Security Guide for Cisco Unified Communications Manager, Release 12.5(1)

First Published: 2019-01-23

Last Modified: 2021-09-24

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

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)

© 2019 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface xvii

Purpose xvii

Audience xviii

Organization xviii

Related Documentation xx

Conventions xx

Obtain Documentation, Support, and Security Guidelines xx

Cisco Product Security Overview xxi

PART I

Security Basics 23

CHAPTER 1

Security Overview 1

Terms and Acronyms 1

System Requirements 6

Features List 6

Security Icons 7

Interactions and Restrictions 8

Interactions 9

Restrictions 9

Authentication and Encryption 10

Barge and Encryption 10

Wideband Codecs and Encryption 10

Media Resources and Encryption 11

Phone Support and Encryption 11

Phone Support and Encrypted Setup Files 11

Security Icons and Encryption 11

Cluster and Device Security Modes 12
Digest Authentication and Encryption 12
Packet Capturing and Encryption 13
Best Practices 13
Device Resets, Server and Cluster Reboots, and Service Restarts 13
Reset Devices, Servers, Clusters, and Services 14
Media Encryption with Barge Setup 14
CTL Client, SSL, CAPF, and Security Token Installation 15
TLS and IPSec 15
Certificates 16
Phone Certificate Types 16
Server Certificate Types 18
Support for Certificates from External CAs 19
Authentication, Integrity, and Authorization 20
Image Authentication 20
Device Authentication 20
File Authentication 21
Signaling Authentication 21
Digest Authentication 21
Authorization 23
Encryption 24
Secure End Users Login Credentials 24
Signaling Encryption 24
Media Encryption 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
Self-encrypting Drive 30
Configuration File Encryption 30
Encrypted iX Channel 30
Encryption Modes 31

Non-Encrypted Modes 31
NMAP Scan Operation 32
Set Up Authentication and Encryption 32
Cipher Management 35
Recommended Ciphers 36
Configure Cipher String 37
Cipher Limitations 39
Cipher Restrictions 49
Where to Find More Information 49

CHAPTER 2 **Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS) 51**
HTTPS 51
HTTPS for Cisco Unified IP Phone Services 53
Cisco Unified IP Phones that Support HTTPS 53
Features That Support HTTPS 53
Cisco Unified IP Phone Services Settings 54
Enterprise Parameter Settings for HTTPS Support 56
Save Certificate to Trusted Folder Using Internet Explorer 8 56
Copy Internet Explorer 8 Certificate to File 57
First-Time Authentication for Firefox with HTTPS 58
Save Certificate to Trusted Folder Using Firefox 3.x 58
Copy Firefox 3.x Certificate to File 59
First-Time Authentication for Safari with HTTPS 60
Save Certificate to Trusted Folder Using Safari 4.x 60
Copy Safari 4.x Certificate to File 61
Where to Find More Information About HTTPS Setup 62

CHAPTER 3 **Default Security Setup 63**
Default Security Features 63
Trust Verification Service 64
TVS Description 64
Initial Trust List 64
Initial Trust List Files 65
ITL File Contents 65

ITL and CTL File Interaction 66
Certificate Management Changes for ITLRecovery Certificate 66
Interactions and Restrictions 67
Update ITL File for Cisco Unified IP Phones 67
Autoregistration 67
Obtain Cisco Unified IP Phone Support List 67
ECDSA Support for Common Criteria for Certified Solutions 68
Certificate Manager ECDSA Support 68
SIP ECDSA Support 68
CAPF ECDSA Support 69
Entropy 70
HTTPS Support for Configuration Download 70
CTI Manager Support 71
Certificate Regeneration 71
Regenerate CAPF Certificate 71
Regenerate TVS Certificate 72
Regenerate TFTP Certificate 72
Regenerate ITLRecovery Certificate 73
Tomcat Certificate Regeneration 74
System Back-Up Procedure After TFTP Certificate Regeneration 75
Refresh Upgrade From Cisco Unified Communications Manager Release 7.x to Release 8.6 Or Later 75
Roll Back Cluster to a Pre-8.0 Release 76
Switch Back to Release 8.6 or Later After Revert 77
Migrate IP Phones Between Clusters with Cisco Unified Communications Manager and ITL Files 78
Bulk Certificate Export 79
Generate Self-Signed Certificate 80
Self-signed Certificate Fields 80
Generate Certificate Signing Request 82
Certificate Signing Request Fields 83
Interactions and Restrictions 85
Reset CTL Localkey 85
View the Validity Period of ITLRecovery Certificate 86
Contact Search Authentication Task Flow 86

Confirm Phone Support for Contact Search Authentication 86
Enable Contact Search Authentication 87
Configure Secure Directory Server for Contact Search 87

