSA** certificate.
Key Type	This field lists the type of keys used for encryption and decryption of the public-private key pair. Unified Communications Manager supports **EC** and **RSA** key types.

Field	Description
Key Length	Choose any of the following values from the drop-down list: • 1024 • 2048 • 3072 • 4096 Depending on the key length, the self-signed certificate request, limits the hash algorithm choices. With the limited hash algorithm choices, you can use a hash algorithm strength that is greater than or equal to the key length strength. • If the key length value is 256, the supported hash algorithms are SHA256, SHA384, or SHA512. • If the key length value is 384, the supported hash algorithms are SHA384 or SHA512. **Note** Certificates with a **key length** value of 3072 or 4096 are chosen only for RSA certificates. These options are not available for ECDSA certificates. **Note** Some phone models might fail to register if the RSA **key length** value chosen for the CallManager **Certificate Purpose** is greater than 2048. For more information, navigate to **Unified CM Phone Feature List Report** on the Cisco Unified Reporting Tool (CURT), to check the **3072/4096 RSA key size support** for the list of supported phone models.
Hash Algorithm	Choose a value that is greater than or equal to the key length from the drop-down list: **Note** • The values in the **Hash Algorithm** drop-down list changes based on the value that you have chosen in the **Key Length** field. • If your system is running in FIPS mode, it is mandatory to choose SHA256 as the hashing algorithm.
Validity Period (in years)	Choose any of the options such as 5, 10, or 20 from the drop-down list to set the validity period of self-signed certificates. **Note** By default, the validity period of all self-signed certificate is five years. When the validity period of a certificate is changed, it does not impact the existing certificates. Only new certificates are impacted.

Regenerate a Certificate

We recommend that you regenerate certificates before they expire. You will receive warnings in RTMT (Syslog Viewer) and an email notification when the certificates are about to expire.

However, you can also regenerate an expired certificate. Perform this task after business hours, because you must restart the phones and reboot the services. You can regenerate only a certificate that is listed as type "cert" in Cisco Unified OS Administration

Caution Regenerating a certificate can affect your system operations. Regenerating a certificate overwrites the existing certificate, including a third-party signed certificate if one was uploaded.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Enter the search parameters to find a certificate and view its configuration details. The system displays the records that match all the criteria in the **Certificate List** window.

Click **Regenerate** button in the certificate details page, a self-signed certificate with the same key length is regenerated.

Note
When regenerating a certificate, the **Certificate Description** field is not updated until you close the **Regeneration** window and open the newly generated certificate.

Click **Generate Self-Signed Certificate** to regenerate a self-signed certificate with a new key length of 3072 or 4096.

Step 2 Configure the fields on the **Generate New Self-Signed Certificate** window. See online help for more information about the fields and their configuration options.

Step 3 Click **Generate**.

Step 4 Restart all services that are affected by the regenerated certificate. See Certificate Names and Descriptions, on page 59 for more information.

Step 5 Update the CTL file (if configured) after you regenerate the CAPF, ITLRecovery Certificates, or CallManager Certificates.

Note
After you regenerate certificates, you must perform a system backup so that the latest backup contains the regenerated certificates. If your backup does not contain the regenerated certificates and you perform a system restoration task, you must manually unlock each phone in your system so that the phone can register.

Important
Phones will automatically reset to receive the updated ITL File after the regeneration or renewal of the CallManager, CAPF, and TVS certificates.

Certificate Names and Descriptions

The following table describes the system security certificates that you can regenerate and the related services that must be restarted. For information about regenerating the TFTP certificate, see the *Cisco Unified Communications Manager Security Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Table 12: Certificate Names and Descriptions

Name	Description	Services to be Restarted
tomcat	This certificate is used by WebServices, Cisco DRF Services, and Cisco CallManager Services when SIP Oauth mode is enabled.	**Note** Restart of the mentioned services after this are applicable for Release 14 onwards. Cisco Tomcat Services, Cisco Intercluster Lookup Service, Cisco Location Bandwidth Manager, Cisco Disaster Recovery System (DRS) Local and Master Services, Cisco Extension Mobility, and Cisco AXL Tomcat web services. If SAML SSO is enabled with Tomcat certificate, you must re-provision the SP metadata on the IDP.
tomcat-ECDSA	This certificate is used by WebServices, Cisco DRF Services, and Cisco CallManager Services when SIP Oauth mode is enabled.	**Note** Restart of the mentioned services after this are applicable for Release 14 onwards. Cisco Tomcat Services, Cisco Disaster Recovery System (DRS) Local and Master Services, Cisco UDS Tomcat, and Cisco AXL Tomcat web services.
ipsec	This self-signed root certificate is generated during installation for IPsec connections with Unified Communications Manager, MGCP, H.323, and IM and Presence Service.	You can restart the IPSec service through the CLI using the **utils ipsec restart** command.

Name	Description	Services to be Restarted
CallManager CallManager-ECDSA	This is used for SIP, SIP trunk, SCCP, TFTP etc.	**Important** For Release 14, restart the following services: • Cisco Call Manager Service and other relevant services including Cisco CTI Manager and HAProxy Service - update CTL file if the server is in secure mode. **Important** Restart of the mentioned services after this are applicable from Release 14 SU1 onwards: • CallManager: HAProxy Service - update CTL file if the server is in secure mode. • CallManager-ECDSA: Cisco CallManager Service and HAProxy Service.
CAPF	Used by the CAPF service running on the Unified Communications Manager Publisher node. This certificate is used to issue LSC to the endpoints (except online and offline CAPF mode).	Restart Cisco HAProxy if SIP OAuth is enabled on the cluster node.
TVS	This is used by Trust verification service, which acts as a secondary trust verification mechanism for the phones in case the server certificate changes.	N/A
ITLRecovery	This certificate signs both the ITL and CTL files. It is also used for signing SAML SSO assertions.	The service is automatically restarted whenever the certificate is regenerated. If SAML SSO is enabled with Tomcat certificate, you must reprovision the SP metadata on the IDP.

Note

- A new enterprise parameter Phone Interaction on Certificate Update under section Security Parameter is introduced to reset phones either manually or automatically as applicable when one of the TVS, CAPF, or TFTP certificates are updated. This parameter is by default set to reset the phones automatically.
- After regeneration, deletion, and updating of certificates, ensure you restart the appropriate services mentioned in the column "Services to be Restarted".
- There is no specific restart needed for TVS, CAPF, and ITLRecovery services whenever a certificate is regenerated.

Important This note is applicable for Release 14SU2 only.

For Release 14SU2, Cisco DRF services need restart post tomcat-ECDSA certificate regeneration or upload. Restart is not needed post tomcat RSA certificate operations.

Important This note is applicable from Release 14SU2 onwards.

We do not support uploading of Multi-SAN certificates via the CLI. These certificates must always be uploaded via the OS Admin GUI.

Regenerate CAPF Certificate

To regenerate the CAPF certificate, perform the following steps:

Note If the CAPF certificate is on the publisher, you might observe the phones restarting automatically to update their ITL file. This behavior is applicable when the Phone interaction on Certificate Update parameter is automatically reset.

Procedure

Step 1 Regenerate the CAPF certificate.

Step 2 If you have a CTL file, then you must update the CTL file.

For more information, see Regenerate a Certificate, on page 58.

Step 3 CAPF service is automatically restarted when the CAPF certificate is regenerated.

See the “Activating the Certificate Authority Proxy Function Service” section, in the *Cisco Unified Communications Manager Security Guide*.

Regenerate TVS Certificate

Note If you plan to regenerate both TVS and TFTP certificates, regenerate the TVS certificate, wait for the possible phone restarts to complete, and then regenerate the TFTP certificate. This is applicable when the Phone interaction on Certificate Update parameter is automatically reset.

Procedure

Regenerate the TVS certificate.

For more information see the *Regenerate Certificate*, section in the Cisco Unified Communications Manager Security Guide.

The CTL file does not include a TVS certificate. So, if the TVS certificate is regenerated, you do not need to update the CTL file.

The TVS service is automatically restarted when the TVS certificate is regenerated.

Regenerate CallManager Certificate

To regenerate a CallManager certificate, follow these steps:

Note If you plan to regenerate multiple certificates you must regenerate the TFTP certificate last. Wait for the possible phone restarts to complete before you regenerate the TFTP certificate. You might need to manually delete the ITL File from all Cisco IP Phones, if you do not follow this procedure. This rule is applicable when the Phone interaction on Certificate Update parameter is automatically reset.

Procedure

Step 1 Regenerate the CallManager certificate.

For more information, see *Administration Guide for Cisco Unified Communications Manager* .

Step 2 If the TFTP service was activated, wait until all the phones have automatically restarted.

Step 3 If your cluster is in mixed mode, update the CTL file.

Step 4 If the cluster is part of an EMCC deployment, repeat the steps for bulk certificate provisioning.

For more information, see *Administration Guide for Cisco Unified Communications Manager* .

System Back-Up Procedure After TFTP Certificate Regeneration

The trust anchor for the ITL File is a software entity: the TFTP private key. If the server crashes, the key gets lost, and phones will not be able to validate new ITL File.

In Unified Communications Manager Release 10.0, the TFTP certificate and private key both get backed up by the Disaster Recovery System. The system encrypts the backup package to keep the private key secret. If the server crashes, the previous certificates and keys will be restored.

Whenever the TFTP certificate gets regenerated, you must create a new system backup. For backup procedures, see the *Administration Guide for Cisco Unified Communications Manager* .

Regenerate ITLRecovery Certificate

Warning Do not regenerate the ITLRecovery Certificate very frequently as this certificate has a long validity with phones and also it contains the CallManager Certificate.

Regenerate ITLRecovery Certificate for Non-Secure Cluster

1. Verify if the ITL File is valid and that all phones in the cluster trust the current ITL File.
2. Regenerate the ITLRecovery Certificate.

   Navigate to the publisher in each cluster to regenerate the ITLRecovery Certificate.

   a. From the Unified OS Administration, choose **Security** > **Certificate Management**

   b. Click **Find**.

      The Certificate List window appears.

   c. Click the ITLRecovery.pem Certificate link from the list of certificates displayed.

   d. Click **Regenerate**, to regenerate the ITLRecovery Certificate.

   e. In the confirmation message pop-up, click **OK**.

3. Sign the ITL file using `utils itl reset localkey` in the CallManager Certificate to accept the new ITL file.
4. Reset in batches all the phones in the cluster.

Note Make sure all the phones in the cluster are registered.

5. Restart TFTP Service to have the ITL file re-signed by the New ITLRecovery Certificate.

   New ITLRecovery Certificates are uploaded on phones while they reset.
6. Reset in batches all phones in the cluster for a second time to pick up the new ITL File.
7. Phones are uploaded with the new ITLRecovery Certificate after the reset.

Regenerate ITLRecovery Certificate for Secure Cluster

If you want to migrate from a token based ITL file to tokenless ITL file, refer the migration section in security guide.

1. Verify if the ITL File is valid and that all phones in the cluster trust the current ITL File.
2. Verify the CTL File using `show ctl` command.
3. Regenerate the ITLRecovery Certificate.

   Navigate to the publisher in each cluster to regenerate the ITLRecovery Certificate.

   a. From the Unified OS Administration, Choose **Security** > **Certificate Management** > **Find**

   b. Click **Find** to find the list of Certificates.

      The Certificate List window appears.

   c. Click the ITLRecovery.pem Certificate link from the list of Certificates displayed.

   d. Click **Regenerate**, to regenerate the ITLRecovery Certificate.

   e. In the confirmation message pop-up, click **OK**.

4. Sign the CTLFile with `utils ctl reset localkey` in the CallManager Certificate. This also updates the CTLFile with the new ITLRecovery Certificate.
5. Reset in batches all the phones in the cluster to pick up the new CTLFile with new ITLRecovery Certificate.

Note
- Make sure all the phones in the cluster are registered.
- Regenerating ITLRecovery will affect SAML SSO login of cluster incase system wide certificate is used for enablement.

6. Update the CTLFile to have it re-signed by the new ITLRecovery Certificate `utils ctl update CTLFile`.
7. Reset in batches all phones in the cluster for a second time to pick up the new CTLFile signed by the new ITLRecovery Certificate.
8. Phones are uploaded with the new ITLRecovery Certificate after the reset.

Tomcat Certificate Regeneration

Note From Release 14 onwards, if SIP OAuth is enabled, you must manually reset the phones after tomcat restart that are configured to use SIP OAuth.

To regenerate the Tomcat certificate, perform the following steps:

Procedure

Step 1 Regenerate the Tomcat certificate.

For more information see *Administration Guide for Cisco Unified Communications Manager* .

Step 2 Restart the Tomcat Service.

For more information see *Administration Guide for Cisco Unified Communications*.

Step 3 If the cluster is part of an EMCC deployment, repeat the steps for bulk certificate provisioning.

For more information see *Administration Guide for Cisco Unified Communications Manager* .

Regenerate Keys for OAuth Refresh Logins

Use this procedure to regenerate both the encryption key and the signing key using the Command Line Interface. Complete this task only if the encryption key or signing key that Cisco Jabber uses for OAuth authentication with Unified Communications Manager has been compromised. The signing key is asymmetric and RSA-based whereas the encryption key is a symmetric key.

After you complete this task, the current access and refresh tokens that use these keys become invalid.

We recommend that you complete this task during off-hours to minimize the impact to end users.

The encryption key can be regenerated only via the CLI below, but you can also use the Cisco Unified OS Administration GUI of the publisher to regenerate the signing key. Choose **Security** > **Certificate Management**, select the **AUTHZ** certificate, and click **Regenerate**.

Procedure

Step 1 From the Unified Communications Manager publisher node, log in to the **Command Line** Interface .

Step 2 If you want to regenerate the encryption key:

a) Run the `set key regen authz encryption` command.

b) Enter `yes`.

Step 3 If you want to regenerate the signing key:

a) Run the `set key regen authz signing` command.

b) Enter `yes`.
The Unified Communications Manager publisher node regenerates keys and replicates the new keys to all Unified Communications Manager cluster nodes, including any local IM and Presence Service nodes.

You must regenerate and sync your new keys on all of your UC clusters:

- IM and Presence central cluster—If you have an IM and Presence centralized deployment, your IM and Presence nodes are running on a separate cluster from your telephony. In this case, repeat this procedure on the Unified Communications Manager publisher node of the IM and Presence Service central cluster.
- Cisco Expressway or Cisco Unity Connection—Regenerate the keys on those clusters as well. See your Cisco Expressway and Cisco Unity Connection documentation for details.

Note
You must restart the Cisco XCP Authentication Service in the following scenarios:

- When you regenerate Authz certificate
- When you make a new entry to the centralized deployment in the IM and Presence administrator console

Add Certificate Authority-Signed CAPF Root Certificate to the Trust Store

Add the root certificate to the Unified Communications Manager trust store when using a Certificate Authority-Signed CAPF Certificate.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate Chain**.

Step 3 In the **Upload Certificate/Certificate Chain** popup window, choose **CallManager-trust** from the **Certificate Purpose** drop-down list and browse to the certificate authority-signed CAPF root certificate.

Step 4 Click **Upload** after the certificate appears in the **Upload File** field.

Update the CTL File

Use this procedure to update the CTL file via a CLI command. If mixed mode is enabled, you must update the CTL file whenever you upload a new certificate.

Procedure

Step 1 From the Unified Communications Manager publisher node, log in to the **Command Line Interface**.

Step 2 Run the `utils ctl update CTLFile` command. When the CTL file regenerates, the file gets uploaded to the TFTP server and sent to phones automatically.

Interactions and Restrictions

- SIP devices that do not support **TLS_ECDHE_ECDSA_WITH_AES256_SHA384** and **TLS_ECDHE_ECDSA_WITH_AES128_SHA256** can still connect with **TLS_ECDHE_RSA_WITH_AES_256_SHA384**, **TLS_ECDHE_RSA_WITH_AES_128_SHA256**, or **AES128_SHA**. These options are dependent on the TLS cipher option that you choose. If you choose **ECDSA only** option, then the device that does not support the ECDSA ciphers will not be able make a TLS connection to the SIP interface. When you choose the **ECDSA only** option, the value of this parameter are **TLS_ECDHE_ECDSA_WITH_AES128_SHA256** and **TLS_ECDHE_ECDSA_WITH_AES256_SHA384**.

- CTI Manager Secure clients do not support **TLS_ECDHE_RSA_WITH_AES_128_SHA256** , **TLS_ECDHE_RSA_WITH_AES_256_SHA384**, **TLS_ECDHE_ECDSA_WITH_AES_128_SHA256**, and **TLS_ECDHE_ECDSA_WITH_AES_256_SHA384**. However, they can connect with **AES128_SHA**.
- The Unified Communications Manager do not support multiple certificates with same SubjectDN to be uploaded on the same trust store. For the server to differenciate between new and existing certificates, We recommend the users to use new CN with a different name or suffix it with characters for example, SubjectDN-issue-CA-G2 or SubjectDN-issue-CA-2023. A hash link would be created for the same.

Certificate Monitoring and Revocation

This section allows you to monitor certificates that have to be renewed and revoke certificates which are expired.

Certificate Monitoring Overview

Administrators must be able to track and renew certificates when services from Unified Communications Manager and IM and Presence Service contain automated systems. Certificate Monitoring helps administrators know the certificate status on an ongoing basis and generate an email alerting you when a certificate is approaching expiration.

Certificate Monitoring Configuration

The Cisco Certificate Expiry Monitor network service must be running. By default, this service is enabled, but you can confirm if the service is running in Cisco Unified Serviceability application by choosing **Tools** > **Control Center - Network Services** and verifying that the **Cisco Certificate Expiry Monitor Service** status is **Running**.

Procedure

Step 1 From the Cisco Unified OS Administration, Choose **Security** > **Certificate Monitor**

Step 2 Enter or choose the configuration details.

Step 3 Click **Save** to save the configuration.

Note
By default, the certificate monitor service runs once every 24 hours. When you restart the certificate monitor service, it starts the service and then calculates the next schedule to run only after 24 hours. The interval doesn't change even when the certificate is close to the expiry date of seven days. It runs every one hour when the certificate either has expired or is going to expire in one day.

Certificate Revocation Overview

This section allows you to understand certificate revocation. Cisco UCM provisions the Online Certificate Status Protocol (OCSP) for monitoring certificate revocation. Every time there's a certificate uploaded and at scheduled timelines, system checks for its status to confirm validity.

For FIPS deployments with Common Criteria mode enabled, OCSP helps your system comply with Common Criteria requirements.

Certificate Revocation Configuration

Unified Communications Manager checks the status of the certificate and confirms validity.

The certificate validation procedure is as follows:

- Unified Communications Manager uses the Delegated Trust Model (DTM) and checks the Root CA or Intermediate CA for the OCSP signing attribute. The Root CA or the Intermediate CA must sign the OCSP Certificate to check the status.
- If the Delegated Trust Model fails, falls back to the Trust Responder Model (TRP). Unified Communications Manager then uses a designated OCSP response signing certificate from an OCSP server to validate certificates.

Note OCSP Responder must be running to check the revocation status of the certificates.

Configure OCSP so that the system revokes expired certificates automatically. Enable the OCSP option in the Certificate Revocation window to provide a secure means of checking certificate revocation in real time. Choose from options to use the OCSP URI from the certificate or from the configured OCSP URI.

Note TLS clients like syslog, FileBeat, SIP, ILS, LBM, and so on, receive the revocation response in real time from OCSP.

Make sure that your system has the certificates required for OCSP checks. You can use Root or Intermediate CA certificates configured with the OCSP response attribute or designated OCSP signing certificates uploaded to the tomcat-trust.

Important This section is applicable from Release 14SU3 onwards.

Certificate revocation is a process that distinguishes invalid and untrusted certificates from valid trusted ones. Where the CAs makes it known that one or more of their digital certificates is no longer trustworthy and essentially invalidates the certificate ahead of its expiration date.

A certificate revocation list (CRL) is a list of digital certificates that the issuing certificate authority has revoked before their actual or assigned expiration date. Certificate Revocation List is integral to public key infrastructure (PKI) and web security. Every CA will have its own CRL list.

This feature is mainly designed for CA-issued CAPF signed phone LSCs. Whenever there is a difference in latest and previously downloaded CRL files from CA, a *CRLChanged* alarm will be generated and displayed

on the RTMT along with a message in the syslog server. For more details on the *CRLChanged* alarm, see the Cisco Unified Real-Time Monitoring Tool.

The administrator needs to address the alarm by renewing and replacing the valid certificate chain and restart the affected services on the Call Manager to terminate the existing TLS new connections that were using the revoked certificates. Later, connections will be established with the valid new certificates.

Procedure

Step 1 From the Cisco Unified OS Administration, choose **Security** > **Certificate Revocation.**

Step 2 Check the **Enable OCSP** check box.

Step 3 Click the **Use OCSP URI from Certificate** option if the certificate is configured with an OCSP responder URI.

OR

Step 4 Click **Use Configured OCSP URI** option if you want to specify an OCSP responder for OCSP checks.

Step 5 Enter the **OCSP Configured URI** of the responder.

Step 6 Check the **Enable Revocation Check** check box to enable a revocation check.

Step 7 Enter a **frequency** to check for revocation status and click the **time interval** from Hours or Days.

Step 8 Check the **Enable CRL** check box.

Step 9 Enter the **CRL Distribution Point URI** from where the CRL File has to be downloaded.

Important
From Release 15SU3 onwards, you can configure up to five distribution point URI settings to support multiple CRL file downloads (1 per Certificate Authority).

Step 10 Click **Save**.

Note
A popup alerts you to restart a list of Cisco Services and enable real-time OCSP. The popup appears only when you check the **Enable OCSP** check box or save the subsequent changes.

The OCSP Responder returns one of the following statuses based on the validations and when the Common Criteria mode is ON.

- **Good—** indicates that the OCSP responder sends a positive response to the status inquiry. The certificate isn't revoked but doesn't mean that the certificate was ever issued or the response time is within the validity interval of the certificate. Response extensions convey more claims made by the responder on the certificate status such as issuance, validity, and so on.
- **Revoked—** indicates that the certificate is in revoked (on hold) status either permanently or temporarily.
- **Unknown—** indicates that the OCSP responder doesn't know about the requested certificate.

  Warning
  When you enable Common Criteria mode, the connection fails in **Revoked** and **Unknown** cases. When you disable Common Criteria mode, the connection succeeds in **Unknown** case.

Step 11 (Optional) If you have CTI, IPsec or LDAP links, you must also complete these steps in addition to the above steps to enable OCSP revocation support for those long uninterrupted connections:

a) From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.
b) Navigate to **Certificate Revocation and Expiry** pane.
c) Set the **Certificate Validity Check** parameter to **Enabled**.
d) Enter a value for the **Validity Check Frequency** parameter.

Note
The interval value of the **Enable Revocation Check** parameter in the **Certificate Revocation** page takes precedence over the value of the **Validity Check Frequency** enterprise parameter.

e) Click **Save**.

Simplified Certificate Management

It is now easier to accomplish certificate requirements due to a collection of updates that reduces a significant number of certificates that you need to manage. Unified Communications Manager has eight identity certificates. They are CallManager, CallManager-ECDSA, Tomcat, Tomcat-ECDSA, IPsec, CAPF, TVS, ITL Recovery for each node. These certificates have to be renewed periodically based on their validity period. Hence, in a multi-cluster deployment scenario, it is difficult to manage these certificates.

Simplified Certificate Management Overview

To manage certificates efficiently, you now have an option to reduce and reuse the number of certificates.

- **TVS Supports Multiserver SAN Certificates**—TVS now supports multi-server SAN certificates for both self-signed and CA-signed options, letting you deploy a single certificate for the cluster. These certificates are cluster-based. For each cluster, there is an option to have only one TVS certificate that reduces the ITL file size and the management overhead. For example, if there were 21 nodes, now you need only one single certificate for each cluster.
- **CAPF Certificates Generated from Publisher Node**—CAPF certificates are now generated only from the publisher node, letting you deploy a single certificate for the cluster. However, the CAPF certificate is available as a trust-certificate (Callmanager-trust) on both the publisher and subscriber nodes for endpoint registration.
- **Support for Multi-server SAN Self-Signed Certificates**—Tomcat, Tomcat-ECDSA, CallManager, CallManager-ECDSA certificates now support multi-server SAN self-signed certificates. Earlier, multi-server SAN certificates were supported only for CA-signed certificates. You can now avoid the cost of managing a CA from a third-party certificate authority by using the multi-server SAN self-signed certificate.
- **Reuse Multi-Server Tomcat certificate for CallManager**—You can now reuse multi-server Tomcat certificates for CallManager certificates, because there is no need to generate separate certificates for each. For more details on how to reuse multi-server tomcat certificates for CallManager certificate, see Reuse Multi-Server Tomcat Certificate for CallManager, on page 71.
- **Validity Period of Self-signed Certificates**—The default validity period of self-signed certificates are reduced. By reducing the validity period, the keys are renewed periodically in a short span, and it removes the outdated certificates. The longer the validity period of the certificates, the higher are the chances of the private key being compromised. The default validity period of all self-signed certificates is five years.

You also have an option to configure the validity period of the self-signed certificates using the **Validity Period** field. For more details, see the Generate New Self-signed certificate section.

Table 13: Cisco Unified Communications Manager CSR Key Usage Extensions

	Earlier than Unified CM Release 14				From Unified CM Release 14 onwards			
Certificates	**Supports Multi-Server SAN Self-Signed**	**Supports Multi-Server SAN CA-Signed**	**No.of certificates to manage in a 10 node cluster**	**Node/Cluster Based**	**Supports Multi-Server SAN Self-Signed**	**Supports Multi-Server CA-Signed**	**No.of certificates to manage in a 10 node cluster**	**Node/Cluster Based**
Tomcat	N	Y	1	Node-Based when self-signed	Y	Y	1	Cluster-based
Tomcat-ECDSA	N	Y	1	Node-Based when self-signed	Y	Y	1	Cluster-based
CallManager	N	Y	1	Node-Based when self-signed	Y	Y	0	Cluster-based
CallManager-ECDSA	N	Y	1	Node-Based when self-signed	Y	Y	0	Cluster-based
TVS	N	N	10	Node-based	Y	Y	1	Cluster-based
CAPF	N	N	10	Node-based	Y	N	1	Only on Publisher
IPsec	N	N	10	Node-based	N	N	0	Node-based
ITLRecovery	N	N	1	Node-based	N	N	1	Cluster-based

Simplified Certificate Management User Interface Updates

The following user interface updates are introduced:

- **Reuse Certificate**—The Certificate Management window includes this new option that lets you share a Tomcat multi-server certificate with the CallManager application. This reduces the size of the ITL file, thereby reducing overhead.
- **Show Certificates**—The Certificate Management window in Cisco Unified OS Administration interface includes new filtering options that let you view the list of identity and trust certificates.

Reuse Multi-Server Tomcat Certificate for CallManager

You can now reuse a Tomcat multi-server certificate for the CallManager application. You can procure one certificate from the CA and reuse it across applications. This ensures lower management overhead and cost optimization.

Note Before you reuse a Tomcat certificate, make sure that it is a multi-server SAN support certificate.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 Click **Reuse Certificate**.
The **Use Tomcat Certificates For Other Services** page appears.

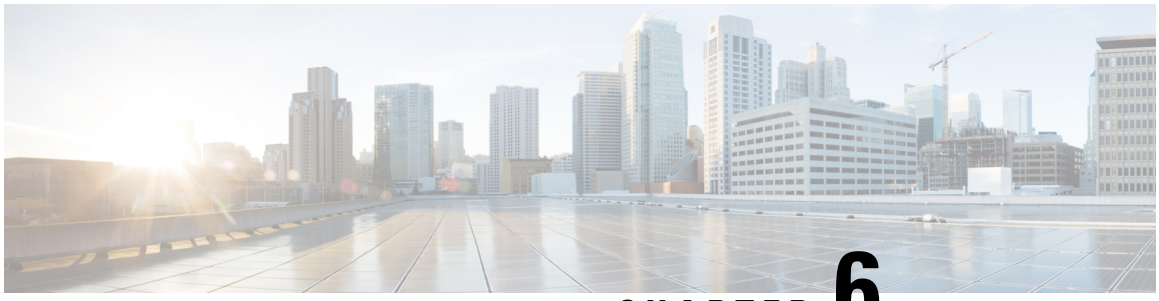
Step 3 From the **Choose Tomcat type** drop-down list, choose either **tomcat** or **tomcat-ECDSA**.

Step 4 From the **Replace Certificate for the following purpose** pane, check either the **CallManager** or **CallManager-ECDSA** check box.

Note
Before you click the **Replace Certificate for the following purpose** button, ensure that you manually upload the CA certificate chain (that signed the tomcat identity certificate) to the CallManager trust store. Refer to the Certificate Names and Descriptions, on page 59 section to check what services must be restarted when you upload the tomcat certificate chain to the CallManager trust.

Step 5 Click **Finish** to replace the CallManager certificate with the tomcat multi-server SAN certificate.

Note
- If you choose tomcat as the certificate type, CallManager is enabled as the replacement.
- If you choose tomcat-ECDSA as the certificate type, CallManager-ECDSA is enabled as the replacement.
- The CallManager certificate will not be visible in the GUI when you reuse the certificate.



CHAPTER 6

Certificate Authority Proxy Function

- Certificates Authority Proxy Function Overview, on page 73
- Certificates Authority Proxy Function Configuration Task Flow, on page 75
- Certificates Authority Proxy Function Administration Task Flow, on page 84
- CAPF System Interactions, on page 86

Certificates Authority Proxy Function Overview

The Certificate Authority Proxy Function (CAPF) issues Locally Significant Certificates (LSCs) and authenticates endpoints.

The CAPF service runs on Unified Communications Manager and performs the following tasks:

- Issues LSCs to supported Cisco Unified IP Phones.
- Authenticates phones while in mixed mode.
- Upgrades existing LSCs for phones.
- Retrieves phone certificates for viewing and troubleshooting.

CAPF Service Certificate

The CAPF service gets automatically installed with the Unified Communications Manager installation and a CAPF-specific system certificate gets generated.



Important The following note is applicable only from Release 14SU2 onwards.

Note For any CAPF certificates, it should include the following default X509 extensions:

X509v3 Basic Constraints:

CA:TRUE, pathlen:0

X509v3 Key Usage:

Digital Signature, Certificate Sign

In the CAPF certificates if these extensions are missing, there will be TLS connection failure.

You can configure CAPF to operate in the following modes:

Table 14: CAPF Running Modes

Modes	Description
Cisco Authority Proxy Function	By default, the CAPF service on Unified Communications Manager issues CAPF service signed LSCs.
Online CA	Use this option to have an external online CA signed LSC for phones. The CAPF service connects automatically to the external CA. When a Certificate Signing Request (CSR) is manually submitted, the CA signs and returns the CA-signed LSC automatically. **Note** Online CA does not support CAPF operations with ECDSA key sizes.
Offline CA	Use this option if you want to use an offline external CA to sign LSC for phones. Manually download the LSC, submit them to the CA, and then upload the CA-signed certificates after they are ready. **Note** We recommend **Online CA** option instead of **Offline CA** when you want to use a third-party CA to sign LSC. **Online CA** is automated, quicker, and less likely to encounter problems.

Before you generate LSCs, make sure that you have the following:

- Unified Communications Manager Release 12.5 or later.
- Endpoints that use CAPF for certificates (includes Cisco Unified IP Phones and Jabber).
- Microsoft Windows Server 2016 and 2022 with CA configured.
- Domain Name Service (DNS).

As a pre-requisite, also decide how you want to authenticate your phones.

Upload CA root and HTTPS certificates before generating LSCs to the required trust stores. The Internet Information Services (IIS) hosts the HTTPS certificate. During a secure SIP connection, HTTPS certificate goes through the CAPF-trust and the CA root certificate goes through both the CAPF-trust and the Unified

Communications Manager-trust. The CA root certificate is used to sign the Certificate Signing Requests (CSRs).

Following are the scenarios to upload the various certificates:

Table 15: Upload Certificate Scenarios

Scenarios	Actions
CA root and HTTPS certificates are same.	Upload the CA root certificate.
CA root and HTTPS certificates are different and the same CA root certificate issues the HTTPS certificates.	Upload the CA root certificate.
CA root certificate issues the intermediate CA and HTTPS certificates which are different.	Upload the CA root certificate.
The same CA root certificate issues CA root and HTTPS certificates which are different.	Upload CA root and HTTPS certificate.

Note We recommend using CAPF during a scheduled maintenance window as generating multiple certificates simultaneously may cause call-processing interruptions.

Certificates Authority Proxy Function Configuration Task Flow

Complete these tasks to configure the Certificate Authority Proxy Function (CAPF) service to issue LSCs for endpoints:

Note You don't have to restart the CAPF service after regenerating or uploading the new CAPF certificate.

Procedure

	Command or Action	Purpose
Step 1	Upload Root Certificate for Third Party CAs	If you want your LSCs to be third-party CA-signed, upload the CA root certificate chain

	Command or Action	Purpose
		to the CAPF-trust store. Otherwise, you can skip this task.
Step 2	Upload Certificate Authority (CA) Root Certificate , on page 77	Upload the CA root certificate to the Unified Communications Manager Trust store.
Step 3	Configure Online Certificate Authority Settings, on page 78	Use this procedure to generate phone LSC certificates.
Step 4	Configure Offline Certificate Authority Settings	Use this procedure to generate phone LSC certificates using an Offline CA.
Step 5	Activate or Restart CAPF Services	After you configure the CAPF system settings, activate essential CAPF services.
Step 6	Configure CAPF settings in Unified Communications Manager using one of the following procedures: • Configure CAPF Settings in a Universal Device Template, on page 80 • Update CAPF Settings via Bulk Admin, on page 81 • Configure CAPF Settings for a Phone, on page 83	Add the CAPF settings to Phone Configuration using one of the following options: • If you haven't synced your LDAP directory, add CAPF settings to a Universal Device Template and apply settings through the initial LDAP sync. • Use Bulk Administration Tool to apply CAPF settings to many phones in a single operation. • You can apply CAPF settings on a phone-by-phone basis.
Step 7	Set KeepAlive Timer, on page 83	Set a keepalive value for the CAPF-Endpoint connection so that it's not timed out by a firewall. The default value is 15 minutes.

Upload Root Certificate for Third-Party CAs

Upload the CA root certificate to the CAPF-trust store and the Unified Communications Manager trust store to use an external CA to sign LSC certificates.

Note Skip this task if you don't want to use a third-party CA to sign LSCs.

Procedure

Step 1 From Cisco Unified OS Administration choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate chain**.

Step 3 From the **Certificate Purpose** drop-down list, choose **CAPF-trust**.

Step 4 Enter a **Description** for the certificate. For example, **Certificate for External LSC-Signing CA**.

Step 5 Click **Browse**, navigate to the file, and then click **Open**.

Step 6 Click **Upload**.

Step 7 Repeat this task, uploading certificates to **callmanager-trust** for the **Certificate Purpose**.

Upload Certificate Authority (CA) Root Certificate

Note Ensure that the intermediate or root CA certificate doesn't contain the 'CAPF−' substring in the Common Name. The 'CAPF−' common name is reserved for CAPF certificates.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate chain**.

Step 3 From the **Certificate Purpose** drop-down list, choose **callmanager-trust**.

Step 4 Enter a **Description** for the certificate. For example, **Certificate for External LSC-Signing CA**.

Step 5 Click **Browse**, navigate to the file, and then click **Open**.

Step 6 Click **Upload**.

Important
This Note is applicable from Release 14 SU2 onwards.

Note
For any root or intermediate CA certificates, it should include the following default X509 extensions:

X509v3 Basic Constraints:

CA:TRUE, pathlen:0

X509v3 Key Usage:

Digital Signature, Certificate Sign

In the certificates if these extensions are missing, there will be TLS connection failure.

Important
This Note is applicable from Release 14 SU3 onwards and only for IPSec certificates.

Note
For any CA-signed IPSec certificates, it should not include the following extensions:

X509v3 Basic Constraints:

CA:TRUE

Configure Online Certificate Authority Settings

Use this procedure in Unified Communications Manager to generate phone LSCs using Online CAPF.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose a node where you activated the Cisco Certificate Authority Proxy Function (Active) service.

Step 3 From the **Service** drop-down list, choose **Cisco Certificate Authority Proxy Function (Active)**. Verify that the word “Active” is displayed next to the service name.

Step 4 From the **Certificate Issuer to Endpoint** drop-down list, choose **Online CA**. For CA-signed certificates, we recommend using an Online CA.

Step 5 In the **Duration Of Certificate Validity (in days)** field, enter a number between 1 and 1825 to represent the number of days that a certificate issued by CAPF is valid.

Step 6 In the **Online CA Parameters** section, set the following parameters to create the connection to the Online CA section.

- Online CA Hostname—The subject name or the Common Name (CN) should be the same as the Fully Qualified Domain Name (FQDN) of the HTTPS certificate.

  Note
  The hostname configured is the same as the Common Names (CN) of the HTTP's certificate hosted by Internet Information Services (IIS) running on Microsoft CA.

- Online CA Port—Enter the port number for Online CA. For example, 443.
- Online CA Template—Enter the name of the template. Microsoft CA creates the template.

  Note
  This field is enabled only if the Online CA Type is Microsoft CA.

- Online CA Type—Choose Microsoft CA or EST Supported CA for automatic enrollment of endpoint certificate.
  - Microsoft CA—Use this option when CA is Microsoft CA to allocate digital certificates to devices.

    Note
    FIPS enabled mode is not supported with Microsoft CA.

  - (Supported from Release 14SU2 onwards) EST Supported CA—Use this option when CA supports inbuilt EST server mode for automatic enrollment.

    Note
    Enrollment of CAPF LSC using EST supported CA is not supported in CC mode.

- Online CA Username—Enter the username of the CA server.
- Online CA Password—Enter the password for the username of the CA server.

- Certificate Enrollment Profile Label—Enter the Digital Identity for EST Supported CA with valid characters.

  Note
  This field is enabled only if the Online CA Type is EST Supported CA.

Step 7 Complete the remaining CAPF service parameters. Click the parameter name to view the service parameter help system.

Step 8 Click **Save**.

Step 9 Restart **Cisco Certificate Authority Proxy Function** for the changes to take effect. It automatically restarts the Cisco Certificate Enrollment service.

Current Online CA limitations

- The Online CA feature does not work if the CA server uses any other language apart from English. The CA server should respond only in English.
- The Online CA feature does not support mTLS authentication with CA.
- While using Online CA for LSC operation, if LSC certificate is not provided with 'Digital signature' and 'key encipherment' key usage Device secure registration will fail.

Configure Offline Certificate Authority Settings

Follow this high-level process if you decide to generate phone LSC certificates using an Offline CA.

Note The offline CA option is more time-consuming than online CAs, involving numerous manual steps. Restart the process if there are any issues (for example, a network outage or phone reset) during the certificate generation and transmission process.

Procedure

Step 1 Download the root certificate chain from the third-party certificate authority.

Step 2 Upload the root certificate chain to the required trusts (CallManager trust CAPF trust) in Unified Communications Manager.

Step 3 Configure Unified Communications Manager to use Offline CAs by setting the **Certificate Issue to Endpoint** service parameter to Offline CA.

Step 4 Generate **CSR**s for your phone LSCs.

Step 5 Send the **CSR**s to the certificate authority.

Step 6 Obtain the signed certificates from the **CSR**.

For more detailed example on how to generate phone LSCs using an Offline CA, see CUCM Third-Party CA-Signed LSCs Generation and Import Configuration.

Activate or Restart CAPF Services

Activate the essential CAPF services after you configure the CAPF system settings. Restart if the CAPF service is already activated.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Server** drop-down list, select the publisher node and click **Go**.

Step 3 From the **Security Services** pane, check the services that apply:

- **Cisco Certificate Enrollment Service**—Check this service if you're using an Online CA else leave it unchecked.
- **Cisco Certificate Authority Proxy Function**—Check this service if unchecked (Deactivated). Restart if the service is already activated.

Step 4 Click **Save** if you modified any settings.

Step 5 If the **Cisco Certificate Authority Proxy Function** service was already checked (Activated), restart it:

a) From the **Related Links** drop-down list, select **Control Center - Feature Services** and click **Go**.
b) From **Security Settings** pane, check the **Cisco Certificate Authority Proxy Function** service and click **Restart**.

Step 6 Complete one of the following procedures to configure CAPF settings against individual phones.

a) Configure CAPF Settings in a Universal Device Template, on page 80
b) Update CAPF Settings via Bulk Admin, on page 81
c) Configure CAPF Settings for a Phone, on page 83

Configure CAPF Settings in a Universal Device Template

Use this procedure to configure CAPF settings to a Universal Device Template. Apply the template against an LDAP directory sync through the feature group template configuration. The CAPF settings in the template apply to all synced devices that use this template.



Note You can only add the Universal Device Template to an LDAP directory that hasn't been synced. If your initial LDAP sync has occurred, use Bulk Administration to update phones. For details, see Update CAPF Settings via Bulk Admin, on page 81.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Universal Device Template**.

Step 2 Do either of the following:

- Click **Find** and **Select** an existing template.
- Click **Add New**.

Step 3 Expand the **Certificate Authority Proxy Function (CAPF) Settings** area.

Step 4 From the **Certificate Operation** drop-down list, select **Install/Upgrade**.

Step 5 From the **Authentication Mode** drop-down list menu, select an option for the device to authenticate itself.

Step 6 If you chose to use an authentication string, enter the **Authentication String** in the text box, or click **Generate String** to have the system generate a string for you.

Note
Authentication fails if this string isn't configured on the device itself.

Step 7 From the remaining fields, configure the key information. For help with the fields, see the online help.

Step 8 Click **Save**.

Note
Make sure you have configured the devices that use this template with the same authentication method that you assigned in this procedure. Otherwise, device authentication fails. See your phone documentation for details on how to configure authentication for phones.

Step 9 Apply the template settings to devices that use this profile.

a) Add the Universal Device Template to a Feature Group Template Configuration.
b) Add the Feature Group Template to an LDAP Directory Configuration that isn't synced.
c) Complete an LDAP sync. The CAPF settings get applied to all synced devices.

For details on configuring feature group templates and LDAP directories, see the "Configure End Users" section of System Configuration Guide for Cisco Unified Communications Manager.

Update CAPF Settings via Bulk Admin

Use **Update Phones** query of Bulk Administration to configure CAPF settings and LSC certificates for many existing phones in a single operation.

Note If you haven't provisioned the phones, use **Insert Phones** menu of the Bulk Administration to provision new phones with CAPF settings from a CSV file. See the "Phones Insertions" section of Bulk Administration Guide for Cisco Unified Communications Manager for details on how to insert phones from CSV files.

Make sure you have configured your phones with the same string and authentication method that you plan to add in this procedure. Else, your phones don't authenticate to CAPF. See your *Phone Documentation* for details on how to configure authentication on the phone.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **Phones** > **Update Phones** > **Query**.

Step 2 Use filter options to limit the search to the phones that you want to update and click **Find**.

For example, use **Find phones where** drop-down list to select all phones, where LSC expires before a specific date or in a specific Device Pool.

Step 3 Click **Next**.

Step 4 From the **Logout/Reset/Restart** section, choose the **Apply Config** radio button. When the job runs, the CAPF updates get applied to all updated phones.

Step 5 Under **Certification Authority Proxy Function (CAPF) Information**, check the **Certificate Operation** check box.

Step 6 From the **Certificate Operation** drop-down list, choose **Install/Upgrade** to have CAPF install a new LSC certificate on the phone.

Step 7 From the **Authentication Mode** drop-down list, choose how you want the phone to authenticate itself during the LSC installation.

Note
Configure the same authentication method on the phone.

Step 8 Complete one of the following steps if you selected **By Authentication String** as the **Authentication Mode**:

- Check **Generate unique authentication string for each device** if you want to use a unique authentication string for each device.
- Enter the string in **Authentication String** text box, or click **Generate String** if you want to use the same authentication string for all devices.

Step 9 Complete the remaining fields in the **Certification Authority Proxy Function (CAPF) Information** section of the **Update Phones** window. For help with the fields and their settings, see the online help.

Step 10 From the **Job Information** section, select **Run Immediately**.

Note
Select **Run Later** if you want run the job at a scheduled time. For details on scheduling jobs, see the "Manage Scheduled Jobs" section in Bulk Administration Guide for Cisco Unified Communications Manager.

Step 11 Click **Submit**.

Note
Apply configurations in the **Phones Configuration** window for all updated phones if you didn't select the **Apply Config** option in this procedure.

Configure CAPF Settings for a Phone

Use this procedure to configure CAPF settings for LSC certificates on an individual phone.

Note Use Bulk Administration or sync LDAP directory to apply CAPF settings to a large number of phones.

Configure your phone with the same string and authentication method that you plan to add in this procedure. Else, the phone doesn't authenticate itself to CAPF. See your *Phone Documentation* for details on how to configure authentication on the phone.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select an existing phone. The **Phone Configuration** page appears.

Step 3 Navigate to the **Certification Authority Proxy Function (CAPF) Information** pane.

Step 4 From the **Certificate Operation** drop-down list, choose **Install/Upgrade** for CAPF to install a new LSC certificate on the phone.