CHAPTER 4 Cisco CTL Client Setup 89
About Cisco CTL Setup 89
Addition of Second SAST Role in the CTL File for Recovery 91
SIP OAuth Configuration Through CLI 91
Activate Cisco CTL Provider Service 92
Cisco CAPF Service Activation 93
Set up Secure Ports 93
Set Up Cisco CTL Client 94
SAST Roles of CTL File 96
Migrate Phones from One Cluster to Another Cluster 97
Migration from eToken-based CTL File to Tokenless CTL File 98
Update CTL File 98
Update Cisco Unified Communications Manager Security Mode 99
Cisco CTL File Details 100
Verify Cisco Unified Communications Manager Security Mode 101
Set Up Smart Card Service to Started or Automatic 101
Verify or Uninstall Cisco CTL Client 102

CHAPTER 5 TLS Setup 103
TLS Overview 103
TLS Prerequisites 103
TLS Configuration Task Flow 104
Set Minimum TLS Version 105
Set TLS Ciphers 105
Configure TLS in a SIP Trunk Security Profile 105
Add Secure Profile to a SIP Trunk 106
Configure TLS in a Phone Security Profile 106
Add Secure Phone Profile to a Phone 107
Add Secure Phone Profile to a Universal Device Template 108
TLS Interactions and Restrictions 108

TLS Interactions 109
TLS Restrictions 109

PART II Certificates 115

CHAPTER 6 Certificate Overview 117
Certificates Overview 117
Third-Party CA-Signed Certificates 118
Certificate Signing Request Key Usage Extensions 119
Server Certificate Types 120
Administration Tasks for Certificates 121
Show Certificates 121
Download Certificates 121
Install Intermediate Certificates 121
Delete a Trust Certificate 122
Regenerate a Certificate 123
Certificate Names and Descriptions 124
Regenerate Keys for OAuth Refresh Logins 124
Generate a Certificate Signing Request 125
Download a Certificate Signing Request 126
Add Certificate Authority-Signed CAPF Root Certificate to the Trust Store 126
Update the CTL File 126
Troubleshoot Certificate Errors 127

CHAPTER 7 Certificate Authority Proxy Function 129
Certificate Authority Proxy Function (CAPF) Overview 129
Phone Certificate Types 130
LSC Generation via CAPF 130
CAPF Prerequisites 131
Certificate Authority Proxy Function Configuration Task Flow 132
Upload Root Certificate for Third-Party CAs 133
Upload Certificate Authority (CA) Root Certificate 133
Configure Online Certificate Authority Settings 133
Configure Offline Certificate Authority Settings 135

Activate or Restart CAPF Services 135
Configure CAPF Settings in a Universal Device Template 136
Update CAPF Settings via Bulk Admin 137
Configure CAPF Settings for a Phone 138
Set KeepAlive Timer 139
CAPF Administration Tasks 139
Certificate Status Monitoring 139
Run Stale LSC Report 139
View Pending CSR List 140
Delete Stale LSC Certificates 140
CAPF System Interactions and Restrictions 140
CAPF Examples with 7942 and 7962 Phones 142
CAPF Interaction with IPv6 Addressing 142

CHAPTER 8 **Certificate Monitoring and Revocation** 145
Certificate Monitoring Overview 145
Certificate Revocation through Online Certificate Status Protocol 145
Certificate Monitoring Task Flow 146
Configure Certificate Monitor Notifications 147
Configure Certificate Revocation via OCSP 148

PART III **Security for Cisco IP Phone and Cisco Voice-Messaging Ports** 149

CHAPTER 9 **Phone Security** 151
Phone Security Overview 151
Trusted Devices 152
Cisco Unified Communications Manager Administration 152
Device Called Trust Determination Criteria 153
Phone Model Support 153
Preferred Vendor SIP Phone Security Set Up 153
Set Up Preferred Vendor SIP Phone Security Profile Per-Device Certificates 154
Set Up Preferred Vendor SIP Phone Security Profile Shared Certificates 154
View Phone Security Settings 155
Set Up Phone Security 155

Phone Security Interactions and Restrictions 156
Where to Find More Information About Phone Security 156

CHAPTER 10 Phone Security Profile Setup 157
Phone Security Profile Overview 157
Phone Security Profile Setup Prerequisites 157
Find Phone Security Profile 158
Set Up Phone Security Profile 159
Phone Security Profile Settings 159
Apply Security Profiles to Phone 169
Synchronize Phone Security Profile with Phones 170
Delete Phone Security Profile 170
Find Phones with Phone Security Profiles 171