Step 5 From the **Authentication Mode** drop-down list, choose how you want the phone to authenticate itself during the LSC installation.

Note
The phone should be configured to use the same authentication method.

Step 6 Enter a text string or click **Generate String** to generate a string for you if you selected **By Authentication String**.

Step 7 Enter the details in the remaining fields in the **Certification Authority Proxy Function (CAPF) Information** pane of the **Phone Configuration** page. For help with the fields and their settings, see the online help.

Step 8 Click **Save**.

Set KeepAlive Timer

Use this procedure to set the clusterwide keepalive timer for the CAPF–Endpoint connection so that the connection doesn't get timed out by a firewall. The timer has a default value of 15 minutes. After each interval, the CAPF service sends a keepalive signal to the phone to keep the connection open.

Procedure

Step 1 Use the Command Line Interface to log in to the publisher node.

Step 2 Run the `utils capf set keep_alive` CLI command.

Step 3 Enter a number between 5 and 60 (minutes) and click **`Enter`**.

Certificates Authority Proxy Function Administration Task Flow

Administer LSC certificates on an ongoing basis once the CAPF is configured andcLSC certificates are issued.

Procedure

	Command or Action	Purpose
Step 1	LSC Generation through CAPF	Configure CAPF and add the configured authentication string on the phone. The keys and certificate exchange occurs between the phone and CAPF.
Step 2	Run Stale LSC Report	Run a Stale LSC report from Cisco Unified Reporting. Stale LSCs are certificates that were generated in response to an endpoint CSR, but were never installed because a new CSR was generated by the endpoint before the old LSC was installed.
Step 3	View Pending CSR List	View a list of pending CAPF CSR files. All CSR files are timestamped.
Step 4	Delete Stale LSC Certificates	Delete stale LSC certificates from the system.

Run Stale LSC Report

Use this procedure to run a Stale LSC report from Cisco Unified Reporting. Stale LSCs are certificates that were generated in response to an endpoint CSR, but were never installed because a new CSR was generated by the endpoint before the stale LSC was installed.

Note You can also obtain a list of stale LSC certificates by running the `utils capf stale-lsc list` CLI command on the publisher node.

Procedure

Step 1 From Cisco Unified Reporting, choose **System Reports**.

Step 2 In the left navigation bar, choose **Stale LSCs**.

Step 3 Click **Generate a new report**.

LSC Generation via CAPF

After you configure CAPF, add the configured authentication string on the phone. The keys and certificate exchange occurs between the phone and CAPF and the following occurs:

- The phone authenticates itself to CAPF using the configured authentication method.
- The phone generates its public-private key pair.
- The phone forwards its public key to CAPF in a signed message.
- The private key remains in the phone and never gets exposed externally.
- CAPF signs the phone certificate and sends the certificate to the phone in a signed message.



Note Be aware that the phone user can abort the certificate operation or view the operation status on the phone.



Note Key generation set at low priority allows the phone to function while the action occurs. Although the phone functions during certification generation, additional TLS traffic may cause minimal call-processing interruptions with the phone. For example, audio glitches may occur when the certificate is written to flash at the end of the installation

View Pending CSR List

Use this procedure to view a list of pending CAPF CSR files. All CSR files are timestamped.

Procedure

Step 1 Use the Command Line Interface to login to the publisher node.

Step 2 Run the `utils capf csr list` CLI command.
A timestamped list of pending CSR files displays.

Delete Stale LSC Certificates

Use this procedure to delete stale LSC certificates from the system.

Procedure

Step 1 Use the Command Line Interface to login to the publisher node.

Step 2 Run the `utils capf stale-lsc delete all` CLI command

The system deletes all stale LSC certificates from the system.

CAPF System Interactions

Table 16: CAPF System Interactions

Feature	Interaction
Authentication String	Enter the same authentication string on the phone after the operation in CAPF authentication method else the operation fails. The phone may fail and not recover until the matching authentication string is entered on the phone if TFTP Encrypted Configuration enterprise parameter is enabled and you fail to enter the authentication string.
Cluster Server Credentials	All servers in the Unified Communications Manager cluster must use the same administrator username and password, so CAPF can authenticate all servers in the cluster
Migrating secure phone	If a secure phone gets moved to another cluster, the Unified Communications Manager doesn't trust the LSC certificate sent by the phone because it was issued by another CAPF, whose certificate isn't in the CTL file. Delete the existing CTL file to enable the secure phone to register. You can then use the Install/Upgrade option to install a new LSC certificate with a new CAPF and reset the phone for the new CTL file (or use the MIC). Use the **Delete** option in the CAPF section on the **Phone Configuration** window to delete the existing LSC before you move the phones.
Cisco Unified IP Phones 6900, 7900, 8900, and 9900 series	We recommend upgrading Cisco Unified IP Phones 6900, 7900, 8900, and 9900 series to use LSCs for TLS connection to Unified Communications Manager and removing MIC root certificates from the Unified Communications Manager trust store to avoid possible future compatibility issues. Some phone models that use MICs for TLS connection to Unified Communications Manager may not be able to register. Administrators should remove the following MIC root certificates from the Unified Communications Manager trust store: • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048

Feature	Interaction
Power Failures	The following information applies when a communication or power failure occurs. • The phone attempts to obtain the certificate three times in 30-second intervals if a communication failure occurs while installing the certificate on the phone. You can't configure these values. • If there's a power failure while the phone attempts a session with CAPF, the phone uses authentication mode stored in flash. System clears the flash value if the phone can't load a new configuration file from the TFTP server.
Certificate Encryption	Beginning from Unified Communications Manager Release 11.5(1) SU1, SHA-256 algorithm signs all the LSC certificates issued by CAPF service. Therefore, IP Phones 7900/8900/9900 series models supports SHA-256 signed LSC certificates and external SHA2 identity certificates (Tomcat, Unified Communications Manager, CAPF, TVS, and so on). Only SHA-1 supports any other cryptographic operation that requires validation of signature. **Note** We recommend using the Unified Communications Manager before 11.5(1) SU1 release for phone models in End of Software Maintenance or End of Life,

CAPF Examples with 7942 and 7962 Phones

Consider how CAPF interacts with the Cisco Unified IP Phone 7962 and 7942 when a user or Unified Communications Manager resets the phone.

Note In the examples, CAPF certificate operation fails if LSC doesn't exist in the phone and you choose **By Existing Certificate** for the CAPF Authentication Mode.

Example-Nonsecure Device Security Mode

The phone resets after you configure the Device Security Mode to **Nonsecure** and the CAPF Authentication Mode to **By Null String** or **By Existing Certificate (Precedence)**. After the phone resets, it immediately registers with the primary Unified Communications Manager and receives the configuration file. The phone then automatically initiates a session with CAPF to download the LSC. After the phone installs the downloaded LSC, configure the Device Security Mode to Authenticated or Encrypted.

Example-Authenticated/Encrypted Device Security Mode

The phone resets after you configure the **Device Security Mode** to **Authenticated** or **Encrypted** and the CAPF Authentication Mode to **By Null String** or **By Existing Certificate (Precedence)**. The phone doesn’t register with the primary Unified Communications Manager until the CAPF session ends and the phone installs the LSC. After the session ends, the phone registers and immediately runs in authenticated or encrypted mode.

You can’t configure **By Authentication String** in this example because the phone doesn’t automatically contact the CAPF server. The registration fails if the phone doesn’t have a valid LSC.

CAPF Interaction with IPv6 Addressing

CAPF issues and upgrades certificates to a phone that uses an IPv4, an IPv6, or both types of addresses. To issue or upgrade certificates for phones running SCCP using an IPv6 address, set the **Enable IPv6** service parameter to **True** in Cisco Unified Communications Manager Administration.

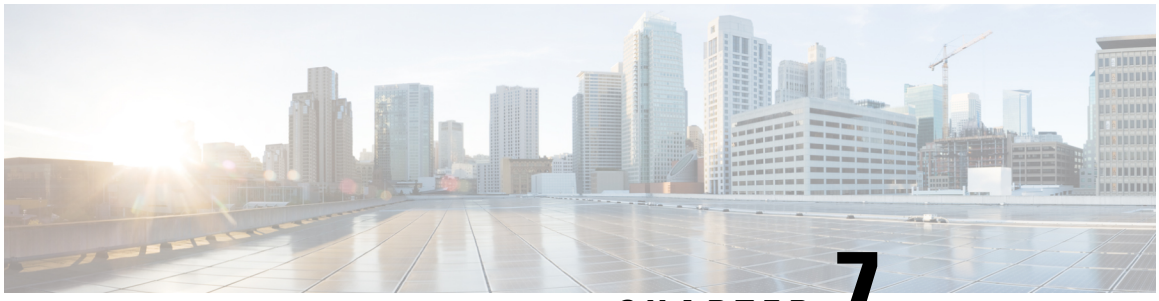
CAPF uses configurations from **Enable IPv6** enterprise parameter to issue or upgrade the certificate to the phone. If the enterprise parameter is **False**, CAPF ignores/rejects connections from phones that use IPv6 addresses, and the phone doesn't receive the certificate.

The following table describes how a phone that has an IPv4, IPv6, or both types of addresses connects to CAPF.

Table 17: How IPv6 or IPv4 Phone Connects to CAPF

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
Two stack	IPv4 and IPv6 available	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF. If the phone can't connect through an IPv6 address, it attempts to connect by using an IPv4 address.
Two stack	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
Two stack	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF. If the attempt fails, the phone uses an IPv4 address to connect to CAPF.
Two stack	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
Two stack	IPv4 and IPv6 available	IPv6	Phone uses and IPv6 address to connect to CAPF.
Two stack	IPv4 and IPv6 available	IPv4	Phone uses an IPv4 address to connect to CAPF.
Two stack	IPv4	IPv6	Phone can't connect to CAPF.
Two stack	IPv6	IPv4	Phone can't connect to CAPF.

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
Two stack	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4 stack	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
IPv6 stack	IPv6	IPv4, IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv4 stack	IPv4	IPv4	Phone uses an IPv4 address to connect to CAPF.
IPv4 stack	IPv4	IPv6	Phone can’t connect to CAPF.
IPv6 stack	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv6 stack	IPv6	IPv4	Phone can’t connect to CAPF.



CHAPTER 7

Security Modes

- Security Modes Overview , on page 91
- Non Secure Mode (Default Mode), on page 91
- Configure Secure Mode, on page 91

Security Modes Overview

To implement security mechanisms to prevent tampering of data or information, Unified Communications Manager provides the following security modes:

- Non-Secure Mode—default mode
- Secure Mode or Mixed Mode—supports secure and non-secure endpoints.
- SIP Auth Mode—uses OAuth refresh tokens for Cisco Jabber authentication in secure environments

Non Secure Mode (Default Mode)

The non secure mode is the default security mode when you install Unified Communications Manager for the first time. In this mode, Unified Communications Manager doesn't provide any secure signaling or media services.

Configure Secure Mode

To apply security, configure the security mode that applies to your deployment.

Procedure

	Command or Action	Purpose
Step 1	Mixed Mode	Enable mixed mode to add security for Cisco IP Phones and Webex devices. Provides information on how to enable and verify mixed mode.

	Command or Action	Purpose
Step 2	SIP OAuth Mode	Configure SIP OAuth Mode to add security for Cisco Jabber clients and other devices.

Mixed Mode

The mixed mode or secure mode supports secure and non-secure endpoints. When you install Unified Communications Manager fresh on a cluster or server, by default it's in non-secure mode. However, you can convert the security mode from non-secure to secure or mixed mode.

To change a cluster from a non-secure mode to a mixed mode (secure mode), perform the following:

- Enable Certificate Authority Proxy Function (CAPF) service on the publisher.
- Enable Certificate Trust List (CTL) service on the publisher.

When a Call Manager certificate is self-signed, the CTL file contains a server certificate, public key, serial number, signature, issuer name, subject name, server function, DNS name, and IP address for each server.

In the case of a Multi-SAN Call Manager certificate, the CTL file contains the Publisher's Call Manager certificate.

The next time that the phone initializes, it downloads the CTL file from the TFTP server. If the CTL file contains a TFTP server entry that has a self-signed certificate, the phone requests a signed configuration file in.sgn format. If no TFTP server contains a certificate, the phone requests an unsigned file.

You can update the CTL file running the following commands:

- **utils ctl set-cluster mixed-mode**

  Updates the CTL file and sets the cluster to mixed mode.

- **utils ctl set-cluster non-secure-mode**

  Updates the CTL file and sets the cluster to non-secure mode.

- **utils ctl update CTLFile**

  Updates the CTL file on each node in the cluster.

Note For endpoint security, Transport Layer Security (TLS) is used for signaling and Secure RTP (SRTP) is used for media.

To enable mixed mode, log in to the Command Line Interface on the publisher node and Run the CLI command `utils ctl set-cluster mixed-mode`.

Note Make sure that Unified Communications Manager is registered with the Cisco Smart Software Manager or Cisco Smart Software Manager satellite. The Registration Token received from the Smart account or Virtual account has Allow Export-Controlled functionality enabled while registering with this cluster.

For the tokenless CTL file, administrators must ensure that the endpoints download the uploaded CTL file generated using USB tokens on Unified Communications Manager Release 12.0(1) or later. After the download, they can switch to tokenless CTL file. Then, they can run the util ctl update CLI command.

You can verify the security mode, if you have changed it from non-secure to secure or mixed mode. To verify the mode, navigate to the **Enterprise Parameters Configuration** page to verify if your cluster or server is in mixed mode or not. See Verify Security Mode topic for more information.

Verify Security Mode

You can verify the security mode, if you have changed it from non-secure to secure or mixed mode. To verify the mode, navigate to the **Enterprise Parameters Configuration** page to verify if your cluster or server is in mixed mode or not.

Perform the following procedure to verify the security mode:

Procedure

Step 1 From Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**.
The **Enterprise Parameters Configuration** page appears.

Step 2 Navigate to the **Security Parameters** pane.
You'll find the **Cluster Security Mode** field with the appropriate value. If the value displays as 1, you have successfully configured Unified Communications Manager for mixed mode. You can't configure this value in Cisco Unified CM Administration page. This value displays after you have entered the CLI command `set utils cli`.

Note
The cluster security mode configures the security capability for a standalone server or a cluster.

SAST Roles of CTL File

Note *Signer, mentioned in the following table, is used to sign the CTL file.

Table 18: System Administrator Security Token (SAST) Roles of CTL File

Cisco Unified Communications Manager Version	SAST Roles in Token-based CTL File	SAST Roles in Tokenless CTL File
12.0(1)	Token 1 (Signer*) Token 2 ITLRecovery CallManager	ITLRecovery (Signer) CallManager
11.5(x)	Token 1 (Signer) Token 2 ITLRecovery CallManager	CallManager (Signer) ITLRecovery
10.5(2)	Token 1 (Signer) Token 2	CallManager (Signer) ITLRecovery
10.5(1) (Not supported)	Token 1 (Signer) Token 2	CallManager (Signer)
10.0(1) (Not supported)	Token 1 (Signer) Token 2	CallManager (Signer)
9.1(2)	Token 1 (Signer) Token 2	Not applicable

SIP OAuth Mode

SIP OAuth mode allows you to use OAuth refresh tokens for Cisco Jabber authentication in secure environments. Supporting OAuth on the Unified Communications Manager SIP line allows secure signalling and media without CAPF. OAuth token validation during SIP registration is completed when OAuth based authorization is enabled on Unified Communication Manager cluster and Cisco Jabber endpoints.

OAuth support for SIP registrations is available for Cisco Jabber devices and certain Phone models. For more information on SIP OAuth, see Feature Configuration Guide for Cisco Unified Communications Manager.

SIP OAuth Configuration Through CLI

Using CLIs, you can configure the Cluster SIP OAuth mode.

Note For more information on how to configure SIP OAuth mode on Cisco Unified Communication Manager, see *Feature Configuration Guide for Cisco Unified Communications Manager, Release 14*.

Consider the following points:

- When Cluster SIP OAuth mode is enabled, Unified Communication Manager accepts SIP registrations with an OAuth token from secure devices. Once enabled, the following TLS ports are opened which are configurable through the Unified Communications Manager user interface.
  - **SIP OAuth Port**
  - **SIP OAuth MRA Port**

  You can configure the ports from Cisco Unified CM Administration. Navigate to **System** > **Cisco Unified CM** > **CallManager**.
- Restart the Cisco CallManager service on all the nodes for the parameter change to take effect.

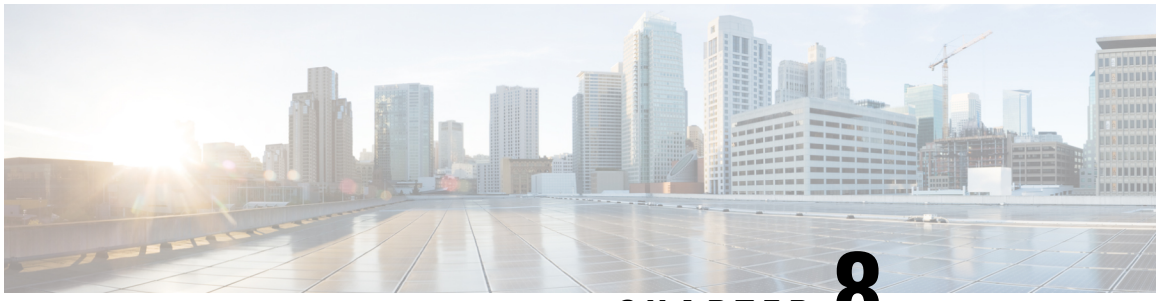
The encryption option consists of the following CLI commands:

utils sipOAuth-mode enable
Enables the SIP OAuth mode in the cluster.

utils sipOAuth-mode disable
Disables the SIP OAuth mode in the cluster.



Note Run the CLI commands only on the publisher node.



CHAPTER 8

SIP OAuth Mode

- SIP OAuth Mode Overview, on page 97
- SIP OAuth Mode Prerequisites, on page 98
- SIP OAuth Mode Configuration Task Flow, on page 99

SIP OAuth Mode Overview

Secure registrations to Unified Communications Manager involves a process of updating CTL files, setting up a mutual certificate trust store and so on. If devices are switching between on-premises and off-premises, it is difficult to update LSCs and renew Certificate Authority Proxy Function (CAPF) enrolment each time when a secure registration is completed.

SIP OAuth mode allows you to use OAuth refresh tokens for all devices authentication in secure environments. This feature enhances the security of Unified Communications Manager.

Unified Communications Manager verifies the token presented by the endpoints and serves the configuration files only to authorized ones. OAuth token validation during SIP registration is completed when OAuth based authorization is enabled on Unified Communications Manager cluster and other Cisco devices.

OAuth support for SIP registrations is extended for

- Cisco Jabber devices from Unified Communications Manager 12.5 Release onwards
- SIP Phones from Unified Communications Manager Release 14 onwards

Note By default, TFTP is secure for SIP phones when SIP OAuth is enabled. TFTP file download happens through secured channel, and only for authenticated phones. SIP OAuth provides end to end secure signaling and media encryption without CAPF on-premises as well as over MRA.

The following are the Phone Security Profile Types that can be configured for OAuth:

- Cisco Dual Mode For iPhone (TCT device)
- Cisco Dual Mode For Android (BOT device)
- Cisco Unified Client Service Framework (CSF device)
- Cisco Jabber for Tablet (TAB device)

- Universal Device Template
- Cisco 7811
- Cisco 7821
- Cisco 7832
- Cisco 7841
- Cisco 7861
- Cisco 8811
- Cisco 8832
- Cisco 8832NR
- Cisco 8841
- Cisco 8845
- Cisco 8851
- Cisco 8851NR
- Cisco 8861
- Cisco 8865
- Cisco 8865NR
- Cisco 8875
- Cisco 8875NR
- Cisco 9811
- Cisco 9841
- Cisco 9851
- Cisco 9861
- Cisco 9861NR
- Cisco 9871
- Cisco 9871NR

SIP OAuth Mode Prerequisites

This feature assumes that you have already completed the following:

- Ensure that Mobile and Remote Access is configured and the connection is established between Unified Communication Manager and Expressway. This rule isn't applicable to On-Prem SIP OAuth deployments.
- Ensure that Unified Communications Manager is registered to a Smart or Virtual account with **allow export-controlled** functionality.

- Ensure that the client firmware supports SIP OAuth.
- The phones must trust both the Tomcat and Tomcat-EC certificates for SIP OAuth to work.
- You can generate and download the self-signed Tomcat and Tomcat-EC certificates, or CA signed root certificate, and then upload this certificate as the Phone-Edge-Trust certificates on the Unified Communications Manager system. The IP Phones can accept a maximum of 16 Phone-Edge-Trust certificates. After uploading, the CA signed root certificates are placed into the caconfig.json file. For verification, you can access the URL at: `http://<cucm>:6970/caconfig.json.sgn`. Your deployment must have the following: Unified CM version 14 and above, Cisco IP Phones with SIP Firmware Release 14.0 and above, and Cisco Expressway X12.7 and above (in case of MRA deployments).

SIP OAuth Mode Configuration Task Flow

Complete the following tasks to configure SIP OAuth for your system.

Procedure

	Command or Action	Purpose
Step 1	Upload CA Certificate to the Phone Edge Trust	Upload CA Certificate to the phone edge trust to get the tokens. This step is not applicable for Cisco Jabber device.
Step 2	Enable OAuth Access Token for Devices	**Important** This step is applicable from Release 14 onwards. Enable OAuth for SIP registrations in Cisco IP Phone 7800 and 8800 enterprise series. This step is not applicable for Cisco Jabber device.
Step 3	Configure Refresh Logins, on page 101	Enable oauth with refresh login flow on Unified Communications Manager to register the device via SIP OAuth.
Step 4	Configure OAuth Ports, on page 101	Assign the ports for OAuth for each node that has OAuth registration.
Step 5	Configure OAuth Connection to Expressway-C, on page 102	Configure a mutually authenticated TLS connection to Expressway-C.
Step 6	Enable SIP OAuth Mode, on page 103	Enable OAuth services using a CLI command on the publisher node.
Step 7	Restart Cisco CallManager Service, on page 103	Restart this service on all nodes that have OAuth registrations.
Step 8	Configure Device Security Mode in Phone Security Profile	Configure OAuth support within a Phone Security Profile if you are deploying encryption for the endpoints.

	Command or Action	Purpose
Step 9	(Optional) Configure SIP OAuth Registered Phones for MRA Mode	**Important** This step is applicable from Release 14 onwards. Configure SIP OAuth registered phones in MRA mode. This step is not applicable for Cisco Jabber device.

Upload CA Certificate to the Phone Edge Trust

Use this procedure to upload the root certificate of Tomcat signed certificate to the Phone Edge Trust from the publisher node. The certificate is only visible on the publisher node.

Note This procedure is performed only for Cisco Phones and not applicable for Cisco Jabber.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate/Certificate chain**.

Step 3 In the **Upload Certificate/Certificate chain** window, from the **Certificate Purpose** drop-down list choose **Phone-Edge-Trust**.

Step 4 In the **Upload File** field, click **Browse** and upload the certificate.

Step 5 Click **Upload**.

Enable OAuth Access Token for Devices

Important This section is applicable from Release 14 onwards.

Use this procedure to enable OAuth access token for phones.

Note Configure this enterprise parameter only for OAuth support for SIP registrations for phones.

The phone certificate (MIC or LSC) must be valid for SIP OAuth to work.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 In **SSO and OAuth Configuration** section, ensure that the value of **OAuth Access Token for Devices** drop-down list is set to **Implicit:Already registered devices**.

Note
Set the value of **OAuth Access Token for Devices** to **Explicit:Activation Code device onboarding required** to disable implicitly receiving tokens for SIP OAuth registration and only support receiving tokens through activation code. The tokens can then be used for SIP OAuth registration if indicated in the security profile.

From Release 14 onwards, the default value of the enterprise parameter **OAuth Access Token for Devices** is **Implicit:Already registered devices**.

Step 3 Click **Save**.

Configure Refresh Logins

Use this procedure to configure Refresh Logins with OAuth access tokens and refresh tokens for Cisco Jabber clients.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Under **SSO and OAuth Configuration**, set the **OAuth with Refresh Login Flow** parameter to **Enabled**.

Step 3 (Optional) Set any other parameters in the **SSO and OAuth Configuration** section. For parameter descriptions, click on the parameter name.

Step 4 Click **Save**.

Configure OAuth Ports

Use this procedure to assign the ports that are used for SIP OAuth.

Procedure

Step 1 From Cisco Unified CM Administration, choose, **System** > **Cisco Unified CM**.

Step 2 Do the following for each server that uses SIP OAuth.

Step 3 Select the server.

Step 4 Under Cisco Unified Communications Manager **TCP Port Settings**, set the port values for the following fields:

- SIP Phone OAuth Port

Default value is 5090. Acceptable configurable range is 1024–49151.

- SIP Mobile and Remote Access Port

  Default value is 5091. Acceptable configurable range is 1024–49151.

Note
Cisco Unified Communications Manager uses SIP Phone OAuth Port (5090) to listen for SIP line registration from Jabber on-premises devices over TLS. However, Unified CM uses SIP Mobile Remote Access Port (default 5091) to listen for SIP line registrations from Jabber over Expressway through mTLS.

Both ports use the Cisco Tomcat certificate and Tomcat-trust for incoming TLS/mTLS connections. Make sure that your Tomcat-trust store is able to verify the Expressway-C certificate for SIP OAuth mode for Mobile and Remote Access to function accurately.

You must perform extra steps to upload the Expressway-C certificate into the Tomcat-Trust certificate store of the Cisco Unified Communications Manager, when:

- Expressway-C certificate and Cisco Tomcat certificate is not signed by the same CA certificate.
- Unified CM Cisco Tomcat certificate is not CA signed.

Step 5 Click **Save**.

Step 6 Repeat this procedure for each server that uses SIP OAuth.

Configure OAuth Connection to Expressway-C

Use this procedure to add the Expressway-C connection to Cisco Unified Communications Manager Administration. You need this configuration for devices in Mobile and Remote Access mode with SIP OAuth.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Expressway-C**.

Step 2 (Optional) In the **Find and List Expressway-C** window, click **Find** to verify X.509 Subject Name/Subject Alternate Name that is pushed from the Expressway-C to Unified Communications Manager.

Note
If required, you can modify the values. Alternatively, if the entries are missing, add Expressway-C information.

If the Expressway-C has a different domain than the Unified Communications Manager, then the administrator needs to access the Cisco Unified CM Administration User Interface and add the domain to the Expressway C in the Unified CM configuration.

Step 3 Click **Add New**.

Step 4 Enter an IP Address, Hostname or fully qualified domain name for the Expressway-C.

Step 5 Enter a Description.

Step 6 Enter the X.509 Subject Name/Subject Alternate Name of the Expressway-C from the Expressway-C certificate.

Step 7 Click **Save**.

Enable SIP OAuth Mode

Use the Command Line Interface to enable SIP OAuth mode. Enabling this feature on the publisher node also enables the feature on all cluster nodes.

Before you begin

From Release 14SU1 onwards, when Proxy TFTP is enabled, you should copy the root CA certificate for the off-cluster Tomcat certificate to the proxy phone edge trust.

Procedure

Step 1 On the Unified Communications Manager publisher node, log in to the Command Line Interface.

Step 2 Run the `utils sipOAuth-mode enable` CLI command.
From Release 14 onwards, the system updates the read-only **Cluster SIPOAuth Mode** enterprise parameter to **Enabled**.

Restart Cisco CallManager Service

After enabling SIP OAuth through CLI, restart the Cisco CallManager service on all nodes where endpoints register through SIP OAuth.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Control Center** > **Feature Services**.

Step 2 From the **Server** drop-down list, select the server.

Step 3 Check the **Cisco CallManager** service and click **Restart**.

Configure Device Security Mode in Phone Security Profile

Use this procedure to configure the device security mode in the phone security profile and is required only if you have set the **Device Security Mode** within that phone's **Phone Security Profile** to **Encrypted**.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 2 Perform either of the following:

- Search for an existing phone security profile
- Click **Add New**

Step 3 In the Phone Security Profile Information section, from the **Device Security Mode** drop-down list, choose **Encrypted**.

Step 4 From the **Transport Type** drop-down list, choose **TLS**.

Step 5 Check the **Enable OAuth Authentication** check box.

Step 6 Click **Save**.

Step 7 Associate the Phone Security Profile to the phone. For more information on how to apply the phone security phones, see "Apply Security Profiles to Phone" section in Security Guide for Cisco Unified Communications Manager.

Note
Reset your phone for the changes to take effect.

Note
When SIP OAuth Mode is enabled, **Enable Digest Authentication** and **TFTP Encrypted Config** options are not supported. Phones will download the TFTP config file securely over **https(6971)** and use the token for authentication.

Configure SIP Oauth Registered Phones for MRA Mode

Use this procedure to configure SIP OAuth registered phones to MRA mode.

Before you begin

Important This section is applicable from Release 14 onwards.

Make sure your phones are configured to use Activation Codes. For more information see *Set Registration Method to use Activation Codes* section in System Configuration Guide for Cisco Unified Communications Manager.

Note When using SIP OAuth over MRA , user cannot use username / password for login but have to use activation code based onboarding

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Click **Find** and select the device which you want to configure for off-premises mode.

Step 3 In the **Device Information** section, do the following:

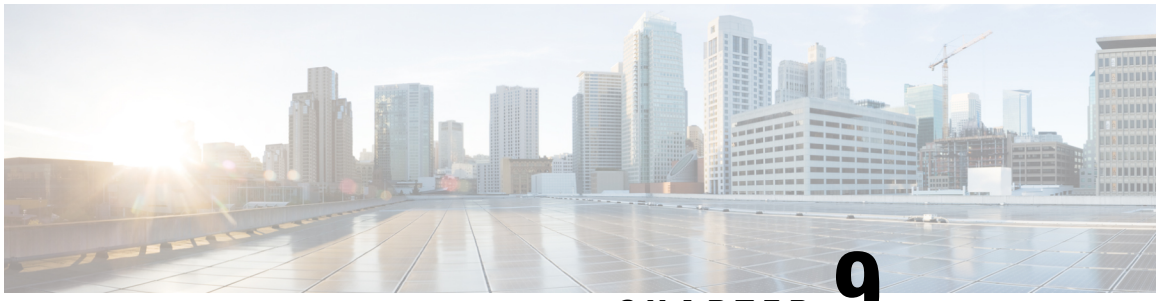
- Check **Allow Activation Code via MRA** check box.
- From the **Activation Code MRA Service Domain** drop-down list, choose the required MRA service domain. For more information on how to configure the MRA service domain see, the *MRA Service Domain Configuration* section in System Configuration Guide for Cisco Unified Communications Manager.

Note
For SIP OAuth over MRA mode, use only activation code and do not use username/password based login.

Step 4 In the **Protocol Specific Information** section, choose the OAuth enabled SIP profile from the **Device Security Profile** drop-down list. Make sure that the phone supports OAuth firmware. For more information, on how to create a security profile, see *Configure Phone Security Profile* section in System Configuration Guide for Cisco Unified Communications Manager.

Step 5 Click **Save** and **Apply Configuration**.

Note
The phone switches to MRA mode and initiates communication with the Expressway. If your internal network does not allow communication with Expressway from on-premises, the phone doesn't register but is ready to contact Expressway when it's powered up off-premises.



CHAPTER 9

TFTP Encryption

- TFTP Encrypted Configuration Files Overview, on page 107
- Encryption for Phone Configuration File Task Flow, on page 109
- Disable TFTP Encrypted Configuration Files, on page 112

TFTP Encrypted Configuration Files Overview

TFTP configuration protects your data during device registration by encrypting the configuration file that the phone downloads from the TFTP server during the registration process. This file contains confidential information such as usernames, passwords, IP addresses, port details, phone SSH credentials, and so on. If this feature is not configured, the configuration file is sent in cleartext. Deploying this feature ensures that an attacker cannot intercept this information during the registration process. This information is unencrypted and sent in cleartext. Hence, we recommend that you encrypt the TFTP configuration file in order to protect your data.

Warning If you have enabled the digest authentication option for SIP phones and disabled the TFTP encrypted configuration option, the digest credentials are sent in the cleartext.

After TFTP configuration, the TFTP server:

- Deletes all the cleartext configuration files on disk
- Generates encrypted versions of the configuration files

If the phone supports encrypted phone configuration files and you have performed the tasks for phone configuration file encryption, the phone requests an encrypted version of the configuration file.

Some phones don't support encrypted phone configuration files. The phone model and protocol determine the method that the system uses to encrypt the configuration file. Supported methods rely on Unified Communications Manager functionality and a firmware load that supports encrypted configuration files. If you downgrade the phone firmware load to a version that doesn't support encrypted configuration files, the TFTP server offers an unencrypted configuration file that provides minimal configuration settings, and the phone may not perform as expected.

Encryption Key Distribution

To ensure that you maintain the privacy of the key information, we recommend that you perform the tasks that are associated with encrypted phone configuration files in a secure environment.

Unified Communications Manager supports the following methods:

- Manual key distribution.
- Symmetric key encryption with a phone public key.

The setup information provided for manual key distribution and symmetric key encryption with a phone public key assume that you have enabled the **TFTP Encrypted Config** option in the Cisco Unified CM Administration user interface.

TFTP Encrypted Configuration Files Tips

We recommend that you enable the TFTP Encrypted Configuration file to secure confidential data in phone downloads. For phones that don't have PKI capabilities, you must also configure a symmetric key in Unified Communications Manager Administration and in the phone. If the symmetric key is missing from either the phone or Unified Communications Manager or if a mismatch occurs when the TFTP Encrypted Configuration file is set, the phone can't register.

Consider the following information when you configure encrypted configuration files in Unified Communications Manager:

- Only phones that support encrypted configuration files display the **TFTP Encrypted Config** check box in the **Phone Security Profile Configuration** page. You can't configure encrypted configuration files for Cisco Unified IP Phones 7800, 7942, and 7962 (SCCP only) because these phones don't receive confidential data in the configuration file download.
- By default, the **TFTP Encrypted Config** check box is unchecked. If you apply this default setting, the non secure profile to the phone, the digest credentials, and secured passwords are sent in the cleartext.
- For Cisco Unified IP Phones that use Public Key Encryption, Unified Communications Manager does not require you to set the Device Security Mode to Authenticated or Encrypted to enable encrypted configuration files. Unified Communications Manager uses the CAPF process for downloading its Public key during registration.
- You may choose to download the unencrypted configuration files to the phones if you know that your environment is secure or to avoid manually configuring symmetric keys for phones that are not PKI-enabled. However, we don't recommend that you use this method.
- For Cisco Unified IP Phones 7800, 7942, and 7962 (SIP only), Unified Communications Manager provides a method of sending digest credentials to the phone that is easier, but less secure, than using an encrypted configuration file. This method, which uses the Exclude Digest Credential in Configuration File setting, is useful for initializing digest credentials because it doesn't require you to first configure a symmetric key and enter it on the phone. With this method, you send the digest credentials to the phone in an unencrypted configuration file. After the credentials are in the phone, we recommend that you disable the **TFTP Encrypted Config** option and then enable the **Exclude Digest Credential in Configuration File** on the **Phone Security Profile Configuration** page. This will exclude digest credentials from future downloads.
- After digest credentials exist in these phones and an incoming file doesn't contain digest credentials, the existing credentials remain in place. The digest credentials remain intact until the phone is factory reset or new credentials (including blanks) are received. If you change digest credentials for a phone or end

user, temporarily disable the **Exclude Digest Credential in Configuration File** on the corresponding **Phone Security Profile Information** page to download the new digest credentials to the phone.

Encryption for Phone Configuration File Task Flow

To set up encryption for TFTP configuration files, verify that the phones in your cluster support manual key encryption and public key encryption, verify that the phones support SHA-1 and SHA-512, and complete the following tasks.



Note If you enable SHA-512 clusterwide, and your phones don't support it, those phones do not work.

Procedure

	Command or Action	Purpose
Step 1	Enable TFTP Encryption, on page 109	Enable the TFTP Configuration File option for your phones. You can enable this option in the Phone Security Profile.
Step 2	Configure SHA-512 Signing Algorithm, on page 110	When TFTP file encryption is enabled, SHA-1 is configured by default as the signing algorithm. Use this procedure to update the system to use the stronger SHA-512 algorithm.
Step 3	Verify LSC or MIC Certificate Installation, on page 110	For phones that use public keys, verify the certificate installation.
Step 4	Update CTL File, on page 111	After you complete your TFTP config file updates, regenerate the CTL file.
Step 5	Restart Services, on page 111	Restart the Cisco CallManager and Cisco TFTP services.
Step 6	Reset Phones, on page 112	After you complete your encrypted TFTP config file updates, reset your phones.

Enable TFTP Encryption

You can enable this TFTP within the phone security profile for a given phone model. Perform this procedure to enable TFTP encryption for files downloaded from the TFTP server.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 2 Click **Find** and choose a phone security profile.

Step 3 Check the **TFTP Encrypted Config** check box.

Step 4 Click **Save**.

Step 5 Repeat these steps for any other phone security profiles that are used in the cluster.

Note
To disable encryption for the phone configuration files, you must uncheck the **TFTP Encrypted Config** check box in the phone security profile in Cisco Unified Communications Manager Administration and then save your change.

Configure SHA-512 Signing Algorithm

SHA-1 is the default algorithm for TFTP file signing. You can use the below optional procedure to upgrade the system to use the stronger SHA-512 algorithm for TFTP configuration files such as digital signatures.



Note Make sure that your phones support SHA-512. If not, the phones don't work after you update your system.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Go to the **Security Parameters** pane.

Step 3 From the **TFTP File Signature Algorithm** drop-down list, choose **SHA-512**.

Step 4 Click **Save**.

Restart the affected services listed in the pop-up window to complete the procedure.

Verify LSC or MIC Certificate Installation

For phones that use public keys, verify the certificate installation.



Note This procedure applies to Cisco Unified IP Phones that uses PKI encryption. To determine, if your phone supports PKI encryption, see Phone Models Supporting Encrypted Configuration File section.

The following procedure assumes that the phone exists in Unified Communications Manager database and you have enabled the TFTP Encrypted Config parameter in Unified Communications Manager.

Procedure

Step 1 Verify that a Manufacture-Installed Certificate (MIC) or a Locally Significant Certificate (LSC) exists in the phone.

Step 2 From Cisco Unified CM Administration, choose **Device > Phone**.
The lists of phones appear.

Step 3 Click the **Device Name**.
The **Phone Configuration** page appears.

Tip
Choose the **Troubleshoot** option in the CAPF settings section from the **Phone Configuration** page, to verify whether an LSC or MIC exists in the phone in Unified Communications Manager. The Delete and Troubleshoot options don't appear when a certificate doesn't exist in the phone.

Tip
You can also verify that an LSC or MIC exists in the phone by checking the security configuration on the phone. For more information, see the administration guides for Cisco Unified IP Phones that support this version of Unified Communications Manager.

Step 4 If a certificate doesn't exist, install an LSC by using the CAPF functionality on the **Phone Configuration** window. For information on how to install an LSC, see topics related to the Certificate Authority Proxy Function.

Step 5 Click **Save** after you configure the CAPF settings.

Step 6 Click **Reset**.
The phone requests an encrypted configuration file from the TFTP server after the phone resets.

Update CTL File

Update the CTL file, when you have done any modifications to Unified Communications Manager. Since you have enabled the TFTP file encryption, you have to regenerate the CTL file.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 On the publisher node, run the **utils ctl update CTLfile** command.

Restart Services

After you have completed your encrypted TFTP configuration file updates, make sure that you restart your Cisco TFTP and Cisco CallManager services for the changes to take effect.

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Control Center – Feature Services**.

Step 2 Choose the following two services.

- Cisco CallManager
- Cisco TFTP

Step 3 Click **Restart**. However, after regenerating or updating CallManager certificate, you don't have to manually restart TFTP service.

Reset Phones

Make sure that you reset your phones after you complete all your encrypted TFTP configuration file updates.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phones**.

Step 2 Click **Find**.

Step 3 Click **Select All**.

Step 4 Click **Reset Selected**.

Disable TFTP Encrypted Configuration Files

Warning If digest authentication is **True** for the phone that is running SIP when the TFTP encrypted configuration setting is **False**, digest credentials may get sent in the clear.

After you update the setting, the encryption keys for the phone remain in the Unified Communications Managerdatabase.

Cisco Unified IP Phones 7911G, 7931G (SCCP only), 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7971G, 7971G-GE, and 7975G request an encrypted file (.enc.sgn file) when the encrypted configuration setting gets updated to **False**, the phone requests an unencrypted, signed file (.sgn file).

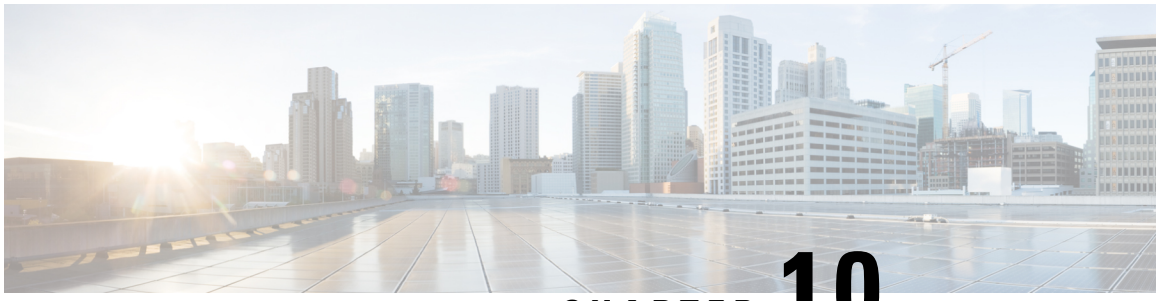
If Cisco Unified IP Phones are running on SCCP and SIP, request an encrypted file when the encryption configuration setting gets updated to **False**. Remove the symmetric key from the phone GUI so that the phone requests an unencrypted configuration file the next time that it is reset.

- Cisco Unified IP Phones running on SCCP: 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7921G, 7925G, 7925G-EX, 7926G, 7931G, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7971G, 7971G-GE, 7975G, 8941, 8945.

- Cisco Unified IP Phones running on SIP: 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7941G, 7941G-GE, 7942G, 7961G, 7961G-GE,7962G, 7965G, 7970G, 7971G, 7971G-GE, 7975G, 8941, 8945, 8961, 9971, 7811, 78321, 7841, 7861, 7832, 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NE, 8821, 8831, 8832, 8832NR.

Procedure

	Command or Action	Purpose
Step 1	To disable encryption for the phone configuration files, Uncheck **TFTP Encrypted Config** check box in the phone security profile associated to the phone.	
Step 2	For Cisco Unified IP Phones 7942 and 7962 (SIP only), Enter a 32-byte 0 as the key value for the symmetric key at the phone screen to disable encryption.	
Step 3	For Cisco Unified IP Phones (SIP only), delete the symmetric key at the phone screen to disable encryption.	For information on how to perform these tasks, see the phone administration guide that supports your phone model.



CHAPTER 10

Cipher Management

- Cipher Management, on page 115
- Configure Cipher String, on page 117
- Cipher Limitations, on page 120
- Cipher Restrictions, on page 128

Cipher Management

Cipher management is an optional feature that enables you to control the set of security ciphers that is allowed for every TLS and SSH connection. Cipher management allows you to disable weaker ciphers and thus enable a minimum level of security.

The **Cipher Management** page has no default values. Instead, the Cipher Management feature takes effect only when you configure the allowed ciphers. Certain weak ciphers are never allowed, even if they are configured on the **Cipher Management** page.

You can configure ciphers on the following TLS and SSH interfaces:

- **All TLS**—The ciphers that are assigned in this field are applicable to all server and client connections that support the TLS protocol on Unified Communications Manager and IM and Presence Service.
- **HTTPS TLS**—The ciphers that are assigned in this field are applicable to all Cisco Tomcat connections on ports 443 and 8443 that support the TLS protocol on Unified Communications Manager and IM and Presence Service.

Note If you assign ciphers on **HTTPS TLS** and **All TLS** fields, the ciphers that are configured on **HTTPS TLS** override **All TLS** ciphers.

- **SIP TLS**—The ciphers that are assigned in this field are applicable to all encrypted connections to or from the SIP TLS interfaces that support the TLS protocol on Unified Communications Manager. It is not applicable for SCCP or CTI devices.

  SIP interface in authenticated mode only supports NULL-SHA ciphers.

  If you configure ciphers in the SIP interface or All interface, authenticated mode is no longer supported.

  If you assign ciphers in **SIP TLS** and **All TLS** fields, then the ciphers you configured on SIP TLS override the All TLS ciphers.

- **SSH Ciphers**—The ciphers that are assigned in this field are applicable to SSH connections on Unified Communications Manager and IM and Presence Service.
- **SSH Key Exchange**—The Key Exchange algorithms that are assigned in this field are applicable to the SSH interface on Unified Communications Manager and IM and Presence Service.

Curve Negotiation

Following are the points for negotiating the curves:

- ECDSA ciphers are negotiated with different EC curves based on the key size of the ECDSA certificate.
- The RSA ciphers are negotiated with all the EC curves irrespective of key size of the certificate.
- The key size of a ECDSA certificate must be same as the curve size for the TLS negotiation to happen.

Example:

The 384 key certificate and ECDSA ciphers are negotiated, when the client offers P-384 EC curve.

Curve negotiation is based on the client preference for both RSA and ECDSA ciphers.

When the certificate size is 384 bits and client offerings are P-521, P-384, P-256 EC curves then TLS negotiation happen with the P-521 curve. Since curve offered by the client is P-521 at the first and P- 384 curve is also available on the list. When the certificate size is 384 bits and client offerings are P-521, P-256 EC curves then TLS negotiation will not happen because the P-384 curve is not offered by the client.

The following are the supported ciphers for EC curves:

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```

Recommended Ciphers

By default, Unified Communications Manager and IM and Presence Service already uses a set of ciphers (see TLS and SSH Ciphers section below) that supports secure integration with most other products, including third-party products. Therefore, it is not required to make changes. If Cipher suite mismatches are causing TLS Handshake failures, Unified Communications Manager Cipher Management can be used to add additional ciphers to the list of supported Ciphers.

Cipher Management can also be used if customers want to be more restrictive and prevent certain Cipher suites from being negotiated during TLS handshake. After configuring the ciphers, restart the affected services or reboot the server for the changes to take effect.

Warning Configuring hmac-sha2-512 in the SSH MAC interface affects the DRS and CDR functionality.

Configuring ciphers aes128-gcm@openssh.com, aes256-gcm@openssh.com in "SSH Cipher's" field or configuring only ecdh-sha2-nistp256 algorithm in "SSH KEX" will break the DRS and CDR functionalities.

CDR, AXL, DRS, and Bulk Certificate Exchange interfaces use the rsa-sha2-256 hostkey algorithm, even when rsa-sha2-512 is configured.

We support the following cipher strings for the TLS and SSH interface configuration:

TLS

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:
ECDHE-RSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA
```

SSH Ciphers

```
aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,
aes256-gcm@openssh.com
```

SSH MAC

```
hmac-sha2-512,hmac-sha2-256,hmac-sha1
```

SSH KEX

```
ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256,
diffie-hellman-group14-sha1, diffie-hellman-group16-sha512, diffie-hellman-group14-sha256
```

Configure Cipher String

- Make sure you enter the cipher string in OpenSSL cipher string format in **All TLS**, **SIP TLS**, and **HTTPS TLS** fields.
- Make sure that you also enter the ciphers or algorithms in OpenSSH format in **SSH Ciphers**,algorithms in **SSH MAC**, and **SSH Key Exchange** fields.
- Review Recommended Ciphers, on page 116.

To configure the cipher string on different secure interfaces, see the Cipher Restrictions section.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Cipher Management**.
The Cipher Management page appears.

Step 2 To configure the cipher string in **All TLS**, **SIP TLS**, or **HTTPS TLS** field, enter the cipher string in OpenSSL cipher string format in the **Cipher String** field.

Step 3 If you don't configure the cipher string in the following fields:

- **All TLS or HTTPS TLS** field—the HTTPS TLS interface port (8443) takes configuration from the **Enterprise parameters** (HTTPS ciphers) page.
- **All TLS or SIP TLS** field—the SIP interface port (5061) takes configuration from the **Enterprise parameters** (TLS ciphers) page in encrypted mode and NULL-SHA ciphers in authenticated mode.

Note
If you don't configure the cipher string in the **HTTPS TLS** or **SIP TLS** field, the system takes the configuration from the **All TLS** field by default.

For more information about OpenSSL cipher string format, see https://www.openssl.org/docs/man1.0.2/apps/ciphers.html.

Step 4 To configure the cipher string in the **SSH Ciphers** field, enter the cipher string in OpenSSH cipher string format in the **Cipher String** field.

For more information about OpenSSH cipher string format for SSH Ciphers, see https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.html.

If you don't configure any cipher string in the **SSH Ciphers** field, the following ciphers are applicable to all SSH connections by default:

In FIPS mode:

```
aes128-ctr, aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-gcm@openssh.com
```

In non-FIPS mode:

```
aes128-ctr, aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-gcm@openssh.com
```

Step 5 To configure the key exchange algorithm in the **SSH Key Exchange** field, enter the algorithm string in OpenSSH string format in the **Algorithm String** field.

For more information about OpenSSH algorithm string format for SSH Key Exchange, see the https://datatracker.ietf.org/doc/rfc9142/.

If you don't configure any key exchange algorithm in the **SSH Key Exchange** field, the following key exchange algorithms are applicable to all SSH connections by default:

In FIPS mode:

```
diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,
ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

In non-FIPS mode:

```
diffie-hellman-group1-sha1, diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,
ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

Step 6 To configure MAC algorithm in the **SSH MAC** field, enter the algorithm string in OpenSSH string format in the **Algorithm String** field.

For more information about OpenSSH algorithm string format for SSH MAC, see https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.html.

If you don't configure any MAC algorithm in the **SSH MAC** field, the following MAC algorithms are applicable to all SSH connections by default:

In FIPS mode:

```
hmac-sha1
```

In non-FIPS mode:

```
hmac-sha1
```

Step 7 Click **Save**.

Note
You can't edit **Cipher Expansion String** and **Algorithm Expansion String** fields.

The system validates the ciphers in the **All TLS**, **SIP TLS**, **HTTPS TLS** , and **SSH Ciphers** fields and auto populates ciphers in the **Cipher Expansion String** field.

If you enter invalid ciphers in the **Cipher String** field, the **Cipher Expansion String** field doesn't auto populate and the following error message appears:

```
You have entered an invalid Cipher String.
```

The system validates the algorithms in the **SSH Key Exchange** and **SSH MAC** fields, and auto populates the algorithms in the **Algorithm Expansion String** field.

If you enter invalid algorithms in the **Algorithm String** field, the **Algorithm Expansion String** field doesn't auto populate and the following error messge appears:

```
You have entered an invalid Algorithm String.
```

Note
The ciphers or algorithms auto populated in **Cipher Expansion String** and **Algorithm Expansion String** fields are not the effective ciphers or algorithms. The system chooses the ciphers or algorithms from the **Cipher Expansion String** or **Algorithm Expansion String** field.

If you have configured ciphers in the corresponding fields, you have to either reboot or restart the respective services.

Table 19: Configured Ciphers and their corresponding Actions

Configured Cipher Fields	Action
All TLS	Reboot all nodes in the cluster for the cipher string to take effect.
HTTPS TLS	Restart the Cisco Tomcat service on all nodes for the cipher string to take effect.
SIP TLS	Restart Unified Communications Manager on all nodes for the cipher string to take effect.

Configured Cipher Fields	Action
SSH Ciphers	Reboot all nodes in the cluster for the cipher string to take effect.
SSH Key Exchange or **SSH MAC**	Reboot all nodes in the cluster for the algorithm string to take effect.

Note You can enable ciphers by entering them in the **Cipher String** fields of the **Cipher Management** page. If you don't enter them, all default ciphers supported by the application are enabled. However, you can also disable certain weak ciphers by not entering them in the **Cipher String** fields of the **Cipher Management** page.

Cipher Limitations

Although the **Cipher Management** configuration page allows you to configure any number of ciphers, each application has a list of ciphers it supports on its interfaces. For example, **All TLS** interfaces may show ECDHE or DHE or ECDSA-based ciphers, but an application such as Unified Communications Manager may not support these ciphers because EC curves or DHE algorithms are not enabled for this application's interfaces. For more information, see the "Application Ciphers Support" section for a list of ciphers supported by individual application interfaces.

Note If you are upgrading a cluster with ciphers configured in the Cipher Management page, ensure that you configure at least one common cipher between ALL and HTTPS fields.

Note Cisco Cloud Onboarding is not part of the Cipher Management suite and will use all the default ciphers that are supported in the server. However, this limitation has been fixed from 12.5(1) SU6 release onwards.

Note If any of the nodes have been disconnected from a cluster and you want to configure the ciphers, ensure that you update the ciphers on both the publisher node and the disconnected node.

Alternatively, you can configure the ciphers again on the publisher node after the cluster is reestablished to synchronize all nodes with the same cipher configuration.

Validation in GUI

The ciphers on **Cipher Management** page are validated according to the OpenSSL guidelines. For example, if a cipher configured is ALL:BAD:!MD5, the cipher string will be considered as valid even though "BAD" is not a recognized cipher suite. OpenSSL considers this as a valid string. If AES128_SHA is configured

instead of AES128-SHA (using an underscore instead of a hyphen) however, OpenSSL identifies this as an invalid cipher suite.

Authenticated Mode (NULL Ciphers)

If NULL ciphers are in use by an application interface, you can revoke the support for NULL ciphers by configuring any cipher list in **All TLS** or **SIP TLS** fields on **Cipher Management** page.

Examples of application interfaces that use NULL ciphers are:

- **All TLS Interface:** Unified Communications Manager SIP Proxy in IM and Presence through the **TLS Context Configuration** page.
- **SIP TLS Interface:** Unified Communications Manager through SIP or SCCP, when any **Device Security Profile** is set to **Authenticated** mode.

Don't configure ciphers for either of these two interfaces if NULL ciphers must be used.

Override Functionality

The settings on the **Cipher Management** page overrides the default settings for each application and any other location where ciphers have been configured. This means that if no ciphers are configured on the **Cipher Management** page, then the original functionality on all interfaces will be retained.

For example, if the **Enterprise Parameter** "**TLS Ciphers**" is configured with "*ALL Supported Ciphers*" and the **Cipher Management** page is configured with ciphers "*AES256-GCM-SHA384:AES256-SHA256*" on **All TLS** interfaces, all application SIP interfaces will support only the "*AES256-GCM-SHA384:AES256-SHA256*" ciphers and ignores the **Enterprise Parameter** value.

Application Ciphers Support

The following table lists the application interfaces and the all corresponding ciphers and algorithms that are supported on TLS and SSH interfaces.

Table 20: Unified Communications Manager Cipher Support for TLS Ciphers

Application / Process	Protocol	Port	Supported Ciphers
Cisco CallManager	TCP / TLS	2443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: ECDHE-RSA-AES256-SHA:

Application / Process	Protocol	Port	Supported Ciphers
DRS	TCP / TLS	4040	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:
Cisco Tomcat	TCP / TLS	8443 / 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA:
Cisco CallManager	TCP / TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:
Cisco Certificate Authority Proxy Function	TCP / TLS	3804	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA

Application / Process	Protocol	Port	Supported Ciphers
CTIManager	TCP / TLS	2749	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:
Cisco Trust Verification Service	TCP / TLS	2445	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES128-SHA256
Cisco Intercluster Lookup Service	TCP / TLS	7501	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:
Secure Configuration download (HAPROXY)	TCP / TLS	6971, 6972	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA:
Authenticated Contact Search	TCP / TLS	9443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA:

Table 21: Unified Communications Manager IM & Presence Cipher Support for TLS Ciphers

Application / Process	Protocol	Port	Supported Ciphers
Cisco SIP Proxy	TCP / TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:
Cisco SIP Proxy	TCP / TLS	5062	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:
Cisco SIP Proxy	TCP / TLS	8083	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:

Application / Process	Protocol	Port	Supported Ciphers
Cisco Tomcat	TCP / TLS	8443, 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA:
Cisco XCP XMPP Federation Connection Manager	TCP /TLS	5269	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:
Cisco XCP Client Connection Manager	TCP / TLS	5222	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:

Table 22: Cipher Support for SSH Ciphers

Service	Ciphers/Algorithms

SSH Server	• Ciphers
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	`aes128-gcm@openssh.com`
	`aes256-gcm@openssh.com`
	• MAC algorithms:
	`hmac-sha2-256`
	`hmac-sha2-512`
	`hmac-sha1`
	• Kex algorithms:
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`ecdh-sha2-nistp256`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group14-sha256`
	`diffie-hellman-group16-sha512`
	• Host Key algorithms in non-FIPS mode:
	`rsa-sha2-256`
	`rsa-sha2-512`
	`ssh-rsa`
	• Host Key algorithms in FIPS mode:
	`rsa-sha2-256`
	`rsa-sha2-512`

Service	Ciphers/Algorithms

SSH Client	• Ciphers:
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	`aes128-gcm@openssh.com`
	`aes256-gcm@openssh.com`
	• MAC algorithms:
	`hmac-sha2-256`
	`hmac-sha2-512`
	`hmac-sha1`
	• Kex algorithms:
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`ecdh-sha2-nistp256`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group14-sha256`
	`diffie-hellman-group16-sha512`
	• Host Key algorithms in non-FIPS mode:
	`rsa-sha2-256`
	`rsa-sha2-512`
	`ssh-rsa`
	• Host Key algorithms in FIPS mode:
	`rsa-sha2-256`
	`rsa-sha2-512`

DRS Client	• Ciphers:
	`aes256-ctr`
	`aes128-ctr`
	`aes192-ctr`
	• MAC algorithms:
	`hmac-sha2-256`
	`hmac-sha1`
	• Kex algorithms:
	`ecdh-sha2-nistp256`
	`ecdh-sha2-nistp384`
	`ecdh-sha2-nistp521`
	`diffie-hellman-group14-sha1`
	Note
	The Kex algorithms diffie-hellman-group-exchange-sha256, diffie-hellman-group-exchange-sha1, and diffie-hellman-group1-sha1 are not supported from Release 12.5(1)SU4 if you have configured Cipher Management functionality in your Unified CM server. If the ciphers are not configured, DRS Client uses these algorithms.

Service	Ciphers/Algorithms

SFTP client	• Ciphers:
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	• MAC algorithms:
	`hmac-sha2-256`
	`hmac-sha1`
	• Kex algorithms:
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group1-sha1`
	`diffie-hellman-group-exchange-sha256`
	`diffie-hellman-group-exchange-sha1`

End Users	`hmac-sha512` `SHA-512 – Hashing (salted)`
DRS Backups / RTMT SFTPs	`AES-128 – Encryption`
Application Users	`AES-256 – Encryption`

Cipher Restrictions

The **Cipher Management** page allows configuration of ciphers supported by OpenSSL or OpenSSH. However, some of the ciphers are disabled internally based on Cisco's security standards to avoid accidental exposure of critical data.

When you configure ciphers on the **Cipher Management** page, the following ciphers are essentially disabled.

TLS Disabled Ciphers

```
EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:ADH-DES-CBC-SHA:
DES-CBC-SHA:KRB5-DES-CBC-SHA:KRB5-DES-CBC-MD5:EXP-EDH-RSA-DES-CBC-SHA:
EXP-EDH-DSS-DES-CBC-SHA:EXP-ADH-DES-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:
EXP-KRB5-RC2-CBC-SHA:EXP-KRB5-DES-CBC-SHA:EXP-KRB5-RC2-CBC-MD5:EXP-KRB5-DES-CBC-MD5:
EXP-ADH-RC4-MD5:EXP-RC4-MD5:EXP-KRB5-RC4-SHA:EXP-KRB5-RC4-MD5:ADH-AES256-GCM-SHA384:
ADH-AES256-SHA256:ADH-AES256-SHA:ADH-CAMELLIA256-SHA:ADH-AES128-GCM-SHA256:ADH-AES128-SHA256:
ADH-AES128-SHA:ADH-SEED-SHA:ADH-CAMELLIA128-SHA:ADH-DES-CBC3-SHA:ADH-RC4-MD5:
AECDH-AES256-SHA:AECDH-AES128-SHA:AECDH-DES-CBC3-SHA:AECDH-RC4-SHA:AECDH-NULL-SHA:
DES-CBC3-MD5:IDEA-CBC-MD5:RC2-CBC-MD5:RC4-MD5:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:
ECDH-RSA-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:PSK-RC4-SHA:KRB5-RC4-SHA:
KRB5-RC4-MD5:IDEA-CBC-SHA:KRB5-IDEA-CBC-SHA:KRB5-IDEA-CBC-MD5:DHE-RSA-SEED-SHA:
DHE-DSS-SEED-SHA:SEED-SHA:KRB5-DES-CBC3-MD5:NULL-MD5:PSK-AES256-CBC-SHA:
PSK-AES128-CBC-SHA:PSK-3DES-EDE-CBC-SHA:ECDHE-RSA-NULL-SHA:ECDHE-ECDSA-NULL-SHA:
ECDH-RSA-NULL-SHA:ECDH-ECDSA-NULL-SHA:NULL-SHA256:NULL-SHA
```

SSH Disabled Ciphers

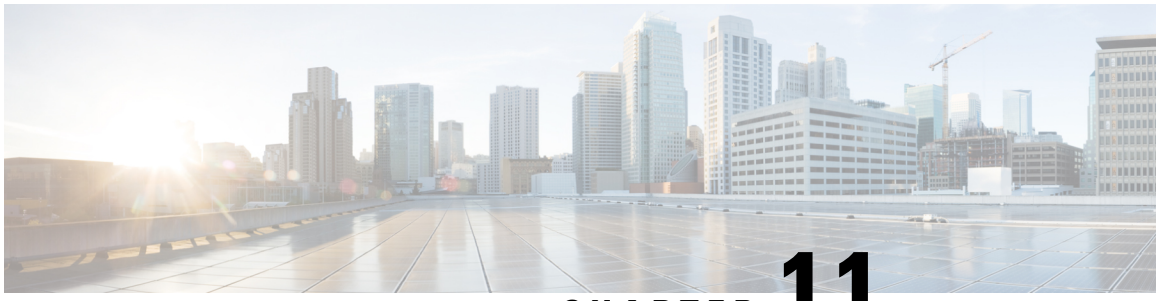
```
3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
```

SSH Disabled KEX Algorithms

```
curve25519-sha256@libssh.org,gss-gex-sha1-,gss-group1-sha1-,gss-group14-sha1-
```

SSH Disabled MAC Algorithms

```
hmac-sha1-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```



CHAPTER 11

Phone Security

- Phone Security Overview, on page 131
- Phone Security Profiles, on page 141
- Digest Authentication for SIP Phones Overview, on page 155

Phone Security Overview

At installation, Unified Communications Manager boots up in nonsecure mode. When the phones boot up after the Unified Communications Manager installation, all devices register as nonsecure with Unified Communications Manager.

After you upgrade from Unified Communications Manager 4.0(1) or a later release, the phones boot up in the device security mode that you enabled prior to the upgrade; all devices register by using the chosen security mode.

The Unified Communications Manager installation creates a self-signed certificate on the Unified Communications Manager and TFTP server. You may also choose to use a third-party, CA-signed certificate for Unified Communications Manager instead of the self-signed certificate. After you configure authentication, Unified Communications Manager uses the certificate to authenticate with supported Cisco Unified IP Phones. After a certificate exists on the Unified Communications Manager and TFTP server, Unified Communications Manager does not reissue the certificates during each Unified Communications Manager upgrade. You must update the ctl file using CLI command **util ctl update CTLFile** with the new certificate entries.

Tip For information on unsupported or nonsecure scenarios, see topics related to interactions and restrictions.

Unified Communications Manager maintains the authentication and encryption status at the device level. If all devices that are involved in the call register as secure, the call status registers as secure. If one device registers as nonsecure, the call registers as nonsecure, even if the phone of the caller or recipient registers as secure.

Unified Communications Manager retains the authentication and encryption status of the device when a user uses Cisco Extension Mobility. Unified Communications Manager also retains the authentication and encryption status of the device when shared lines are configured.

Tip When you configure a shared line for an encrypted Cisco IP Phone, configure all devices that share the lines for encryption; that is, ensure that you set the device security mode for all devices to encrypted by applying a security profile that supports encryption.

Phone Hardening Overview

This section provides an overview of the phone hardening behaviours like Gratuitous ARP Disable, Web Access Disable, PC Voice VLAN Access Disable, Setting Access Disable and PC Port Disable and so on.

The following optional settings are used to harden the connection to Cisco IP Phones. These settings appear in the Product-Specific Configuration Layout of the **Phone Configuration** window.

To apply them to a set of phones, or all phones enterprise-wide, these settings also appear in the **Common Phone Profile Configuration** window and the **Enterprise Phone Configuration** window.

Table 23: Phone Hardening Behaviour

Phone Hardening Behaviour	Description	
Gratuitous ARP Disable	By default, Cisco Unified IP Phones accept Gratuitous ARP packets. Gratuitous ARP packets, which devices use, announce the presence of the device on the network. However, attackers can use these packets to spoof a valid network device; for example, an attacker could send out a packet that claims to be the default router. If you choose to do so, you can disable Gratuitous ARP in the **Phone Configuration** window. **Note** Disabling this functionality does not prevent the phone from identifying its default router.	

Phone Hardening Behaviour	Description	
Web Access Disable	Disabling the web server functionality for the phone blocks access to the phone internal web pages, which provide statistics and configuration information. Features, such as CiscoQuality Report Tool, do not function properly without access to the phone web pages. Disabling the web server also affects any serviceability application, such as CiscoWorks, that relies on web access. To determine whether the web services are disabled, the phone parses a parameter in the configuration file that indicates whether the services are disabled or enabled. If the web services are disabled, the phone does not open the HTTP port 80 for monitoring purposes and blocks access to the phone internal web pages.	
PC Voice VLAN Access Disable	By default, Cisco IP Phones forward all packets that are received on the switch port (the one that faces the upstream switch) to the PC port. If you choose to disable the PC Voice VLAN Access setting in the Phone Configuration window, packets that are received from the PC port that use voice VLAN functionality will drop. Various Cisco IP Phones use this functionality differently. • Cisco Unified IP Phones 7942 and 7962 drop any packets that are tagged with the voice VLAN, in or out of the PC port. • Cisco Unified IP Phone 7970G drops any packet that contains an 802.1Q tag on any VLAN, in or out of the PC port.	

Phone Hardening Behaviour	Description	
Setting Access Disable	By default, pressing the Applications button on a Cisco IP Phone provides access to a variety of information, including phone configuration information. Disabling the Setting Access parameter in the Phone Configuration window prohibits access to all options that normally display when you press the Applications button on the phone; for example, the Contrast, Ring Type, Network Configuration, Model Information, and Status settings. The preceding settings do not display on the phone if you disable the setting in Unified Communications Manager Administration. If you disable this setting, the phone user cannot save the settings that are associated with the Volume button; for example, the user cannot save the volume. Disabling this setting automatically saves the current Contrast, Ring Type, Network Configuration, Model Information, Status, and Volume settings that exist on the phone. To change these phone settings, you must enable the Setting Access setting in Unified Communications Manager Administration.	

Phone Hardening Behaviour	Description	
PC Port Disable	By default, Unified Communications Manager enables the PC port on all Cisco IP Phones that have a PC port. If you choose to do so, you can disable the PC Port setting in the Phone Configuration window. Disabling the PC port proves useful for lobby or conference room phones. **Note** The PC port is available on some phones and allows the user to connect their computer to the phone. This connection method means that the user only needs one LAN port.	

Set Up Phone Hardening

Phone Hardening consists of optional settings that you can apply to your phones in order to harden the connection. You can apply settings using one of three configuration windows:

- Phone Configuration - use **Phone Configuration** window to apply the settings to an individual phone
- Common Phone Profile - use the **Common Phone Profile** window to apply the settings to all of the phones that use this profile
- Enterprise Phone - use the **Enterprise Phone** window to apply the settings to all of your phones enterprise wide

Note If conflicting settings appear in each of these windows, following is the priority order the phone uses to determine the correct setting: 1) Phone Configuration, 2) Common Phone Profile, 3)Enterprise Phone

To setup phone hardening, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Specify the criteria to find the phone and click **Find** to display a list of all phones.

Step 3 Click the device name.

Step 4 Locate the following product-specific parameters:

a) PC Port
b) Settings Access

c) Gratuitous ARP
d) PC Voice VLAN Access
e) Web Access

Tip
To review information on these settings, click the help icon that appears next to the parameters in the **Phone Configuration** window.

Step 5 Choose **Disabled** from the drop-down list for each parameter that you want to disable. To disable the speakerphone or speakerphone and headset, check the corresponding check boxes.

Step 6 Click **Save**.

Step 7 Click **Reset**.

Trusted Devices

Unified Communications Manager allows Security icons to be enabled by phone model on Cisco IP Phones. The Security icon indicates whether the call is secure and the connected device is trusted.

A Trusted Device represents a Cisco device or a third-party device that has passed Cisco security criteria for trusted connections. This includes, but is not limited to, signaling/media encryption, platform hardening, and assurance. If a device is trusted, a Security icon displays and a secure tone plays on supported devices. Also, the device may provide other features or indicators that are related to secure calls.

Unified Communications Manager determines whether a device is trusted when you add it to your system. The security icon displays for information purposes only, and the administrator cannot configure it directly.

Unified Communications Manager also indicates whether a gateway is trusted by displaying an icon and a message in Unified Communications Manager Administration.

This section describes the behavior of the security icon for trusted devices on both the Cisco IP Phones and in Unified Communications Manager Administration.

Cisco Unified Communications Manager Administration

The following windows in Unified Communications Manager Administration indicate whether a device is trusted:

Gateway Configuration

For each gateway type, the Gateway Configuration window (**Device** > **Gateway**) displays either **Device is trusted** or **Device is not trusted**, along with a corresponding icon.

The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.

Phone Configuration

For each phone device type, the Phone Configuration window (**Device** > **Phone**) displays either **Device is trusted** or **Device is not trusted**, along with a corresponding icon.

The system determines whether the device is trusted, based on the device type. You cannot configure whether the device is trusted.

Device Called Trust Determination Criteria

The type of device that a user calls affects the security icon that displays on the phone. The system considers the following three criteria to determine whether the call is secure:

- Are all devices on the call trusted?
- Is the signaling secure (authenticated and encrypted)?
- Is the media secure?

Before a supported Cisco Unified IP Phone displays the Lock Security icon, be aware that all three of these criteria must be met. For calls that involve a device that is not trusted, regardless of signaling and media security, the overall status of the call will stay unsecure, and the phone will not display the Lock icon. For example, if you include an untrusted device in a conference, the system considers its call leg, as well as the conference itself, to be unsecure.

Phone Model Support

There are two categories of phone models which support security in Unified Communications Manager: Secure Cisco phones and Secure Preferred Vendor phones. Secure Cisco phones are pre-installed with a Manufacture-Installed Certificate (MIC) and support automatic generation and exchange of Locally-Significant Certificates (LSC) using the Certificate Authority Proxy Function (CAPF). Secure Cisco phones are capable of registering with Cisco Unified CM using the MIC without additional certificate management. For additional security, you can create and install an LSC on the phone using CAPF. See topics related to phone security setup and settings for more information.

Secure Preferred Vendor phones do not come pre-installed with a MIC, and do not support CAPF for generating LSCs. In order for Secure Preferred Vendor phones to connect to Cisco Unified CM, a certificate must be provided with the device, or generated by the device. The phone supplier must provide the details on how to acquire or generate a certificate for the phone. Once you obtain the certificate, you must upload the certificate to the Cisco Unified CM using the OS Administration Certificate Management interface. See topics related to preferred vendor SIP phone security set up for more information.

For a list of security features that are supported on your phone, refer to the phone administration and user documentation that supports this Unified Communications Manager release or the firmware documentation that supports your firmware load.

You can also use Cisco Unified Reporting to list the phones that support a particular feature. For more information about using Cisco Unified Reporting, see the Cisco Unified Reporting Administration Guide.

View Phone Security Settings

You can configure and view certain security-related settings on phones that support security; for example, you can view whether a phone has a locally significant certificate or manufacture-installed certificate installed. For additional information on the security menu and icons, refer to the *Cisco IP Phone Administration Guide* and *Cisco IP Phone User Guide* that supports your phone model.

When Unified Communications Manager classifies a call as authenticated or encrypted, an icon is displayed on the phone and indicates the call state. It also determines when Unified Communications Manager classifies the call as authenticated or encrypted.

Set Up Phone Security

The following procedure describes the tasks to configure security for supported phones.

Procedure

Step 1 If you have not already done so, execute the **utils ctl** CLI command and ensure that the Unified Communications Manager security mode equals Mixed Mode.

Step 2 If the phone does not contain a locally significant certificate (LSC) or manufacture-installed certificate (MIC), install a LSC by using the Certificate Authority Proxy Function (CAPF).

Step 3 Configure phone security profiles.

Step 4 Apply a phone security profile to the phone.

Step 5 After you configure digest credentials, choose the Digest User from the Phone Configuration window.

Step 6 On Cisco Unified IP Phone 7962 or 7942 (SIP only), enter the digest authentication username and password (digest credentials) that you configured in the End User Configuration window.

Note
This document does not provide procedures on how to enter the digest authentication credentials on the phone. For information on how to perform this task, see Administration Guide for Cisco Unified Communications Manager that supports your phone model and this version of Unified Communications Manager.

Make sure to run the **utils ctl** CLI command set after you upload a third-party CA-signed certificate to the platform to update the CTL file.

Step 7 Encrypt the phone configuration file, if the phone supports this functionality.

Step 8 To harden the phone, disable phone settings.

Preferred Vendor SIP Phone Security Set Up

Secure Preferred Vendor phones are phone types that are manufactured by third-party vendors but are installed in the Cisco Unified database via a COP file. Unified Communications Manager provides security for a preferred vendor SIP phone. In order to support security, you must enable Security Encryption or Security Authentication for the preferred vendor SIP phone in the COP file. These phone types appear in the drop-down list in the Add a New Phone window. While all preferred vendor phones support Digest Authorization, not all preferred vendor phones support TLS security. Security capabilities is based on the phone model. If the Phone Security Profile includes a “Device Security Mode” field, then it supports TLS security.

If the preferred vendor phone supports TLS security, there are two modes that are possible: per-device certificate and shared certificate. The phone supplier must specify which mode is applicable for the phone as well as instructions on generating or acquiring a certificate for the phone.

Set Up Preferred Vendor SIP Phone Security Profile Per-Device Certificates

To configure the preferred vendor SIP phone security profile with per-device certificates, perform the following procedure:

Procedure

Step 1 Upload the certificate for each phone using the OS Administration Certificate Management interface.

Step 2 In the Cisco Unified Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 3 Configure a new Phone Security Profile for the device type of this phone and in the **Device Security Mode** drop-down list, choose **Encrypted** or **Authenticated**.

Step 4 To configure the new SIP phone in the CCMAdmin interface, choose **Device** > **Phone** > **Add New**.

Step 5 Select Phone type.

Step 6 Fill in the required fields.

Step 7 In the **Device Security Profile** drop-down list, select the profile you just created.

Set Up Preferred Vendor SIP Phone Security Profile Shared Certificates

To configure the preferred vendor SIP phone security profile with shared certificates, perform the following procedure:

Procedure

Step 1 Using instructions from the phone vendor, generate a certificate with a Subject Alternate Name (SAN) string. The SAN must be of type DNS. Make a note of the SAN specified in this step. For example, X509v3 extensions:

- X509v3 Subject Alternative Name
- DNS:AscomGroup01.acme.com

Note
The SAN must be of type DNS or security will not be enabled.

Step 2 Upload the shared certificate using the OS Administration Certificate Management interface.

Step 3 In the Cisco Unified Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 4 In the **Name** field, enter the name of the Subject Alt Name (SAN), which is the name on the certificate provided by the preferred vendor, or if there is no SAN enter the Certificate Name.

Note
The name of the security profile must match the SAN in the certificate exactly or security will not be enabled.

Step 5 In the **Device Security Mode** drop-down list, choose **Encrypted** or **Authenticated**.

Step 6 In the Transport type drop-down list, choose **TLS**.

Step 7 To configure the new SIP phone in the CCMAdmin interface, choose **Device** > **Phone** > **Add New**.

Step 8 Select Phone type.

Step 9 Fill in the required fields

Step 10 In the **Device Security Profile** drop-down list, select the profile you just created.

Migrate Phones from One Cluster to Another Cluster

Use the following procedure to migrate phones from one cluster to another. For example, from cluster 1 to cluster 2.

Procedure

Step 1 On cluster 2, from Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Find**.

Step 3 From the list of Certificates, click the ITLRecovery certificate and click either **Download .PEM File** or **Download .DER File** to download the certificate in one of the file formats to your computer.
The details of certificate appear.

Step 4 From the list of Certificates, click the CallManager certificate and click either **Download .PEM File** or **Download .DER File** to download the certificate in one of the file formats to your computer.
The details of certificate appear.

Step 5 On cluster 1, from Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 6 Click **Upload Certificate Chain** to upload the downloaded certificate.

Step 7 From the **Certificate Purpose** drop-down list, choose **Phone-SAST-trust**.

Step 8 For the **Upload File** field, click **Choose File**, browse to the ITLRecovery file that you downloaded in Step 3, and then click **Upload File**.

The uploaded ITLRecovery file appears for the **Phone-SAST-Trust** certificate on **Certificate List** window of cluster 1. If the new ITL file has a ITLRecovery certificate for cluster 2, run the command `show itl`.

Step 9 If the phones in cluster 1 have Locally Significant Certificates (LSC), then the CAPF certificate from cluster 1 has to be uploaded in the CAPF-trust store of cluster 2.

Step 10 (Optional) This step is applicable only if the cluster is in mixed mode. Run the **utils ctl update CTLFile** command on the CLI to regenerate the CTL file on cluster 1.

Note

- Run the `show ctl` CLI command to ensure that the ITLRecovery certificate and CallManager certificate of cluster 2 are included in the CTL file with the role as SAST.
- Ensure that the phones have received the new CTL and ITL files. The updated CTL file has the ITLRecovery certificate of cluster 2.

The phones that you want to migrate from cluster 1 to cluster 2 will now accept the ITLRecovery certificate of cluster 2.

Step 11 Migrate the phone from one cluster to another.

Phone Security Interactions and Restrictions

This section provides the interaction and restriction on Phone Security.

Table 24: Phone Security Interactions and Restrictions

Feature	Interaction and Restriction
Certificate Encryption	Beginning from Unified Communications Manager Release 11.5(1) SU1, all the LSC certificates issued by CAPF service are signed with SHA-256 algorithm. Therefore, Cisco Unified IP Phone 7900 Series, 8900 Series, and 9900 Series supports SHA-256 signed LSC certificates and external SHA2 identity certificates (Tomcat, CallManager, CAPF, TVS, and so on). For any other cryptographic operation that require validation of signature, only SHA-1 is supported. **Note** If you use phone models which are in End of Software Maintenance or End of Life, we strongly recommend using the Unified Communications Manager before 11.5(1)SU1 release.

Phone Security Profiles

Unified Communications Manager, groups the security-related settings for phone type and protocol into security profiles. Hence, you can assign this single security profile to multiple phones. The security-related settings include device security mode, digest authentication, and some of the CAPF settings. Installing Unified Communications Manager provides a set of predefined, non-secure security profiles for auto-registration.

You can apply the configured settings to a phone by choosing the security profile in the **Phone Configuration** window. To enable security features for a phone, you must configure a new security profile for the device type and protocol, and then apply that profile to the phone. Only the security features that the selected device and protocol support are displayed in the **security profile settings** window.

Prerequisites

Consider the following information before you configure the phone security profiles:

- When you configure phones, choose a security profile in the **Phone Configuration** window. If the device does not support security or a secure profile, apply a non-secure profile.
- You cannot delete or change the predefined non-secure profiles.
- You cannot delete a security profile that is currently assigned to a device.
- If you change the settings in a security profile that is already assigned to a phone, the re-configured settings apply to all phones that are assigned that particular profile.
- You can rename security files that are assigned to devices. The phones that are assigned with the earlier profile name and settings assume the new profile name and settings.
- The CAPF settings, the authentication mode and the key size, are displayed in the **Phone Configuration** window. You must configure CAPF settings for certificate operations that involve MICs or LSCs. You can update these fields directly in the **Phone Configuration** window.
- If you update the CAPF settings in the security profile, the settings are also updated in the **Phone Configuration** window.
- If you update the CAPF settings in the Phone Configuration window and a matching profile is found, Unified Communications Manager applies the matching profile to the phone.

- If you update the CAPF settings in the Phone Configuration window, and no matching profiles are found, Unified Communications Manager creates a new profile and applies that profile to the phone.
- If you have configured the device security mode earlier to an upgrade, Unified Communications Manager creates a profile that is based on that model and protocol and applies the profile to the device.
- We recommend that you use MICs for LSC installation only. Cisco support LSCs to authenticate the TLS connection with Unified Communications Manager. Since MIC root certificates can be compromised, users who configure phones to use MICs for TLS authentication or for any other purpose do so at their own risk. Cisco assumes no liability if MICs are compromised.
- We recommend that you upgrade Cisco IP Phones to use LSCs for TLS connections and remove the MIC root certificates from the CallManager trust store to avoid compatibility issues.

Phone Security Profile Settings

The following table describes the settings for the security profile for the phone that is running SCCP.

Only settings that the selected phone type and protocol support display.

Table 25: Security Profile for Phone That Is Running SCCP

Setting	Description
Name	Enter a name for the security profile. When you save the new profile, the name displays in the **Device Security Profile** drop-down list in the **Phone Configuration window** for the phone type and protocol. **Tip** Include the device model and protocol in the security profile name to find the correct profile while searching for a profile or updating a profile.
Description	Enter a description for the security profile. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Setting	Description
Device Security Mode	

Setting	Description
	From the drop-down list, choose one of the following options: • **Non Secure**—No security features except image, file, and device authentication exist for the phone. A TCP connection opens to Unified Communications Manager. • **Authenticated**—Unified Communications Manager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens for signaling. • **Encrypted**—Unified Communications Manager provides integrity, authentication, and signalling encryption for the trunk. The following are the supported ciphers: **TLS Ciphers** This parameter defines the ciphers that are supported by the Unified Communications Manager for establishing SIP TLS and inbound CTI Manager TLS connections. Strongest- AES-256 SHA-384 only: RSA Preferred • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` **Note** It is recommended that the value of the parameter 'SRTP Ciphers' be set to the value 'Strongest - AEAD AES-256 GCM cipher only'. With this option chosen, the phones will not register on authenticated mode. Strongest- AES-256 SHA-384 only: ECDSA Preferred • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` Medium- AES-256 AES-128 only: RSA Preferred **Note** It is recommended that the value of the parameter 'SRTP Ciphers' be set to the value 'Strongest - AEAD AES-256 GCM cipher only'. With this option chosen, the phones will not register on authenticated mode. • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES128_GCM_SHA256` • `TLS_ECDHE_ECDSA with AES128_GCM_SHA256` **Note** It is recommended that the value of the parameter 'SRTP Ciphers' be set to the value 'Medium - AEAD AES-256,AES-128 GCM ciphers only'. With this option chosen, the phones will not register on authenticated mode. Medium- AES-256 AES-128 only: ECDSA Preferred

Setting	Description
	• TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256 **Note** It is recommended that the value of the parameter 'SRTP Ciphers' be set to the value 'Medium - AEAD AES-256,AES-128 GCM ciphers only'. With this option chosen, the phones will not register on authenticated mode. All Ciphers, RSA Preferred: • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES128_GCM_SHA256 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_RSA with AES_128_CBC_SHA1 All Ciphers, ECDSA Preferred: • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256 • TLS_RSA with AES_128_CBC_SHA1 **Note** If the trunks are configured with Device Security Profile option selected as Authenticated, then Unified Communications Manager starts a TLS connection that uses NULL_SHA cipher (without data encryption). These trunks will not register or make calls if the destination devices do not support NULL_SHA cipher. For destination devices that do not support NULL_SHA cipher, the trunks should be configured with Device Security Profile option selected as Encrypted. With this device security profile, the trunks offer additional TLS ciphers that enables data encryption.
TFTP Encrypted Config	When this check box is checked, Unified Communications Manager encrypts a phone downloads from the TFTP server.

Setting	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. From the drop-down list box, choose one of the following options: • **By Authentication String**—Installs or upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • **By Null String**—Installs or upgrades, deletes, or troubleshoots a locally significant certificate without the user intervention. This option provides no security. We recommend that you choose this option only for closed, secure environments. • **By Existing Certificate (Precedence to LSC)**—Installs or upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If an LSC exists in the phone, authentication occurs through the LSC, regardless whether a MIC exists in the phone. If a MIC and an LSC exist in the phone, authentication occurs through the LSC. If an LSC does not exist in the phone, but a MIC exists, authentication occurs through the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF although a MIC and an LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate through the other certificate, you must update the authentication mode. • **By Existing Certificate (Precedence to MIC)**—Installs or upgrades, deletes, or troubleshoots a locally significant certificate if an LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs through the MIC, regardless whether an LSC exists in the phone. If an LSC exists in the phone, but a MIC does not exist, authentication occurs through the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. **Note** The CAPF settings that are configured in the **Phone Security Profile** window interact with the CAPF parameters that are configured in the **Phone Configuration** window.

Setting	Description
Key Order	This field specifies the sequence of the key for CAPF. Select one of the following values from the drop-down list: • **RSA Only** • **EC Only** • **EC Preferred, RSA Backup** **Note** When you add a phone, that is based on the value in **Key Order**, **RSA Key Size**, and **EC Key Size** fields, the device security profile is associated with the phone. If you select the **EC Only** value, with the **EC Key Size** value of 256 bits, then the device security profile appends with **EC-256** value.
RSA Key Size (Bits)	From the drop-down list box, choose one of the values—**512**, **1024**, **2048, 3072**, or **4096**. **Note** Some phone models may fail to register if the RSA **key length** that is selected for the CallManager **Certificate Purpose** is greater than 2048. From the *Unified CM Phone Feature List Report* on the *Cisco Unified Reporting Tool (CURT)*, you can check the 3072/4096 RSA key size support feature for the list of supported phone models.
EC Key Size (Bits)	From the drop-down list, choose one of the values—**256**, **384**, or **521**.

The following table describes the settings for the security profile for the phone that is running SIP.

Table 26: Security Profile for Phone That Is Running SIP

Setting	Description
Name	Enter a name for the security profile. When you save the new profile, the name displays in the **Device Security Profile** drop-down list in the **Phone Configuration** window for the phone type and protocol. **Tip** Include the device model and protocol in the security profile name to help you find the correct profile when you are searching for or updating a profile.
Description	Enter a description for the security profile.
Nonce Validity Time	Enter the number of minutes (in seconds) that the nonce value is valid. The default value equals 600 (10 minutes). When the time expires, Unified Communications Manager generates a new value. **Note** A nonce value, a random number that supports digest authentication, gets used to calculate the MD5 hash of the digest authentication password.

Setting	Description
Device Security Mode	From the drop-down list, choose one of the following options: • **Non Secure**—No security features except image, file, and device authentication exist for the phone. A TCP connection opens to Unified Communications Manager. • **Authenticated**—Unified Communications Manager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens for signaling. • **Encrypted**—Unified Communications Manager provides integrity, authentication, and encryption for the phone. A TLS connection that uses AES128/SHA opens for signaling, and SRTP carries the media for all phone calls on all SRTP-capable hops. **Note** If the trunks are configured with Device Security Profile option selected as Authenticated, then Unified Communications Manager starts a TLS connection that uses NULL_SHA cipher (without data encryption). These trunks will not register or make calls if the destination devices do not support NULL_SHA cipher. For destination devices that do not support NULL_SHA cipher, the trunks should be configured with Device Security Profile option selected as Encrypted. With this device security profile, the trunks offer additional TLS ciphers that enables data encryption.
Transport Type	When Device Security Mode is **Non Secure**, choose one of the following options from the drop-down list (some options may not display): • **TCP**—Choose the Transmission Control Protocol to ensure that packets get received in the same order as the order in which they are sent. This protocol ensures that no packets get dropped, but the protocol does not provide any security. • **UDP**—Choose the User Datagram Protocol to ensure that packets are received quickly. This protocol, which can drop packets, does not ensure that packets are received in the order in which they are sent. This protocol does not provide any security. • **TCP + UDP**—Choose this option if you want to use a combination of TCP and UDP. This option does not provide any security. When Device Security Mode is **Authenticated** or **Encrypted**, TLS specifies the Transport Type. TLS provides signaling integrity, device authentication, and signaling encryption (encrypted mode only) for SIP phones. If Device Security Mode cannot be configured in the profile, the transport type specifies UDP.

Setting	Description
Enable Digest Authentication	If you check this check box, Unified Communications Manager challenges all SIP requests from the phone. Digest authentication does not provide a device authentication, integrity, or confidentiality. Choose a security mode of authenticated or encrypted to use these features.
TFTP Encrypted Config	When this check box is checked, Unified Communications Manager encrypts the phone downloads from the TFTP server. This option exists for Cisco phones only. **Tip** We recommend that you enable this option and configure a symmetric key to secure digest credentials and administrative passwords.
Enable OAuth Authentication	This check box is available, when you choose **Encrypted** from the **Device Security Profile** drop-down list. When this check box is checked, Unified Communications Manager allows the device that is associated with the phone security profile to register on the SIP OAuth port. By default, this check box is unchecked. You can enable the SIP OAuth when: • Transport type is TLS. • Device security mode is encrypted. • Digest authentication is disabled. • Encrypted configuration is disabled. **Note** From Unified Communications Manager Release 12.5, Jabber devices support SIP OAuth authentication.
Exclude Digest Credentials in Configuration File	When this check box is checked, Unified Communications Manager omits digest credentials in the phone downloads from the TFTP server. This option exists for Cisco IP Phones, 7942, and 7962 (SIP only).