CHAPTER 11 Secure and Nonsecure Indication Tone Setup 173
Secure and Non-Secure Indication Tone Overview 173
Protected Devices 173
Supported Devices 174
Secure and Non-Secure Indication Tone Tips 174
Secure and Non-Secure Indication Tone Configuration Tasks 175

CHAPTER 12 Encryption to Analog Endpoint Setup 177
Analog Phone Security Profile 177
Certificate Management for Secure Analog Phones 177

CHAPTER 13 Encrypted Phone Configuration File Setup 179
TFTP Encrypted Configuration Files Overview 179
Manual Key Distribution 180
Symmetric Key Encryption with Phone Public Key 180
Phone Models That Support Encryption 181
TFTP Encrypted Configuration Files Tips 182
Encryption for Phone Configuration File Task Flow 183
Enable TFTP Encryption 184
Configure SHA-512 Signing Algorithm 184

Set Up Manual Key Distribution 185
Manual Key Distribution Settings 185
Enter Phone Symmetric Key 186
Verify LSC or MIC Certificate Installation 187
Update CTL File 187
Restart Services 188
Reset Phones 188
Disable TFTP Encrypted Configuration Files 188
Exclude Digest Credentials From Phone Configuration File Download 189

CHAPTER 14 **Digest Authentication for SIP Phones Setup** 191
Enable Digest Authentication in Phone Security Profile 191
Configure SIP Station Realm 192
Assign Digest Credentials to Phone User 192
End User Digest Credential Settings 192
Assign Digest Authentication to the Phone 193

CHAPTER 15 **Phone Hardening** 195
Gratuitous ARP Disable 195
Web Access Disable 195
PC Voice VLAN Access Disable 196
Setting Access Disable 196
PC Port Disable 196
Set Up Phone Hardening 196
Where to Find More Information About Phone Hardening 197

CHAPTER 16 **Secure Conference Resources Setup** 199
Secure Conference 199
Conference Bridge Requirements 200
Secure Conference Icons 201
Secure Conference Status 201
Ad Hoc Conference Lists 202
Meet-Me Conference with Minimum Security Level 203
Cisco Unified IP Phone Secure Conference and Icon Support 204

Secure Conference CTI Support 204
Secure Conference Over Trunks and Gateways 204
CDR Data 205
Interactions and Restrictions 205
Cisco Unified Communications Manager Interactions with Secure Conference 205
Cisco Unified Communications Manager Restrictions with Secure Conference 206
Securing Conference Resources Tips 206
Set Up Secure Conference Bridge 207
Set Up Secure Conference Bridge in Cisco Unified Communications Manager Administration 208
Set Up Minimum Security Level for Meet-Me Conferences 209
Set Up Packet Capturing for Secure Conference Bridge 210
Where to Find More Information About Secure Conferences Resources 210

CHAPTER 17 **Voice-Messaging Ports Security Setup** 211
Voice-Messaging Security 211
Voice-Messaging Security Setup Tips 211
Set Up Secure Voice-Messaging Port 212
Apply Security Profile to Single Voice-Messaging Port 213
Apply Security Profile Using Voice Mail Port Wizard 214
Where to Find More Information About Voice-messaging Security 214

CHAPTER 18 **Call Secure Status Policy** 215
About Call Secure Status Policy 215
Setup Call Secure Status Policy 216

CHAPTER 19 **Secure Call Monitoring and Recording Setup** 217
About Secure Call Monitoring and Recording Setup 217
Set Up Secure Call Monitoring and Recording 218

PART IV **Virtual Private Networks for Cisco Unified IP Phones** 219

CHAPTER 20 **VPN Client** 221
VPN Client Overview 221
VPN Client Configuration Task Flow 221

Complete Cisco IOS Prerequisites 222
Configure Cisco IOS SSL VPN to Support IP Phones 223
Complete ASA Prerequisites for AnyConnect 224
Configure ASA for VPN Client on IP Phone 225
Upload VPN Concentrator Certificates 227
Configure VPN Gateway 228
VPN Gateway Fields for VPN Client 228
Configure VPN Group 229
VPN Group Fields for VPN Client 229
Configure VPN Profile 230
VPN Profile Fields for VPN Client 230
Configure VPN Feature Parameters 231
VPN Feature Parameters 231
Add VPN Details to Common Phone Profile 233

PART V **Cisco CTI, JTAPI, and TAPI Application Security** 235

CHAPTER 21 **Authentication and Encryption Setup for CTI, JTAPI, and TAPI** 237
Authentication for CTI, JTAPI, and TAPI Applications 237
Encryption for CTI, JTAPI, and TAPI Applications 238
CAPF Functions for CTI, JTAPI, and TAPI Applications 239
CAPF System Interactions and Requirements for CTI, JTAPI, and TAPI Applications 240
Certificate Authority Proxy Function Service Activation 241
Set Up Application User or End User CAPF Profile 241
CAPF Settings 242
Update CAPF Service Parameters 243
Delete Application User CAPF or End User CAPF Profile 244
Securing CTI, JTAPI, and TAPI 245
Add Application and End Users to Security-Related Access Control Groups 246
Set Up JTAPI/TAPI Security-Related Service Parameters 247
View Certificate Operation Status for Application or End User 247

PART VI **Security for SRST References, Trunks, and Gateways** 249

CHAPTER 22 **Secure Survivable Remote Site Telephony (SRST) Reference** 251

Securing SRST 251

Securing SRST Tips 252

Set Up Secure SRST 253

Set Up Secure SRST References 253

SRST Reference Security Settings 254

Delete Security From SRST Reference 256

SRST Certificate Deletion From Gateway 256

CHAPTER 23 **Encryption Setup for Gateways and Trunks** 257

Cisco IOS MGCP Gateway Encryption 257

H.323 Gateway and H.323/H.225/H.245 Trunk Encryption 258

SIP Trunk Encryption 259

Set Up Secure Gateways and Trunks 260

IPsec Setup Within Network Infrastructures 261

IPsec Setup Between Unified Communications Manager and Gateway or Trunks 261

Allow SRTP Using Unified Communications Manager Administration 262

Where to Find More Information About Gateway and Trunk Encryption 262

CHAPTER 24 **SIP Trunk Security Profile Setup** 263

About SIP Trunk Security Profile Setup 263

SIP Trunk Security Profile Setup Tips 263

Find SIP Trunk Security Profile 264

Set Up SIP Trunk Security Profile 264

SIP Trunk Security Profile Settings 265

Apply SIP Trunk Security Profile 270

Synchronize SIP Trunk Security Profile with SIP Trunks 271

Delete SIP Trunk Security Profile 271

Where to Find More Information About SIP Trunk Security Profiles 272

CHAPTER 25 **Digest Authentication Setup for SIP Trunks** 273

Set Up SIP Trunk Digest Authentication 273

Set Up Digest Authentication Enterprise Parameters 274

Set Up Digest Credentials 274
Application User Digest Credential Settings 274
Find SIP Realm 275
Configure SIP Realm 275
SIP Realm Settings 276
Delete SIP Realm 276

CHAPTER 26 Cisco Unified Mobility Advantage Server Security Profile Setup 279
About Cisco Unified Mobility Advantage Server Security Profile Setup 279
Find Cisco Unified Mobility Advantage Server Security Profile 280
Set Up Cisco Unified Mobility Advantage Server Security Profile 280
Cisco Unified Mobility Advantage Server Security Profile Settings 281
Cisco Unified Mobility Advantage Server Security Profile Client Application 282
Delete Cisco Unified Mobility Advantage Server Security Profile 282
Where to Find More Information About Cisco Unified Mobility Advantage Server Security Profile 283

CHAPTER 27 FIPS 140-2 Mode Setup 285
FIPS Mode Not Supported in Some 12.x Versions 285

CHAPTER 28 Cisco V.150 Minimum Essential Requirements (MER) 287
V.150 Overview 287
Prerequisites for Cisco V.150.1 MER 287
Configure V.150 Task Flow 288
Configure Media Resource Group Task Flow 289
Configure Media Resource Group for Non-V.150 Endpoints 290
Configure a Media Resource Group List for Non-V.150 Endpoints 290
Configure Media Resource Group for V.150 Endpoints 290
Configure a Media Resource Group List for V.150 Endpoints 291
Configure the Gateway for Cisco V.150 (MER) 291
Configure V.150 MGCP Gateway Port Interface 292
Configure V.150 SCCP Gateway Port Interface 292
Configure V.150 Support for Phone 293
Configure SIP Trunk Task Flow 294
Configure SIP Profile for V.150 294

Set the Clusterwide V.150 Filter 294
Add V.150 Filter to SIP Trunk Security Profile 295
Configure SIP Trunk for V.150 296

Preface

- Purpose, on page xvii
- Audience, on page xviii
- Organization, on page xviii
- Related Documentation, on page xx
- Conventions, on page xx
- Obtain Documentation, Support, and Security Guidelines, on page xx
- Cisco Product Security Overview, on page xxi

Purpose

Cisco Unified Communications Manager Security Guide helps system and phone administrators perform the following tasks:

- Configure authentication.
- Configure encryption.
- Configure digest authentication.
- Install server authentication certificate that is associated with HTTPS
- Configure the Cisco CTL Client.
- Configure security profiles.
- Configure Certificate Authority Proxy Function (CAPF) to install, upgrade, or delete locally significant certificates on supported Cisco Unified IP Phone models.
- Configure phone hardening.
- Configure Survivable Remote Site Telephony (SRST) references for security.
- Configure gateways and trunks for security.
- Configure FIPS (Federal Information Processing Standard) 140-2 mode.