Setting	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. This option exists for Cisco phones only. From the drop-down list, choose one of the following options: • **By Authentication String**—Installs or upgrades or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • **By Null String**—Installs or upgrades or troubleshoots a locally significant certificate without the user intervention. This option provides no security; we recommend that you choose this option only for closed, secure environments. • **By Existing Certificate (Precedence to LSC)**—Installs or upgrades or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If an LSC exists in the phone, authentication occurs through the LSC, regardless whether a MIC exists in the phone. If an LSC does not exist in the phone, but a MIC does exist, authentication occurs through the MIC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. At any time, the phone uses only one certificate to authenticate to CAPF although a MIC and an LSC can exist in the phone at the same time. If the primary certificate, which takes precedence, becomes compromised for any reason, or, if you want to authenticate through the other certificate, you must update the authentication mode. • **By Existing Certificate (Precedence to MIC)**—Installs or upgrades or troubleshoots a locally significant certificate if an LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs through the MIC, regardless whether an LSC exists in the phone. If an LSC exists in the phone, but a MIC does not exist, authentication occurs through the LSC. Before you choose this option, verify that a certificate exists in the phone. If you choose this option and no certificate exists in the phone, the operation fails. **Note** The CAPF settings that are configured in the **Phone Security Profile** window interact with the CAPF parameters that are configured in the **Phone Configuration** window.

Setting	Description
Key Size	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list. The default setting equals 1024. The other option for key size is 512. If you choose a higher key size than the default setting, the phones take longer to generate the entropy that is required to generate the keys. Key generation, which is set at low priority, allows the phone to function while the action occurs. Depending on the phone model, you may notice that key generation takes up to 30 or more minutes to complete. **Note** The CAPF settings that are configured in the **Phone Security Profile** window interact with the CAPF parameters that are configured in the **Phone Configuration** window.
SIP Phone Port	This setting applies to phones that are running SIP that uses UDP transport. Enter the port number for Cisco Unified IP Phone (SIP only) that use UDP to listen for SIP messages from Unified Communications Manager. The default setting equals 5060. Phones that use TCP or TLS ignore this setting.

Phone Security Configuration Task Flow

Perform the following tasks to configure phone security:

Procedure

	Command or Action	Purpose
Step 1	(Optional) Find Phone Security Profile, on page 152	Search for the phone security profile to secure a phone.
Step 2	Set up Phone Security Profile	Set up the phone security profile to secure a phone.
Step 3	Apply Phone Security Profile	Apply the phone security profile to secure a phone.
Step 4	Synchronize Phone Security Profile with Phones	Synchronize all the phone security profiles with selected phones.
Step 5	(Optional) Delete Phone Security Profile	Delete all the phone security profiles associated to a phone.
Step 6	Find Phones with Phone Security Profiles	Find all phones associated with phone security profiles.
Step 7	SIP Trunk Security Profile Interactions and Restrictions	SIP trunk security profile interations and restrictions

Find Phone Security Profile

To find a phone security profile, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System** > **Security Profile** > **Phone Security Profile**.

Records from an active (prior) query may also display in the window.

Step 2 To find all records in the database, ensure the dialog box is empty; go to Step 3, on page 152.

To filter or search records

a) From the first drop-down list, choose a search parameter.
b) From the second drop-down list, choose a search pattern.
c) Specify the appropriate search text, if applicable.

Note
To add additional search criteria, click the + button. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click the – button to remove the last added criterion or click **Clear Filter** to remove all added search criteria.

Step 3 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the Rows per Page drop-down list.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note
To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the record that you choose.

Set Up Phone Security Profile

To setup a phone security profile, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System > Security Profile > Phone Security Profile**.

Step 2 Perform one of the following tasks:

a) To add a new profile, click **Add New**.
b) To copy an existing security profile, locate the appropriate profile, click **Copy** next to the security profile that you want to copy, and continue.

c) To update an existing profile, locate the appropriate security profile and continue.

When you click **Add New**, the configuration window displays with the default settings for each field. When you click **Copy**, the configuration window displays the copied settings.

Step 3 Enter appropriate settings for phones that are running SCCP or SIP.

Step 4 Click **Save**.

Apply Security Profiles to Phone

Before you apply a security profile that uses certificates for authentication of the phone, make sure that the particular phone contains a Locally Significant Certificate (LSC) or Manufacture-Installed Certificate (MIC).

To enable security features for a phone, you must configure a new security profile for the device type and protocol and apply it to the phone. However, if the phone does not contain a certificate, perform the following tasks:

- In the **Phone Configuration** window, apply a non-secure profile.
- In the **Phone Configuration** window, install a certificate by configuring the CAPF settings.
- In the **Phone Configuration** window, apply a device security profile that is configured for authentication or encryption.

To apply a phone security profile to a device, perform the following procedure:

Procedure

Step 1 Go to the **Protocol Specific Information** section in the **Phone Configuration** window.

Step 2 From the **Device Security Profile** drop-down list, choose the security profile that applies to the device. The phone security profile that is configured only for the phone type and the protocol is displayed.

Step 3 Click **Save**.

Step 4 To apply the changes to the applicable phone, click **Apply Config**.

Note
To delete security profiles, check the check boxes next to the appropriate security profile in the **Find and List** window, and click **Delete Selected**.

Synchronize Phone Security Profile with Phones

To synchronize phone security profile with phones, perform the following procedure:

Procedure

Step 1 From Unified Communications Manager Administration, choose **System** > **Security Profile** > **Phone Security Profile**.

Step 2 Choose the search criteria to use and click **Find**.
The window displays a list of phone security profiles that match the search criteria.

Step 3 Click the phone security profile to which you want to synchronize the applicable phones.

Step 4 Make any additional configuration changes.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.
The **Apply Configuration Information** dialog box appears.

Step 7 Click **OK**.

Delete Phone Security Profile

Before you can delete a security profile from Unified Communications Manager, you must apply a different profile to the devices or delete all devices that use the profile.

To find out which devices use the profile, perform Step 1:

Procedure

Step 1 In the **Security Profile Configuration** window, choose **Dependency Records** from the **Related Links** drop-down list and click **Go**.

If the dependency records feature is not enabled for the system, go to **System** > **Enterprise Parameters Configuration** and change the Enable Dependency Records setting to **True**. A message displays information about high CPU consumption that relates to the dependency records feature. Save your change to activate dependency records. For more information about dependency records, see System Configuration Guide for Cisco Unified Communications Manager

This section describes how to delete a phone security profile from the Unified Communications Manager database.

Step 2 Find the security profile to delete.

Step 3 To delete multiple security profiles, check the check boxes next to the appropriate check box in the **Find and List** window; then, click **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

Step 4 To delete a single security profile, perform one of the following tasks:

a) In the **Find and List** window, check the check box next to the appropriate security profile; then, click **Delete Selected**.

Step 5 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Find Phones with Phone Security Profiles

To find the phones that use a specific security profile, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 From the first drop-down list, choose the search parameter **Security Profile**.

a) From the drop-down list, choose a search pattern.
b) Specify the appropriate search text, if applicable.

Note
To add additional search criteria, click +. When you add criteria, the system searches for a record that matches all criteria that you specify. To remove criteria, click – to remove the last added criterion or click **Clear Filter** to remove all added search criteria.

Step 3 Click **Find**.

All matching records display. You can change the number of items that display on each page by choosing a different value from the **Rows per Page** drop-down list.

Step 4 From the list of records that display, click the link for the record that you want to view.

Note
To reverse the sort order, click the up or down arrow, if available, in the list header.

The window displays the record that you choose.

SIP Trunk Security Profile Interactions and Restrictions

The following table contains feature interactions and restrictions for SIP Trunk Security Profiles.

Table 27: SIP Trunk Security Profile Interactions and Restrictions

Feature	Interactions and Restrictions
90-day Evaluation License	You cannot deploy a secure SIP trunk while running with a 90-day evaluation period. To deploy a secure SIP trunk, your system must have registered to a Smart Software Manager account with the **Allow export-controlled functionality** product registration token selected.

Digest Authentication for SIP Phones Overview

Digest authentication allows Unified Communications Manager to challenge request messages for phones that are running SIP. This includes all request messages with the exception of keepalives. Unified Communications Manager authenticates through digest credentials the end user, as configured in the **End User Configuration** window, to validate the credentials that the phone offers.

If the phone supports Extension Mobility, Unified Communications Manager uses the digest credentials for the Extension Mobility end user, as configured in the **End User Configuration** window, when the Extension Mobility user logs in.

Digest Authentication for SIP Phones Prerequisite

If you enable digest authentication for a device, the device requires a unique digest user ID and password to register. You must configure SIP digest credentials in the Unified Communications Manager database for a phone user or an application user.

Make sure that you do the following:

- For applications, specify digest credentials in the Application User Configuration window.
- For phones that are running SIP, specify the digest authentication credentials in the End User Configuration window.

  To associate the credentials with the phone after you configure the user, choose a Digest User, in the Phone Configuration window. After you reset the phone, the credentials exist in the phone configuration file that the TFTP server offers to the phone.
- For challenges received on SIP trunks, configure a SIP realm, which specifies the realm username (device or application user) and digest credentials.

Note Be aware that the cluster security mode has no effect on digest authentication.

Digest Authentication for SIP Phones Configuration Task Flow

Complete these tasks to configure Digest Authentication for SIP phones.

Procedure

	Command or Action	Purpose
Step 1	Assign Digest Credentials to Phone User	Assign the digest credentials to the end user whom owns the phone.
Step 2	Enable Digest Authentication in Phone Security Profile	Enable digest authentication in the Phone Security Profile that associates to the phone.
Step 3	Assign Digest Authentication to the Phone	In Phone Configuration, assign the user as a digest user. Make sure the digest authentication-enabled security profile is assigned.
Step 4	End User Digest Credential Settings	Set the end user digest credentials.
Step 5	Configure SIP Station Realm, on page 158	Assign the string for the Realm field that Unified CM uses to challenge a SIP request due to a 401 Unauthorized message.

Assign Digest Credentials to Phone User

Use this procedure to assign digest credentials to the end user who owns the phone. Phones use the credentials to authenticate.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.

Step 2 Click **Find** and choose the end user who owns the phone.

Step 3 Enter the credentials in the following fields:

- Digest Credentials
- Confirm Digest Credentials

Step 4 Click **Save**.

Enable Digest Authentication in Phone Security Profile

Use this procedure to enable digest authentication for a phone through the Phone Security Profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 2 Click **Find** and choose the phone security profile that is associated to the phone.

Step 3 Check the **Enable Digest Authentication** check box.

Step 4 Click **Save**.

Assign Digest Authentication to the Phone

Use this procedure to associate the digest user and digest authentication-enabled security profile to the phone.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device > Phone**.

Step 2 Click **Find** and choose the phone for which you want to assign digest authentication.

Step 3 From the **Digest User** drop-down list, assign the end user for whom you assigned digest credentials.

Step 4 Make sure that the phone security profile for which you enabled digest authentication is assigned through the **Device Security Profile** drop-down list.

Step 5 Click **Save**.

Step 6 Click **Reset**.

After you associate the end user with the phone, save the configuration and reset the phone.

Configure SIP Station Realm

Assign the string that Cisco Unified Communications Manager uses in the Realm field when challenging a SIP phone in the response to a 401 Unauthorized message. This applies when the phone is configured for digest authentication.

Note The default string for this service parameter is ccmsipline.

Procedure

Step 1 From Unified Communications Manager, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose a node where you activated the CiscoCallManager service.

Step 3 From the **Service** drop-down list, choose the CiscoCallManager service. Verify that the word "Active" displays next to the service name.

Step 4 Update the **SIP Realm Station** parameter, as described in the help. To display help for the parameters, click the question mark or the parameter name link.

Step 5 Click **Save**.

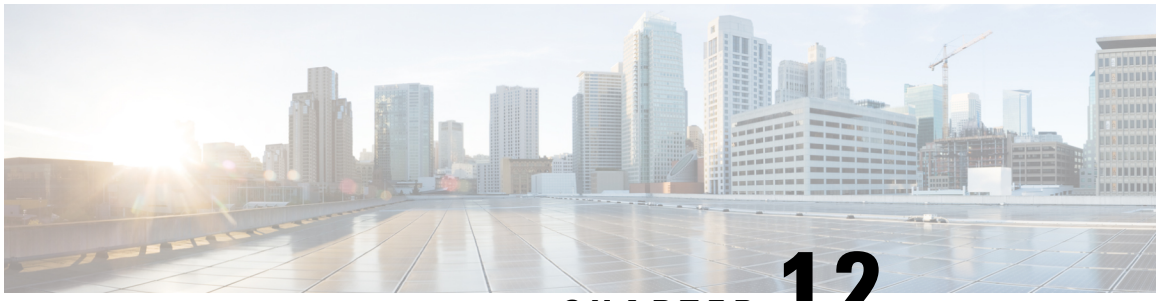
End User Digest Credential Settings

To view the digest credentials details, perform the following procedure:

From Cisco Unified Communications Manager Administration, choose **User Management > End User** and click the User ID and the **End User Configuration** window appears. The digest credentials are available in the **User Information** pane of the **End User Configuration** window.

Table 28: Digest Credentials

Setting	Description
Digest Credentials	Enter a string of alphanumeric characters.
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, enter the credentials in this field.



CHAPTER 12

Secure Conference Resources Setup

This chapter provides information about secure conference resources setup.

- Secure Conference, on page 159
- Conference Bridge Requirements, on page 160
- Secure Conference Icons, on page 161
- Secure Conference Status, on page 161
- Cisco Unified IP Phone Secure Conference and Icon Support, on page 164
- Secure Conference CTI Support, on page 164
- Secure Conference Over Trunks and Gateways, on page 164
- CDR Data, on page 165
- Interactions and Restrictions, on page 165
- Securing Conference Resources Tips, on page 166
- Set Up Secure Conference Bridge, on page 168
- Set Up Secure Conference Bridge in Cisco Unified Communications Manager Administration, on page 169
- Set Up Minimum Security Level for Meet-Me Conferences, on page 169
- Set Up Packet Capturing for Secure Conference Bridge, on page 170

Secure Conference

The Secure Conferencing feature provides authentication and encryption to secure a conference. A conference gets considered secure when all participating devices have encrypted signaling and media. The secure conference feature supports SRTP encryption over a secure TLS or IPSec connection.

The system provides a security icon for the overall security status of the conference, which is determined by the lowest security level of the participating devices. For example, a secure conference that includes two encrypted connections and one authenticated connection has a conference security status of authenticated.

To configure secure ad hoc and meet-me conferences, you configure a secure conference bridge.

- If a user initiates a conference call from a phone that is authenticated or encrypted, Unified Communications Manager allocates the secure conference bridge
- If a user initiates a call from a phone that is nonsecure, Unified Communications Manager allocates a nonsecure conference bridge.

When you configure conference bridge resources as nonsecure, the conference remains nonsecure, regardless of the security configuration for the phone.

Note Unified Communications Manager allocates a conference bridge from the Media Resource Group List (MRGL) for the phone that is initiating the conference. If a secure conference bridge is not available, Unified Communications Manager assigns a nonsecure conference bridge, and the conference is nonsecure. Likewise, if a nonsecure conference bridge is not available, Unified Communications Manager assigns a secure conference bridge, and the conference is nonsecure. If no conference bridge is available, the call will fail.

For meet-me conference calls, the phone that initiates the conference must also meet the minimum security requirement that is configured for the meet-me number. If no secure conference bridge is available or if the initiator security level does not meet the minimum, Unified Communications Manager rejects the conference attempt.

To secure conferences with barge, configure phones to use encrypted mode. After the Barge key is pressed and if the device is authenticated or encrypted, Unified Communications Manager establishes a secure connection between the barging party and the built-in bridge at the target device. The system provides a conference security status for all connected parties in the barge call.

Note Nonsecure or authenticated Cisco Unified IP Phones that are running release 8.3 or later can now barge encrypted calls.

Conference Bridge Requirements

A conference bridge can register as a secure media resource when you add a hardware conference bridge to your network and configure a secure conference bridge in Unified Communications Manager Administration.

Note Due to the performance impact to Unified Communications Manager processing, Cisco does not support secure conferencing on software conference bridge.

A Digital Signal Processor (DSP) farm, which provides conferencing on a H.323 or MGCP gateway, acts as the network resource for IP telephony conferencing. The conference bridge registers to Unified Communications Manager as a secure SCCP client.

- The conference bridge root certificate must exist in CallManager trust store, and the Cisco CallManager certificate must exist in the conference bridge trust store.
- The secure conference bridge security setting must match the security setting in Unified Communications Manager to register.

For more information about conferencing routers, refer to the IOS router documentation that is provided with your router.

Unified Communications Manager assigns conference resources to calls on a dynamic basis. The available conference resource and the enabled codec provide the maximum number of concurrent, secure conferences

allowed per router. Because transmit and receive streams are individually keyed for each participating endpoint (so no rekeying is necessary when a participant leaves the conference), the total secure conference capacity for a DSP module equals one-half the nonsecure capacity that you can configure.

See *Feature Configuration Guide for Cisco Unified Communications Manager* for more information.

Secure Conference Icons

Cisco IP Phones display a conference security icon for the security level of the entire conference. These icons match the status icons for a secure two-party call, as described in the user documentation for your phone.

The audio and video portions of the call provide the basis for the conference security level. The call gets considered secure only if both the audio and video portions are secure.

For ad hoc and meet-me secure conferences, the security icon for the conference displays next to the conference softkey in the phone window for conference participants. The icon that displays depends on the security level of the conference bridge and all participants:

- A lock icon displays if the conference bridge is secure and all participants in the conference are encrypted.
- A shield icon displays if the conference bridge is secure and all participants in the conference are authenticated. Some phone models do not display the shield icon.
- When the conference bridge or any participant in the conference is nonsecure, the call state icon (active, hold, and so on) displays, or, on some older phone models, no icon displays.



Note The "Override BFCP Application Encryption Status When Designating Call Security Status" service parameter displays the lock icon when parameter value is True and audio is secure. This condition ignores the security statuses of all other media channels. The default parameter value is False.

When an encrypted phone connects to a secure conference bridge, the media streaming between the device and the conference bridge gets encrypted; however, the icon for the conference can be encrypted, authenticated, or nonsecure depending on the security levels of the other participants. A nonsecure status indicates that one of the parties is not secure or cannot be verified.

When a user presses Barge, the icon that displays next to the Barge softkey provides the security level for the barge conference. If the barging device and the barged device support encryption, the system encrypts the media between the two devices, but the barge conference status can be nonsecure, authenticated, or encrypted, depending on the security levels of the connected parties.

Secure Conference Status

Conference status can change as participants enter and leave the conference. An encrypted conference can revert to a security level of authenticated or nonsecure if an authenticated or nonsecure participant connects to the call. Likewise, the status can upgrade if an authenticated or nonsecure participant drops off the call. A nonsecure participant that connects to a conference call renders the conference nonsecure.

Conference status can also change when participants chain conferences together, when the security status for a chained conference changes, when a held conference call is resumed on another device, when a conference call gets barged, or when a transferred conference call completes to another device.

Note The Advanced Ad Hoc Conference Enabled service parameter determines whether ad hoc conferences can be linked together by using features such as conference, join, direct transfer, and transfer.

Unified Communications Manager provides these options to maintain a secure conference:

- Ad hoc conference lists
- Meet-Me conference with minimum security level

Ad Hoc Conference Lists

A conference list displays on participating phones when the ConfList softkey is pressed during a conference call. The conference list provides the conference status as well as the security status for each participant to identify participants that are not encrypted.

Conference list displays these security icons: nonsecure, authenticated, encrypted, held. The conference initiator can use the conference list to eject participants with a low security status.

Note The Advanced Ad Hoc Conference Enabled service parameter determines whether conference participants other than the conference initiator can eject conference participants.

As participants join the conference, they get added to the top of the conference list. To remove nonsecure participants from a secure conference with the ConfList and RmLstC softkeys, refer to the user documentation for your phone.

The following sections describe secure ad hoc conference interactions with other features.

Secure Ad Hoc Conference and Conference Chaining

When an ad hoc conference is chained to another ad hoc conference, the chained conference displays in the list as member “Conference” with its own security status. Unified Communications Manager includes the security level for the chained conference to determine the overall conference security status.

Secure Ad Hoc Conference and cBarge

When a user presses the cBarge softkey to join an active conference, Unified Communications Manager creates an ad hoc conference and allocates a conference bridge according to the security level and MRGL of the barged device. The cbarge member names display in the conference list.

Secure Ad Hoc Conference and Barge

If a participant in a secure ad hoc conference gets barged, the barge call security status shows in the conference list next to the barge target. The security icon for the barge target may show authenticated when, in fact, the media is encrypted between the barge target and the conference bridge, because the barge caller has an authenticated connection.

If the barge target is secure but in an unsecured ad hoc conference, if the ad hoc conference status later changes to secure, the barge caller icon will update as well.

Secure Ad Hoc Conference and Join

Authenticated or encrypted phone users can use the Join softkey at a Cisco Unified IP Phone (only phones that are running SCCP) to create or join a secure ad hoc conference. If a user presses Join to add a participant with an unknown security status to an existing conference, Unified Communications Manager downgrades the conference status to unknown. A participant who adds a new member with Join becomes the conference initiator and can eject the new member or any other participant from the conference list (if the Advanced Ad Hoc Conference Enabled setting is True).

Secure Ad Hoc Conference and Hold/Resume

When a conference initiator puts the conference call on hold to add a participant, the conference status remains unknown (nonsecure) until the added participant answers the call. After the new participant answers, conference status updates in the conference list.

If a caller on a shared line resumes a held conference call at another phone, the conference list updates when the caller presses Resume.

Meet-Me Conference with Minimum Security Level

As administrator, you can specify a minimum security level for a conference when you configure a meet-me pattern or number as nonsecure, authenticated, or encrypted. Participants must meet the minimum security requirement, or the system blocks the participant and drops the call. This action applies to meet-me conference call transfers, resumed meet-me conference calls on shared lines, and chained Meet-Me conferences.

The phone that initiates the meet-me conference must meet the minimum security level, or the system rejects the attempt. When the minimum security level specifies authenticated or encrypted and a secure conference bridge is not available, the call fails.

If you specify nonsecure as the minimum level for the conference bridge, the conference bridge accepts all calls, and the conference status is nonsecure.

The following sections describe secure meet-me conference interactions with other features.

Meet-Me Conference and Ad Hoc Conference

To add a meet-me conference to an ad hoc conference or add an ad hoc conference to a meet-me conference, the ad hoc conference must meet the minimum security level for the meet-me conference, or the call is dropped. The conference icon can change when the conference gets added.

Meet-Me Conference and Barge

Unless a barge caller meets the minimum security requirement when the caller barges a meet-me conference participant, the security level of the barged device downgrades, and both the barge caller and the barged call get dropped.

Meet-Me Conference and Hold/Resume

A phone on a shared line cannot resume a meet-me conference unless the phone meets the minimum security level. If a phone does not meet the minimum security level, all phones on the shared line get blocked when the user presses Resume.

Cisco Unified IP Phone Secure Conference and Icon Support

These Cisco Unified IP Phones support secure conference and secure conference icons:

- Cisco Unified IP Phones 7942 and 7962 (SCCP only, authenticated secure conference only)
- Cisco Unified IP Phones 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7921G, , 7931G, 7942, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7970G, 7971G, 7971G-GE, 7975G, 8941, and 8945. (SCCP only)
- Cisco Unified IP Phones 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7941G, 7941G-GE, 7942G, 7961G, 7961G-GE,7962G, 7965G, 7970G, 7971G, 7971G-GE, 7975G, 8941, 8945, 8961, 9971, and 9971.

  Cisco IP Phones 7811, 7821, 7841, 7861, Cisco IP Conference Phone7832, Cisco IP Phones 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR, Cisco Wireless IP Phone 8821, Cisco Unified IP Conference Phone 8831, Cisco IP Conference Phone 8832.

Warning To obtain the full benefit of secure conference features, Cisco recommends upgrading Cisco Unified IP Phones to release 8.3 or later, which supports the encryption features in this release. Encrypted phones that run earlier releases do not fully support these new features. These phones can only participate in secure conference as authenticated or nonsecure participants.

Cisco Unified IP Phones that are running release 8.3 with an previous release of Cisco Unified Communications Manager will display their connection security status, not the conference security status, during a conference call, and do not support secure conference features like conference list.

See topics related to Unified Communications Manager secure conference restrictions for more restrictions that apply to Cisco Unified IP Phones.

For additional information about secure conference calls and security icons, refer to the *Cisco IP Phone Administration Guide and Cisco IP Phone User Guide* for your phone.

Secure Conference CTI Support

Unified Communications Manager supports secure conference over licensed CTI devices. Refer to the *Unified Communications Manager JTAPI Developers Guide* and *Unified Communications Manager TAPI Developers Guide* for this release for more information.

Secure Conference Over Trunks and Gateways

Unified Communications Manager supports secure conference over intracluster trunks (ICTs), H.323 trunks/gateways, and MGCP gateways; however, encrypted phones that are running release 8.2 or earlier will revert to RTP for ICT and H.323 calls, and the media does not get encrypted.

If a conference involves a SIP trunk, the secure conference status is nonsecure. In addition, SIP trunk signaling does not support secure conference notifications to off-cluster participants.

CDR Data

CDR data provides the security status of each call leg from the phone endpoint to the conference bridge as well as the security status of the conference itself. The two values use two different fields inside the CDR database.

CDR data provides termination cause code 58 (Bearer capability not presently available) when a meet-me conference rejects a join attempt that does not meet the minimum security level requirement. See the *CDR Analysis and Reporting Administration Guide* for more information.

Interactions and Restrictions

This section contains information on the following topics:

- Cisco Unified Communications Manager Interactions with Secure Conference, on page 165
- Cisco Unified Communications Manager Restrictions with Secure Conference, on page 166

Cisco Unified Communications Manager Interactions with Secure Conference

This section describes Unified Communications Manager interactions with the secure conference feature.

- To keep a conference secure, if a participant in a secure ad hoc conference puts a call on hold or parks the call, the system does not play MOH, even if the Suppress MOH to Conference Bridge service parameter is set to False. The secure conference status does not change.
- In intercluster environments, if an off-cluster conference participant presses hold in a secure ad hoc conference, the media stream to the device stops, MOH plays, and the media status changes to unknown. If the off-cluster participant resumes a held call with MOH, the conference status may upgrade.
- A secure MeetMe call across an intercluster trunk (ICT) will clear if the remote user invokes a phone feature such a hold/resume, which changes the media status to unknown.
- Annunciator tones or announcements for Unified Communications Manager Multilevel Precedence and Preemption that play on a participant phone during a secure ad hoc conference change the conference status to nonsecure.
- If a caller barges a secure SCCP phone call, the system uses an internal tone-playing mechanism at the target device, and the conference status remains secure.
- If a caller barges a secure SIP phone call, the system provides tone-on-hold, and the conference status remains nonsecure during the tone.
- If a conference is secure and RSVP is enabled, the conference remains secure.
- For conference calls that involve the PSTN, the security conference icon shows the security status for only the IP domain portion of the call.
- The Maximum Call Duration Timer service parameter also controls the maximum conference duration.
- Conference bridge supports packet capture. During a packet capture session, the phone displays a nonsecure status for the conference, even if the media stream is encrypted.

- The media security policy that is configured for your system may alter secure conference behavior; for example, an endpoint will use media security according to the system media security policy, even when participating in a conference call with endpoints that do no support media security.

Cisco Unified Communications Manager Restrictions with Secure Conference

This section describes Unified Communications Manager restrictions with secure conferencing feature.

- Encrypted Cisco IP Phones that are running release 8.2 or earlier can only participate in a secure conference as authenticated or nonsecure participants.
- Cisco Unified IP Phones that are running release 8.3 with an previous release of Unified Communications Manager will display their connection security status, not the conference security status, during a conference call and do not support secure conference features like conference list.
- Cisco Unified IP Phones 7800 and 7911G do not support conference list.
- Due to bandwidth requirements, Cisco Unified IP Phones 7942 and 7962 do not support barge from an encrypted device on an active encrypted call. The barge attempt will fail.
- Cisco Unified IP Phone 7931G does not support conference chaining.
- Phones that are calling over SIP trunks get treated as nonsecure phones, regardless of their device security status.
- If a secure phone attempts to join a secure meet-me conference over a SIP trunk, the call gets dropped. Because SIP trunks do not support providing the “device not authorized” message to a phone that is running SIP, the phone does not update with this message. In addition, 7962 phones that are running SIP do not support the “device not authorized” message.
- In intercluster environments, the conference list does not display for off-cluster participants; however, the security status for the connection displays next to the Conference softkey as long as the connection between the clusters supports it. For example, for H.323 ICT connections, the authentication icon does not display (the system treats the authenticated connection as nonsecure), but the encryption icon displays for an encrypted connection.

  Off-cluster participants can create their own conference that connects to another cluster across the cluster boundary. The system treats the connected conferences as a basic, two-party call.

Securing Conference Resources Tips

Consider the following information before you configure secure conference bridge resources:

- Use localization if you want the phone to display custom text for secure conference messages. Refer to the Unified Communications Manager Locale Installer documentation for more information.
- The conference or built-in bridge must support encryption to secure conference calls.
- To enable secure conference bridge registration, set the cluster security mode to mixed mode.
- Ensure the phone that initiates a conference is authenticated or encrypted to procure a secure conference bridge.

- To maintain conference integrity on shared lines, do not configure devices that share a line with different security modes; for example, do not configure an encrypted phone to share a line with an authenticated or nonsecure phone.
- Do not use SIP trunks as ICTs when you want to share conference security status between clusters.
- If you set the cluster security mode to mixed mode, the security mode that is configured for the DSP farm (nonsecure or encrypted) must match the conference bridge security mode in Unified Communications Manager Administration, or the conference bridge cannot register. The conference bridge registers as encrypted when both security modes specify encrypted; the conference bridge registers as nonsecure when both security modes specify nonsecure.
- If you set the cluster security mode to mixed mode, if the security profile you applied to the conference bridge is encrypted, but the conference bridge security level is nonsecure, Unified Communications Manager rejects conference bridge registration.
- If you set the cluster security mode to nonsecure mode, configure the security mode at the DSP farm as nonsecure, so the conference bridge can register. The conference bridge registers as nonsecure even if the setting in Unified Communications Manager Administration specifies encrypted.
- During registration, the conference bridge must pass authentication. To pass authentication, the DSP farm system must contain one or more the Unified Communications Manager CallManager.pem certificates, and Unified Communications Manager must contain certificates for the DSP farm system and the DSP connection in the CallManager-trust store. The common Name specified in the X.509 Subject attribute must begin with the conference bridge name defined in Cisco Unified Communications Manager and on the DSP farm system using the associate **profile <profile-identifier> register <device-name>?** command. The Subject Alternate Name attribute is not supported. For example, if the certificate Subject Common Name is ?CN=example.cisco.com? then the Conference Bridge Name in Unified Communications Manager must be ?example? and the DSP farm system command must be **?associate profile <profile-identifier> register** example. If you have multiple secure conference bridges on the same DSP farm system, each requires a separate certificate.

Tip Make sure that the Conference Bridge Name is unique and that it can not be configured in any other place under the "Device" table. This applies to the Route list, SIP trunks, IP phones, and so on.

- If conference bridge certificates expire or change for any reason, use the certificate management feature in Cisco Unified Communications Operating System Administration to update the certificates in the trusted store. The TLS authentication fails when certificates do not match, and conference bridge does not work because it cannot register to Unified Communications Manager.
- The secure conference bridge registers to Unified Communications Manager through TLS connection at port 2443; a nonsecure conference bridge registers to Unified Communications Manager through TCP connection at port 2000.
- Changing the device security mode for the conference bridge requires a reset of Unified Communications Manager devices and a restart of the Cisco CallManager service.

Set Up Secure Conference Bridge

The following procedure provides the tasks used to add secure conferencing to your network.

Procedure

Step 1 Verify that you installed and configured the CiscoCTL Client for Mixed Mode.

Step 2 Verify that you configured the DSP farm security settings for Unified Communications Manager connection, including adding the Unified Communications Manager certificate to the trust store. Set the DSP farm security level to encrypted.

Refer to the documentation for your conference bridge.

Tip
The DSP farm establishes the TLS port connection to Unified Communications Manager on port 2443.

Step 3 Verify the DSP farm certificate is in the CallManager trust store.

To add the certificate, use the certificate management function in the Cisco Unified Communications Operating System to copy the DSP certificate to the trusted store in Unified Communications Manager.

When you have finished copying the certificate, restart the CiscoCallManager service on the server.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* and the *Cisco Unified Serviceability Administration Guide*.

Tip
Be sure to copy the certificate to each server in the cluster and restart the CiscoCallManager service on each server in the cluster.

Step 4 In Unified Communications Manager Administration, configure Cisco IOS Enhanced Conference Bridge as the conference bridge type and select Encrypted Conference Bridge for device security mode.

Tip
When you upgrade to this release, Unified Communications Manager automatically assigns a nonsecure conference bridge security profile to Cisco IOS Enhanced Conference Bridge configurations.

Step 5 Configure a minimum security level for Meet-Me Conferences.

Tip
When you upgrade to this release, Unified Communications Manager automatically assigns a minimum security level of nonsecure to all Meet Me patterns.

Step 6 Configure packet capturing for the secure conference bridge.

See the *Troubleshooting Guide for Unified Communications Manager* for more information.

Tip
Set packet capture mode to batch mode and capture tier to SRTP.

Set Up Secure Conference Bridge in Cisco Unified Communications Manager Administration

To configure a secure conference bridge in Unified Communications Manager Administration, perform the following procedure. After you configure encryption for the conference bridge, you must reset Unified Communications Manager devices and restart the CiscoCallManager service.

Ensure that you installed certificates in Unified Communications Manager and in the DSP farm to secure the connection between the devices.

Before you begin

Before You Begin

Procedure

Step 1 Choose **Media Resources** > **Conference Bridge**.

Step 2 In the **Find and List Conference Bridges** window, verify that a Cisco IOS Enhanced Conference Bridge is installed and go to Set Up Secure Conference Bridge, on page 168.

Step 3 If the device does not exist in the database, click **Add New**; go to Set Up Secure Conference Bridge in Cisco Unified Communications Manager Administration, on page 169.

Step 4 In the Conference Bridge Configuration window, select **Cisco IOS Enhanced Conference Bridge** in the **Conference Bridge Type** drop-down list box. Configure the Conference Bridge Name, Description, Device Pool, Common Device Configuration, and Location settings as described in the *Administration Guide for Cisco Unified Communications Manager* .

Step 5 In the Device Security Mode field, select **Encrypted Conference Bridge**.

Step 6 Click **Save**.

Step 7 Click **Reset**.

What to do next

To perform additional conference bridge configuration tasks, you can jump to the Meet-Me/Number Pattern Configuration window or the Service Parameter Configuration window by selecting the option from the Related Links drop-down list box and clicking **Go**.

Set Up Minimum Security Level for Meet-Me Conferences

To configure a minimum security level for Meet-Me conferences, perform the following procedure.

Procedure

Step 1 Choose **Call Routing** > **Meet-Me Number/Pattern**.

Step 2 In the Find and List Conference Bridges window, verify that the Meet-Me number/pattern is configured and go to Set Up Secure Conference Bridge, on page 168.

Step 3 If the Meet-Me number/pattern is not configured, click **Add New**; go to Set Up Minimum Security Level for Meet-Me Conferences, on page 169.

Step 4 In the **Meet-Me Number Configuration** window, enter a Meet-Me number or range in the Directory Number or Pattern field. Configure the Description and Partition settings as described in the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Step 5 In the Minimum Security Level field, select **Non Secure**, **Authenticated**, or **Encrypted**.

Step 6 Click **Save**.

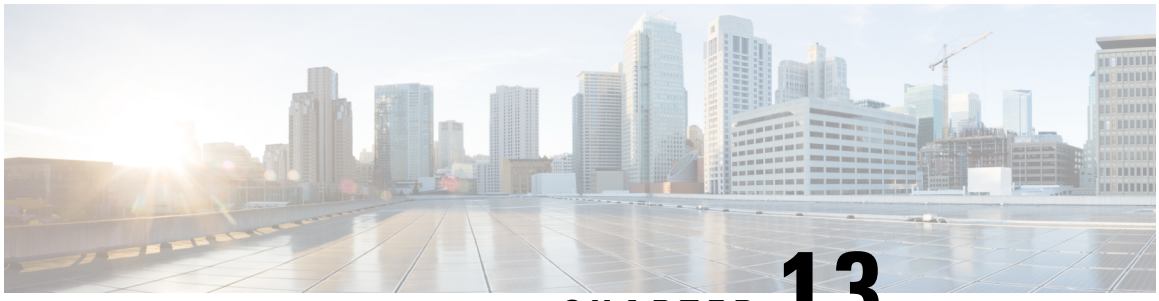
What to do next

If you have not yet installed a secure conference bridge, install and configure a secure conference bridge.

Set Up Packet Capturing for Secure Conference Bridge

To configure packet capturing for a secure conference bridge, enable packet capturing in the **Service Parameter Configuration** window; then, set the packet capture mode to batch mode and capture tier to SRTP for the phone, gateway, or trunk in the device configuration window. Refer to the *Troubleshooting Guide for Cisco Unified Communications Manager* for more information.

During a packet capture session, the phone displays a nonsecure status for the conference, even if the media stream is encrypted.



CHAPTER 13

Voice-Messaging Ports Security Setup

This chapter provides information about voice-messaging ports security setup.

- Voice-Messaging Security, on page 171
- Voice-Messaging Security Setup Tips, on page 171
- Set Up Secure Voice-Messaging Port, on page 172
- Apply Security Profile to Single Voice-Messaging Port, on page 173
- Apply Security Profile Using Voice Mail Port Wizard, on page 174

Voice-Messaging Security

To configure security for Unified Communications Manager voice-messaging ports and Cisco Unity devices that are running SCCP or Cisco Unity Connection devices that are running SCCP, you choose a secure device security mode for the port. If you choose an authenticated voicemail port, a TLS connection opens, which authenticates the devices by using a mutual certificate exchange (each device accepts the certificate of the other device). If you choose an encrypted voicemail port, the system first authenticates the devices and then sends encrypted voice streams between the devices.

Cisco Unity Connection connects to Unified Communications Manager through the TLS port. When the device security mode is nonsecure, Cisco Unity Connection connects to Unified Communications Manager through the SCCP port.

Note In this chapter, the use of the term “server” refers to a Unified Communications Manager server. The use of the phrase “voicemail server” refers to a Cisco Unity server or to a Cisco Unity Connection server.

Voice-Messaging Security Setup Tips

Consider the following information before you configure security:

- For Cisco Unity, you must perform security tasks by using the Cisco Unity Telephony Integration Manager (UTIM); for Cisco Unity Connection, you must perform security tasks by using Cisco Unity Connection Administration. For information on how to perform these tasks, refer to the applicable Unified Communications Manager integration guide for Cisco Unity or for Cisco Unity Connection.

- In addition to the procedures that are described in this chapter, you must use the certificate management feature in Unified Communications Manager to save the Cisco Unity certificate to the trusted store.

  For more information, see the "To Add Voice Messaging Ports in Cisco Unity Connection Administration" procedure in the *Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection* at the following URL:

  http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/integration/guide/cucm_sccp/guide/cucintcucmskinny230.html

  After you copy the certificate, you must restart the CiscoCallManager service on each Unified Communications Manager server in the cluster.
- If Cisco Unity certificates expire or change for any reason, use the certificate management feature in the *Administration Guide for Cisco Unified Communications Manager* to update the certificates in the trusted store. The TLS authentication fails when certificates do not match, and voice messaging does not work because it cannot register to Unified Communications Manager.
- When configuring voice-mail server ports, you must select a device security mode.
- The setting that you specify in the Cisco Unity Telephony Integration Manager (UTIM) or in Cisco Unity Connection Administration must match the voice-messaging port device security mode that is configured in Unified Communications Manager Administration. In Cisco Unity Connection Administration, you apply the device security mode to the voice-messaging port in the Voice Mail Port Configuration window (or in the Voice Mail Port Wizard).

Tip If the device security mode settings do not match, the voicemail server ports fail to register with Unified Communications Manager, and the voicemail server cannot accept calls on those ports.

- Changing the security profile for the port requires a reset of Unified Communications Manager devices and a restart of the voicemail server software. If you apply a security profile in Unified Communications Manager Administration that uses a different device security mode than the previous profile, you must change the setting on the voicemail server.
- You cannot change the Device Security Mode for existing voice-mail servers through the VoiceMail Port Wizard. If you add ports to an existing voicemail server, the device security mode that is currently configured for the profile automatically applies to the new ports.

Set Up Secure Voice-Messaging Port

The following procedure provides the tasks used to configure security for voice-messaging ports.

Procedure

Step 1 Verify that Unified Communications Manager is in mixed mode by running the **utils ctl** CLI command.

Step 2 Verify that you configured the phones for authentication or encryption.

Step 3 Use the certificate management feature in Cisco Unified Communications Operating System Administration to copy the Cisco Unity certificate to the trusted store on the Unified Communications Manager server; then restart the CiscoCallManager service.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* and *Cisco Unified Serviceability Administration Guide*.

Note
The below mentioned tip is not valid for release 14SU3 onwards.

Tip
Activate the Cisco CTL Provider service on each Unified Communications Manager server in the cluster; then restart the CiscoCallManager service on all servers.

Step 4 In Unified Communications Manager Administration, configure the device security mode for the voice-messaging ports.

Step 5 Perform security-related configuration tasks for Cisco Unity or Cisco Unity Connection voice-messaging ports; for example, configure Cisco Unity to point to the Cisco TFTP server.

For more information, see *Unified Communications Manager Integration Guide for Cisco Unity* or for *Cisco Unity Connection*

Step 6 Reset the devices in Unified Communications Manager Administration and restart the Cisco Unity software.

For more information, see the *Unified Communications ManagerIntegration Guide for Cisco Unity* or for *Cisco Unity Connection*.

Apply Security Profile to Single Voice-Messaging Port

To apply a security profile to a single voice-messaging port, perform the following procedure.

This procedure assumes that you added the device to the database and installed a certificate in the phone, if a certificate does not already exist. After you apply a security profile for the first time or if you change the security profile, you must reset the device.

Before you begin

Before you apply a security profile, review topics related to voice-messaging security and secure voice-messaging port setup.

Procedure

Step 1 Find the voice-messaging port, as described in the *Administration Guide for Cisco Unified Communications Manager*.

Step 2 After the configuration window for the port displays, locate the **Device Security Mode** setting. From the drop-down list box, choose the security mode that you want to apply to the port. The database predefines these options. The default value specifies **Not Selected**.

Step 3 Click **Save**.

Step 4 Click **Reset**.

Apply Security Profile Using Voice Mail Port Wizard

Use this procedure to apply the Device Security Mode setting in the Voice Mail Port Wizard for a new voice-mail server.

To change the security setting for an existing voice-mail server, see topics related to applying the security profile to a single voice-messaging port.

Before you begin

Before you apply a security profile, review topics related to voice-messaging security and secure voice-messaging port setup.

Procedure

Step 1 Unified Communications Manager Administration, choose **Voice Mail** > **Cisco Voice Mail Port Wizard**.

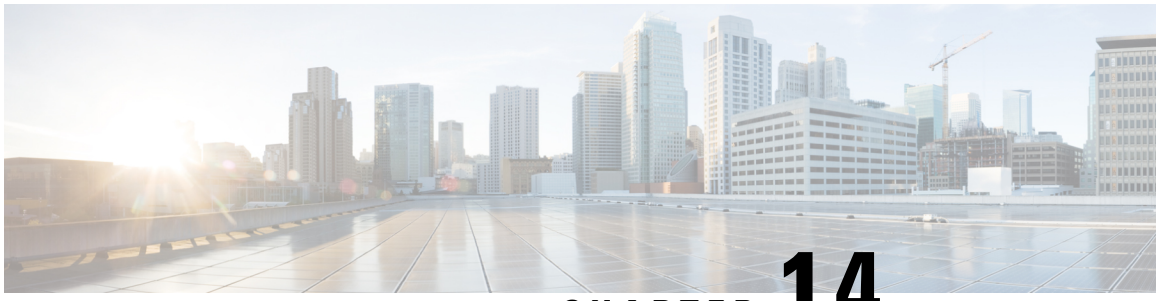
Step 2 Enter the name of the voice-mail server; click **Next**.

Step 3 Choose the number of ports that you want to add; click **Next**.

Step 4 In the **Cisco Voice Mail Device Information** window, choose a **Device Security Mode** from the drop-down list box. The database predefines these options. The default value specifies **Not Selected**.

Step 5 Configure the other device settings, as described in the *Administration Guide for Cisco Unified Communications Manager*. Click **Next**.

Step 6 Continue the configuration process, as described in the *Administration Guide for Cisco Unified Communications Manager*. When the **Summary** window displays, click **Finish**.



CHAPTER 14

Secure Tones and Icons

- Secure Tones and Icons Overview, on page 175
- Secure Icons and Tones Tips , on page 177
- Secure Icons and Tones Configuration Tasks, on page 179
- Secure Calls and Tones Limitations and Restrictions , on page 181

Secure Tones and Icons Overview

Secure Icons and Secure Tone provide audio and visual indicators that alert you as to the security status of a call. Both of these features alert call participants of the security level of a call, so that participants know whether it's safe to exchange confidential information.