Audience

This guide provides a reference and procedural guide for system and phone administrators who plan to configure call security features for Cisco Unified Communications Manager.

Organization

The following table lists the major sections of this guide:

Table 1: Guide Overview

Chapter	Description
Security Basics	
Security Overview	Provides an overview of security terminology, system requirements, interactions and restrictions, installation requirements, and a configuration checklist; describes the different types of authentication and encryption.
Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS)	Provides an overview of HTTPS and describes how to install the server authentication certificate in the trusted folder.
Default Security Setup	Provides information about the Security by Default feature, which provides automatic security features for Cisco Unified IP Phones.
Cisco CTL Client Setup	Describes how to configure authentication by installing and configuring the CiscoCTL Client.
TLS Setup	
Certificates	
Certificate Overview	
Security for Phones and Voice Mail Ports	
Phone Security	Describes how Unified Communications Manager and the phone use security; provides a list of tasks that you perform to configure security for the phone.
Phone Security Profile Setup	Describes how to configure the security profile and apply it to the phones in Unified Communications Manager.
Secure and Nonsecure indication Tone Setup	Describes how to configure a phone to play a secure-indication tone.
Encryption to Analog Endpoint Setup	Describes how to configure a secure SCCP connection to analog endpoints.
Encrypted Phone Configuration File Setup	Describes how to configure encrypted phone configuration files in Unified Communications Manager.

Chapter	Description
Digest Authentication for SIP phones Setup	Describes how to configure digest authentication on the phone that is running SIP in Unified Communications Manager Administration.
Phone Hardening	Describes how to tighten the security on the phone by using Unified Communications Manager Administration.
Secure Conference Resources Setup	Describes how to configure media encryption for secure conferences.
Voice-Messaging Ports Security Setup	Describes how to configure security for voice mail ports in Unified Communications Manager Administration.
Secure Call Monitoring and Recording Setup	Describes how to configure secure call monitoring and recording.
Virtual Private Networks for CiscoIPPhones	
Security for CTI, JTAPI, and TAPI	
Authentication and Encryption Setup for CTI, JTAPI and TAPI	Describes how to configure the Application User CAPF Profile and End User CAPF Profiles in Unified Communications Manager.
Security for SRST References, Gateways, Trunks, and Cisco Unified Mobility Advantage Servers	
Secure Survivable Remote Site Telephony (SRST) Reference	Describes how to configure the SRST reference for security in Unified Communications Manager Administration.
Encryption Setup for Gateways and Trunks	Describes how Unified Communications Manager communicates with a secure gateway or trunk; describes IPSec recommendations and considerations.
SIP Trunk Security Profile Setup	Describes how to configure and apply the SIP trunk security profile in Unified Communications Manager Administration.
Digest Authentication setup for SIP Trunks	Describes how to configure digest authentication for the SIP trunk in Unified Communications Manager Administration.
Cisco Unified Mobility Advantage Server security Profile Setup	Describes how to configure a Cisco Unified Mobility Advantage server security profile in Unified Communications Manager Administration.
FIPS 140-2 Mode Setup	Describes how to configure FIPS (Federal Information Processing Standard) 140-2 mode in Unified Communications Manager Administration.
Cisco V.150 Minimum Essential Requirements (MER)	Describes how to configure the V.150 feature, which allows you to make secure calls in a modem over IP network.

Related Documentation

Each chapter contains a list of related documentation for the chapter topic.

Refer to the following documents for further information about related CiscoIP telephony applications and products:

- *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco Unified Communications Manager Integration Guide for Cisco Unity*
- *Cisco Unified Communications Manager Integration Guide for Cisco Unity Connection*
- Cisco Unified Survivable Remote Site Telephony (SRST) administration documentation that supports the SRST-enabled gateway
- *Cisco IP Phone Administration Guide* for your phone model

Conventions

Notes use the following conventions:

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

Tips use the following conventions:

Tip Means *the following are useful tips*.

Cautions use the following conventions:

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

Obtain Documentation, Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Ciscodocuments, see the monthly *What'sNew in CiscoProduct Documentation*, which also lists all new and revised Ciscotechnical documentation, at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco Product Security Overview

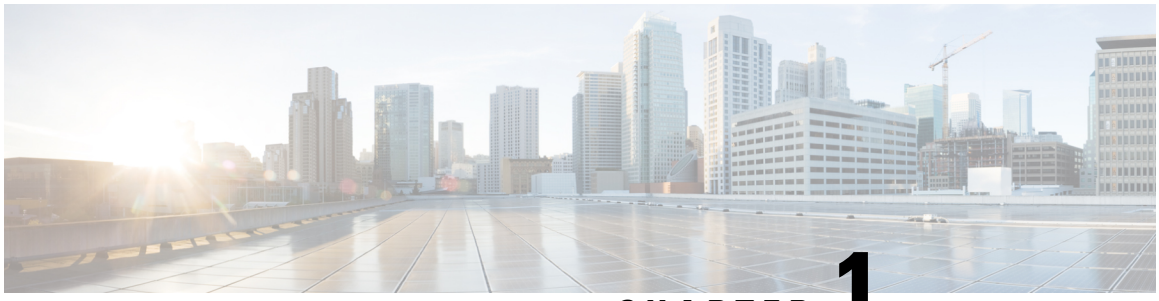
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

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

PART I

Security Basics

- Security Overview, on page 1
- Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS), on page 51
- Default Security Setup, on page 63
- Cisco CTL Client Setup, on page 89
- TLS Setup, on page 103



CHAPTER 1

Security Overview

Implementing security mechanisms in the 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.

- Terms and Acronyms, on page 1
- System Requirements, on page 6
- Features List, on page 6
- Security Icons, on page 7
- Interactions and Restrictions, on page 8
- Best Practices, on page 13
- CTL Client, SSL, CAPF, and Security Token Installation, on page 15
- TLS and IPSec, on page 15
- Certificates, on page 16
- Authentication, Integrity, and Authorization, on page 20
- Encryption, on page 24
- NMAP Scan Operation, on page 32
- Set Up Authentication and Encryption, on page 32
- Cipher Management, on page 35
- Where to Find More Information, on page 49

Terms and Acronyms

The definitions in the following table apply when you configure authentication, encryption, and other security features for your CiscoIPtelephony network:

Table 2: Terminology

Term	Definition
Access Control List (ACL)	List that defines rights and permissions to access system functions and resources. See Method List.

Term	Definition
Authentication	Process that verifies the identity of the communicating entity.
Authorization	Process that specifies whether an authenticated user, service, or application has the necessary permissions to perform a requested action; in Unified Communications Manager, the security process that restricts certain trunk-side SIP requests to authorized users.
Authorization Header	A SIP user agent response to a challenge.
Certificate	A message that contains the certificate holder name, the public key, and the digital signature of the certificate authority that is issuing the certificate.
Certificate Authority (CA)	Trusted entity that issues certificates: Cisco or a third-party entity.
Certificate Authority Proxy Function (CAPF)	Process by which supported devices can request locally significant certificates by using Unified Communications Manager Administration.
Certificate Trust List (CTL)	A file, which is created either with the CLI command set **utils cli** or with the CTL Client and signed by the Cisco Site Administrator Security Token (security token), that contains a list of certificates for servers that the phone is to trust.
Challenge	In digest authentication, a request to a SIP user agent to authenticate its identity.
Cisco Site Administrator Security Token (security token; etoken)	A portable hardware security module that contains a private key and an X.509v3 certificate that the Cisco Certificate Authority signs; used for file authentication, it may be used to sign the CTL file. Hardware security tokens are required for only the CTL Client. The CLI command set **utils ctl** does not require hardware security tokens.
Device Authentication	Process that validates the identity of the device and ensures that the entity is what it claims to be before a connection is made.
Digest Authentication	A form of device authentication where an MD5 hash of a shared password (among other things) gets used to establish the identity of a SIP user agent.
Digest User	User name that is included in an authorization request that phones that are running SIP or SIP trunks send.

Term	Definition
Digital Signature	Value that is generated by hashing the message and then encrypting the message with the private key of the signer; the recipient decrypts the message and the hash with the signer public key, produces another hash with the same hash function, then compares the two hashes to ensure that the messages match and the content is intact.
DSP	Digital signaling processor.
DSP Farm	A network resource for IP telephony conferencing that is provided by DSPs on a H.323 or MGCP gateway.
Encryption	Process of translating data into ciphertext, which ensures the confidentiality of the information and that only the intended recipient can read the data. Requires an encryption algorithm and encryption key.
File Authentication	Process that validates digitally signed files that the phone downloads. The phone validates the signature to make sure that file tampering did not occur after the file creation.
H.323	An internet standard that defines a common set of codecs, call setup and negotiating procedures, and basic data transport methods.
hash	A number, usually in hexadecimal, that is generated from a string of text by using a hash function, which creates a small digital “fingerprint” for the data.
Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)	An IETF-defined protocol that ensures (at a minimum) the identity of the HTTPS server; by using encryption, ensures the confidentiality of the information that is exchanged between the Tomcat server and the browser client.
Image Authentication	Process whereby a phone validates the integrity and source of a binary image prior to loading it on the phone.
Integrity	Process that ensures that data tampering did not occur between entities.
IPSec	Transport that provides secure H.225, H.245, and RAS signaling channels for end-to-end security.
Locally Significant Certificate (LSC)	A digital X.509v3 certificate that CAPF issues; installed on the phone or JTAPI/TAPI/CTI application.