- Secure Icons—Refers to an icon that displays on the phone to indicate the level of security for a call.
- Secure Tones—Refers to a 2-second tone that plays at the start of a call to indicate whether the call is secure or non-secure.

Secure Icons

Security icons provide a visual indicator that appears on the phone display, letting you know whether a call is secure or nonsecure. The icon appears on the phone right next to the call duration timer.

The following table displays the security icons along with a description of its meaning:

Table 29: Secure Icons

Security Icon	Security Level	Description
Lock 	Encrypted Call	Both call signaling (with TLS) and call media (with SRTP) are encrypted. **Note** It's always required that the audio stream be encrypted in order for the Encryption icon to display on the phone. Encryption for additional media streams (video, BFCP and iX channel) may be required depending on how you configure the Call Secure Status Policy parameter. The default value is that the media is considered encrypted so long as the audio and video streams are both encrypted.

Security Icon	Security Level	Description
Shield 	Authenticated call	Call signaling is encrypted with TLS, call media is either unencrypted or partially encrypted. For example, the audio is encrypted, but not video. However, the Call Secure Status Policy indicates both must be encrypted for the call to have an Encrypted status.
No icon	Non secure call	Unauthenticated device with non secure audio and video

Additional Information

- Some phone models display only the lock icon (encrypted) and do not display the shield icon (authenticated)
- The security status of a call can change for point-to-point, intracluster, intercluster, and multihop calls. SCCP line, SIP line, and H.323 signal toning support notification of call security status changes to participating endpoints.
- For conference and barge calls, the security icon displays the security status of the conference.

Secure Tones Overview

Secure Tones can be configured to play on a Protected Phone at the start of a call. The tone alerts you to whether the other device in the call is secure or non secure—if the other device is non secure, you hear the nonsecure tone, if the other device is secure, you hear the secure tone.

Unlike Secure Icons, which display on all phones, Secure Tones play only on phones that are configured as a Protected Device. If both phones in a call are secured, but only one phone is Protected, only the Protected Phone hears the tone.

The following table lists the type of tone and what each means:

Table 30: Secure Tones

Secure Tones	Description
Three long beeps	Secure call. Other phone is a secure phone.
Six short beeps	Non secure call. Other phone is non secure.

Midcall Changes

If the security status of the call changes during the call, a new secure or nonsecure tone plays midcall in order to alert the caller on a Protected Device of the new security status. Only a user who is on a Protected Device hears the tone:

Types of Calls

Secure tone works for the following types of calls:

- Intracluster calls (IP to IP)
- Intercluster calls that are deemed protected

- IP to TDM calls over an MGCP gateway E1 connection (the MGCP gateway must be a protected device)

Secure Phone Call Identification

You can establish and identify a secure call when your phone and the phone on the other end is configured for secure calling. Conference calls support secure calls after secure conference bridge is set.

A secured call is established when you initiate a call from a secured phone (secured mode). A secure icon appears on the phone screen and indicates that the phone is configured for secure calls, but does not mean that the other phone connected is also secured.

You will hear a security tone if the call connects to another secured phone, indicating that both ends of the conversation are encrypted and secured.

Note If the call connects to a non secure phone, you will not hear the security tone.

Secure Icons and Tones Tips

Secure calling is supported between two phones. For protected phones, features such as conference calling, shared lines, and Extension Mobility, are not available when secure calling is configured. Only callers on protected phones can hear secure and non secure indication tones. Callers on non protected phones don't hear these tones. For video calls, the system plays secure and non secure indication tones on protected devices.

All phones that support security icons display call security level.

- The phone displays a shield icon for calls with a signaling security level of authentication. A shield icon identifies a secured connection between Cisco IP devices. This icon indicates that the devices use encrypted signaling.
- The phone displays a lock icon for calls with encrypted media. This icon indicates that the devices use encrypted signaling and encrypted media.
- Some phone models display only the lock icon.

The security status of a call can change for point-to-point, intracluster, intercluster, and multihop calls. SCCP line, SIP line, and H.323 signaling support notification of call security status changes to participating endpoints.

The protected phones only play the secure or nonsecure indication tones. The non protected phones never play indication tones. If the overall call status changes during the call, the indication tone changes and the protected phone play the appropriate tone.

Below are few scenarios when a protected phone plays an appropriate tone:

- If you enable the **Play Secure Indication Tone** option.
- When end-to-end secure media is established and the call status is secure, the phone plays the secure indication tone—three long beeps with pauses.
- When end-to-end non-secure media is established and the call status is non secure, the phone plays the non secure indication tone—six short beeps with brief pauses.

- If you disable the **Play Secure Indication Tone** option, the tones are not played.

Supported Devices Secure Tones

Use this procedure to obtain a list of phones that support secure tones.

Procedure

Step 1 From Cisco Unified Reporting, click **System Reports**.

Step 2 Click **Unified CM Phone Features List**.

Step 3 Click **Generate a New Report**.

Step 4 From the **Features** drop-down list, choose **Secure Tone**.

Step 5 Click **Submit**.

For more information about using Cisco Unified Reporting, see Administration Guide for Cisco Unified Communications Manager.

Protected Devices Secure Tones

You can configure only supported Cisco Unified IP Phones and MGCP E1 PRI gateways as protected devices in Unified Communications Manager. Unified Communications Manager can also direct an MGCP IOS gateway to play secure and non secure indication tones when the system determines the protected status of a call.

You can make the following types of calls that use secure and non secure indication tones:

- Intracluster IP-to-IP calls
- Intercluster calls that the system determines are protected
- IP-to-Time-Division-Multiplexing (TDM) calls through a protected MGCP E1 PRI gateway

For video calls, the system plays secure and nonsecure indication tones on protected devices.

The protected devices provide the following functions:

- You can configure phones that are running SCCP or SIP as protected devices.
- Protected devices can call non protected devices that are either encrypted or non-encrypted. In such cases, the call specifies non protected and the system plays non secure indication tone to the phones on the call.
- When a protected phone calls another protected phone, and the media is not encrypted, the system plays a nonsecure indication tone to the phones on the call.

To set a phone to protected state, check the **Protected Device** check box in the **Phone Configuration** window of the **Cisco Unified CM Administration** page.

Secure Icons and Tones Configuration Tasks

You can configure secure icons and secure tones using the following tasks:

Procedure

	Command or Action	Purpose
Step 1	Set up Call Secure Status Policy	Call Secure Status Policy outlines which media streams within a call must be encrypted for the Secure Icon feature to display the call as Encrypted. The default is that audio and video (for video calls) must both be encrypted. You can reconfigure the setting to consider BFCP and iX Channel as well.
Step 2	Enable Secure Indication Tone	Enable the secure indication tone on a protected phone.
Step 3	Configure Phone as a Protected Device	Configure supported Cisco Unified IP Phones as protected devices in Unified Communications Manager.

Set Up Secure Icon Policy

Call Secure Status Policy controls display of secure status icon on phones. The following are the policy options:

- All media except BFCP and iX application streams must be encrypted

  This is the default value. The security status of the call is not dependent on the encryption status of BFCP and iX application streams.

- All media except iX application streams must be encrypted

  The security status of the call is not dependent on the encryption status iX application streams.

- All media except BFCP application streams must be encrypted

  The security status of the call is not dependent on the encryption status BFCP.

- All media in a session must be encrypted

  The security status of the call is dependent on the encryption status of all the media streams of an established phone session.

- Only Audio must be encrypted

  The security status of the call is dependent on the encryption of the audio stream.

Note Changes to the policy impacts display of the secure icon and playing of secure tone on the phone.

Procedure

Step 1 From Unified Communications Manager Administration, choose **System > Service Parameters**.

Step 2 From **Select Server and Service** pane, choose your server and the CallManager service.

Step 3 Go to **Clusterwide Parameters (Feature - Call Secure Status Policy)** pane.

Step 4 From the **Secure Call Icon Display Policy** field, choose a policy from the drop-down list.
A warning message with the impact on video calls and secure tone is displayed.

Step 5 Click **Save**.
The window refreshes, and Unified Communications Manager updates the policy in the **Service Parameter Configuration** page.

Enable Secure Indication Tone for Cluster

The secure indication tone plays on a protected phone when the overall status of the call specifies protected, when the system determines that the call is encrypted. You have to set the indication tone to True.

Procedure

Step 1 From Unified Communications Manager Administration, choose **System > Service Parameters**.

Step 2 From **Select Server and Service** pane, choose your server and the CallManager service.

Step 3 Navigate to **Clusterwide Parameters (Feature - Secure Tone)** pane.

Step 4 Set the **Play Tone to Indicate Secure/Non-Secure Call Status** option to **True**. By default, the option is **False**.

After configuring the cluster for Secure Indication Tone, configure individual phones as Protected Phones. Only a protected phone can hear the secure and non secure tones.

Configure Phone As a Protected Device

You can configure supported Cisco Unified IP Phones as protected devices in Unified Communications Manager. Only callers on a protected phone can hear the secure and non secure indication tones.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device > Phone**.
The list of phone appears.

Step 2 Click the phone for which you want to set the secure tone parameters.

Step 3 Navigate to the **Device Information** pane and perform the following:

a. From the **Softkey Template** drop-down list, choose **Standard Protected Phone**

Note
You must use a new softkey template without supplementary service softkeys for a protected phone.

b. Check the **Protected Device** check box.

Step 4 Navigate to the **Protocol Specific Information** pane.

Step 5 From the **Device Security Profile** drop-down list, choose an encrypted security phone profile that is already configured in the **Phone Security Profile Configuration** page.

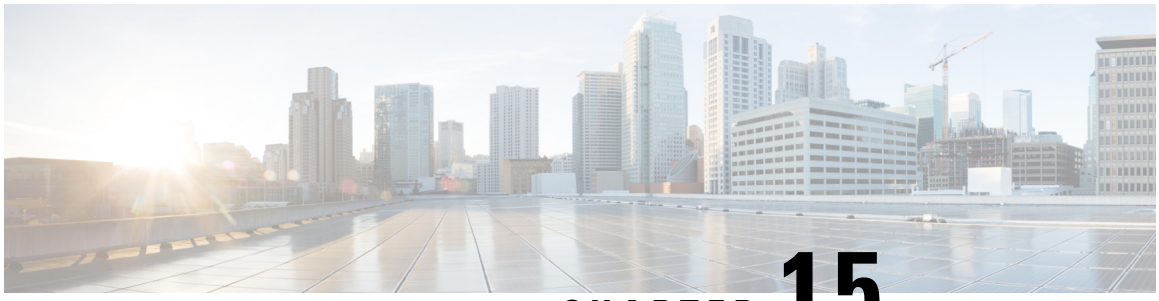
Step 6 Click **Save**.

Secure Calls and Tones Limitations and Restrictions

The following are the limitations and restrictions with reference to the secure calls and tones:

Table 31: Secure Icons and Secure Tones Interactions and Restrictions

Feature	Interactions and Restrictions
H.323 Trunks	Secure icons not supported over H.323 trunks
Call Transfer and Hold	The encryption lock icon may not display on the phone when you perform tasks such as transferring or putting a call on hold. The status changes from encrypted to non-secure if the media streams that are associated with these tasks are not encrypted.
PSTN calls	For calls that involve the PSTN, the security icon shows the security status for only the IP domain portion of the call.
Barge	With secure icons: • Non secure or authenticated Cisco IP Phones can barge encrypted calls. The security icon indicates the security status for the conference calls. With secure tones: • If a caller barges a secure SIP call, the system provides tone-on-hold, and Unified Communications Manager classifies the call as non secure during the tone. • If a caller barges a secure SCCP call, the system uses an internal tone-playing mechanism at the target device and the status remains secure.



CHAPTER 15

Trunk and Gateway SIP Security

- Trunk and Gateway SIP Security Overview, on page 183
- Configure Trunk and Gateway SIP Security Task Flow, on page 187

Trunk and Gateway SIP Security Overview

This section provides an overview of SIP trunk encryption, gateway encryptions and security profile setup tips.

SIP Trunk Encryption

SIP trunks can support secure calls both for signaling as well as media; TLS provides signaling encryption and SRTP provides media encryption.

To configure signaling encryption for the trunk, choose the following options when you configure the SIP trunk security profile (in the **System** > **Security Profile** > **SIP Trunk Security Profile** window):

- From the **Device Security Mode** drop-down list, choose “Encrypted.”
- From the **Incoming Transport Type** drop-down list, choose “TLS.”
- From the **Outgoing Transport Type** drop-down list, choose “TLS.”

After you configure the SIP trunk security profile, apply it to the trunk (in the **Device** > **Trunk** > **SIP Trunk** configuration window).

To configure media encryption for the trunk, check the **SRTP Allowed** check box (also in the **DeviceTrunkSIP Trunk** configuration window).



Caution If you check this check box, we recommend that you use an encrypted TLS profile, so that keys and other security-related information do not get exposed during call negotiations. If you use a non- secure profile, SRTP will still work but the keys will be exposed in signaling and traces. In that case, you must ensure the security of the network between Unified Communications Manager and the destination side of the trunk.

Cisco IOS MGCP Gateway Encryption

Unified Communications Manager supports gateways that use the MGCP SRTP package, which the gateway uses to encrypt and decrypt packets over a secure RTP connection. The information that gets exchanged during call setup determines whether the gateway uses SRTP for a call. If the devices support SRTP, the system uses a SRTP connection. If at least one device does not support SRTP, the system uses a RTP connection. SRTP-to-RTP fallback (and vice versa) may occur for transfers from a secure device to a non-secure device, conferencing, transcoding, music on hold, and so on.

When the system sets up an encrypted SRTP call between two devices, Unified Communications Manager generates a master encryption key and salt for secure calls and sends them to the gateway for the SRTP stream only. Unified Communications Manager does not send the key and salt for SRTCP streams, which the gateway also supports. These keys get sent to the gateway over the MGCP signaling path, which you should secure by using IPSec. Although Unified Communications Manager does not recognize whether an IPSec connection exists, the system sends the session keys to the gateway in the cleartext if IPSec is not configured. Confirm that the IPSec connection exists, so the session keys get sent through a secure connection.

Tip If the MGCP gateway, which is configured for SRTP, is involved in a call with an authenticated device, for example, an authenticated phone that is running SCCP, a shield icon displays on the phone because Unified Communications Manager classifies the call as authenticated. Unified Communications Manager classifies a call as encrypted if the SRTP capabilities for the devices are successfully negotiated for the call. If the MGCP gateway is connected to a phone that can display security icons, the phone displays the lock icon when the call is encrypted.

The following are the facts about MGCP E1 PRI gateways:

- You must configure the MGCP gateway for SRTP encryption. Configure the gateway using the following command: **mgcppackage-capabilitysrtp-package**
- The MGCP gateway must specify an Advanced IP Services or Advanced Enterprise Services image.

  For example, **c3745-adventerprisek9-mz.124-6.T.bin**
- Protected status gets exchanged with the MGCP E1 PRI gateway by using proprietary FacilityIE in the MGCP PRI Setup, Alert, and Connect messages.
- Unified Communications Manager plays the secure indication tone only to the Cisco Unified IP Phone. A PBX in the network plays the tone to the gateway end of the call.
- If the media between the Cisco Unified IP Phone and the MGCP E1 PRI gateway is not encrypted, the call drops.

Note For more information about encryption for MGCP gateways, see *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* for the version of Cisco IOS software that you are using.

H.323 Gateway and H.323/H.225/H.245 Trunk Encryption

H.323 gateways and gatekeeper or non-gatekeeper controlled H.225/H.323/H.245 trunks that support security can authenticate to Unified Communications Manager if you configure an IPSec association in the Cisco Unified Communications Operating System. For information on creating an IPSec association between Unified Communications Manager and these devices, refer to the *Administration Guide for Cisco Unified Communications Manager* .

The H.323, H.225, and H.245 devices generate the encryption keys. These keys get sent to Unified Communications Manager through the signaling path, which you secure through IPSec. Although Unified Communications Manager does not recognize whether an IPSec connection exists, the session keys get sent in the clear if IPSec is not configured. Confirm that the IPSec connection exists, so the session keys get sent through a secure connection.

In addition to configuring an IPSec association, you must check the SRTP Allowed check box in the device configuration window in Unified Communications Manager Administration; for example, the H.323 Gateway, the H.225 Trunk (Gatekeeper Controlled), the Inter-Cluster Trunk (Gatekeeper Controlled), and the Inter-Cluster Trunk (Non-Gatekeeper Controlled) configuration windows. If you do not check this check box, Unified Communications Manager uses RTP to communicate with the device. If you check the check box, Unified Communications Manager allows secure and nonsecure calls to occur, depending on whether SRTP is configured for the device.



Caution If you check the SRTP Allowed check box in Unified Communications Manager Administration, Cisco strongly recommends that you configure IPSec, so security-related information does not get sent in the clear.

Unified Communications Manager does not confirm that you configured the IPSec connection correctly. If you do not configure the connection correctly, security-related information may get sent in the clear.

If the system can establish a secure media or signaling path and if the devices support SRTP, the system uses a SRTP connection. If the system cannot establish a secure media or signaling path or if at least one device does not support SRTP, the system uses a RTP connection. SRTP-to-RTP fallback (and vice versa) may occur for transfers from a secure device to a non-secure device, conferencing, transcoding, music on hold, and so on.

Tip If the call uses pass-through capable MTP, if the audio capabilities for the device match after region filtering, and if the MTP Required check box is not checked for any device, Unified Communications Manager classifies the call as secure. If the MTP Required check box is checked, Unified Communications Manager disables audio pass-through for the call and classifies the call as nonsecure. If no MTP is involved in the call, Unified Communications Manager may classify the call as encrypted, depending on the SRTP capabilities of the devices.

For SRTP-configured devices, Unified Communications Manager classifies a call as encrypted if the SRTP Allowed check box is checked for the device and if the SRTP capabilities for the devices are successfully negotiated for the call. If the preceding criteria are not met, Unified Communications Manager classifies the call as nonsecure. If the device is connected to a phone that can display security icons, the phone displays the lock icon when the call is encrypted.

Unified Communications Manager classifies outbound faststart calls over a trunk or gateway as nonsecure. If you check the SRTP Allowed check box in Unified Communications Manager Administration, Unified Communications Manager disables the **Enable Outbound FastStart** check box.

Unified Communications Manager allows some types of gateways and trunks to transparently pass through the shared secret (Diffie-Hellman key) and other H.235 data between two H.235 endpoints, so the two endpoints can establish a secure media channel.

To enable the passing through of H.235 data, check the **H.235 pass through allowed** check box in the configuration settings of the following trunks and gateways:

- H.225 Trunk
- ICT Gatekeeper Control
- ICT non-Gatekeeper Control
- H.323 Gateway

For information about configuring trunks and gateways, see the *Administration Guide for Cisco Unified Communications Manager* .

About SIP Trunk Security Profile Setup

Unified Communications Manager Administration groups security-related settings for the SIP trunk to allow you to assign a single security profile to multiple SIP trunks. Security-related settings include device security mode, digest authentication, and incoming/outgoing transport type settings. You apply the configured settings to the SIP trunk when you choose the security profile in the **Trunk Configuration** window.

Installing Unified Communications Manager provides a predefined, nonsecure SIP trunk security profile for autoregistration. To enable security features for a SIP trunk, configure a new security profile and apply it to the SIP trunk. If the trunk does not support security, choose a nonsecure profile.

Only security features that the SIP trunk supports display in the security profile settings window.

SIP Trunk Security Profile Setup Tips

Consider the following information when you configure SIP trunk security profiles in Unified Communications Manager Administration:

- When you are configuring a SIP trunk, you must select a security profile in the Trunk Configuration window. If the device does not support security, apply a nonsecure profile.
- You cannot delete a security profile that is currently assigned to a device.
- If you change the settings in a security profile that is already assigned to a SIP trunk, the reconfigured settings apply to all SIP trunks that are assigned that profile.
- You can rename security files that are assigned to devices. The SIP trunks that are assigned the old profile name and settings assume the new profile name and settings.
- If you configured the device security mode prior to a Unified Communications Manager 5.0 or later upgrade, Unified Communications Manager creates a profile for the SIP trunk and applies the profile to the device.

Configure Trunk and Gateway SIP Security Task Flow

Complete the following task to configure Gateway and SIP security.

Procedure

	Command or Action	Purpose
Step 1	Set Up Secure Gateways and Trunks	Enable secure Gateways and Trunks for security.
Step 2	Set Up SIP Trunk Security Profile	Add, update, or copy a SIP trunk security profile.
Step 3	Apply SIP Trunk Security Profile	Enable a SIP trunk security profile to the trunk and apply security profile to a device .
Step 4	Synchronize SIP Trunk Security Profile with SIP Trunks	Synchronize SIP trunks with a SIP Trunk security profile.
Step 5	Allow SRTP Using Unified Communications Manager Administration	Configure the SRTP Allowed option for H.323 gateways and gatekeeper or non-gatekeeper controlled H.323/H.245/H.225 trunks or SIP trunks.

Set Up Secure Gateways and Trunks

Use this procedure in conjunction with the document, *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*, which provides information on how to configure your CiscoIOS MGCP gateways for security.

Procedure

Step 1 Verify that you have run the **utils ctl** command to set the cluster in mixed mode.

Step 2 Verify that you configured the phones for encryption.

Step 3 Configure IPSec.

Tip
You may configure IPSec in the network infrastructure, or you may configure IPSec between Unified Communications Manager and the gateway or trunk. If you implement one method to set up IPSec, you do not need to implement the other method.

Step 4 For H.323 IOS gateways and intercluster trunks, check the **SRTP Allowed** check box in Unified Communications Manager.

The **SRTP Allowed** check box displays in the **Trunk Configuration** or **Gateway Configuration** window. For information on how to display these windows, refer to the trunk and gateway chapters in the Administration Guide for Cisco Unified Communications Manager.

Step 5 For SIP trunks, configure the SIP trunk security profile and apply it to the trunk(s), if you have not already done so. Also, be sure to check the **SRTP Allowed** check box in the **Device** > **Trunk** > **SIP Trunk Configuration** window.

Caution
If you check the **SRTP Allowed** check box, we recommend that you use an encrypted TLS profile, so that keys and other security-related information does not get exposed during call negotiations. If you use a non-secure profile, SRTP will still work but the keys will be exposed in signaling and traces. In that case, you must ensure the security of the network between Unified Communications Manager and the destination side of the trunk.

Step 6 Perform security-related configuration tasks on the gateway.

For more information, see *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*.

Set Up SIP Trunk Security Profile

To add, update, or copy a SIP trunk security profile, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System** > **Security Profile** > **SIP Trunk Security Profile**.

Step 2 Perform one of the following tasks:

a) To add a new profile, click **Add New** in the **Find** window.

(You can also display a profile and then click **Add New**.)

The configuration window displays the default settings for each field.

b) To copy an existing security profile, locate the appropriate profile and click the **Copy** icon for that record in the Copy column.

(You can also display a profile and then click **Copy**.)

The configuration window displays the configured settings.

c) To update an existing profile, locate and display the appropriate security profile as described in Find SIP Trunk Security Profile.

The configuration window displays the current settings.

Step 3 Enter the appropriate settings as described in SIP Trunk Security Profile Settings.

Step 4 Click **Save**.

After you create the security profile, apply it to the trunk. If you configured digest authentication for SIP trunks, you must configure the digest credentials in the **SIP Realm** window for the trunk and **Application User** window for applications that are connected through the SIP trunk, if you have not already done so. If you enabled application-level authorization for applications that are connected through the SIP trunk, you must configure the methods that are allowed for the application in the **Application User** window, if you have not already done so.

SIP Trunk Security Profile Settings

The following table describes the settings for the SIP Trunk Security Profile.

Table 32: SIP Trunk Security Profile Configuration Settings

Setting	Description
Name	Enter a name for the security profile. When you save the new profile, the name displays in the **SIP Trunk Security Profile** drop-down list in the **Trunk Configuration** window.
Description	Enter a description for the security profile. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), or angle brackets (<>).

Setting	Description
Device Security Mode	From the drop-down list, choose one of the following options: • **Non Secure**—No security features except image authentication apply. A TCP or UDP connection opens to Unified Communications Manager. • **Authenticated**—Unified Communications Manager provides integrity and authentication for the trunk. A TLS connection that uses NULL/SHA opens. • **Encrypted**— Unified Communications Manager provides integrity, authentication, and signaling encryption for the trunk. A TLS connection that uses AES128/SHA opens for signaling. **Note** If the trunks are configured with Device Security Profile option selected as **Authenticated**, then Unified Communications Manager starts a TLS connection that uses NULL_SHA cipher (without data encryption). These trunks will not register or make calls if the destination devices do not support NULL_SHA cipher. For destination devices that do not support NULL_SHA cipher, the trunks should be configured with Device Security Profile option selected as **Encrypted**. With this device security profile, the trunks offer additional TLS ciphers that enables data encryption.
Incoming Transport Type	When Device Security Mode is Non Secure TCP+UDP specifies the transport type. When Device Security Mode is Authenticated or Encrypted, TLS specifies the transport type. **Note** The Transport Layer Security (TLS) protocol secures the connection between Unified Communications Manager and the trunk.
Outgoing Transport Type	From the drop-down list, choose the outgoing transport mode. When Device Security Mode is Non Secure, choose TCP or UDP. When Device Security Mode is Authenticated or Encrypted, TLS specifies the transport type. **Note** TLS ensures signaling integrity, device authentication, and signaling encryption for SIP trunks. **Note** You must use UDP as the outgoing transport type only when connecting SIP trunks between Unified Communications Manager systems and other application do not support TCP. Else, use TCP as the default option.

Setting	Description
Enable Digest Authentication	Check this check box to enable digest authentication. If you check this check box, Unified Communications Manager challenges all SIP requests from the trunk. Digest authentication does not provide device authentication, integrity or confidentiality. Choose a security mode of Authenticated or Encrypted to use these features. **Tip** Use digest authentication to authenticate SIP trunk users on trunks that are using TCP or UDP transport.
Nonce Validity Time	Enter the number of minutes (in seconds) that the nonce value is valid. The default value equals 600 (10 minutes). When the time expires, Unified Communications Manager generates a new value. **Note** A nonce value, a random number that supports digest authentication, gets used to calculate the MD5 hash of the digest authentication password.
Secure Certificate Subject or Subject Alternate Name	This field applies if you configured TLS for the incoming and outgoing transport type. For device authentication, enter the name of the Secure Certificate Subject or Subject Alternate Name certificate for the SIP trunk device. If you have a Unified Communications Manager cluster or if you use SRV lookup for the TLS peer, a single trunk may resolve to multiple hosts, which results in multiple Secure Certificate Subject or Subject Alternate Name for the trunks. If multiple Secure Certificate Subject or Subject Alternate Name exists, enter one of the following characters to separate the names: space, comma, semicolon, or a colon. You can enter up to 4096 characters in this field. **Tip** The subject name corresponds to the source connection TLS certificate. Ensure that subject names are unique for each subject name and port. You cannot assign the same subject name and incoming port combination to different SIP trunks. Example: SIP TLS trunk1 on port 5061 has Secure Certificate Subject or Subject Alternate Name my_cm1, my_cm2. SIP TLS trunk2 on port 5071 has Secure Certificate Subject or Subject Alternate Name my_cm2, my_cm3. SIP TLS trunk3 on port 5061 can have Secure Certificate Subject or Subject Alternate Name my_ccm4 but cannot have Secure Certificate Subject or Subject Alternate Name my_cm1.

Setting	Description
Incoming Port	Choose the incoming port. Enter a value that is a unique port number from 0-65535. The default port value for incoming TCP and UDP SIP messages specifies 5060. The default SIP secured port for incoming TLS messages specifies 5061. The value that you enter applies to all SIP trunks that use the profile. **Tip** All SIP trunks that use TLS can share the same incoming port; all SIP trunks that use TCP + UDP can share the same incoming port. You cannot mix SIP TLS transport trunks with SIP non-TLS transport trunk types on the same port. **Tip** If the incoming packet rate on a SIP trunk UDP port from a single IP address exceeds the configured SIP Trunk UDP Port Throttle Threshold during normal traffic, reconfigure the threshold. When a SIP trunk and SIP station share the same incoming UDP port, Unified Communications Manager throttles packets based on the higher of the two service parameter values. You must restart the Cisco CallManager service for changes to this parameter to take effect.
Enable Application Level Authorization	Application-level authorization applies to applications that are connected through the SIP trunk. If you check this check box, you must also check the **Enable Digest Authentication** check box and configure digest authentication for the trunk. Unified Communications Manager authenticates a SIP application user before checking the allowed application methods. When application level authorization is enabled, trunk-level authorization occurs first, and application-level authorization then occurs, which means that Unified Communications Manager checks the methods that are authorized for the trunk (in this security profile) before the methods that are authorized for the SIP application user in the **Application User Configuration** window. **Tip** Consider using application-level authorization if you do not trust the identity of the application or if the application is not trusted on a particular trunk; that is, application requests may come from a different trunk than you expect.
Accept Presence Subscription	If you want Unified Communications Manager to accept presence subscription requests that come via the SIP trunk, check this check box. If you checked the **Enable Application Level Authorization** check box, go to the **Application User Configuration** window and check the **Accept Presence Subscription** check box for any application users that are authorized for this feature. When application-level authorization is enabled, if you check the **Accept Presence Subscription** check box for the application user but not for the trunk, a 403 error message gets sent to the SIP user agent that is connected to the trunk.

Setting	Description
Accept Out-of-Dialog Refer	If you want Unified Communications Manager to accept incoming non-INVITE, Out-of-Dialog REFER requests that come via the SIP trunk, check this check box. If you checked the Enable Application Level Authorization check box, go to the **Application User Configuration** window and check the **Accept Out-of-Dialog Refer** check box for any application users that are authorized for this method.
Accept Unsolicited Notification	If you want Unified Communications Manager to accept incoming non-INVITE, unsolicited notification messages that come via the SIP trunk, check this check box. If you checked the **Enable Application Level Authorization** check box, go to the **Application User Configuration** window and check the **Accept Unsolicited Notification** check box for any application users that are authorized for this method.
Accept Replaces Header	If you want Unified Communications Manager to accept new SIP dialogs, which have replaced existing SIP dialogs, check this check box. If you checked the **Enable Application Level Authorization** check box, go to the **Application User Configuration** window and check the **Accept Header Replacement** check box for any application users that are authorized for this method.
Transmit Security Status	If you want Unified Communications Manager to transmit the security icon status of a call from the associated SIP trunk to the SIP peer, check this check box. Default: This box is not checked.
SIP V.150 Outbound SDP Offer Filtering	From the drop-down list, select one of the following filter options: • **Use Default Filter**—The SIP trunk uses the default filter that is indicated in the SIP V.150 Outbound SDP Offer Filtering service parameter. To locate the service parameter, go to **System** > **Service Parameters** > **Clusterwide Parameters (Device-SIP)** in Cisco Unified Communications Manager Administration. • **No Filtering**—The SIP trunk performs no filtering of V.150 SDP lines in outbound offers. • **Remove MER V.150**—The SIP trunk removes V.150 MER SDP lines in outbound offers. Select this option to reduce ambiguity when the trunk is connected to a pre-MER V.150 Unified Communications Manager. • **Remove Pre-MER V.150**—The SIP trunk removes any non-MER compliant V.150 lines in outbound offers. Select this option to reduce ambiguity when your cluster is contained in a network of MER-compliant devices that are incapable of processing offers with pre-MER lines.

Setting	Description
SIP V.150 Outbound SDP Offer Filtering	From the drop-down list, select one of the following filter options: • **Use Default Filter**—The SIP trunk uses the default filter that is indicated in the SIP V.150 Outbound SDP Offer Filtering service parameter. To locate the service parameter, go to **System** > **Service Parameters** > **Clusterwide Parameters (Device-SIP)** in Cisco Unified Communications Manager Administration. • **No Filtering**—The SIP trunk performs no filtering of V.150 SDP lines in outbound offers. • **Remove MER V.150**—The SIP trunk removes V.150 MER SDP lines in outbound offers. Select this option to reduce ambiguity when the trunk is connected to a pre-MER V.150 Unified Communications Manager. • **Remove Pre-MER V.150**—The SIP trunk removes any non-MER compliant V.150 lines in outbound offers. Select this option to reduce ambiguity when your cluster is contained in a network of MER compliant devices that are incapable of processing offers with pre-MER lines. **Note** You have to configure IOS on SIP for V.150 to make a secure call connection. For more information to configure IOS on Unified Communications Manager, see http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t4/mer_cg_15_1_4M.html.

Apply SIP Trunk Security Profile

You apply a SIP trunk security profile to the trunk in the **Trunk Configuration** window. To apply a security profile to a device, perform the following procedure:

Procedure

Step 1 Find the trunk, as described in the Administration Guide for Cisco Unified Communications Manager.

Step 2 After the **Trunk Configuration** window displays, locate the **SIP Trunk Security Profile** setting.

Step 3 From the **security profile** drop-down list, choose the security profile that applies to the device.

Step 4 Click **Save**.

Step 5 To reset the trunk, click **Apply Config**.
If you applied a profile enabling digest authentication for SIP trunks, you must configure the **digest credentials** in the **SIP Realm** window for the trunk. If you applied a profile enabling application-level authorization, you must configure the digest credentials and allowed authorization methods in the **Application User** window, if you have not already done so.

Synchronize SIP Trunk Security Profile with SIP Trunks

To synchronize SIP trunks with a SIP Trunk Security Profile that has undergone configuration changes, perform the following procedure, which will apply any outstanding configuration settings in the least-intrusive manner possible. (For example, you may not need to perform a reset/restart on some affected devices.)

Procedure

Step 1 Choose **System** > **Security Profile** > **SIP Trunk Security Profile**.

Step 2 Choose the search criteria to use.

Step 3 Click **Find**.

The window displays a list of SIP trunk security profiles that match the search criteria.

Step 4 Click the SIP trunk security profile to which you want to synchronize applicable SIP trunks.

Step 5 Make any additional configuration changes.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

The **Apply Configuration Information** dialog appears.

Step 8 Click **OK**.

Allow SRTP Using Unified Communications Manager Administration

The SRTP Allowed check box displays in the following configuration windows in Unified Communications Manager:

- H.323 Gateway Configuration window
- H.225 Trunk (Gatekeeper Controlled) Configuration window
- Inter-Cluster Trunk (Gatekeeper Controlled) Configuration window
- Inter-Cluster Trunk (Non-Gatekeeper Controlled) Configuration window
- SIP Trunk Configuration window

To configure the SRTP Allowed check box for H.323 gateways and gatekeeper or non-gatekeeper controlled H.323/H.245/H.225 trunks or SIP trunks, perform the following procedure:

Procedure

Step 1 Find the gateway or trunk, as described in the Unified Communications Manager.

Step 2 After you open the configuration window for the gateway/trunk, check the **SRTP Allowed** check box.

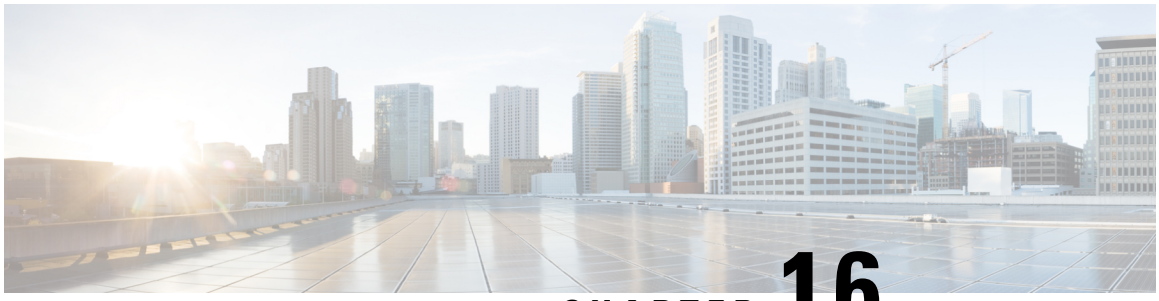
Caution

If you check the **SRTP Allowed** check box for a SIP trunk, we recommend that you use an encrypted TLS profile, so keys and other security-related information are not exposed during call negotiations. If you use a non-secure profile, SRTP will still work but the keys will be exposed in signaling and traces. In that case, you must ensure the security of the network between Unified Communications Manager and the destination side of the trunk.

Step 3 Click **Save**.

Step 4 To reset the device, click **Reset**.

Step 5 Verify that you configured IPSec correctly for H323. (For SIP, make sure you configured TLS correctly.)



CHAPTER 16

TLS Setup

- TLS Overview, on page 197
- TLS Prerequisites, on page 197
- TLS Configuration Task Flow, on page 198
- TLS Interactions and Restrictions, on page 203

TLS Overview

Transport Layer Security (TLS) provides secure and reliable signaling and data transfer between two systems or devices, by using secure ports and certificate exchange. TLS secures and controls connections among Unified Communications Manager-controlled systems, devices, and processes to prevent access to the voice domain.

TLS Prerequisites

Before you configure the minimum TLS version, make sure that your network devices and applications both support the TLS version. Also, make sure that they are enabled for TLS that you want to configure with Unified Communications Manager and IM and Presence Services. If you have any of the following products deployed, confirm that they meet the minimum TLS requirement. If they do not meet this requirement, upgrade those products:

- Skinny Client Control Protocol (SCCP) Conference Bridge
- Transcoder
- Hardware Media Termination Point (MTP)
- SIP Gateway
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment
- Cisco Unified Border Element (CUBE)
- Cisco Expressway

- Cisco TelePresence Conductor

You will not be able to upgrade conference bridges, Media Termination Point (MTP), Xcoder, Prime Collaboration Assurance, Prime Collaboration Provisioning, Cisco Unity Connection, Cisco Meeting Server, Cisco IP Phones, Cisco Room Devices, Cloud services like Fusion Onboarding Service (FOS), Common Identity Service, Smart License Manager (SLM), Push REST service, and Cisco Jabber and Webex App clients along with other third-party applications.



Note If you are upgrading from an earlier release of Unified Communications Manager, make sure that all your devices and applications support the higher version of TLS before you configure it. For example, Unified Communications Manager and IM and Presence Services, Release 9.x supports TLS 1.0 only.

TLS Configuration Task Flow

Complete the following tasks to configure Unified Communications Manager for TLS connections.

Procedure

	Command or Action	Purpose
Step 1	Set Minimum TLS Version, on page 199.	By default, Unified Communications Manager supports a minimum TLS version of 1.0. If your security needs require a higher version of TLS, reconfigure the system to use TLS 1.1 or 1.2.
Step 2	(Optional) Set TLS Ciphers, on page 199.	Configure the TLS cipher options that Unified Communications Manager supports.
Step 3	Configure TLS in a SIP Trunk Security Profile, on page 200.	Assign TLS connections to a SIP Trunk. Trunks that use this profile use TLS for signaling. You can also use the secure trunk to add TLS connections to devices, such as conference bridges.
Step 4	Add Secure Profile to a SIP Trunk, on page 200.	Assign a TLS-enabled SIP trunk security profile to a SIP trunk to allow the trunk to support TLS. You can use the secure trunk to connect resources, such as conference bridges.
Step 5	Configure TLS in a Phone Security Profile, on page 201.	Assign TLS connections to a phone security profile. Phones that use this profile use TLS for signaling.
Step 6	Add Secure Phone Profile to a Phone, on page 201.	Assign the TLS-enabled profile that you created to a phone.
Step 7	Add Secure Phone Profile to a Universal Device Template, on page 202.	Assign a TLS-enabled phone security profile to a universal device template. If you have the

	Command or Action	Purpose
		LDAP directory synchronization configured with this template, you can provision phones with security through the LDAP sync.

Set Minimum TLS Version

By default, Unified Communications Manager supports a minimum TLS version of 1.0. Use this procedure to reset the minimum supported TLS version for Unified Communications Manager and the IM and Presence Service to a higher version, such as 1.1 or 1.2.

Make sure that the devices and applications in your network support the TLS version that you want to configure. For details, see TLS Prerequisites, on page 197.

Procedure

Step 1 Log in to the **Command Line Interface**.

Step 2 To confirm the existing TLS version, run the **show tls min-version** CLI command.

Step 3 Run the **set tls min-version** <*minimum*> CLI command where <*minimum*> represents the TLS version.

For example, run **set tls min-version 1.2** to set the minimum TLS version to 1.2.

Note
Until Release 15SU1, perform **Step 3** on all Unified Communications Manager and IM and Presence Service Service cluster nodes.

Set TLS Ciphers

You can disable the weaker cipher, by choosing available strongest ciphers for the SIP interface. Use this procedure to configure the ciphers that Unified Communications Manager supports for establishing TLS connections.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 In **Security Parameters**, configure a value for the **TLS Ciphers** enterprise parameter. For help on the available options, refer to the enterprise parameter online help.

Step 3 Click **Save**.

Note
All TLS Ciphers will be negotiated based on client cipher preference

Configure TLS in a SIP Trunk Security Profile

Use this procedure to assign TLS connections to a SIP Trunk Security Profile. Trunks that use this profile use TLS for signaling.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **SIP Trunk Security Profile**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new SIP trunk security profile.
- Click **Find** to search and select an existing profile.

Step 3 In the **Name** field, enter a name for the profile.

Step 4 Configure the **Device Security Mode** field value to **Encrypted** or **Authenticated**.

Step 5 Configure both the **Incoming Transport Type** and **Outgoing Transport Type** field values to **TLS**.

Step 6 Complete the remaining fields of the **SIP Trunk Security Profile** window. For help on the fields and their configuration, see the online help.

Step 7 Click **Save**.

Add Secure Profile to a SIP Trunk

Use this procedure to assign a TLS-enabled SIP trunk security profile to a SIP trunk. You can use this trunk to create a secure connection to resources, such as conference bridges.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Trunk**.

Step 2 Click **Find** to search and select an existing trunk.

Step 3 For the **Device Name** field, enter a device name for the trunk.

Step 4 From the **Device Pool** drop-down list, choose a device pool.

Step 5 From the **SIP Profile** drop-down list, choose a SIP Profile.

Step 6 From the **SIP Trunk Security Profile** drop-down list, choose the TLS-enabled SIP Trunk Profile that you created in the previous task.

Step 7 In the **Destination** area, enter the destination IP address. You can enter up to 16 destination addresses. To enter additional destinations, click the (+) button.

Step 8 Complete the remaining fields in the **Trunk Configuration** window. For help with the fields and their configuration, see the online help.

Step 9 Click **Save**.

Note

If you are connecting the trunk to a secure device, you must upload a certificate for the secure device to Unified Communications Manager. For certificate details, see the **Certificates** section.

Configure TLS in a Phone Security Profile

Use this procedure to assign TLS connections to a Phone Security Profile. Phones that use this profile use TLS for signaling.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new profile.
- Click **Find** to search and select an existing profile.

Step 3 If you are creating a new profile, select a phone model and protocol, and click **Next**.

Note
If you want to use a universal device template and LDAP sync to provision security through the LDAP sync, select **Universal Device Template** as the **Phone Security Profile Type**.

Step 4 Enter a name for the profile.

Step 5 From the **Device Security Mode** drop-down list, select either **Encrypted** or **Authenticated**.

Step 6 (For SIP phones only) From the Transport Type, select **TLS**.

Step 7 Complete the remaining fields of the **Phone Security Profile Configuration** window. For help with the fields and their configuration, see the online help.

Step 8 Click **Save**.

Add Secure Phone Profile to a Phone

Use this procedure to assign the TLS-enabled phone security profile to a phone.

Note To assign a secure profile to a large number of phones at once, use the Bulk Administration Tool to reassign the security profile for them.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Phone**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new phone.
- Click **Find** to search and select an existing phone.

Step 3 Select the phone type and protocol and click **Next**.

Step 4 From the **Device Security Profile** drop-down list, assign the secure profile that you created to the phone.

Step 5 Assign values for the following mandatory fields:

- MAC address
- Device Pool
- SIP Profile
- Owner User ID
- Phone Button Template

Step 6 Complete the remaining fields of the **Phone Configuration** window. For help with the fields and their configuration, see the online help.

Step 7 Click **Save**.

Add Secure Phone Profile to a Universal Device Template

Use this procedure to assign a TLS-enabled phone security profile to a universal device template. If you have LDAP directory sync configured, you can include this universal device template in the LDAP sync through a feature group template and user profile. When the sync occurs, the secure profile is provisioned to the phones.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User/Phone Add** > **Universal Device Template**.

Step 2 Perform one of the following steps:

- Click **Add New** to create a new template.
- Click **Find** to search and select an existing template.

Step 3 For the **Name** field, enter a name for the template.

Step 4 From the **Device Pool** drop-down list, select a device pool.

Step 5 From the **Device Security Profile** drop-down list, select the TLS-enabled security profile that you created.

Note
The Phone Security Profile must have been created with **Universal Device Template** as the device type.

Step 6 Select a **SIP Profile**.

Step 7 Select a **Phone Button Template**.

Step 8 Complete the remaining fields of the **Universal Device Template Configuration** window. For help with the fields and their configuration, see the online help.

Step 9 Click **Save**.

Include the Universal Device template in an LDAP directory synchronization. For details on how to set up an LDAP Directory sync, see the “Configure End Users” part of the System Configuration Guide for Cisco Unified Communications Manager.