Term	Definition
Manufacture Installed Certificate (MIC)	A digital X.509v3 certificate that is signed by the Cisco Certificate Authority and installed in supported phones by Cisco Manufacturing; used as the authentication mechanism to CAPF when LSCs are installed in phones.
Man-in-the-Middle Attacks	Process that allows an attacker to observe and modify the information flow between Unified Communications Manager and the phone.
Multipoint Control Unit (MCU)	A flexible system to connect multiple H.323 endpoints and allow multiple users to participate in IP-based video conferences.
MD5	A hash function that is used with encryption.
Media Encryption	Process whereby the confidentiality of the media is protected with cryptographic procedures. Media encryption uses Secure Real-Time Protocol (SRTP) as defined in IETFRFC3711.
Message/Data Tampering	Event when an attacker attempts to alter messages in transit, including ending a call prematurely.
Method List	Tool to restrict certain categories of messages that can come in on a SIP trunk during the authorization process; defines which SIP nonINVITE methods are allowed for a trunk-side application or device. Also method ACL.
Mixed Mode	Unified Communications Manager security mode that you configure to allow devices with secure/nonsecure profiles and RTP/ SRTP media to connect to Unified Communications Manager.
Nonce	A unique, random number that the server generates for each digest authentication request; used to generate an MD5 hash.
Nonsecure Mode	Unified Communications Manager security mode that you configure to allow devices with nonsecure profiles and RTP media to connect to Unified Communications Manager.
Nonsecure Call	Call in which at least one device is not authenticated or encrypted.
Nonsecure Device	Device that uses UDP or TCP signaling and nonsecure media.

Term	Definition
PKI	Public key infrastructure, which comprises the set of elements that is needed for public key encryption, including secure public key distribution, certificates, and certificate authorities.
Public / Private key	Keys that are used in encryption. Public keys are widely available, but private keys are held by their respective owners. Asymmetrical encryption combines both types.
Replay Attack	Event when an attacker captures information that identifies a phone or proxy server and replays information while pretending to be the actual device; for example, by impersonating the proxy server private key.
RTP	Real-Time Transport Protocol
Simple Certificate Enrollment Protocol (SCEP)	A protocol that is used to communicate with a certificate authority that issues X.509 certificates.
Secure Call	Call in which all devices are authenticated, signaling is encrypted, and the media (voice stream) is encrypted.
Signaling Authentication	TLS process that validates that no tampering occurred to signaling packets during transmission.
Signaling Encryption	Process that uses cryptographic methods to protect the confidentiality of all signaling messages that are sent between the device and the Unified Communications Manager server.
SIP Realm	A string (name) that Unified Communications Manager uses to respond to a challenge.
SRTP	Secure Real-Time Transport Protocol that secures voice conversation in the network and provides protection against replay attacks.
SSL	A cryptographic protocol that secures data communications such as e-mail on the Internet; equivalent to TLS, its successor.
Transport Layer Security (TLS)	A cryptographic protocol that secures data communications such as e-mail on the Internet; functionally equivalent to SSL.
Trust List	Certificate list without digital signatures.

Term	Definition
Trust Store	A repository of X.509 certificates that an application, such as Unified Communications Manager, explicitly trusts.
X.509	An ITU-T cryptographic standard for importing PKI certificates, which includes certificate formats.

System Requirements

The following system requirements exist for authentication or encryption:

- The Administrator password can differ on every server in a cluster.
- The username and password that are used at the Cisco CTL client (to log in to the Unified Communications Manager server) must match the Unified Communications Manager Administration username and password (the username and password that are used to log in to Unified Communications Manager Administration).
- Before you configure voicemail ports for security, verify that you installed a version of Cisco Unity or Cisco Unity Connection system that supports this Unified Communications Manager release.

Features List

Unified Communications Manager system uses a multilayered approach to call security, from the transport layer to the application layer.

Transport layer security includes TLS and IPSec for signaling authentication and encryption to control and prevent access to the voice domain. SRTP adds media authentication and encryption to secure privacy and confidentiality for voice conversation and other media.

The following table provides a summary of the authentication and encryption features that Unified Communications Manager can implement during an SCCP call session, depending on the features that are supported and configured.