TLS Interactions and Restrictions

This chapter provides information about the TLS Interactions and Restrictions.

TLS Interactions

Table 33: TLS Interactions

Feature	Interaction
Common Criteria mode	You can enable Common Criteria mode along with configuration of minimum TLS version. If you do so, the applications continue to comply with Common Criteria requirements and disable TLS 1.0 secure connections at application level. When the common criteria mode is enabled, you can configure the minimum TLS version as either 1.1 or 1.2 for the applications. For details on Common Criteria mode, see the 'Compliance to Common Criteria' topic of the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

TLS Restrictions

The following table highlights issues that you may run into when implementing Transport Layer Security (TLS) version 1.2 on legacy phones, such as 79xx, 69xx, 89xx, 99xx, 39xx, and IP Communicator. To verify whether your phone supports secure mode in this release, see the Phone Feature List Report in Cisco Unified Reporting. The feature restrictions on legacy phones and the workaround to implement the feature is listed in the following table:

Note The workarounds are designed to get the impacted feature functioning in your system. However, they do not guarantee TLS 1.2 compliance for that feature.

Table 34: Transport Layer Security Version 1.2 Restrictions

Feature	Restriction
Legacy phones in Encrypted Mode	Legacy phones in Encrypted Mode do not work. There is no workaround.
Legacy phones in Authenticated Mode	Legacy phones in Authenticated Mode do not work. There is no workaround.

Feature	Restriction
IP Phone services using secure URLs based on HTTPS.	IP Phone services using secure URLs based on HTTPS do not work. Workaround to use IP Phone services: Use HTTP for all underlying service options. For example, corporate directory and personal directory. However, HTTP is not recommended as HTTP is not as secure if you need to enter sensitive data for features, such as Extension Mobility. The drawbacks of using HTTP include: • Provisioning challenges when configuring HTTP for legacy phones and HTTPS for supported phones. • No resiliency for IP Phone services. • Performance of the server handling IP phone services can be affected.
Extension Mobility Cross Cluster (EMCC) on legacy phones	EMCC is not supported with TLS 1.2 on legacy phones. Workaround: Complete the following tasks to enable EMCC: 1. Enable EMCC over HTTP instead of HTTPS. 2. Turn on mixed-mode on all Unified Communications Manager clusters. 3. Use the same USB eTokens for all Unified Communications Manager clusters.
Locally Significant Certificates (LSC) on legacy phones	LSC is not supported with TLS 1.2 on legacy phones. As a result, 802.1x and phone VPN authentication based on LSC are not available. Workaround for 802.1x: Authentication based on MIC or password with EAP-MD5 on older phones. However, those are not recommended. Workaround for VPN: Use phone VPN authentication based on end-user username and password.
Encrypted Trivial File Transfer Protocol (TFTP) configuration files	Encrypted Trivial File Transfer Protocol (TFTP) configuration files are not supported with TLS 1.2 on legacy phones even with Manufacturer Installed Certificate (MIC). There is no workaround.
CallManager certificate renewal causes legacy phones to lose trust	Legacy phones lose trust when the CallManager certificate is renewed. For example, a phone cannot get new configurations after renewing the certificate. This is applicable only in Unified Communications Manager 11.5.1 Workaround: To prevent legacy phones from losing trust, complete the following steps: 1. Before you enable the CallManager certificate, set the **Cluster For Roll Back to Pre 8.0** enterprise parameter to **True**. By default, this setting disables the security. 2. Temporarily allow TLS 1.0 (multiple Unified Communications Manager reboots).

Feature	Restriction
Connections to non-supported versions of Cisco Unified Communications Manager	TLS 1.2 connections to older versions of Unified Communications Manager that do not support the higher TLS version do not work. For example, a TLS 1.2 SIP trunk connection to Unified Communications Manager Release 9.x does not work because that release does not support TLS 1.2. You can use one of the following workarounds: • Workaround to enable connections: Use nonsecure trunks, although this is not a recommended option. • Workaround to enable connections while using TLS 1.2: Upgrade the non-supported version to a release that does support TLS 1.2.
Certificate Trust List (CTL) Client	CTL client does not support TLS 1.2. You can use one of the following workarounds: • Temporarily allow TLS 1.0 when using the CTL client and then move the Cluster to Common Criteria mode. Configure Minimum TLS to 1.1 or 1.2 • Migrate to the Tokenless CTL by using the CLI Command **utils ctl set-cluster mixed-mode** in Common Criteria mode. Configure Minimum TLS to 1.1 or 1.2
Address Book Synchronizer	There is no workaround.

Cisco Unified Communications Manager Ports Affected by Transport Layer Security Version 1.2

The following table lists the Unified Communications Manager Ports Affected By TLS Version 1.2:

Table 35: Cisco Unified Communications Manager Ports Applicable for Transport Layer Security Version 1.2

Application	Protocol	Destination / Listener	Cisco Unified Communications Manager Operating in Normal mode			Cisco Unified Communications Manager Operating in Common Criteria Mode		
			Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2
Tomcat	HTTPS	443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS v1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
SCCP - SEC - SIG	Signalling Connection Control Part (SCCP)	2443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2

Application	Protocol	Destination / Listener	Cisco Unified Communications Manager Operating in Normal mode			Cisco Unified Communications Manager Operating in Common Criteria Mode		
			Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2
CTL-SERV	Proprietary	2444	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
Computer Telephony Integration (CTI)	Quick Buffer Encoding (QBE)	2749	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
CAPF-SERV	Transmission Control Protocol (TCP)	3804	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
Intercluster Lookup Service (ILS)	Not applicable	7501	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
Administrative XML (AXL)	Simple Object Access Protocol (SOAP)	8443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
High Available-Proxy (HA-Proxy)	TCP	9443	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.2	TLS 1.2
SIP-SIG	Session Initiation Protocol (SIP)	5061 (configurable)	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
HA Proxy	TCP	6971, 6972	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
Cisco Tomcat	HTTPS	8080, 8443	8443: TLS 1.0, TLS 1.1, TLS 1.2	8443: TLS 1.1, TLS 1.2	8443: TLS 1.2	TLS 1.1	8443: TLS 1.1, TLS 1.2	8443: TLS 1.2

Application	Protocol	Destination / Listener	Cisco Unified Communications Manager Operating in Normal mode			Cisco Unified Communications Manager Operating in Common Criteria Mode		
			Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2
Trust Verification Service (TVS)	Proprietary	2445	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2

Instant Messaging and Presence Service Ports Affected by Transport Layer Security Version 1.2

The following table lists the IM and Presence Service Ports Affected By Transport Layer Security Version 1.2:

Table 36: Instant Messaging & Presence Ports Applicable for Transport Layer Security Version 1.2

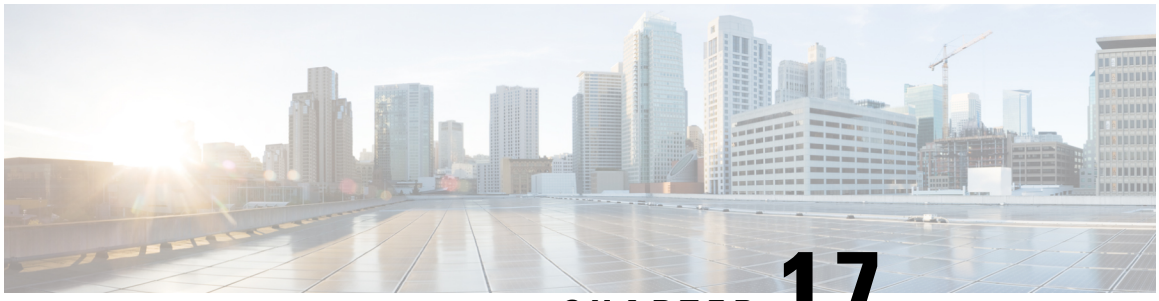
Destination/Listener	Instant Messaging & Presence Operating in Normal mode			Instant Messaging & Presence Operating in Common Criteria mode		
	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2	Minimum TLS version 1.0	Minimum TLS version 1.1	Minimum TLS version 1.2
443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
5061	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
5062	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
5280	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
8083	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2
8443	TLS 1.0, TLS 1.1, TLS 1.2	TLS 1.1, TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1, TLS 1.2	TLS 1.2



PART III

User Security

- Identity Management, on page 211
- Credential Policies, on page 217
- Contact Search Authentication, on page 225



CHAPTER 17

Identity Management

- User Security Overview, on page 211
- Identity Management Overview, on page 212

User Security Overview

User Access

User Security consists of the platforms which protect our users, endpoints, and their online activity to more efficiently correlate threats. As users are increasingly logging in to networks through their personal devices, securing personal devices are as important as securing company owned devices.

For more information on Users and Security, see **Configure End Users** in System Configuration Guide for Cisco Unified Communications Manager and **Manage Security** in Administration Guide for Cisco Unified Communications Manager.

Assign end users to Access Control Groups associated to Roles to manage User Access in Unified Communications Manager.

Access Control essentially allows the right people to access your network while simultaneously blocking those people who shouldn't be. Access Control refers to the visibility of who and what is accessing your network. It ensures that the right people are using the right devices, to access the right resources. Access Control regulates the spread of information and prevents unwanted visitors gaining access to your data.

Roles and Access Control Groups provide multiple levels of security to Unified Communications Manager. Each role defines a set of permissions for a specific resource within Unified Communications Manager. End Users get access permissions defined by the role when you assign roles and then assign end users to an access control group.

Upon installation, Unified Communications Manager comes with predefined default roles assigned to predefined default access control groups. You can assign end users to the default access control groups, or you can customize access settings by setting up new access control groups and roles.

For more information on Users and Access Control, see **Configure End Users** in System Configuration Guide for Cisco Unified Communications Manager and **Manage Users** in Administration Guide for Cisco Unified Communications Manager.

Identity Management

Use SAML Single Sign-On (SSO) to access a defined set of Cisco applications after signing into one of those applications. SAML describes the exchange of security-related information between trusted business partners. It's an authentication protocol used by service providers (such as Cisco Unified Communications Manager) to authenticate a user. With SAML, an identity provider and a service provider exchanges security authentication information. This feature provides secure mechanisms to use common credentials and relevant information across various applications. For more information on Identity management, see Manage SAML Single Sign-On in Administration Guide for Cisco Unified Communications Manager.

Contact Search Authentication

Contact Search Authentication requires you to authenticate yourselves before searching the directory for other users. Navigate to the following topics for more information on Contact Search Authentication.

1. Confirm Phone Support for Contact Search Authentication, on page 226
2. Enable Contact Search Authentication, on page 226
3. Configure Secure Directory Server for Contact Search, on page 226

Identity Management Overview

Identity Management is an essential component of your Cisco Collaboration deployment. Because Identity is often the main target for hackers, it’s essential to configure secure authentication and authorization services in order to secure your system. Cisco Unified Communications Manager provides a number of options for managing identity, authentication and authorization for services.

- SAML SSO Deployment with Third-Party Identity Provider
- LDAP authentication
- Local DB Authentication

SAML SSO Deployment

SAML SSO improves your enterprise security, while improving productivity at the same time. Using the SAML 2.0 protocol, SAML SSO connects your Cisco Collaboration infrastructure to a third-party Identity Provider for secure login and authentication services for administrator and client logins across domains and across products. Worker productivity is improved as the Identity Provider stores a single login—once you login successfully to one of your Collaboration applications, you can access any of them without having to login again.

SAML SSO provides the following benefits to your Identity Framework:

- Reduces password fatigue by removing the need for entering different user name and password combinations.
- Transfers the authentication from your system that hosts the applications to a third party system.
- Protects and secures authentication information. SAML SSO provides encryption functions to protect authentication information passed between the IdP, service provider, and user. SAML SSO can also hide authentication messages passed between the IdP and the service provider from any external user.

- Improves productivity because you spend less time re-entering credentials for the same identity.
- Reduces costs as fewer help desk calls are made for password reset, thereby leading to more savings.

Trust Relationship with IdP

SAML SSO Deployments rely on the creation of a trust relationship between a Service Provider (Cisco Unified Communications Manager) and the third-party Identity Provider. You can configure a SAML SSO relationships using one of two SSO modes:

- Per Node agreement—The UC metadata zip file contains separate XML files for each node
- Per Cluster agreement—A single metadata file for the cluster

This trust relationship is created through an initial exchange of metadata files. The Cisco UC metadata file is an XML file which contains the following information:

- A unique identifier
- Organization
- Expiration time for this information
- Caching period
- XML signature of this information
- Contact persons
- Unique identifier of the entity (entity ID)
- Description of SAML role of this SAML instance (identity provider, service provider, and so forth)

Authorization

Once authentication is provided by the IdP, user access to Cisco Unified Communications Manager resources is determined by locally configured access control groups and the role permissions that those groups provide.

SAML SSO Configuration and Identity Provider Requirements

For more detailed information on SAML SSO, including configuration information and requirements for Identity Providers, see the *SAML SSO Deployment Guide for Cisco Unified Communications Applications*.

LDAP Authentication

If you have not deployed SAML SSO, and you have users synced against a company LDAP Directory, LDAP Authentication lets you authenticate user passwords against the credentials that are stored in the company LDAP directory. This option enables the Identity Management System (IMS) library on Cisco Unified Communications Manager to use the company LDAP directory to authenticate user passwords for LDAP synchronized users.

When end users login to the Self-Care Portal, they enter their company password (for example, their AD password), as configured in the company LDAP directory.

When this option is configured:

- End user passwords of users imported from LDAP are authenticated against the corporate directory by a simple bind operation.
- End user passwords for local users are authenticated against the Unified CM database.
- Application user passwords are authenticated against the Unified CM database.
- End user PINs are authenticated against the Unified CM database.

Configure LDAP Authentication

Use this procedure to enable LDAP Authentication for end user passwords. You can add LDAP Authentication to an existing LDAP Directory sync.

Note If the LDAP certificate is renewed, the administrator must restart the SSOP-Tomcat service for the user authentication to go through.

Before you begin

This procedure assumes you already have an existing LDAP Directory sync configured. If you have not yet configured an LDAP Directory sync, refer to the System Configuration Guide for Cisco Unified Communications Manager to set one up.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Authentication**.

Step 2 Check the **Use LDAP Authentication for End Users** check box.

Step 3 For the **LDAP Manager Distinguished Name**, enter the user ID of the LDAP Manager who is an administrative user that has access rights to the LDAP directory in question.

Step 4 Enter the **Password** and **Confirm the Password**.

Step 5 Enter the LDAP Directory server address information.

Step 6 Complete the remaining fields in the **LDAP Authentication Configuration** window.

Step 7 Click **Save**.

Local Database Authentication

Local Authentication against the Cisco Unified Communications Manager database is required for end users if you are not deploying SAML SSO with a third-party Identity provider, or if you do not have LDAP Authentication configured. With this option, user passwords are stored in the local database and are managed via the End User Configuration.

For both application users and end user PINs, local database authentication is always used to manage authentication. The following table highlights the three main password types and how they are managed.

Table 37:

Password Types	Credential Management
End User Passwords	If you are not using SAML SSO or LDAP authentication, end user passwords are managed locally in the End User Configuration window for individual end users. All passwords can be updated via the End User Configuration. End users can edit their own passwords via the Self-Care Portal.
End User PINs	Irrespective of whether you have SAML SSO or LDAP Authentication deployed, end user PINs are always managed in End User Configuration window of Cisco Unified CM Administration. As administrator, you can edit existing end user PINs via the End User Configuration window.
Application User Passwords	Irrespective of whether you have SAML SSO or LDAP Authentication deployed, application user passwords are stored in the local database and are managed in the Application User Configuration window of Cisco Unified CM Administration.

Note All local passwords and PINs are stored in the database in an encrypted format.

OAuth Framework

The OAuth Authorization Framework is defined by IETF under RFC 6749. The OAuth 2.0 authorization protocol lets a resource owner (for example, Cisco Unified Communications Manager) authorize a third-party application to obtain limited access to an HTTP service. With Cisco Unified Communications Manager, the OAuth framework uses access tokens to provide access and refresh tokens to provide access to resources over the life of the token. OAuth eliminates the need for web sites to ask for passwords when you are attempting to access information. With OAuth, the resource owner authorizes a client to access resources on a server.

Cisco Jabber clients use OAuth Refresh Logins to obtain access to resources from Cisco Unified Communications Manager. After an initial login, OAuth access tokens and refresh tokens provide seamless access to resources over the life of the tokens.

OAuth Refresh Logins

With OAuth Refresh Logins, short-lived access tokens let Jabber authenticate, providing access while the token is valid the life of the token (the default lifespan for an access token is 60 minutes). The longer-lived refresh tokens provide Jabber with new access tokens as the old access tokens expire. So long as the refresh token is valid (the default life is 60 days) the Jabber client can obtain new access tokens dynamically, thereby providing seamless acess, without the user having to reauthenticate.

Every time when the OAuth token reaches 75% of its lifespan, the enduser application requests for new access token and CUCM will provide new access token to authorize the end user. If the refresh token reaches 100% of its lifespan, they will need to reauthenticate before they can generate new access tokens.

SIP OAuth Mode

SIP OAuth Mode enhances the OAuth framework, enabling the usage of OAuth access tokens and refresh tokens for SIP lines, thereby removing the need to install LSC certificates on Jabber clients. SIP OAuth Mode allows for secure signing and media for Jabber without CAPF. Token validation is completed during SIP registration. In this mode, Jabber can perform media and signaling encryption without an LSC, and without the need to enable mixed-mode on Unified CM.

Regenerating Keys for OAuth

If you believe the keys that are used for signing and encrypting OAuth tokens have been compromised, use the following CLI commands to generate new keys. The signing key is asymmetric and RSA-based whereas the encryption key is a symmetric key.

- `set key regen authz encryption`
- `set key regen authz signing`



Note When OAuth keys are regenerated, you must restart the Cisco XCP Authentication Service on all IM and Presence nodes for Jabber OAuth login to work.

Configure SIP OAuth Mode

For detailed procedures on how to configure SIP OAuth Mode so that you can use OAuth Refresh Logins for SIP lines, refer to the "SIP OAuth Mode" chapter of the *Feature Configuration Guide for Cisco Unified Communications Manager.*

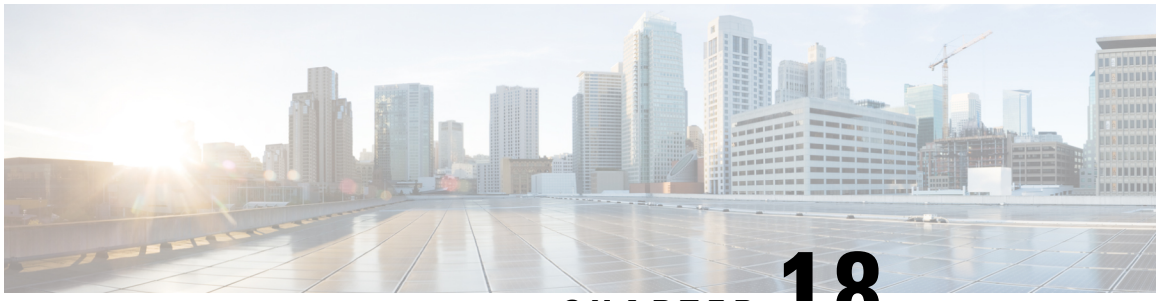
Revoke Existing OAuth Refresh Tokens

Use an AXL API to revoke existing OAuth refresh tokens. For example, if an employee leaves your company, you can use this API to revoke that employee's current refresh token so that they cannot obtain new access tokens and will no longer be able to log in to the company account. The API is a REST-based API that is protected by AXL credentials. You can use any command-line tool to invoke the API. The following command provides an example of a cURL command that can be used to revoke a refresh token:

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

where:

- `admin:password` is the login ID and password for the Cisco Unified Communications Manager administrator account.
- `UCMaddress` is the FQDN or IP address of the Cisco Unified Communications Manger publisher node.
- `end_user` is the user ID for the user for whom you want to revoke refresh tokens.



CHAPTER 18

Credential Policies

- Credential Policy Overview, on page 217
- Configure Default Credential Policy, on page 219
- Edit User Credentials or Credential Policy, on page 220
- Enable PIN Synchronization , on page 220
- Monitor Authentication Activity, on page 221
- Configuring Credential Caching, on page 222
- Manage Session Termination, on page 223

Credential Policy Overview

Credential policies control the authentication process for resources in Unified Communications Manager. A credential policy defines password requirements and account lockout details such as failed login attempts, expiration periods and lockout durations for end user passwords, end user PINs, and application user passwords. Credential policies can be assigned broadly to all accounts of a specific credential types, such as all end user PINs, or they can be customized for a specific application user, or end user.

Credential Types

In Credential Policy Configuration, you can configure a new credential policy and then apply that new policy as the default credential policy for each of the following three credential types:

- End User PINs
- End User Passwords
- Application User Passwords

You can also apply the credential policy to a specific end user PIN, end user password, or application user password.

Credential Policies with LDAP Authentication Enabled

If your system is configured for LDAP Authentications with the corporate directory:

- With LDAP Authentication enabled, credential policies do not apply to end user passwords.
- Credential policies do apply to end user PINs and application user passwords, irrespective of whether LDAP Authentication is enabled. These password types use local authentication.

Note Credential policies do not apply to operating system users or CLI users. These administrators use standard password verification procedures that the operating system supports.

Trivial Passwords

The system can be configured to check for trivial passwords and PINs. A trivial password is a credential that can be easily hacked, such as a password that be guessed easily, such as using ABCD as your password or 123456 as your PIN.

Non-trivial passwords meet the following requirements:

- The password must contain at least one uppercase letter, one lowercase letter, one numeric character, and one special character.
- Must not use a character or number more than three times consecutively.
- Must not repeat or include the alias, username, or extension.
- Cannot consist of consecutive characters or numbers. For example, passwords such as 654321 or ABCDEFG are not allowed.

PINs can contain digits (0-9) only. A non-trivial PIN meets the following criteria:

- Must not use the same number more than two times consecutively.
- Must not repeat or include the user extension, mailbox, or the reverse of the user extension or mailbox.
- Must contain three different numbers. For example, a PIN such as 121212 is trivial.
- Must not match the numeric representation (that is, dial by name) for the first or last name of the user.
- Must not contain groups of repeated digits, such as 408408, or patterns that are dialed in a straight line on a keypad, such as 2580, 159, or 753.

JTAPI and TAPI Support for Credential Policies

Because the Cisco Unified Communications Manager Java telephony applications programming interface (JTAPI) and telephony applications programming interface (TAPI) support the credential policies that are assigned to application users, developers must create applications that respond to the password expiration, PIN expiration, and lockout return codes for credential policy enforcement.

Applications use an API to authenticate with the database or corporate directory, regardless of the authentication model that an application uses.

For more information about JTAPI and TAPI for developers, see the developer guides at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html.

Configure Default Credential Policy

Use this procedure to configure clusterwide default credential policies that get applied to newly provisioned users. You can apply a separate credential policy for each of the following credential types:

- Application User Passwords
- End User Passwords
- End User PINs

Procedure

Step 1 Configure settings for a credential policy:

a) From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy**.
b) Do either of the following:
   - Click **Find** and select an existing credential policy.
   - Click **Add New** to create a new credential policy.
c) If you want the system to check for easily hacked passwords such as ABCD or 123456, check the **Check for Trivial Passwords** check box.
d) Complete the fields in the **Credential Policy Configuration** window. For help with the fields and their settings, see the online help.
e) Click **Save**.
f) If you want to create a different credential policy for one of the other credential types, repeat these steps.

Step 2 Apply the credential policy to one of the credential types:

a) From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy Default**.
b) Select the credential type to which you want to apply your credential policy.
c) From the **Credential Policy** drop-down, select the credential policy that you want to apply for this credential type. For example, you might select the credential policy that you created.
d) Enter the default passwords in both the **Change Credential** and **Confirm Credential** fields. Users have to enter these passwords at next login.
e) Configure the remaining fields in the **Credential Policy Default Configuration** window. For help with the fields and their settings, see the online help.
f) Click **Save**.
g) If you want to assign a credential policy for one of the other credential types, repeat these steps.

Note For individual users, you can also assign a policy to a specific user credential from the **End User Configuration** window or **Application User Configuration** window for that user. Click the **Edit Credential** button that is adjacent to the credential type (password or PIN) to open the **Credential Configuration** settings for that user credential.

Edit User Credentials or Credential Policy

Use this procedure if you want to edit an existing user credential or to edit the policy that is assigned to a user credential. After resetting the credential, you can apply a rule such as mandating that the user update credentials at next login. You may want to do this if:

- You have local DB authentication configured, and you want to reset an end user password
- You want to reset an end user PIN or application user password
- You want to change the credential policy that is assigned to a specific user credential

Procedure

Step 1 From Cisco Unified CM Administration, choose one of the following:

- For end user passwords and PINs, choose **User Management** > **End Users**.
- For application user passwords, choose **User Management** > **Application Users**.

Step 2 Click **Find** and select the appropriate user.

Step 3 If you want to change an existing password or PIN, enter the new credential in the **Password**/**Confirm Password** or **PIN**/**Confirm PIN** fields and click **Save**.

Step 4 If you want to change the credential policy that is assigned to a user credential, or if you want to apply rules such as requiring that the user enter a new password or PIN at next login:

a) Click the **Edit Credential** button that is adjacent to the **Password** or **PIN**. The **Credential Configuration** window opens for that user credential.
b) Optional. To assign a new credential policy, select the policy from the **Authentication Rule** drop-down.
c) Optional. Check the **User Must Change at Next Login** check box if you want the user to update the password or PIN at the next login.
d) Complete the remaining fields. Refer to the online help for field descriptions.
e) Click **Save**.

Enable PIN Synchronization

Use this procedure to enable PIN synchronization so that the end users can log in to Extension Mobility, Conference Now, Mobile Connect, and the Cisco Unity Connection Voicemail using the same PIN.

Note The pin synchronization between Cisco Unity Connection and Cisco Unified Communications Manager is successful, only when Cisco Unified Communications Manager publisher database server is running and completes its database replication. Following error message is displayed when the pin synchronization fails on Cisco Unity Connection: `Failed to update PIN on CUCM. Reason: Error getting the pin.`

If the PIN Synchronization is enabled and the end user changes the pin, then pin is updated in Cisco Unified Communications Manager. This happens only when the pin update is successful in at least one of the configured Unity Connection Application servers.

Note For PIN Synchronization to take effect, administrators must force the users to change their PIN after successfully enabling the feature.

Before you begin

This procedure assumes that you already have your application server connection to Cisco Unity Connection setup. If not, for more information on how to add a new application server, see the Related Topics section.

To enable PIN Synchronization feature, you need to first upload a valid certificate for the Cisco Unity Server connection from the Cisco Unified OS Administration page to the Cisco Unified Communications Manager tomcat-trust. For more information on how to upload the certificate, see the "Manage Security Certificates" chapter in the *Administration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

The user ID in the Cisco Unity Connection Server must match the user ID in Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Application Servers**.

Step 2 Select the application server that you set up for Cisco Unity Connection.

Step 3 Check the **Enable End User PIN Synchronization** check box.

Step 4 Click **Save**.

Related Topics

Configure Application Servers

Monitor Authentication Activity

The system shows the most current authentication results, such as last hack attempt time, and counts for failed logon attempts.

The system generates log file entries for the following credential policy events:

- Authentication success
- Authentication failure (bad password or unknown)
- Authentication failure because of
  - Administrative lock
  - Hack lock (failed logon lockouts)
  - Expired soft lock (expired credential)
  - Inactive lock (credential not used for some time)
  - User must change (credential set to user must change)
  - LDAP inactive (switching to LDAP authentication and LDAP not active)
- Successful user credential updates
- Failed user credential updates



Note If you use LDAP authentication for end user passwords, LDAP tracks only authentication successes and failures.

All event messages contain the string “ims-auth” and the user ID that is attempting authentication.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End Users**.

Step 2 Enter search criteria, click **Find**, and then choose a user from the resulting list.

Step 3 Click **Edit Credential** to view the user's authentication activity.

What to do next

You can view log files with the Cisco Unified Real-Time Monitoring Tool (Unified RTMT). You can also collect captured events into reports. For detailed steps about how to use Unified RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Configuring Credential Caching

Enable credential caching to increase system efficiency. Your system does not have to perform a database lookup or invoke a stored procedure for every single login request. An associated credential policy is not enforced until the caching duration expires.

This setting applies to all Java applications that invoke user authentication.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Perform the following tasks as needed:

- Set the **Enable Caching** enterprise parameter to **True**. With this parameter enabled, Cisco Unified Communications Manager uses cached credentials for up to 2 minutes.
- Set the **Enable Caching** enterprise parameter to **False** to disable caching, so that the system does not use cached credentials for authentication. The system ignores this setting for LDAP authentication. Credential caching requires a minimal amount of additional memory per user.

Step 3 Click **Save**.

Manage Session Termination

Administrators can use this procedure to terminate a user's active sign-in session specific to each node.



Note

- An administrator with privilege level 4 only can terminate the sessions.
- Session Management terminates the active sign-in sessions on a particular node. If the administrator wants to terminate all the user sessions across different nodes, then the administrator has to sign-in to each node and terminate the sessions.

This applies to the following interfaces:

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Cisco Unified Communications Self Care Portal
- Cisco Unified CM IM and Presence Administration
- Cisco Unified IM and Presence Serviceability
- Cisco Unified IM and Presence Reporting

Procedure

Step 1 From Cisco Unified OS Administration or Cisco Unified IM and Presence OS Administration, choose **Security** > **Session Management**.

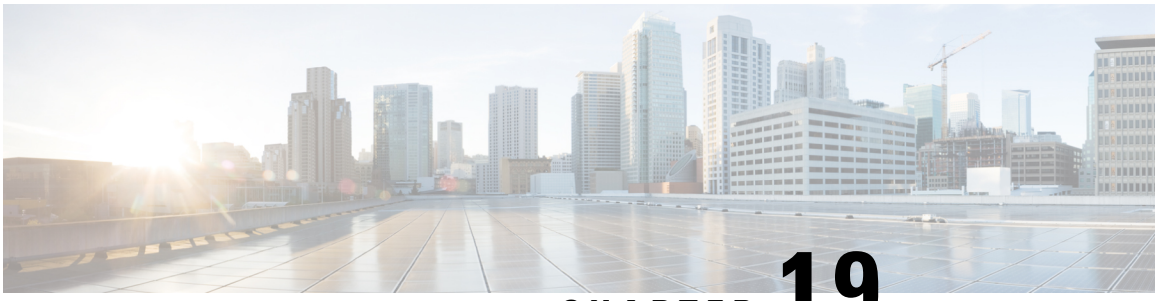
The Session Management window is displayed.

Step 2 Enter the user ID of the active signed-in user in the **User ID** field.

Step 3 Click **Terminate Session**.

Step 4 Click **OK**.

If the terminated user refreshes the signed-in interface page, then the user is signed out. An entry is made in the audit log and it displays the terminated `userID`.



CHAPTER 19

Contact Search Authentication

- Contact Search Authentication Overview, on page 225
- Contact Search Authentication Task Flow, on page 225

Contact Search Authentication Overview

Contact Search Authentication provides additional security for your system by ensuring that users whom access the company directory must authenticate themselves. This feature secures the directory from being accessed by external parties.

Contact Search Authentication Task Flow

Complete the following tasks to set up Contact Search Authentication in Unified Communications Manager. When this feature is configured, users must authenticate themselves before searching the directory for other users.

Procedure

	Command or Action	Purpose
Step 1	Confirm Phone Support for Contact Search Authentication, on page 226	Confirm that your phones support this feature. Run the **Unified CM Phone Feature List** report in Cisco Unified Reporting to get a list of phone models that support the feature.
Step 2	Enable Contact Search Authentication, on page 226	Configure Unified Communications Manager for Contact Search Authentication.
Step 3	Configure Secure Directory Server for Contact Search, on page 226	Use this procedure to configure Unified Communications Manager with the URL to which phone users are directed when they search the directory for other users.

Confirm Phone Support for Contact Search Authentication

Confirm that the phones in your deployment support contact search authentication. Run a Phone Feature List report to obtain a full list of phone models that support the feature.

Procedure

Step 1 From Cisco Unified Reporting, click **System Reports**.

Step 2 Select **Unified CM Phone Feature**.

Step 3 Click the **Unified CM Phone Feature** report.

Step 4 Leave the **Product** field at the default value.

Step 5 From the **Feature** drop-down, choose **Authenticated Contact Search**.

Step 6 Click **Submit**.

Enable Contact Search Authentication

Use this procedure on Unified Communications Manager to configure contact search authentication for phone users.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run the **utils contactsearchauthentication status** command to confirm the contact search authentication setting on this node.

Step 3 If you need to configure contact search authentication:

- To enable authentication, run the **utils contactsearchauthentication enable** command.
- To disable authentication, run the **utils contactsearchauthentication disable** command.

Step 4 Repeat this procedure on all Unified Communications Manager cluster nodes.

Note
You must reset phones in order for the changes to take effect.

Configure Secure Directory Server for Contact Search

Use this procedure to configure Unified Communications Manager with the directory server URL to which UDS sends user search requests. The default value is `https://<cucm-fqdn-or-ip>:port/cucm-uds/users`.

Note The default UDS port is 8443. When contact search authentication becomes enabled, the default UDS port switches to 9443. If you then disable contact search authentication, you must change the UDS port back to 8443 manually.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**.

Step 2 In the **Secure Contact Search URL** text box, enter the URL for secure UDS directory requests.

Note
We recommend that for the URL, you choose a node that is not running the Cisco TFTP service. The CiscoTFTP and UDS services may disrupt each other if either service gets restarted.

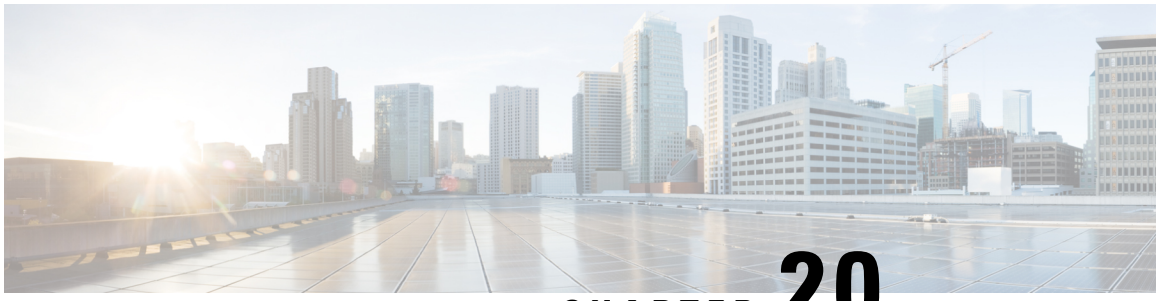
Step 3 Click **Save**.



PART IV

Advanced System Security

- FIPS Mode Setup, on page 231
- V.150 Minimum Essential Requirements, on page 245
- IPSec Setup, on page 255
- Authentication and Encryption Setup for CTI, JTAPI, and TAPI, on page 257
- Secure Recording and Monitoring, on page 271
- VPN Client, on page 273
- Operating System and Security Hardening, on page 287



CHAPTER 20

FIPS Mode Setup

- FIPS Setup, on page 231
- Enhanced Security Mode, on page 239
- Common Criteria Mode, on page 241

FIPS Setup

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

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

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

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

Unified Communications Manager

- Reboots
- Runs certification self-tests at startup
- Performs the cryptographic modules integrity check
- Regenerates the keying materials

When you enable FIPS 140-2 mode. At this point, Unified Communications Manager operates in the FIPS 140-2 mode.

FIPS requirements include the following:

- Performance of startup self-tests
- Restriction to a list of approved cryptographic functions

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



Important These versions are applicable for Release 14 and 14SU1 only.

- CiscoSSL 1.0.2y.6.2.403 with FIPS Module CiscoSSL FOM 6_2_0
- CiscoJ 5.3.7
- OpenSSH 7.5.14i
- Libreswan
- NSS



Important These versions are applicable for Release 14SU2 and SU3 only.

- CiscoSSL 1.1.1n.7.2.390 with FIPS Module CiscoSSL FOM 7.2a
- CiscoSSH - 1.9.29
- BC FIPS - 1.0.2.3.jar
- BCTLS FIPS - 1.0.12.3.jar
- BCPKIX FIPS -1.0.5.jar
- Libreswan
- NSS



Important These versions are applicable for Release 14SU4 only.

- CiscoSSL 1.1.1v.7.2.539 with FIPS Module CiscoSSL FOM 7.2a
- CiscoSSH - 1.11.34
- BC FIPS - 1.0.2.3.jar
- BCTLS FIPS - 1.0.12.3.jar
- BCPKIX FIPS - 1.0.5.jar
- Strongswan - 5.9.8



Important These versions are applicable for Release 14SU5 only.

- CiscoSSL - 1.1.1v.7.2.539 with FIPS Module CiscoSSL FOM 7.2a
- CiscoSSH - 1.13.48.11

- BC FIPS - 1.0.2.3
- BCTLS FIPS - 1.0.12.3
- BCPKIX FIPS - 1.0.5
- Strongswan - 5.9.8

Important These versions are applicable for Release 14SU6 only.

- CiscoSSL - 1.1.1v.7.2.539 with FIPS Module CiscoSSL FOM 7.2a
- CiscoSSH - 1.13.48.11
- BC FIPS - 1.0.2.3
- BCTLS FIPS - 1.0.12.3
- BCPKIX FIPS - 1.0.5
- Strongswan - 5.9.8

Note For more information on the Unified Communications Manager upgrade, see the 'COP File Installation Guidelines' section in the Installation Guide for Cisco Unified Communications Manager and the IM and Presence Service.

You can perform the following FIPS-related tasks:

- Enable FIPS 140-2 mode
- Disable FIPS 140-2 mode
- Check the status of FIPS 140-2 mode

Note

- By default, your system is in the non-FIPS mode. You must enable it.
- Ensure that the security password length is a minimum of 14 characters before you upgrade to FIPS, Common Criteria, or Enhanced Security mode on the cluster. Update the password even if the prior version was FIPS enabled.

If you generate a Self-Signed Certificate or Certificate Signing Request (CSR) on FIPS mode, certificates must be encrypted using the SHA256 hashing algorithm and can't select SHA1.

Enable FIPS 140-2 Mode

Consider the following before you enable FIPS 140-2 mode on Unified Communications Manager:

- When you switch from non-FIPS to FIPS mode, the MD5 and DES protocols aren't functional.

- In single-server clusters, because certificates are regenerated, you need to run the CTL Client or apply the Prepare Cluster for Rollback to pre-8.0 enterprise parameter before you enable FIPS mode. If you do not perform either of these steps, you must manually delete the ITL file after you enable FIPS mode.
- In a cluster, all nodes should be either in FIPS or Non FIPS mode. Each node being in different modes is not allowed. For example, Node A in FIPS mode and Node B in Non-FIPS mode is not allowed.
- After you enable FIPS mode on a server, please wait until the server reboots and the phones re-register successfully before enabling FIPS on the next server.



Caution Before you enable FIPS mode, we strongly recommend that you perform a system backup. If FIPS checks fail at start-up, the system halts and requires a recovery CD to be restored.

Make sure that all cluster nodes are set to FIPS mode or Non-FIPS mode during deployment. You cannot deploy mixed nodes in a cluster. A cluster must be either a FIP or a non-FIPS node.

Procedure

Step 1 Start a CLI session.

For more information, see “Start CLI Session” in the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Step 2 **Important**
This step ONLY applies to releases below 15SU3. Skip this step for Release 15SU3 or later.

In the CLI, enter **utils fips enable**

If you enter a password fewer than 14 characters, the following prompt appears:

```
The cluster security password must be at least 14 characters long before
 security modes such as FIPS, Common Criteria and Enhanced Security modes can be
 enabled. Update the cluster security password using the 'set password user
security' CLI command on all nodes and retry this command.
**********************************************************************************
Executed command unsuccessfully
```

If you enter a password more than 14 characters, the following prompts appear:

```
Security Warning: The operation will regenerate certificates for

1)CallManager
2)Tomcat
3)IPsec
4)TVS
5)CAPF
6)SSH
7)ITLRecovery
Any third party CA signed certificates that have been uploaded for the above
components will need to be re-uploaded. If the system is operating in mixed
mode, then the CTL client needs to be run again to update the CTL file.
If there are other servers in the cluster, please wait and do not change
```

```
the FIPS Settings on any other node until the FIPS operation on this node
is complete and the system is back up and running.

If the enterprise parameter 'TFTP File Signature Algorithm' is configured
with the value 'SHA-1' which is not FIPS compliant in the current version of the
Unified Communications Manager, though the signing operation
will continue to succeed, it is recommended the parameter value be changed to
SHA-512 in order to be fully FIPS. Configuring SHA-512 as the signing algorithm
may reqiure all the phones that are provisioned in the cluster to be capable of
verifying SHA-512 signed configuration file, otherwise the phone registration
may fail. Please refer to the Cisco Unified Communications Manager Security Guide
for more details.
********************************************************************************
This will change the system to FIPS mode and will reboot.
********************************************************************************
WARNING: Once you continue do not press Ctrl+C. Canceling this operation after
it
starts will leave the system in an inconsistent state; rebooting the system and
running "utils fips status" will be required to recover.
********************************************************************************
Do you want to continue (yes/no)?
```

Step 3 Enter **Yes**.

The following message appears:

```
Generating certificates...Setting FIPS mode in operating system.
FIPS mode enabled successfully.
******************************************************
It is highly recommended that after your system restarts
that a system backup is performed.
******************************************************
The system will reboot in a few minutes.
```

Unified Communications Manager reboots automatically.

Note

- Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.
- If you have a single-server cluster and applied the **Prepare Cluster for Rollback to pre 8.0** enterprise parameter before you enabled FIPS 140-2 mode, you must disable this enterprise parameter after making sure that all the phones registered successfully to the server.
- To enable FIPS in a cluster, first enable the Publisher and make sure all the configured services are properly initialized which will take some time to come up. Then enable fips in all other nodes one after the other within the cluster.

Note

In FIPS mode, Unified Communications Manager uses Libreswan (FIPS validated) in place of Racoon (non-FIPS validated). If the security policies in Racoon contain functions that aren't FIPS approved, the CLI command asks you to redefine security policies with FIPS approved functions and abort. For more information, see topics related to IPsec Management in the Administration Guide for Cisco Unified Communications Manager.

CiscoSSH Support

Unified Communications Manager supports CiscoSSH. When you enable FIPS mode on your system, CiscoSSH is enabled automatically with no extra configuration required. For more information, see the Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service.

Disable FIPS 140-2 Mode

Consider the following information before you disable FIPS 140-2 mode on Unified Communications Manager:

- In single or multiple server clusters, we recommend you to run the CTL Client. If the CTL Client is not run on a single server cluster, you must manually delete the ITL File after disabling FIPS mode.
- In multiple server clusters, each server must be disabled separately, because FIPS mode is not disabled cluster-wide but rather on a per-server basis.

To disable FIPS 140-2 mode, perform the following procedure:

Procedure

Step 1 Start a CLI Session.

For more information, see the Starting a CLI Session section in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Step 2 In the CLI, enter **utils fips disable**

Unified Communications Manager reboots and is restored to non-FIPS mode.

Note
Certificates and SSH key are regenerated automatically.

Check FIPS 140-2 Mode Status

To confirm if the FIPS 140-2 mode is enabled, check the mode status from the CLI.

To check the status of FIPS 140-2 mode, perform the following procedure:

Procedure

Step 1 Start a CLI Session.

For more information, see the Starting a CLI Session section in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Step 2 In the CLI, enter **utils fips status**

The following message appears to confirm that FIPS 140-2 mode is enabled.

Note
This result is applicable for release 14SU1 and below only .

```
admin:utils fips status
The system is operating in FIPS mode. Self test status:

- S T A R T ---------------------
Executing FIPS selftests
runlevel is N 3
Start time: Thu Apr 28 15:59:24 PDT 2011
NSS self tests passed.
Kernel Crypto tests passed.
Operating System OpenSSL self tests passed.
Openswan self tests passed.
OpenSSL self tests passed.
CryptoJ self tests passed...
```

Note
This result is applicable for release 14SU2 and 14SU3 only .

```
admin:utils fips status
The system is operating in FIPS mode. Self test status:

- S T A R T ---------------------
Executing FIPS selftests
runlevel is multi-user.target
Start time: Fri Jul 28 11:28:28 IST 2023
NSS self tests passed.
Kernel Crypto tests passed.
Operating System OpenSSL self tests passed.
Libreswan self tests passed.
OpenSSL self tests passed.
CryptoJ self tests passed.
BCFIPS self tests passed.
```

FIPS 140-2 Mode Server Reboot

FIPS startup self-tests in each of the FIPS 140-2 modules are triggered after rebooting when Unified Communications Manager server reboots in FIPS 140-2 mode.

Caution If any of these self-tests fail, the Unified Communications Manager server halts.

Note Unified Communications Manager server is automatically rebooted when FIPS is enabled or disabled with the corresponding CLI command. You can also initiate a reboot.

Caution If the startup self-test failed because of a transient error, restarting the Unified Communications Manager server fixes the issue. However, if the startup self-test error persists, it indicates a critical problem in the FIPS module and the only option is to use a recovery CD.

FIPS Mode Restrictions

Feature	Restrictions
SNMP v3	FIPS mode does not support SNMP v3 with MD5 or DES. If you have SNMP v3 configured while FIPS mode is enabled, you must configure **SHA** as the Authentication Protocol and **AES128** as the Privacy Protocol.
Certificate Remote Enrolment	FIPS mode does not support Certificate Remote Enrolment.
SFTP Server	All SFTP client (for example, DRS and CDR) connections uses the following host key algorithms: • FIPS mode only supports **rsa-sha2-256** • Non-FIPS mode only supports **ssh-rsa** The **rsa-sha2-256** (SHA256WithRSA) support is available only from OpenSSH 6.8 version onwards.
SSH Host Key Algorithms	Deprecated Algorithm: • **ssh-rsa** (SHA1withRSA) New Supported Algorithm: • **rsa-sha2-256** • **rsa-sha2-512** **Note** Before upgrading to 14SU2 and above releases, we recommend that you refer to the “Supported Upgrade and Migration Paths with COP Files” section in the Upgrade and Migration Guide for Cisco Unified Communications Manager and the IM and Presence Service.

Feature	Restrictions
IPSec Policy	In Common Criteria (CC) mode, Certificate Exchange operation is recommended first between clusters/nodes before configuring IPSec policies for Certificate based IPSec Policy. Certificate based IPSec Policy will not work when moving from Non-FIPS to FIPS/Common Criteria mode or vice-versa. Perform the following when you should move from Non-FIPS mode to FIPS/CC Mode or vice-versa. If you have a certificate based IPSec policy and it is in the enabled state, then: 1. Disable the IPSec policy before moving to FIPS/CC mode or vice versa. 2. Recertify the certificate and exchange the new certificate after moving to FIPS/CC mode or vice versa. 3. Enable IPSec policy.

Enhanced Security Mode

Enhanced Security Mode runs on a FIPS-enabled system. Both Unified Communications Manager and the IM and Presence Service can be enabled to operate in Enhanced Security Mode, which enables the system with the following security and risk management controls:

- Stricter credential policy is implemented for user passwords and password changes.
- Contact search authentication feature becomes enabled by default.
- If the protocol for remote audit logging is set to TCP or UDP, the default protocol is changed to TCP. If the protocol for remote audit logging is set to TLS, the default protocol remains TLS. In Common Criteria Mode, strict hostname verification is implemented. Hence, you should configure the server with a fully qualified domain name (FQDN) which matches the certificate.

When Unified Communications Manager is in FIPS mode, the devices that you set as a backup device must be FIPS compliance. The key exchange algorithm **diffie-hellman-group1-sha1** isn't supported in FIPS mode. If you configure **diffie-hellman-group1-sha1** algorithm in a non-FIPS mode of Unified Communications Manager, this algorithm is automatically removed from SSH Key Exchange when you enable FIPS mode.

Credential Policy Updates

When Enhanced Security Mode is enabled, a stricter credential policy takes effect for new user passwords and password changes. After Enhanced Security Mode is enabled, administrators can use the **set password ***** series of CLI commands to modify any of these requirements:

- Password Length should be between 14 to 127 characters.
- Password should have at least 1 lowercase, 1 uppercase, 1 digit and 1 special character.
- Any of the previous 24 passwords can't be reused.
- Minimum age of the password is 1 day and Maximum age of the password is 60 days.

- Any newly generated password's character sequence needs to differ by at least 4 characters from the old password's character sequence.

Note When Unified Communications Manager and Cisco Instant and Messaging are operating in Enhanced Security mode, before Jabber login with an existing local end-user or new local end-user, the user needs to follow the below steps:

- Log into the Selfcare portal first, then reset the user's password before logging into Jabber. Then log in to Jabber for the local end-user.
- URL for Selfcare portal: **https://<IPaddress>/ucmuser**

Note When Unified Communications Manager is enabled to operate in Enhanced mode, ensure that you change the user credentials for IPMASysUser and IPMASecureSysUser. Else, the IPMA functionalities won't be in a working state and the 'IPMANotStarted' alarms will be triggered. The CLI sessions will be flooded on the next Cisco Tomcat service restart or IPMA service restart.

You can change the application user password credentials at documented in the "Manage Application User Password Credential Information" section at: Administration Guide for Cisco Unified Communications Manager.

From Cisco Unified CM Administration user interface, navigate to **User Management > Application User** and click **Edit Credential**. From the Authentication Rule drop-down list, select **Enhanced Security Credential Policy** and ensure that you keep the **User Must Change at Next Login check box** unchecked. You can view the Enhanced Security Mode policies as described in the 'Credential Policy Updates' section.

Configure Enhanced Security Mode

Enable FIPS before you enable Enhanced Security Mode.

Use this procedure on all Unified Communications Manager or IM and Presence Service cluster nodes to configure Enhanced Security Mode.

Note You must ensure that services in the IM and Presence Service publishers are in the 'STARTED' state ("Cisco IM and Presence Data Monitor" service and SyncAgent), when you are changing the password on the Unified Communications Manager publisher after enabling the Enhanced Security Mode.

Procedure

Step 1 Log in to the Command Line Interface.

Step 2 Run **utils EnhancedSecurityMode status** command to confirm whether Enhanced Security Mode is enabled.

Step 3 Run one of the following commands on a Unified Communications Manager cluster node:

- To enable Enhanced Security Mode, run **utils EnhancedSecurityMode enable** command.
- To disable Enhanced Security Mode, run **utils EnhancedSecurityMode disable** command.

Step 4 After enabling Enhanced Security Mode, change the password in the Cisco Unified CM Administration user interface with a new password containing 14 characters.

Perform the following after enabling Enhanced Security Mode on Unified Communications Manager publisher:

a. Enable Enhanced Security Mode on Unified Communications Manager subscribers.

b. Enable Enhanced Security Mode on IM and Presence Service publisher.

c. Enable Enhanced Security Mode on IM and Presence Service subscribers.

Note
Do not run either **utils EnhancedSecurityMode enable** or **utils EnhancedSecurityMode disable** CLI commands on all nodes simultaneously.

Common Criteria Mode

Common Criteria mode allows both Unified Communications Manager and IM and Presence Service Service to comply with Common Criteria guidelines. Common Criteria mode can be configured with the following set of CLI commands on each cluster node:

- `utils fips_common_criteria enable`
- `utils fips_common_criteria disable`
- `utils fips_common_criteria status`

Common Criteria Configuration Task Flow

- FIPS mode must be running to enable Common Criteria mode. If FIPS isn't already enabled, you'll be prompted to enable it when you try to enable Common Criteria mode. Enabling FIPS does require certificate regeneration. For more information, see Enable FIPS 140-2 Mode, on page 233.
- In Common Criteria mode, Certificate Exchange operation is mandatory between clusters/nodes before configuring IPSec policies for Certificate based IPSec Policy.
- X.509 v3 certificates are required in Common Criteria mode. X.509 v3 certificates enable secure connections when using TLS 1.2 as a communication protocol for the following:
  - Remote audit logging
  - Establishing connection between the FileBeat client and the logstash server.

To configure Unified Communications Manager and IM and Presence Service for Common Criteria mode, perform the following:

Procedure

	Command or Action	Purpose
Step 1	Enable TLS, on page 242	TLS is a prerequisite for configuring Common Criteria mode.
Step 2	Configure Common Criteria Mode, on page 243	Configure Common Criteria mode on all Unified Communications Manager and IM and Presence Service cluster nodes.

Enable TLS

TLS 1.2 version or TLS version 1.1 is a requirement for Common Criteria mode. Secure connections using TLS version 1.0 are not permitted after enabling Common Criteria mode.

- During establishment of a TLS connection, the `extendedKeyUsage` extension of the peer certificate is checked for proper values.
  - The peer certificate should have `serverAuth` as `extendedKeyUsage` extension if the peer is a server.
  - The peer certificate should have `clientAuth` as `extendedKeyUsage` extension if the peer is a client.

If the `extendedKeyUsage` extension does not exist in the peer certificate or is not set properly, the connection is closed.

To support TLS version 1.2, perform the following:

Procedure

Step 1 Install Soap UI version 5.2.1.

Step 2 If you are running on the Microsoft Windows platform:

a) Navigate to `C:\Program Files\SmartBear\SoapUI-5.2.1\bin`.

b) Edit the `SoapUI-5.2.1.vmoptions` file to add `-Dsoapui.https.protocols=TLSv1.2,TLSv1,SSLv3` and save the file.

Step 3 If you are running on Linux, edit the `bin/soaup.sh` file to add `JAVA_OPTS="$JAVA_OPTS -Dsoapui.https.protocols=SSLv3,TLSv1.2"` and save the file.

Step 4 If you are running OSX:

a) Navigate to `/Applications/SoapUI-{VERSION}.app/Contents`.

b) Edit the `vmoptions.txt` file to add `-Dsoapui.https.protocols=TLSv1.2,TLSv1,SSLv3` and save the file.

Step 5 Restart the SoapUI tool and proceed with AXL testing

Configure Common Criteria Mode

Use this procedure to configure Common Criteria mode for Unified Communications Manager and IM and Presence Service Service.



Note Cisco's CTL client is no longer supported from Release 14. We recommend that you use the CLI command to switch the Unified Communications Manager server to Mixed Mode instead of the Cisco CTL Plugin.

Procedure

Step 1 Log in to the Command Line Interface prompt.

Step 2 Run `utils fips_common_criteria status` command to verify whether the system is operating in Common Criteria mode.

Step 3 Run one of the following commands on a cluster node:

- To enable the Common Criteria mode, run `utils fips_common_criteria enable`.
- To disable the Common Criteria mode, run `utils fips_common_criteria disable`.

  When Common Criteria mode is disabled, a prompt is displayed to set the minimum TLS version.

Note
Do not run these commands on all nodes simultaneously.

Step 4 To enable Common Criteria Mode across a single cluster, repeat this procedure on all Unified Communications Manager and IM and Presence Service cluster nodes.

Note
- CTL client does not connect to Unified Communications Manager node when server is in the Common Criteria mode, as CTL client does not support TLS 1.1 and TLS 1.2 protocols.
- Only phone models that support TLS 1.1 or TLS 1.2 such as DX series and 88XX series phones are supported in Common Criteria mode. Phone models that support only TLSv1.0 such as 7975 and 9971 are not supported in the Common Criteria mode.
- Temporarly allow TLS 1.0 when using the CTL Client and then move the Cluster to Common Criteria mode. Configure Minimum TLS to 1.1 or 1.2.
- Migrate to Tokenless CTL by using the CLI Command **utils ctl set-cluster mixed-mode** in Common Criteria mode. Configure Minimum TLS to 1.1 or 1.2.

Step 5 To enable the Common Criteria mode in a multi cluster setup where ICSA is already configured between the nodes, enable Common Criteria mode in each of the nodes in the following order:

a. Unified Communications Manager - Cluster 1 (Publisher)

b. IM and Presence Service - Cluster 1 (Publisher)

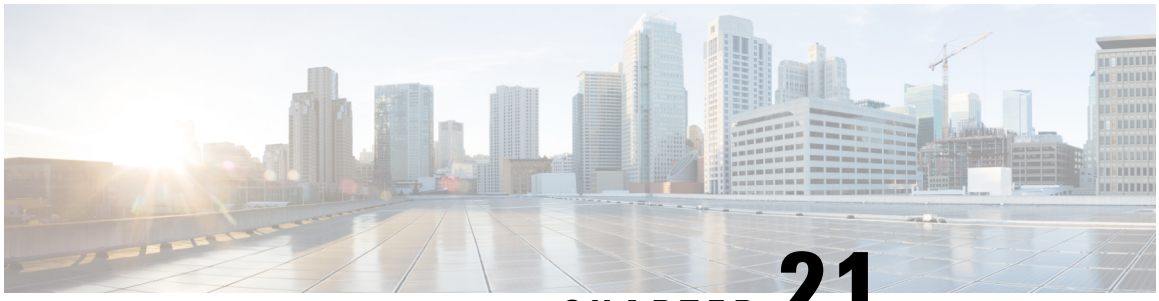
c. IM and Presence Service - Cluster 1 (Subscriber or subscribers)

d. Unified Communications Manager - Cluster 2 (Publisher)

e. IM and Presence Service - Cluster 2 (Publisher)

f. IM and Presence Service - Cluster 2 (Subscriber or subscribers)

Step 6 In case of a cert sync failure, see.



CHAPTER 21

V.150 Minimum Essential Requirements

- V.150 Overview, on page 245
- Configure V.150 Task Flow, on page 245

V.150 Overview

The V.150 Minimum Essential Requirements feature allows you to make secure calls in a modem over an IP network. The feature uses a dial-up modem for large installed bases of modems and telephony devices operating on a traditional public switched telephone network (PSTN). The V.150.1 recommendation specifically defines how to relay data from modems and telephony devices on a PSTN into and out of an IP network through a modem. The V.150.1 is an ITU-T recommendation for using a modem over IP networks that support dial-up modem calls.

The Cisco V.150.1 Minimum Essential Requirements feature complies with the requirements of the National Security Agency (NSA) SCIP-216 Minimum Essential Requirements (MER) for V.150.1 recommendation. The SCIP-216 recommendation has simplified the existing V.150.1 requirements.

Cisco V.150.1 MER feature supports the following interfaces:

- Media Gateway Control Protocol(MGCP) T1(PRI and CAS) and E1(PRI) trunks
- Session Initiation Protocol (SIP) trunks
- Skinny Client Control Protocol (SCCP) for analog gateway endpoints
- Secure Communication Interoperability Protocol-End Instruments (SCIP-EI)

Configure V.150 Task Flow

Complete these tasks to add V.150 support in Unified Communications Manager.

Procedure

	Command or Action	Purpose
Step 1	To Configure Media Resource Group Task Flow, on page 247, perform the following subtasks: • Configure Media Resource Group for Non-V.150 Endpoints, on page 247 • Configure a Media Resource Group List for Non-V.150 Endpoints, on page 248 • Configure Media Resource Group for V.150 Endpoints, on page 248 • Configure a Media Resource Group List for V.150 Endpoints, on page 248	Add Media Resource Group and Media Resource Group List for V.150 and non V.150 devices.
Step 2	Configure the Gateway for Cisco V.150 (MER), on page 249	Add V.150 functionality to a gateway.
Step 3	Configure V.150 MGCP Gateway Port Interface, on page 250	If you want to use V.150 support across an MGCP gateway, add V.150 support to the port interface.
Step 4	Configure V.150 SCCP Gateway Port Interface, on page 250	If you want to use V.150 support across an SCCP gateway, add V.150 support to the port interface.
Step 5	Configure V.150 Support for Phone, on page 251	Add V.150 support to the phones that will be placing V.150 calls.
Step 6	To Configure SIP Trunk Task Flow, on page 251, perform one or any of the following subtasks: • Configure SIP Profile for V.150, on page 252 • Set the Clusterwide V.150 Filter, on page 252 • Add V.150 Filter to SIP Trunk Security Profile, on page 253 • Configure SIP Trunk for V.150, on page 254	Add V.150 support to the SIP trunk that will be used for V.150 calls.
Step 7	To use the V.150 MER feature, you also need to configure IOS on your gateway to support the feature.	For more information on IOS gateway configuration settings, see http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t4/mer_cg_15_1_4M.html.

Configure Media Resource Group Task Flow

Your system should already be set up with basic call control functionality. For instructions on how to set up the call control system, see System Configuration Guide for Cisco Unified Communications Manager.

For Unified Communications Manager, you must have one of the following releases installed:

- The minimum version is Release 10.5(2) SU3
- For 11.0, the minimum version will be 11.0(1) SU2
- All releases from 11.5(1) on support this feature
- You must have *Cisco IOS Release* 15.6(2)T or later.

V.150 is not supported with Media Termination Point (MTP). We recommend that you remove MTP from devices, trunks, and gateways that are handling V.150 calls.

Complete these tasks to configure two sets of media resource groups: a media resource group with MTP resources for non-V.150 calls, and a media resource group without MTP resources for V.150 calls.

Procedure

	Command or Action	Purpose
Step 1	Configure Media Resource Group for Non-V.150 Endpoints, on page 247	You can configure the Media Resource Group with MTP for non-V.150 endpoints.
Step 2	Configure a Media Resource Group List for Non-V.150 Endpoints, on page 248	Configure a Media Resource Group list that includes your MTP Media Resources for non-V.150 endpoints.
Step 3	Configure Media Resource Group for V.150 Endpoints, on page 248	Configure Media Resource Group without MTP resources for secure V.150 calls.
Step 4	Configure a Media Resource Group List for V.150 Endpoints, on page 248	Configure a Media Resource Group list without MTP after adding the required resources in the Media Resource Group for secure V.150 endpoints.

Configure Media Resource Group for Non-V.150 Endpoints

Use this procedure to add a new media resource group that includes MTP resources for non-V.150 endpoints.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Media Resources** > **Media Resource Group**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter the media resource group name as **Do not use with V.150 devices**.

Step 4 From the **Available Media Resources** field, choose only MTP devices and click the **down-arrow key**.

The selected devices appear in the **Selected Media Resources** field.

Step 5 Click **Save**.

Configure a Media Resource Group List for Non-V.150 Endpoints

Configure Media Resource Group for Non-V.150 Endpoints, on page 247

Use this procedure to add new media resource group list with MTP resources for non-V.150 end points.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Media Resources** > **Media Resource Group List**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name for the media resource group list as **Non- V.150**.

Step 4 From the **Available Media Resources** field, choose the V.150 MER resource group named **Do not use with V.150 Devices** and click the **down-arrow key**.
The selected devices appear in the **Selected Media Resources** field.

Step 5 Click **Save**.

Configure Media Resource Group for V.150 Endpoints

Use this procedure to add new media resource group without MTP resources for V.150 devices.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Media Resources** > **Media Resource Group**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter the media resource group name as **For use with V.150 devices**.

Step 4 From the **Available Media Resources** field, choose multiple devices except the MTP resources and click the **down-arrow key**.
The selected devices appear in the **Selected Media Resources** field.

Step 5 Click **Save**.

Configure a Media Resource Group List for V.150 Endpoints

Configure Media Resource Group for V.150 Endpoints, on page 248

Use this procedure to add a media resource group list without MTP resources for V.150 devices.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Media Resources** > **Media Resource Group List**.

Step 2 Click **Add New**.

Step 3 In the **Name** field, enter a name for the media resource group list as **V.150**.

Step 4 From the **Available Media Resources** field, choose the V.150 MER resource group named **For V.150 Devices** and click the **down-arrow key**.
The selected media resource groups appear in the **Selected Media Resources** field.

Step 5 Click **Save**.

Configure the Gateway for Cisco V.150 (MER)

Use this procedure to configure the gateway for Cisco V.150 (MER).

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Gateway**.

Step 2 Click **Add New**.

Step 3 Choose the gateway from the **Gateway Type** drop-down list.

Step 4 Click **Next**.

Step 5 From the **Protocol** drop-down list, choose a protocol.

Step 6 Depending on which Protocol you chose for the gateway, perform:

- For MGCP, in the **Domain Name** field, enter the domain name that is configured on the gateway.
- For SCCP, in the **MAC Address (Last 10 Characters)** field, enter the gateway MAC address.

Step 7 From the **Unified Communications Manager Group** drop-down list, choose **Default**.

Step 8 In the **Configured Slots, VICs and Endpoints** area, perform the following steps:

a) From each **Module** drop-down list, select the slot that corresponds to the Network Interface Module hardware that is installed on the gateway.
b) From each **Subunit** drop-down list, select the VIC that is installed on the gateway.
c) Click **Save**.
The **port icons** appear. Each **port icon** corresponds to an available **port interface** on the gateway. You can configure any **port interface** by clicking the corresponding **port icon**.

Step 9 Complete the remaining fields in the **Gateway Configuration** window. See the online help for more information about the fields and their configuration options.

Step 10 Click **Save**.

Configure V.150 MGCP Gateway Port Interface

Use this procedure to configure V.150 MGCP gateway port interface.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Gateway**.

Step 2 Enter the appropriate search criteria to modify the settings for an existing gateway and click **Find**.

Step 3 In the **Configured Slots, VICs, and Endpoints** area, locate the module and subunit on which you want to configure a port for V.150 MER and click the corresponding **port icon**.

Step 4 From the **Device Protocol** drop-down list, choose **Digital Access T1** or **Digital Access PRI** and click **Next**.

Note
The **Device Protocol** drop-down list is displayed only if T1 port is selected in the **Configured Slots, VICs, and Endpoints** area.

The **Gateway Configuration** window now displays the port interface configuration.

Step 5 Select the **Media Resource Group List** named **V.150**.

Step 6 Check the **V150 (subset)** check box.

Step 7 Configure the remaining fields, if applicable. See the online help for more information about the fields and their configuration options.

Step 8 Click **Save**.

Step 9 (Optional) If you want to configure additional port interfaces for the gateway, from the **Related Links** drop-down list, choose **Back to MGCP Configuration** and click **Go**. You can select a different port interface.

Configure V.150 SCCP Gateway Port Interface

Use this procedure to configure V.150 SCCP gateway port interface.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Gateway**.

Step 2 Enter the appropriate search criteria to modify the settings for an existing SCCP gateway and click **Find**.

Step 3 In the **Configured Slots, VICs, and Endpoints** area, locate the module and subunit on which you want to configure a port for V.150 MER and click the corresponding **port icon**.

Step 4 Select the **Media Resource Group List** named "**V.150**".

Step 5 In the **Product Specific Configuration Layout** area, if the **Latent Capability Registration Setting** drop-down list appears, select **Modem Relay** or **Modem Relay and Passthrough**.

Step 6 Configure the remaining fields, if applicable. See the online help for more information about the fields and their configuration options.

Step 7 Click **Save**.

Configure V.150 Support for Phone

Use this procedure to add V.150 support for a phone. The following phone types support V.150:

- Cisco 7962—Third party SCCP end point registered as Cisco 7962
- Cisco 7961G-GE—Third party SCCP end point registered as Cisco 7961G-GE
- Third Party AS-SIP Endpoints

Procedure

Step 1 Required: Create an End User with the User ID same as the intended phone number.

Step 2 Required: Configure the **Digest Credentials** field in the **End User Configuration** window for Third Party AS-SIP SIP endpoints.

For more information on how to configure a new End User, see the "Provision End Users Manually" chapter in the System Configuration Guide for Cisco Unified Communications Manager

Step 3 From Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 4 Perform either of the following steps:

- To configure V.150 on an existing phone, click **Find** and select the phone.
- To configure a new phone for V.150, click **Add New**.

Step 5 From the **Phone Type** drop-down list, select one of the phone types that supports V.150, and click **Next**.

Step 6 For third party SCCP endpoints registered as Cisco 7962, select **SCCP** from the **Device Protocol** drop-down list, and click **Next**.

Step 7 From the **Media Resource Group List** drop-down menu, select **V.150**.

Step 8 For third party AS-SIP SIP endpoints only, Configure the following fields:

- From the **Digest User** drop-down select the end user for this phone. The end user will be used for digest authentication.
- Leave the **Media Termination Point Required** check box unchecked.
- Check the **Early Offer support for voice and video calls** check box.

Step 9 Click **Save**.

Step 10 Click **Apply Config**.

Step 11 Click **OK**.

Configure SIP Trunk Task Flow

Use this procedure to configure SIP Trunk task flow.

Procedure

	Command or Action	Purpose
Step 1	Configure SIP Profile for V.150, on page 252	Configure a SIP Profile with SIP Best Effort Early Offer support for the SIP trunk.
Step 2	Set the Clusterwide V.150 Filter, on page 252	Optional. Configure a clusterwide default setting for SIP V.150 SDP Offer Filtering.
Step 3	Add V.150 Filter to SIP Trunk Security Profile, on page 253	Configure a V.150 Filter within a SIP Trunk Security Profile that you can assign to specific SIP trunks.
Step 4	Configure SIP Trunk for V.150, on page 254	Configure V.150 support for the SIP trunks that will handle V.150 calls.

Configure SIP Profile for V.150

Use this procedure to configure a SIP Profile with SIP Best Effort Early Offer support for the SIP trunk.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **SIP Profile** .

Step 2 Perform either of the following steps:

- To create a new profile, click **Add New**.
- To select an existing profile, click **Find** and select a SIP profile.

Step 3 In the **Name** field, enter the SIP name for V.150.

Step 4 In the **Description** field, enter the description for V.150.

Step 5 From the **Early Offer Support for Voice and video class** drop-down list, choose **Select Best Effort (no MTP inserted)**.

Step 6 Enter any other configuration settings that you want. See the online help for more information about the fields and their configuration options.

Step 7 Click **Save**.

Set the Clusterwide V.150 Filter

Use this procedure to configure a clusterwide default setting for SIP V.150 SDP Offer filtering.

Note If you configure a **SIP V.150 SDP Offer Filtering** value within a SIP Trunk Security Profile that is different than the clusterwide service parameter setting, the security profile setting overrides the cluster-wide service parameter setting for the trunks that use that security profile.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose an active server.

Step 3 From the **Service** drop-down list, choose **Cisco CallManager**.

Step 4 In the **Clusterwide Parameters (Device- SIP)** section, configure a value for the **SIP V.150 SDP Offer Filtering** service parameter.

Step 5 Choose **SIP V.150 SDP Offer Filtering** from the drop-down list.

Step 6 Specify the desired filtering action.

Step 7 Click **Save**.

Add V.150 Filter to SIP Trunk Security Profile

Use this procedure to assign a V.150 Filter within a SIP Trunk Security Profile.

Note If you configure a **SIP V.150 SDP Offer Filtering** value within a SIP Trunk Security Profile that is different than the clusterwide service parameter, the security profile setting overrides the cluster-wide service parameter setting for the trunks that use that security profile.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System** > **Security** > **SIP Trunk Security Profile**.

Step 2 Perform one of the following tasks:

- Enter search criteria and Click **Find** to choose an existing profile from the list to modify the settings for an existing SIP Trunk Security Profile.
- Click **Add New** to add a new SIP Trunk Security Profile.

Step 3 Configure a value for the **SIP V.150 Outbound SDP Offer Filtering** drop-down list.

Note
The default setting is to use the value of the **SIP V.150 Outbound SDP Offer Filtering** cluster-wide service parameter.

Step 4 Configure any remaining fields in the **SIP Trunk Security Profile Configuration** window. See the online help for more information about the fields and their configuration options.

Step 5 Click **Save**.

Configure SIP Trunk for V.150

Use this procedure to configure settings for a SIP trunk.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **Device** > **Trunk**.

Step 2 Perform either of the following steps:

- To create a new profile, click **Add New**.
- Click **Find** and select a SIP trunk, to select an existing trunk.

Step 3 For new trunks, do the following:

- From the **Trunk Type** drop-down list, choose **SIP Trunk**.
- From the **Protocol Type** drop-down list, choose **SIP**.
- From the **Trunk Service Type** drop-down list, choose **None(Default)**.
- Click **Next**.

Step 4 Enter the SIP trunk name in the **Name** field.

Step 5 Enter the SIP trunk description in the **Description** field.

Step 6 From the **Media Resource Group List** drop-down list, choose the Media resource group list named "V.150".

Step 7 Configure the destination address for the SIP trunk:

a) In the **Destination Address** text box, enter an IPv4 address, fully qualified domain name, or DNS SRV record for the server or endpoint that you want to connect to the trunk.
b) If the destination is a DNS SRV record, check the **Destination Address is an SRV** check box.
c) To add additional destinations, click **(+)** button. You can add up to 16 destinations for a SIP trunk.

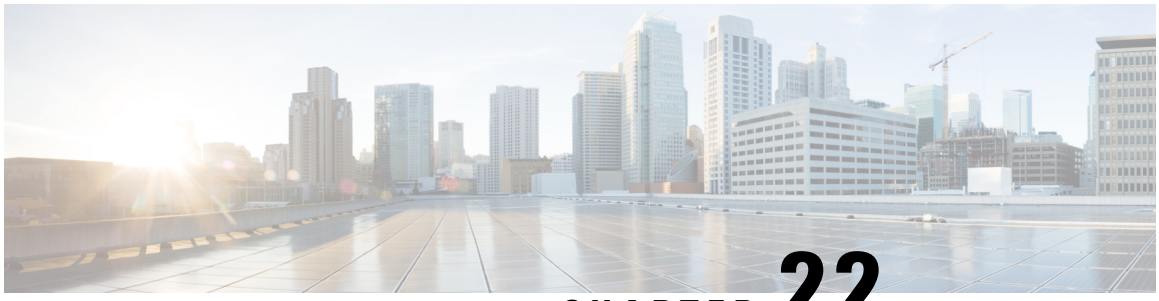
Step 8 From the **SIP Trunk Security Profile** drop-down list, assign the SIP trunk security profile that you configured for this trunk.

Step 9 From the **SIP Profile** drop-down list, assign the SIP profile that you set up with the Best Effort Early Offer setting.

Step 10 Leave the **Media Termination Point Required** check box unchecked.

Step 11 Configure any additional fields in the **Trunk Configuration** window. See the online help for more information about the fields and their configuration options.

Step 12 Click **Save**.



CHAPTER 22

IPSec Setup

- IPSec Overview, on page 255

IPSec Overview

IPsec is a framework that ensures private, secure communications over IP networks through the use of cryptographic security services. IPsec policies are used to configure IPsec security services. The policies provide varying levels of protection for most traffic types in your network. You can configure IPsec policies to meet the security requirements of a computer, organizational unit (OU), domain, site, or global enterprise.

IPsec Setup Within Network Infrastructures

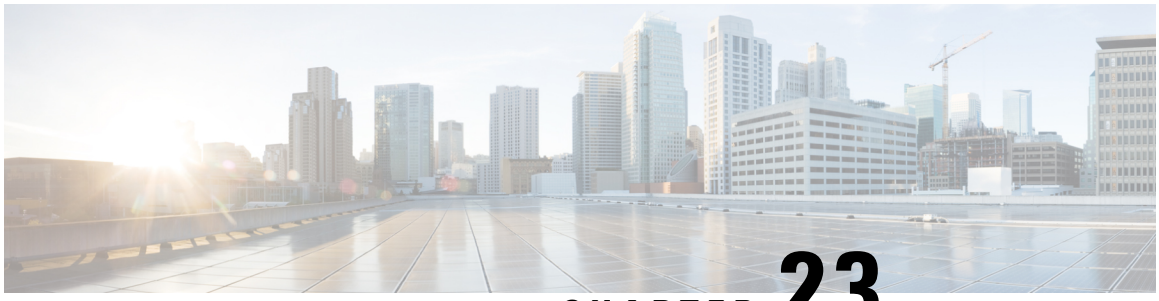
This section does not describe how to configure IPsec. Instead, it provides considerations and recommendations for configuring IPsec in your network infrastructure. If you plan to configure IPsec in the network infrastructure and not between Unified Communications Manager and the device, review the following information before you configure IPsec:

- We recommend you to provision IPsec in the infrastructure rather than in the Unified Communications Manager itself.
- Before you configure IPsec, consider existing IPsec or VPN connections, platform CPU impact, bandwidth implications, jitter or latency, and other performance metrics.
- Review the *Voice and Video Enabled IPsec Virtual Private Networks Solution Reference Network Design Guide*.
- Review the *CiscoIOS Security Configuration Guide, Release 12.2* (or later).
- Terminate the remote end of the IPsec connection in the secure CiscoIOS MGCP gateway.
- Terminate the host end in a network device within the trusted sphere of the network where the telephony servers exist; for example, behind a firewall, access control list (ACL), or other layer three device.
- The equipment that you use to terminate the host-end IPsec connections depends on the number of gateways and the anticipated call volume to those gateways; for example, you could use Cisco VPN 3000 Series Concentrators, Catalyst 6500 IPsec VPN Services Module, or Cisco Integrated Services Routers.
- Perform the steps in the order that is specified in the topics related to setting up secure gateways and trunks.

Caution Failing to configure the IPsec connections and verify that the connections are active and may compromise privacy of the media streams.

Configure and Manage IPsec Setup Between Unified Communications Manager and Gateway or Trunks

For information on configuring IPSec between Unified Communications Manager and the gateways or trunks that are described, see the chapter "Manage IPSec Policies" in the Administration Guide for Cisco Unified Communications Manager.



CHAPTER 23

Authentication and Encryption Setup for CTI, JTAPI, and TAPI

This chapter provides a brief overview of how to secure the CTI, JTAPI, and TAPI applications. It also describes the tasks that you must perform in Unified Communications Manager Administration to configure authentication and encryption for CTI/TAPI/JTAPI applications.

This document does not describe how to install the CiscoJTAPI or TSP plug-ins that are available in Unified Communications Manager Administration, nor does it describe how to configure the security parameters during the installation. Likewise, this document does not describe how to configure restrictions for CTI-controlled devices or lines.

- Authentication for CTI, JTAPI, and TAPI Applications, on page 257
- Encryption for CTI, JTAPI, and TAPI Applications, on page 259
- CAPF Functions for CTI, JTAPI, and TAPI Applications, on page 260
- Securing CTI, JTAPI, and TAPI, on page 266
- Add Application and End Users to Security-Related Access Control Groups, on page 267
- Set Up JTAPI/TAPI Security-Related Service Parameters, on page 268
- View Certificate Operation Status for Application or End User, on page 269

Authentication for CTI, JTAPI, and TAPI Applications

Unified Communications Manager allows you to secure the signaling connections and media streams between CTIManager and CTI/JTAPI/TAPI applications.

Note We assume that you configured security settings during the CiscoJTAPI/TSP plug-in installation. We also assume that the Cluster Security Mode equals Mixed Mode, as configured in the Cisco CTL Client or through the CLI command set **utils ctl**. If these settings are not configured when you perform the tasks that are described in this chapter, CTIManager and the application connect via a nonsecure port, Port2748.

Cisco's CTL client is no longer supported from Release 14. We recommend that you use the CLI command to switch the Unified Communications Manager server to Mixed Mode instead of the Cisco CTL Plugin.

CTIManager and the application verify the identity of the other party through a mutually authenticated TLS handshake (certificate exchange). When a TLS connection occurs, CTIManager and the application exchange QBE messages via the TLS port, Port 2749.

To authenticate with the application, CTIManager uses the Unified Communications Manager certificate — either the self-signed certificate that installs automatically on the Unified Communications Manager server during installation or a third-party, CA-signed certificate that you uploaded to the platform.

After you generate the CTL file through the CLI command set **utils ctl** or the Cisco CTL Client, this certificate is added automatically to the CTL file. Before the application attempts to connect to CTIManager, the application downloads the CTL file from the TFTP server.

The first time that the JTAPI/TSP client downloads the CTL file from the TFTP server, the JTAPI/TSP client trusts the CTL file. We recommend that the download occur in a secure environment because the JTAPI/TSP client does not validate the CTL file. The JTAPI/TSP client verifies subsequent downloads of the CTL file; for example, after you update the CTL file, the JTAPI/TSP client uses the security tokens in the CTL file to authenticate the digital signature of the new CTL file it downloads. Contents of the file include the Unified Communications Manager certificates and CAPF server certificate.

If the CTL file appears compromised, the JTAPI/TSP client does not replace the downloaded CTL file; the client logs an error and attempts to establish a TLS connection by using an older certificate in the existing CTL file. The connection may not succeed if the CTL file has changed or is compromised. If the CTL file download fails and more than one TFTP server exists, you can configure another TFTP server to download the file. The JTAPI/TAPI client does not connect to any port under the following circumstances:

- The client cannot download the CTL file for some reason; for example, no CTL file exists.
- The client does not have an existing CTL file.
- You configured the application user as a secure CTI user.

To authenticate with CTIManager, the application uses a certificate that the Certificate Authority Proxy Function (CAPF) issues. To use TLS for every connection between the application and CTIManager, each instance that runs on the application PC must have a unique certificate. One certificate does not cover all instances. To ensure that the certificate installs on the node whereCisco Unified Communications Manager Assistant service is running, you configure a unique Instance ID for each Application User CAPF Profile Configuration or End User CAPF Profile Configuration in Cisco Unified Communications Manager Administration, as described in Application and End User CAPF Profile Configuration Settings .



Tip If you uninstall the application from one PC and install it on another PC, you must install a new certificate for each instance on the new PC.

You must also add the application users or the end users to the Standard CTI Secure Connection user group in Unified Communications Manager to enable TLS for the application. After you add the user to this group and install the certificate, the application ensures that the user connects via the TLS port.

Encryption for CTI, JTAPI, and TAPI Applications

Tip Authentication serves as the minimum requirement for encryption; that is, you cannot use encryption if you have not configured authentication.

Unified Communications Manager, Cisco QRT, and Cisco Web Dialer do not support encryption. CTI clients that connect to the CTIManager service may support encryption if the client sends voice packets.

To secure the media streams between the application and CTIManager, add the application users or the end users to the Standard CTI Allow Reception of SRTP Key Material user group in Unified Communications Manager. If these users also exist in the Standard CTI Secure Connection user group and if the cluster security mode equals Mixed Mode, CTIManager establishes a TLS connection with the application and provides the key materials to the application in a media event

Note Cluster security mode configures the security capability for your standalone server or cluster.

Although applications do not record or store the SRTP key materials, the application uses the key materials to encrypt its RTP stream and decrypt the SRTP stream from CTIManager.

If the application connects to the nonsecure port, Port 2748, for any reason, CTIManager does not send the keying material. If CTI/JTAPI/TAPI cannot monitor or control a device or directory number because you configured restrictions, CTIManager does not send the keying material.

Tip For an application to receive SRTP session keys, the application or end user must exist in three groups: Standard CTI Enabled, Standard CTI Secure Connection, and Standard CTI Allow Reception of SRTP Key Material.

Although Unified Communications Manager can facilitate secure calls to and from CTIports and route points, you must configure the application to support secure calls because the application handles the media parameters.

CTIports/route points register through dynamic or static registration. If the port/route point uses dynamic registration, the media parameters get specified for each call; for static registration, media parameters get specified during registration and cannot change per call. When CTIports/route points register to CTIManager through a TLS connection, the device registers securely, and the media gets encrypted via SRTP if the application uses a valid encryption algorithm in the device registration request and if the other party is secure.

When the CTI application begins to monitor a call that is already established, the application does not receive any RTP events. For the established call, the CTI application provides a DeviceSnapshot event, which defines whether the media for the call is secure or nonsecure; this event provides no keying material.

Stronger Cipher Suites on CTI Ports

When the CTI port registers to CTI Manager through a TLS connection, the device registers securely, and the media gets encrypted through Secure Real-Time Transport Protocol (SRTP) if the application uses a valid encryption algorithm in the device registration request and if the other party is secure.

Unified Communications Manager provides a stronger cipher suite on the Skinny Client Control Protocol (SCCP) interface for CTI ports and allows the secure media notification between the calling and called party. To enable SRTP on CTI ports, CTI application registers by providing supported algorithm IDs of cipher strength.

Unified Communications Manager is enhanced to allow negotiation of these added algorithms on a secure call involving CTI ports:

- CCM_AES_CM_128_HMAC_SHA1_32 (CiscoMediaEncryptionAlgorithmType.AES_128_COUNTER)
- CCM_AES_CM_128_HMAC_SHA1_80 (CiscoMediaEncryptionAlgorithmType.AES_128_COUNTER)
- CCM_AEAD_AES_128_GCM (CiscoMediaEncryptionAlgorithmType.AEAD_128_COUNTER)
- CCM_AEAD_AES_256_GCM (CiscoMediaEncryptionAlgorithmType.AEAD_256_COUNTER)

When you receive a call, Unified Communications Manager negotiates the media and encryption capabilities as specified by the CTI application while registering the CTI port with those of the called phone. If there is a matching algorithm, the Unified CM sends the key information to both sides to decrypt the packets and monitor or record the media.

Limitations

Unified Communications Manager does not support the CCM_F8_128_HMAC_SHA1_32 and CCM_F8_128_HMAC_SHA1_80 algorithms. If the CTI application tries to register a CTI Port terminating media with these unsupported algorithms, the Unified CM ignores it and selects the best of the remaining available algorithms. If the system does not consist of any algorithm other than these two then the Unified CM will switches to the existing behavior and selects the CCM_AES_CM_128_HMAC_SHA1_32, by default.

CAPF Functions for CTI, JTAPI, and TAPI Applications

Certificate Authority Proxy Function (CAPF), which automatically installs with Unified Communications Manager, performs the following tasks for CTI/TAPI/TAPI applications, depending on your configuration:

- Authenticates to the JTAPI/TSP client via an authentication string.
- Issues Locally Significant Certificates (LSC) to CTI/JTAPI/TAPI applicationusers or end users.
- Upgrades existing Locally Significant Certificates.
- Retrieves certificates for viewing and troubleshooting.

When the JTAPI/TSP client interacts with CAPF, the client authenticates to CAPF by using an authentication string; the client then generates its public key and private key pair and forwards its public key to the CAPF server in a signed message. The private key remains in the client and never gets exposed externally. CAPF signs the certificate and then sends the certificate back to the client in a signed message.

You issue certificates to application users or end users by configuring the settings in the Application User CAPF Profile Configuration window or End User CAPF Profile Configuration window, respectively. The

following information describes the differences between the CAPF profiles that Unified Communications Manager supports:

- **Application User CAPF Profile**—This profile allows you to issue locally significant certificates to secure application users so that a TLS connection opens between the CTIManager service and the application.

  One Application User CAPF Profile corresponds to a single instance of the service or application on a server. If you activate multiple web services or applications on the same server, you must configure multiple Application User CAPF Profiles, one for each service on the server.

  If you activate a service or application on two servers in the cluster, you must configure two Application User CAPF Profiles, one for each server.

- **End User CAPF Profile**—This profile allows you to issue locally significant certificates to CTI clients so that the CTI client communicates with the CTIManager service via a TLS connection.

Tip The JTAPI client stores the LSC in Java Key Store format in the path that you configure in the JTAPI Preferences window. The TSP client stores the LSC in an encrypted format in the default directory or in the path that you configure.

The following information applies when a communication or power failure occurs.

- If a communication failure occurs while the certificate installation is taking place, the JTAPI client attempts to obtain the certificate three more times in 30-second intervals. You cannot configure this value.

  For the TSP client, you can configure the retry attempts and the retry timer. Configure these values by specifying the number of times that the TSP client tries to obtain the certificate in an allotted time. For both values, the default equals 0. You can configure up to 3 retry attempts by specifying 1 (for one retry), 2, or 3. You can configure no more than 30 seconds for each retry attempt.

- If a power failure occurs while the JTAPI/TSP client attempts a session with CAPF, the client attempts to download the certificate after power gets restored.

CAPF System Interactions and Requirements for CTI, JTAPI, and TAPI Applications

The following requirements exist for CAPF:

- Before you configure the Application User and End User CAPF Profiles, verify that the Cluster Security Mode in the **Enterprise Parameters Configuration** window is 1 (mixed mode).
- To use CAPF, you must activate the Cisco Certificate Authority Proxy Function service on the publisher node.
- Generating many certificates at the same time may cause call-processing interruptions and we recommend that you use CAPF during a scheduled maintenance window.
- Ensure that the publisher node is functional and running during the entire certificate operation.
- Ensure that the CTI/ JTAPI/TAPI application is functional during the entire certificate operation.

Certificate Authority Proxy Function Service Activation

Unified Communications Managerdoes not automatically activate the Certificate Authority Proxy Function service in Cisco Unified Serviceability.

To use the CAPF functionality, you must activate this service on the first node.

You must update the CTL file if you did not activate this service before moving Unified Communications Manager to mixed mode.

After you activate the Cisco Certificate Authority Proxy Function service, CAPF automatically generates a key pair and certificate that is specific to CAPF. The CAPF certificate is then displayed on the Cisco Unified Communications Operating System GUI as a verification that the CAPF certificate exists.

Set Up Application User or End User CAPF Profile

Use Application and End User CAPF Profile Configuration Settings as a reference when you install/upgrade/troubleshoot locally significant certificates for JTAPI/TAPI/CTI applications.

Tip We recommend that you configure Application User CAPF Profiles before you configure End User CAPF Profiles.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose one of the following options:
a) **User Management** > **User Settings** > **Application User CAPF Profile**
b) **User Management** > **User Settings** > **End User CAPF Profile**.

Step 2 Perform one of the following tasks:
a) To edit an existing profile, click **Find** and select the existing profile.
b) To create a new profile, click **Add New**.
c) To copy settings from an existing profile to a new profile, click **Find** and select the existing profile with the settings that you want. Click **Copy** and name the new profile that will contain those settings. Then edit the new profile as needed.

Step 3 Enter the appropriate settings as described in Application and End User CAPF Profile Configuration Settings.

Step 4 Click **Save**.

Step 5 Repeat this procedure to create additional CAPF Profiles. Create as many profiles as your users need. If you configured the **CCMQRTSecureSysUser**, **IPMASecureSysUser**, or **WDSecureSysUser** in the **Application User CAPF Profile Configuration** window, you must configure **Service Parameters**.

CAPF Settings

The following table describes the CAPF settings in the **Application User CAPF Profile Configuration** and **End User CAPF Profile Configuration** windows.

Table 38: Application and End User CAPF Profile Configuration Settings

Setting	Description
Application User	From the drop-down list, choose the **application user for the CAPF operation**.This setting shows configured application users. This setting does not display in the **End User CAPF Profile** window.
End User ID	From the drop-down list, choose the **end user for the CAPF operation**. This setting shows configured end users. This setting does not display in the **Application User CAPF Profile** window.
Instance ID	Enter 1-128 alphanumeric characters (a-zA-Z0-9). The Instance ID identifies the user for the certificate operation. You can configure multiple connections (instances) of an application.To secure the connection between the application and CTIManager, ensure that each instance that runs on the application PC (for end users) or server (for application users) has a unique certificate. This field relates to the CAPF Profile Instance ID for Secure Connection to CTIManager service parameter that supports web services and applications.
Certificate Operation	From the drop-down list, choose one of the following options: • **No Pending Operation**—Displays when no certificate operation is occurring. (Default Setting) • **Install/Upgrade**—Installs a new or upgrades an existing Locally Significant Certificate for the application.
Authentication Mode	The authentication mode for the Install/Upgrade certificate operation specifies By Authentication String, which means CAPF installs/upgrades or troubleshoots a locally significant certificate only when the user/administrator enters the CAPF authentication string in the **JTAPI/TSP Preferences** window.
Authentication String	Manually enter a unique string or generate a string by clicking the **Generate String** button. Ensure that the string contains 4 to 10 digits. To install or upgrade a Locally Significant Certificate, you must enter the authentication string in the **JTAPI/TSP preferences** GUI on the applicationPC. This string supports one-time use only; after you use the string for the instance, you cannot use it again.
Generate String	If you want CAPF to automatically generate an authentication string, click the **Generate String** button. The 4- to10-digit authentication string displays in the **Authentication String** field.

Setting	Description
Key Order	This field specifies the sequence of the key for CAPF. Select one of the following values from the drop-down list: • **RSA Only** • **EC Only** • **EC Preferred, RSA Backup** **Note** When you add a phone based on the value in **Key Order**, **RSA Key Size**, and **EC Key Size** fields, the device security profile is associated with the phone. If you select the **EC Only** value with the **EC Key Size** value of 256 bits then the device security profile appends with **EC-256** value.
RSA Key Size (Bits)	From the drop-down list, choose one of the these values—**512**, **1024**, **2048, 3072**, or **4096**.
EC Key Size (Bits)	From the drop-down list, choose one of the these values—**256**, **384**, or **521**.
Operation Completes by	This field, which supports all certificate operations, specifies the date and time by which you must complete the operation. The values displayed apply for the first node. Use this setting with the **CAPF Operation Expires in (days)** enterprise parameter, which specifies the default number of days in which the certificate operation must be completed. You can update this parameter any time.
Certificate Operation Status	This field displays the progress of the certificate operation, such as pending, failed, or successful. You cannot change the information that displays in this field.

Update CAPF Service Parameters

The **Service Parameter** window contains optional settings for the Cisco Certificate Authority Proxy Function. You can configure settings such as the Certificate Issuer, Online CA connection settings, Certificate Validity duration, and key size for the CAPF certificate.

For the CAPF service parameters to display as Active in Cisco Unified Communications Manager Administration, Activate the **Certificate Authority Proxy Function** service in Cisco Unified Serviceability.

Tip If you updated the CAPF service parameters when you used CAPF for the phones, you do not need to update the service parameters again.

To update the CAPF service parameters, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the server.

Tip
You must choose the publisher node in the cluster.

Step 3 From the **Service** drop-down list, choose the **CiscoCertificate Authority Proxy Function** service. Verify that the word "Active" displays next to the service name.

Step 4 Update the **CAPF service parameters**, as described in the Online help. To display help for the **CAPF service parameters**, click the question mark or the parameter name link.

Step 5 For the changes to take effect, restart the **Cisco Certificate Authority Proxy Function** service in Cisco Unified Serviceability.

Note
For more information on how to configure the Certificate Authority Proxy Function, See **Certificate Authority Proxy Function** chapter.

Delete Application User CAPF or End User CAPF Profile

Before you can delete an Application User CAPF Profile or End User CAPF Profile from Cisco Unified Communications Manager Administration, you must apply a different profile to the devices or delete all devices that use the profile. To find out which devices use the profile, choose **Dependency Records** from the **Related Links** drop-down list in the **Security Profile Configuration** window and click **Go**.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records; the message also displays information about high CPU consumption that is related to the dependency records feature. For more information about dependency records, refer to the System Configuration Guide for Cisco Unified Communications Manager.

This section describes how to delete an Application User CAPF Profile or End User CAPF Profile from the Unified Communications Manager database.

Procedure

Step 1 Find the Application User CAPF Profile or End User CAPF Profile.

Step 2 Perform one of the following tasks:

a) To delete multiple profiles, check the check boxes next to the appropriate check box in the **Find and List** window; then, click **Delete Selected**. You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

b) To delete a single profile, check the check box next to the appropriate profile In the **Find and List** window; then, click **Delete Selected**.

Step 3 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Securing CTI, JTAPI, and TAPI

The following procedure provides the tasks that you perform to secure the CTI/JTAPI/TAPI application.

Procedure

Step 1 Verify that the CTI application and any JTAPI/TSP plug-ins are installed and running.

Tip
Assign the application user to the Standard CTI Enabled group.

See the following documentation for more information:

- *Cisco JTAPI Installation Guide for Unified Communications Manager*
- *Cisco TAPI Installation Guide for Unified Communications Manager*

Step 2 Verify that the following Unified Communications Manager security features are installed (if not installed, install and configure these features):

- Verify if the Unified Communications Manager is in Mixed Mode by running the utlis ctl command set.
- Verify if the CAPF service is installed and that the service is activated. If necessary, update CAPF service parameters.

  Tip
  The CAPF service must run for the **utils ctl** CLI command to include the CAPF certificate in the CTL file. If you updated these parameters when you used CAPF for the phones, you do not need to update the parameters again.

- Verify if the cluster security mode is set to Mixed Mode. (Cluster security mode configures the security capability for your standalone server or cluster.)

  Tip
  The CTI/JTAPI/TAPI application cannot access the CTL file if the cluster security mode does not equal Mixed Mode.

Step 3 Assign your end users and application users to access control groups that contain the permissions they need. Assign your users to all of the following groups so that they can use **TLS** and **SRTP** over CTI connections:

- Standard CTI Enabled
- Standard CTI Secure Connection
- Standard CTI Allow Reception of SRTP Key Material

Tip
A CTI application can be assigned to either an application user or an end user, but not both.

The user must already exist in the **Standard CTI Enabled and Standard CTI Secure Connection** user group. The application or end user cannot receive SRTP session keys if it does not exist in these three groups. For more information, see topics related to User access control group configurations.

Note
Cisco Unified Communications Manager Assistant, Cisco QRT, and Cisco Web Dialer do not support encryption. CTI clients that connect to the CTIManager service may support encryption if the client sends voice packets.

Step 4 Configure CAPF Profiles for your end users and application users. For more information, see **Certificate Authority Proxy Function** chapter.

Step 5 Enable the corresponding security-related parameters in the CTI/JTAPI/TAPI application.

Add Application and End Users to Security-Related Access Control Groups

The Standard CTI Secure Connection user group and the Standard CTI Allow Reception of SRTP Key Material user group display in Unified Communications Manager by default. You cannot delete these groups.

To secure the user connection to CTIManager, you must add the application user or end users to the Standard CTI Secure Connection user group. You can assign a CTI application to either an application user or an end user, but not both.

If you want the application and CTIManager to secure the media streams, you must add the application user or end users to the Standard CTI Allow Reception of SRTP Key Material user group.

Before the application and end user can use SRTP, the user must exist in the Standard CTI Enabled and Standard CTI Secure Connection user groups, which serve as a baseline configuration for TLS. SRTP connections require TLS. After the user exists in these groups, you can add the user to the Standard CTI Allow Reception of SRTP Key Material user group. For an application to receive SRTP session keys, the application or end user must exist in three groups: **Standard CTI Enabled**, **Standard CTI Secure Connection**, and **Standard CTI Allow Reception of SRTP Key Material**.

You do not need to add the application users, CCMQRTSecureSysUser, IPMASecureSysUser, and the WDSecureSysUser, to the Standard CTI Allow Reception of SRTP Key Material user group because Cisco Unified Communications Manager Assistant, CiscoQRT, and Cisco Web Dialer do not support encryption.

Tip For information on deleting an application or end user from a user group, refer to the Administration Guide for Cisco Unified Communications Manager. For information about security-related settings in the **Role Configuration** window, refer to the Administration Guide for Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **User Groups**.

Step 2 To display all **user groups**, click **Find**.

Step 3 Depending on what you want to accomplish, perform one of the following tasks:

a) Verify that the application or end users exist in the Standard CTI Enabled group.
b) To add an application user or end users to the **Standard CTI Secure Connection user group**, click the **Standard CTI Secure Connection** link.
c) To add an application user or end users to the **Standard CTI Allow Reception of SRTP Key Material user group**, click the **Standard CTI Allow Reception of SRTP Key Material** link.

Step 4 To add an application user to the group, perform steps 5 through 7.

Step 5 Click **Add Application Users to Group**.

Step 6 To find an application user, specify the search criteria; then, click **Find**.

Clicking Find without specifying search criteria displays all available options.

Step 7 Check the check boxes for the application users that you want to add to the group; then, click **Add Selected**.

The users are displayed in the **User Group** window.

Step 8 To add end users to the group, perform steps 9 through 11.

Step 9 Click **Add Users to Group**.

Step 10 To find an end user, specify the search criteria; then, click **Find**.

Clicking Find without specifying search criteria displays all available options.

Step 11 Check the check boxes for the end users that you want to add to the group; then, click **Add Selected**.

The users are displayed in the **User Group** window.

Set Up JTAPI/TAPI Security-Related Service Parameters

After you configure the Application User CAPF Profile or End User CAPF Profile, you must configure the following service parameters for **Cisco IP Manager Assistant** service:

- CTIManager Connection Security Flag
- CAPF Profile Instance ID for Secure Connection to CTIManager

To access the service parameters, perform the following procedure:

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the server where the **Cisco IP Manager Assistant** service is activated.

Step 3 From the **Service** drop-down list, choose the **Cisco IP Manager Assistant** service.

Step 4 After the parameters display, locate the **CTIManager Connection Security Flag** and **CAPF Profile Instance ID** for Secure Connection to **CTIManager parameters**.

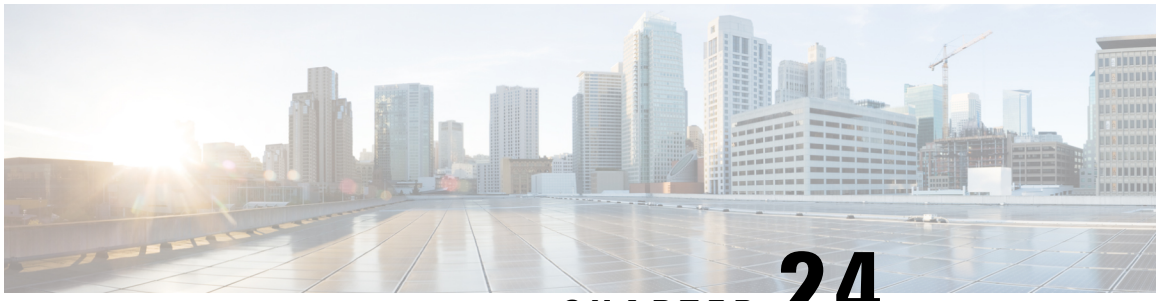
Step 5 Update the parameters, as described in the help that displays when you click the question mark or parameter name link.

Step 6 Click **Save**.

Step 7 Repeat the procedure on each server where the service is activated.

View Certificate Operation Status for Application or End User

You can view the certificate operation status in a specific **Application User** or **End User CAPF Profile configuration** window (not the **Find/List** window) or in the **JTAPI/TSP Preferences** GUI window.



CHAPTER 24

Secure Recording and Monitoring

- About Secure Call Monitoring and Recording Setup, on page 271
- Set Up Secure Call Monitoring and Recording, on page 272

About Secure Call Monitoring and Recording Setup

Secure calls can be monitored and recorded, as described in this section:

- A supervisor can establish a secured monitoring session for a secured or a non-secured call.
- The call security of the original call is never impacted or downgraded as a result of a call monitoring request.
- The monitoring call is allowed to proceed only when it can be established and maintained at the same security level as the device capability of the agent.
- The original call between the agent and customer must have different crypto keys than that of monitoring call. In a monitoring session, the system encrypts the mixed voices of the agent and customer with the new key first before sending to the supervisor.

Note Unified Communications Manager supports call recording for authenticated calls while using a nonsecure recorder. For calls with a secure call recorder, recording is allowed only if the recorder supports SRTP fallback, so that the media stream to the recorder falls back to RTP.

To record calls that use authenticated phones:

- Set the **Authenticated Phone Recording**, a Cisco CallManager service parameter, to **Allow Recording**. In this case, the call is authenticated, but the connection to the recording server is unauthenticated and unencrypted.
- Unified Communications Manager should be always configured in a Mixed mode cluster security for SIP OAuth enabled phones to make secure recordings.

Set Up Secure Call Monitoring and Recording

Use this procedure to configure Secure Call Monitoring and Recording.

Procedure

Step 1 Provision secure capability on agent and supervisor phones.

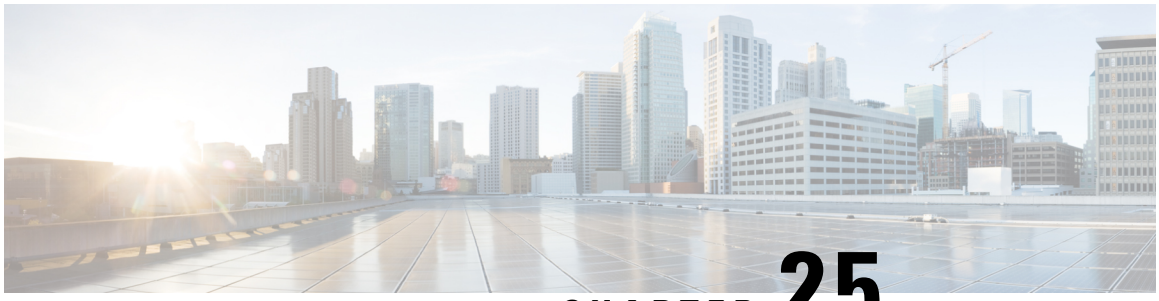
Step 2 Create a secure SIP trunk with the following configuration:

- Set the **Device Security Mode** to Encrypted.
- Check the **Transmit Security Status** check box.
- Check the **SRTP Allowed** check box.
- Configure the **TLS SIP trunk** to the recorder.

Step 3 Configure monitoring and recording, in the same way you would for non-secure monitoring and recording.

a) Configure a built-in bridge for the agent phone.
b) Configure the Recording Option (**Automatic Call Recording Enabled and Application Invoked Call Recording Enabled**.) using the **Directory Number** page on the agent phone.
c) Create a **route pattern** for the recorder.
d) Add a **call recording profile** to the Directory Number.
e) Provision monitoring and recording tones as needed.

For more information and detailed procedures, see the "Monitoring and Recording" chapter in the Feature Configuration Guide for Cisco Unified Communications Manager.



CHAPTER 25

VPN Client

- VPN Client Overview, on page 273
- VPN Client Configuration Task Flow, on page 273

VPN Client Overview

The Cisco VPN Client for Cisco Unified IP Phone creates a secure VPN connection for employees who telecommute. All settings of the Cisco VPN Client are configured through Cisco Unified Communications Manager Administration. After the phone is configured within the Enterprise, the users can plug it into their broadband router for instant connectivity.

Note The VPN menu and its options are not available in the U.S. export unrestricted version of Unified Communications Manager.

VPN Client Configuration Task Flow

Pre-provision the phone and establish the initial connection inside the corporate network to retrieve the phone configuration. You can make subsequent connections using VPN, as the configuration is already retrieved on the phone.

Procedure

	Command or Action	Purpose
Step 1	Complete Cisco IOS Prerequisites, on page 274	Complete Cisco IOS prerequisites. Perform this action if you want to configure Cisco IOS VPN.
Step 2	Configure Cisco IOS SSL VPN to Support IP Phones , on page 275	Configure Cisco IOS for VPN client on an IP Phone. Perform this action if you want to configure Cisco IOS VPN.

	Command or Action	Purpose
Step 3	Complete ASA Prerequisites for AnyConnect, on page 277	Complete ASA prerequisites for AnyConnect. Perform this action if you want to configure ASA VPN.
Step 4	Configure ASA for VPN Client on IP Phone, on page 277	Configure ASA for VPN client on an IP Phone. Perform this action if you want to configure ASA VPN.
Step 5	Configure the VPN concentrators for each VPN Gateway.	To avoid long delays when the user upgrades the firmware or configuration information on a remote phone, set up the VPN concentrator close in the network to the TFTP or Unified Communications Manager server. If this is not feasible in your network, you can set up an alternate TFTP or load server that is next to the VPN concentrator.
Step 6	Upload VPN Concentrator Certificates, on page 279	Upload the VPN concentrator certificates.
Step 7	Configure VPN Gateway, on page 280	Configure the VPN gateways.
Step 8	Configure VPN Group, on page 281	After you create a VPN group, you can add one of the VPN gateways that you just configured to it.
Step 9	Perform one of the following: • Configure VPN Profile, on page 282 • Configure VPN Feature Parameters, on page 283	You must configure a VPN profile only if you have multiple VPN groups. The VPN Profile fields take precedence over the VPN Feature Configuration fields.
Step 10	Add VPN Details to Common Phone Profile, on page 285	Add the VPN Group and VPN Profile to a Common Phone Profile.
Step 11	Upgrade the firmware for Cisco Unified IP Phone to a version that supports VPN.	To run the Cisco VPN client, a supported Cisco Unified IP Phone must be running firmware release 9.0(2) or higher. For more information about upgrading the firmware, see *Cisco Unified IP Phone Administration Guide* for Unified Communications Manager for yourCisco Unified IP Phone model.
Step 12	Using a supported Cisco Unified IP Phone, establish the VPN connection.	Connect your Cisco Unified IP Phone to a VPN.

Complete Cisco IOS Prerequisites

Use this procedure to complete Cisco IOS Prerequisites.

Procedure

Step 1 Install Cisco IOS Software version 15.1(2)T or later.

Feature Set/License: Universal (Data & Security & UC) for IOS ISR-G2 and ISR-G3

Feature Set/License: Advanced Security for IOS ISR

Step 2 Activate the SSL VPN License.

Configure Cisco IOS SSL VPN to Support IP Phones

Use this procedure to complete Cisco IOS SSL VPN to Support IP Phones.

Procedure

Step 1 Configure Cisco IOS locally.

a) Configure the Network Interface.

Example:

```
router(config)# interface GigabitEthernet0/0
router(config-if)# description "outside interface"
router(config-if)# ip address 10.1.1.1 255.255.255.0
router(config-if)# duplex auto
router(config-if)# speed auto
router(config-if)# no shutdown
router#show ip interface brief (shows interfaces summary)
```

b) Configure static and default routes by using this command:

router(config)# **ip route** <*dest_ip*> < *mask*> < *gateway_ip*>

Example:

```
router(config)# ip route 10.10.10.0 255.255.255.0 192.168.1.1
```

Step 2 Generate and register the CAPF certificate to authenticate the IP phones with an LSC.

Step 3 Import the CAPF certificate from Unified Communications Manager.

a) From the Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Note
This location changes based on the Unified Communications Manager version.

b) Find the Cisco_Manufacturing_CA and CAPF certificates. Download the.pem file and save as.txt file.

c) Create trustpoint on the Cisco IOS software.

```
hostname(config)# crypto pki trustpoint trustpoint_name
hostname(config-ca-trustpoint)# enrollment terminal
hostname(config)# crypto pki authenticate trustpoint
```

When prompted for the base 64-encoded CA certificate, copy and paste the text in the downloaded .pem file along with the BEGIN and END lines. Repeat the procedure for the other certificates.

d) Generate the following Cisco IOS self-signed certificates and register them with Unified Communications Manager, or replace with a certificate that you import from a CA.

- Generate a self-signed certificate.

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 2048 2048
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Generate a self-signed certificate with Host-id check enabled on the VPN profile in Unified Communications Manager.

  Example:

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# fqdn <full domain
name>Router(config-ca-trustpoint)# subject-name CN=<full domain
name>, CN=<IP>Router(ca-trustpoint)#authorization username
subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Register the generated certificate with Unified Communications Manager.

  Example:

```
Router(config)# crypto pki export <name> pem terminal
```

  Copy the text from the terminal and save it as a.pem file and upload it to the Unified Communications Manager using the Cisco Unified OS Administration.

Step 4 Install AnyConnect on Cisco IOS.

Download the Anyconnect package from cisco.com and install to flash.

Example:

```
router(config)#webvpn install svc
flash:/webvpn/anyconnect-win-2.3.2016-k9.pkg
```

Step 5 Configure the VPN feature.

Note
To use the phone with both certificate and password authentication, create a user with the phone MAC address. Username matching is case sensitive. For example:

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
```

Complete ASA Prerequisites for AnyConnect

Use this procedure to complete ASA Prerequisites for AnyConnect.

Procedure

Step 1 Install ASA software (version 8.0.4 or later) and a compatible ASDM.

Step 2 Install a compatible AnyConnect package.

Step 3 Activate License.

a) Check features of the current license using the following command:

show activation-key detail

b) If necessary, obtain a new license with additional SSL VPN sessions and enable the Linksys phone.

Step 4 Make sure that you configure a tunnel-group with a non-default URL as follows:

```
tunnel-group phonevpn type remote-access
tunnel-group phonevpn general-attribute
  address-pool vpnpool
tunnel-group phonevpn webvpn-attributes
  group-url https://172.18.254.172/phonevpn enable
```

Consider the following when configuring non-default URL:

- If the IP address of the ASA has a public DNS entry, you can replace it with a Fully Qualified Domain Name (FQDN).
- You can only use a single URL (FQDN or IP address) on the VPN gateway in Unified Communications Manager.
- It is preferred to have the certificate CN or subject alternate name match the FQDN or IP address in the group-url.
- If the ASA certificate CN or SAN does not match with the FQDN or IP address, uncheck the host ID check box in the Unified Communications Manager.

Configure ASA for VPN Client on IP Phone

Use this procedure to configure ASA for VPN Client on IP Phone.

Note Replacing ASA certificates results in non-availability of Unified Communications Manager.

Procedure

Step 1 Local configuration

a) Configure network interface.

Example:

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.89.79.135 255.255.255.0
ciscoasa(config-if)# duplex auto
ciscoasa(config-if)# speed auto
ciscoasa(config-if)# no shutdown
ciscoasa#show interface ip brief (shows interfaces summary)
```

b) Configure static routes and default routes.

ciscoasa(config)# **route** <interface_name> <ip_address> <netmask> <gateway_ip>

Example:

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.89.79.129
```

c) Configure the DNS.

Example:

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

Step 2 Generate and register the necessary certificates for Unified Communications Manager and ASA.

Import the following certificates from the Unified Communications Manager.

- CallManager - Authenticating the Cisco UCM during TLS handshake (Only required for mixed-mode clusters).
- Cisco_Manufacturing_CA - Authenticating IP phones with a Manufacturer Installed Certificate (MIC).
- CAPF - Authenticating IP phones with an LSC.

To import these Unified Communications Manager certificates, do the following:

a) From the Cisco Unified OS Administration, choose **Security** > **Certificate Management**.
b) Locate the certificates Cisco_Manufacturing_CA and CAPF. Download the `.pem` file and save asa `.txt` file.
c) Create trustpoint on the ASA.

Example:

```
ciscoasa(config)# crypto ca trustpoint trustpoint_name
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate trustpoint_name
```

When prompted for base 64 encoded CA Certificate, copy-paste the text in the downloaded `.pem` file along with the BEGIN and END lines. Repeat the procedure for the other certificates.

d) Generate the following ASA self-signed certificates and register them with Unified Communications Manager, or replace with a certificate that you import from a CA.

- Generate a self-signed certificate.

  Example:

```
ciscoasa> enable
ciscoasa# configure terminal
```

```
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# keypair <name>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Generate a self-signed certificate with Host-id check enabled on the VPN profile in Unified Communications Manager.

  Example:

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# fqdn <full domain name>
ciscoasa(config-ca-trustpoint)# subject-name CN=<full domain name>,CN=<IP>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Register the generated certificate with Unified Communications Manager.

  Example:

```
ciscoasa(config)# crypto ca export <name> identity-certificate
```

  Copy the text from the terminal and save it as a.pem file and upload it to Unified Communications Manager.

Step 3 Configure the VPN feature. You can use the Sample ASA configuration summary below to guide you with the configuration.

Note
To use the phone with both certificate and password authentication, create a user with the phone MAC address. Username matching is case sensitive. For example:

```
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB attributes
ciscoasa(config-username)# vpn-group-policy GroupPhoneWebvpn
ciscoasa(config-username)#service-type remote-access
```

ASA Certificate Configuration

For more information on *ASA certificate configuration*, see Configure AnyConnect VPN Phone with Certificate Authentication on an ASA

Upload VPN Concentrator Certificates

Generate a certificate on the ASA when you set it up to support the VPN feature. Download the generated certificate to your PC or workstation and then upload it to Unified Communications Manager using the procedure in this section. Unified Communications Manager saves the certificate in the Phone-VPN-trust list.

The ASA sends this certificate during the SSL handshake, and the Cisco Unified IP Phone compares it against the values stored in the Phone-VPN-trust list.

If a Locally Significant Certificate (LSC) is installed on the Cisco Unified IP Phone, it will send its LSC by default.

To use device level certificate authentication, install the root MIC or CAPF certificate in the ASA, so that the Cisco Unified IP Phone are trusted.

To upload certificates to Unified Communications Manager, use the Cisco Unified OS Administration.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Certificate Management**.

Step 2 Click **Upload Certificate**.

Step 3 From the **Certificate Purpose** drop-down list, choose **Phone-VPN-trust**.

Step 4 Click **Browse** to choose the file that you want to upload.

Step 5 Click **Upload File**.

Step 6 Choose another file to upload or click **Close**.

For more information, see *Certificate Management* chapter.

Configure VPN Gateway

Ensure that you have configured VPN concentrators for each VPN gateway. After configuring the VPN concentrators, upload the VPN concentrator certificates. For more information, see Upload VPN Concentrator Certificates, on page 279.

Use this procedure to configure the VPN Gateway.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **VPN** > **VPN Gateway**.

Step 2 Perform one of the following tasks:

a) Click **Add New** to configure new profile.
b) Click the **Copy** next to the VPN gateway that you want to copy.
c) Locate the appropriate VPN gateway and modify the settings to update an existing profile.

Step 3 Configure the fields in the **VPN Gateway Configuration** window. For more information, see VPN Gateway Fields for VPN Client, on page 281.

Step 4 Click **Save**.

VPN Gateway Fields for VPN Client

The table describes the VPN Gateway fields for VPN Client.

Table 39: VPN Gateway Fields for VPN Client

Field	Description
VPN Gateway Name	Enter the name of the VPN gateway.
VPN Gateway Description	Enter a description of the VPN gateway.
VPN Gateway URL	Enter the URL for the main VPN concentrator in the gateway. **Note** You must configure the VPN concentrator with a group URL and use this URL as the gateway URL. For configuration information, refer to the documentation for the VPN concentrator, such as the following: • *SSL VPN Client (SVC) on ASA with ASDM Configuration Example*
VPN Certificates in this Gateway	Use the up and down arrow keys to assign certificates to the gateway. If you do not assign a certificate for the gateway, the VPN client fails to connect to that concentrator. **Note** You can assign up to 10 certificates to a VPN gateway, and you must assign at least one certificate to each gateway. Only certificates that are associated with the Phone-VPN-trust role appear in the available VPN certificates list.

Configure VPN Group

Use this procedure to configure VPN Group.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **VPN** > **VPN Group**.

Step 2 Perform one of the following tasks:

a) Click **Add New** to configure new profile.
b) Click **Copy** next to the VPN group that you want to copy an existing VPN group.
c) Locate the appropriate VPN group and modify the settings to update an existing profile.

Step 3 Configure the fields in the **VPN Group Configuration** window. For more information, see VPN Gateway Fields for VPN Client, on page 281 for the field description details.

Step 4 Click **Save**.

VPN Group Fields for VPN Client

The table describes the VPN Group Fields for VPN Client.

Table 40: VPN Group Fields for VPN Client

Field	Definition
VPN Group Name	Enter the name of the VPN group.
VPN Group Description	Enter a description of the VPN group.
All Available VPN Gateways	Scroll to see all available VPN gateways.
Selected VPN Gateways in this VPN Group	Use the up and down arrow buttons to move available VPN gateways into and out of this VPN group. If the VPN client encounters critical error and cannot connect to a particular VPN gateway, it will attempt to move to the next VPN gateway in the list. **Note** You can add up to a maximum of three VPN gateways to a VPN group. Also, the total number of certificates in the VPN group cannot exceed 10.

Configure VPN Profile

Use this procedure to configure the VPN Profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **VPN** > **VPN Profile**.

Step 2 Perform one of the following tasks:

a) Click **Add New** to configure new profle.
b) Click **Copy** next to the VPN profile that you want to copy an existing profile.
c) To update an existing profile, specify the appropriate filters in the **Find VPN Profile Where**, click **Find**, and modify the settings.

Step 3 Configure the fields in the **VPN Profile Configuration** window. For more information, see VPN Profile Fields for VPN Client, on page 282 for the field description details.

Step 4 Click **Save**.

VPN Profile Fields for VPN Client

The table describes the VPN profile field details.

Table 41: VPN Profile Field Details

Field	Definition
Name	Enter a name for the VPN profile.
Description	Enter a description for the VPN profile.
Enable Auto Network Detect	When you check this check box, the VPN client can only run when it detects that it is out of the corporate network. Default: Disabled.
MTU	Enter the size, in bytes, for the Maximum Transmission Unit (MTU). Default: 1290 bytes.
Fail to Connect	This field specifies the amount of time to wait for login or connect operations to complete while the system creates the VPN tunnel. Default: 30 seconds
Enable Host ID Check	When you check this check box, the gateway certificate subjectAltName or CN must match the URL to which the VPN client is connected. Default: Enabled
Client Authentication Method	From the drop-down list, choose the client authentication method: • User and password • Password only • Certificate (LSC or MIC)
Enable Password Persistence	When you check this check box, a user password gets saved in the phone until either a failed log in attempt occurs, a user manually clears the password, or the phone resets or loses power.

Configure VPN Feature Parameters

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **VPN** > **VPN Feature Configuration**.

Step 2 Configure the fields in the **VPN Feature Configuration** window. For more information, see VPN Feature Parameters, on page 284.

Step 3 Click **Save**.

Perform the following tasks:

- Upgrade the firmware for Cisco Unified IP Phones to a version that supports VPN. For more information about upgrading the firmware, see *Cisco Unified IP Phone Administration Guide* for your Cisco Unified IP Phone model.

- Using a supported Cisco Unified IP Phone, establish the VPN connection.

VPN Feature Parameters

The table describes the VPN feature parameters.

Table 42: VPN Feature Parameters

Field	Default
Enable Auto Network Detect	When True, the VPN client can only run when it detects that it is out of the corporate network. Default: False
MTU	This field specifies the maximum transmission unit: Default: 1290 bytes Minimum: 256 bytes Maximum: 1406 bytes
Keep Alive	This field specifies the rate at which the system sends the keep alive message. **Note** If it is non zero and less than the value specified in Unified Communications Manager, the keep alive setting in the VPN concentrator overwrites this setting. Default: 60 seconds Minimum: 0 Maximum: 120 seconds
Fail to Connect	This field specifies the amount of time to wait for login or connect operations to complete while the system creates the VPN tunnel. Default: 30 seconds Minimum: 0 Maximum: 600 seconds
Client Authentication Method	From the drop-down list, choose the client authentication method: • User and password • Password only • Certificate (LSC or MIC) Default: User And Password

Field	Default
Enable Password Persistence	When True, a user password gets saved in the phone, if Reset button or "**#**" is used for reset. The password does not get saved and the phone prompts for credentials if the phone loses power or you initiate a factory reset. Default: False
Enable Host ID Check	When True, the gateway certificate subjectAltName or CN must match the URL to which the VPN client is connected. Default: True

Add VPN Details to Common Phone Profile

Use this procedure to add VPN details to common phone profile.

Procedure

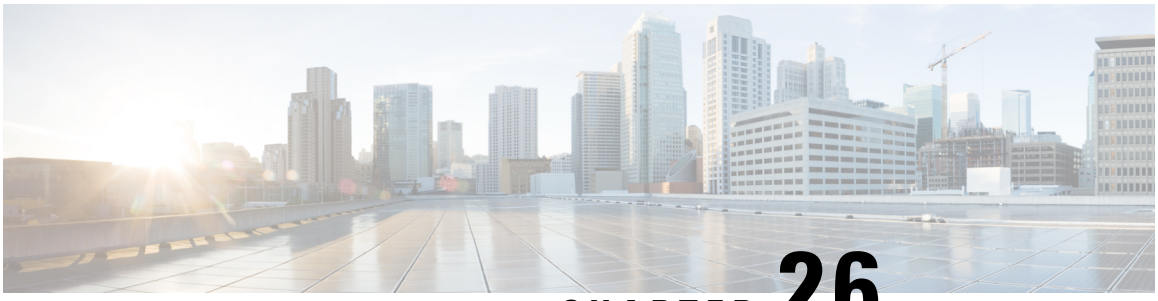
Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Common Phone Profile**.

Step 2 Click **Find** and choose common phone profile to which you want to add the VPN details.

Step 3 In the **VPN Information** section, choose the appropriate **VPN Group** and **VPN Profile**.

Step 4 Click **Save** and then **Apply Config**.

Step 5 Click **OK** in apply configuration window.



CHAPTER 26

Operating System and Security Hardening

- Security Hardening, on page 287

Security Hardening

Unified Communications Manager runs as a virtual machine on top of virtualized hardware based on VMware vSphere ESXi. Unlike conventional server-based products, Unified Communications Manager is a software product distributed as a closed-system, turnkey-packaged, “appliance” workload, which:

- Reduces the attack surface
- Provides a more stable, higher performance configuration
- Avoids vulnerabilities from configuration errors
- Simplifies administration and corrective maintenance without requiring OS / DB skill sets

Highlights of Unified Communications Manager workload-layer hardening include:

- Unified Communications Manager isn't a general-purpose / open-system workload.
  - It doesn't use a general-purpose OS distribution.
    - Unused modules are excluded from the image and unused services are disabled / removed.
    - We make proprietary hardening changes to specific modules (for example, OpenSSL is hardened by Cisco’s Security and Trust Organization; the resulting CiscoSSL is incorporated into the product).
  - Native interfaces to guest Operating System, Database, runtime, and other workload software components are not exposed.
    - They are either removed or hidden and locked-down.
    - Access is only through Cisco-provided browser-based GUI, CLI, or API, with various mechanisms to secure those interfaces (e.g., CLI via SSH, or pull files into workload via Secure FTP).
  - The product comprises a carefully controlled stack that contains all software required to operate, maintain, secure, and manage the application. We specify, install and update all this software through images provided and digitally signed by Cisco.

- All of the above information are subject to the development and test processes of the Cisco Secure Product Lifecycle development approach, as described here: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-development-lifecycle.pdf

- The Unified Communications Manager workload layer does not support insertion of non-Cisco software or software updates/changes outside the above-mentioned controlled Cisco-provided interfaces.
  - All software within the workload is provided by Cisco and digitally signed and delivered as a monolithic image (.ISO file).
  - The only way to install, upgrade and update software is by using a Cisco-provided .ISO or .COP file.
  - .ISO file installs or updates one, some, or all of the software elements in the Cisco image .COP files are used to update single elements, most commonly user locales and phone firmware updates.
  - The following are not enabled or possible:
    - onboard agents like anti-virus clients, UPS agents, management agents and so on.
    - customer-uploadable or externally-uploadable software.
    - 3rd-party applications.

- “Root access” to the guest OS inside the workload is not enabled:
  - Customers use authentication in the Cisco-provided GUI, CLI, and/or API.
  - All exposed interfaces to the workload are secured (e.g., enforced password complexity rules, SSH instead of telnet, TLS 1.2 with configurable minimum version and so on.)
  - For emergency issues that are not fixable in the field thru the normal GUI/CLI/API, customers can set up a temporary "Remote Account" so that a Cisco Technical Assistance Center (TAC) expert can gain root access. The customer maintain controls and can turn on or turn off this account with auto-expiry. The customer can see what the TAC representative is doing with all actions being performed by TAC being logged.

- Built-in Intrusion Prevention Capabilities:
  - SELinux enforcing mode, providing host-based intrusion protection.
    - SELinux enforcing mode is enabled by default. This mode enforces mandatory access controls that confine applications, daemons, etc. to the “least privilege” required to do their job.
  - IPTables host-based firewall:
    - IPTables is enabled by default.
    - The rules are adjusted by Cisco Service Activation to open the appropriate ports and include the correct rate limiting for the services being used on that server.
    - The IPTable rules can be displayed using the following commands:
      - **utils firewall ipv4 list**
      - **utils firewall ipv6 list**

In addition to the above hardening features, Unified Communications Manager workload performs security audit logging for OS, DB and application software. There are three security audit logs included:

- Linux auditd log.
- Unified CM Application audit log.
- Informix database audit log.

There are also configuration settings that allow the system administrator to configure the system to comply with the organization's infosec requirements. The system administrator-configurable security settings and utilities include, but are not limited to:

- Defining password policies. All passwords and PINs are hashed or encrypted and not stored as clear text.
- Account lockout settings and credential policy.
- Warning banner text.
- Enabling TLS/SRTP for signaling and media.
- Phone hardening settings.
- IPSec to secure connections which do not use TLS.
- Changing the self-signed PKI certificates to CA signed.
- Enabling FIPS mode or Common Criteria mode.
- Enabling SAML Single Sign-On which includes support for smart cards or bio-metric readers.
- View all network connections, processes, active packages.
    - "show network status detail all nodns" Retrieves details on open ports, equivalent to a "netstat -an" Unix command.
    - "show process list detail" Retrieves a list of all the processes and critical information about each process, equivalent to a "ps -ef" Unix command.
    - "show packages active" Displays the name and version for installed and active packages.

More details on configurable security options are in the Security Guide for Cisco Unified Communications Manager.

Cisco's UC offerings are regularly tested and validated to be compliant with a range of government certifications, including:

- Department of Defense Information Network Approved Products List (DoDIN APL)
- FIPS 140-2 Level 1
- FedRAMP
- Common Criteria
- Applicable U.S. Department of Defense Security Technical Implementation Guides (STIGs)

For additional information on Cisco government certifications, see https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications.html

For security vulnerability alerts and management, the entire Unified Communications Manager workload falls under the umbrella of the Cisco Product Security Incident Response Team (PSIRT). Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of information about security vulnerabilities and issues related to Cisco products. You should:

- Monitor the Cisco Security Advisories and Alerts page (https://tools.cisco.com/security/center/publicationListing.x) for alerts concerning security issues that may affect your deployment.
- View the Cisco.com security advisory page for a given PSIRT to learn affected products, workarounds, and permanent fixes.

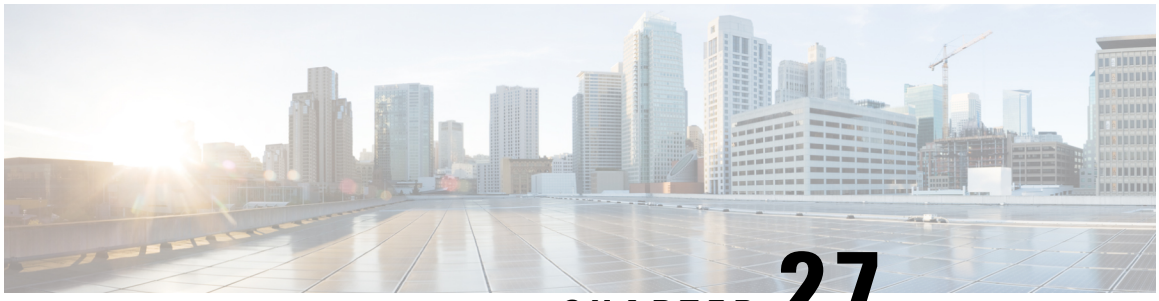
For more information, see: https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html



PART V

Troubleshooting

- Security Troubleshooting Overview, on page 293



CHAPTER 27

Security Troubleshooting Overview

- Remote Access, on page 293
- Cisco Secure Telnet, on page 294
- Set up a Remote Account, on page 295

Remote Access

Remote access provides you with the ability to establish Terminal Services (remote port 3389), HTTP (remote port 80), and Telnet (remote port 23) sessions to all the necessary equipment.

Caution When you are setting up dial-in, do not use **login:cisco** or **password:cisco** because they constitute a vulnerability to the system.

You may resolve many issues very quickly by allowing the TAC engineer remote access to the devices through one of the following methods:

- Equipment with public IP address.
- Dial-in access—In decreasing order of preference: analog modem, Integrated Services Digital Network (ISDN) modem, virtual private network (VPN).
- Network Address Translation (NAT)—IOS and private Internet exchange (PIX) to allow access to equipment with private IP addresses.

Ensure that firewalls do not obstruct IOS traffic and PIX traffic during engineer intervention and that all necessary services, such as Terminal Services, start on the servers.

Note TAC handles all access information with the utmost discretion, and no changes will get made to the system without customer consent.

Cisco Secure Telnet

Cisco Secure Telnet offers Cisco Service Engineers (CSE) transparent firewall access to Unified Communications Manager servers on your site.

Cisco Secure Telnet works by enabling a Telnet client inside the Cisco Systems firewall to connect to a Telnet daemon behind your firewall. This secure connection allows remote monitoring and maintenance of your Unified Communications Manager servers without requiring firewall modifications.

Note Cisco accesses your network only with your permission. You must provide a network administrator at your site to help initiate the process.

Firewall Protection

Virtually all internal networks use firewall applications to restrict outside access to internal host systems. These applications protect your network by restricting IP connections between the network and the public Internet.

Firewalls work by automatically blocking TCP/IP connections that are initiated from the outside, unless the software is reconfigured to allow such access.

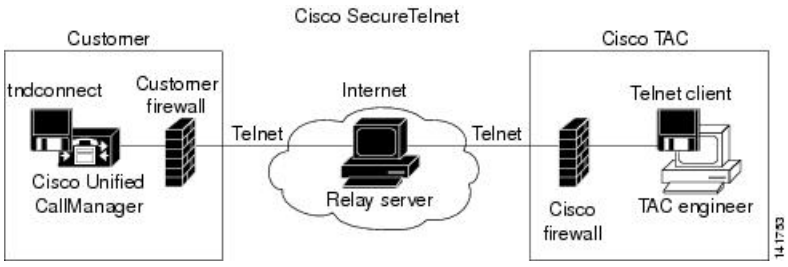
Corporate networks normally permit communication with the public Internet but only if connections directed to outside hosts originate from inside the firewall.

Cisco Secure Telnet Design

Cisco Secure Telnet takes advantage of the fact that Telnet connections can easily be initiated from behind a firewall. Using an external proxy machine, the system relays TCP/IP communications from behind your firewall to a host behind another firewall at the *Cisco Technical Assistance Center* (TAC).

Using this relay server maintains the integrity of both firewalls while secure communication between the shielded remote systems get supported.

Figure 1: Cisco Secure Telnet System



Cisco Secure Telnet Structure

The external relay server establishes the connection between your network and Cisco Systems by building a Telnet tunnel. This enables you to transmit the IP address and password identifier of your Unified Communications Manager server to your CSE.



Note The password comprises a text string upon which your administrator and the CSE mutually agree.

Your administrator starts the process by initiating the Telnet tunnel, which establishes a TCP connection from inside your firewall out to the relay server on the public Internet. The Telnet tunnel then establishes another connection to your local Telnet server, creating a two-way link between the entities.



Note The Telnet client at the Cisco TAC runs in compliance with systems that run on Windows NT and Windows 2000 or with UNIX operating systems.

After the Cisco Communications Manager at your site accepts the password, the Telnet client that is running at the Cisco TAC connects to the Telnet daemon that is running behind your firewall. The resulting transparent connection allows the same access as if the machine were being used locally.

After the Telnet connection is stable, the CSE can implement all remote serviceability functionality to perform maintenance, diagnostic, and troubleshooting tasks on your Unified Communications Manager server.

You can view the commands that the CSE sends and the responses that your Unified Communications Manager server issues, but the commands and responses may not always be completely formatted.

Set up a Remote Account

Configure a remote account in the Unified Communications Manager so that Cisco support can temporarily gain access to your system for troubleshooting purposes.

Procedure

Step 1 From Cisco Unified Operating System Administration, choose **Services** > **Remote Support**.

Step 2 In the **Account Name** field, enter a name for the remote account.

Step 3 In the **Account Duration** field, enter the account duration in days.

Step 4 Click **Save**.
The system generates an encrypted pass phrase.

Step 5 Contact Cisco support to provide them with the remote support account name and pass phrase.