Table 3: SCCP Call Security Features

Security Feature	Line Side	Trunk Side
Transport/Connection/Integrity	Secure TLS port	IPSec associations
Device Authentication	TLS certificate exchange w/Unified Communications Manager and/or CAPF	IPSec certificate exchange or preshared key
Signaling Authentication/Encryption	TLS Mode: authenticated or encrypted	IPSec [authentication header, encryption (ESP), or both]
Media Encryption	SRTP	SRTP

Security Feature	Line Side	Trunk Side
Authorization	Presence requests	Presence requests
Note Supported features on a device vary by device type.		

The following table provides a summary of the authentication and encryption features that Unified Communications Manager can implement during a SIP call session, depending on the features that are supported and configured.

Table 4: SIP Call Security Features

Security Feature	Line Side	Trunk Side
Transport/Connection/Integrity	Secure TLS port	Secure TLS port
Device Authentication	TLS certificate exchange w/Unified Communications Manager and/or CAPF	IPSec certificate exchange or preshared key
Digest Authentication	Each SIP device uses unique digest user credentials.	SIP trunk user agents use unique digest credentials.
Signaling Authentication/Encryption	TLS Mode: authenticated or encrypted (except Cisco Unified IP Phones 7942/7962).	TLS Mode: authenticated or encrypted mode
Media Encryption	SRTP	SRTP
Authorization	Presence requests	Presence requests Method list
Note Supported features on a device vary by device type.		

Security Icons

Unified Communications Manager provides security status for a call, according to security levels that are configured for the Unified Communications Manager server(s) and devices that are participating in the call.

Phones that support security icons display the call security level.

- The phone displays a shield icon for calls with a signaling security level of authenticated. A shield identifies a secured connection between CiscoIP devices, which means that the devices have authenticated or encrypted signaling.
- The phone displays a lock icon for calls with encrypted media, which means that the devices are using encrypted signaling and encrypted media.

Note 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. Refer to topics related to security icons and encryption for restrictions that are associated with security icons.

The audio and video portions of the call provide basis for the call security status. Consider the call secure only if both the audio and video portions are secure. The following table describes the rules that determine whether a security icon displays, and which icon appears.

Table 5: Security Icon Display Rules

Media and Device Types In the Call	Phones That Display Both Shield and Lock Icons	Phones That Display Only the Lock Icon
Secure audio only	Lock	Lock
Secure audio with unsecure video	Shield	None
Secure audio with secure video	Lock	Lock
Authenticated device with nonsecure audio only	Shield	None
Authenticated device with nonsecure audio and video	Shield	None
Unauthenticated device with nonsecure audio only	None	None
Unauthenticated device with nonsecure audio and video	None	None

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.

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

Interactions and Restrictions

This section contains interaction and restriction information.

See the related topics for information about interactions and restrictions that are associated with the secure conference feature.

Interactions

This section provides information on the Interaction of Cisco Security features with Unified Communications Manager applications.

Presence

Configure presence groups to restrict presence requests sent to authorized users. You can add presence group authorization for phones and trunks that are running SIP.

Refer to Feature Configuration Guide for Cisco Unified Communications Manager for more information about configuring presence groups.

Configure Unified Communications Manager to allow and accept presence requests on SIP trunk. If required, Configure Unified Communications Manager to accept and authenticate incoming presence requests from remote devices or applications.

SIP Trunk

Configure SIP Trunk Security Profile to accept incoming, out of dialog, REFER requests to use SIP-initiated transfer features and other advanced transfer features on SIP trunks. For Example, Web Transfer and Click to Dial.

Configure SIP Trunk Security Profile to accept Unsolicited Notification SIP requests to report events (MWI support) and to reduce per-call MTP allocations (from a voice-messaging server).

Configure SIP Trunk Security Profile to accept SIP requests which replaces header in REFERS and INVITES. The Unified Communications Manager can now transfer an external call for a SIP trunk to an external device or party.

Extension Mobility

For Extension Mobility, SIP digest credentials change when a user logs in and out as different end users have different credentials.

Computer Telephony Integration (CTI)

Cisco Unified Communications Manager Assistant supports a secure connection to CTI (transport layer security connection) when you configure a CAPF profile (one for each Cisco Unified Communications Manager Assistant node).

CTI TLS support requires you to configure a unique InstanceID (IID) for every application instance, when multiple instances of a CTI/JTAPI/TAPI application are running. The IID secures the signaling and media communication streams between CTI Manager and JTAPI/TSP/CTI applications.

When the device security mode equals authenticated or encrypted, the Cisco Unity-CM TSP connects to Unified Communications Manager through the Unified Communications Manager TLS port. When the security mode equals nonsecure, the Cisco Unity TSP connects to Unified Communications Manager through the CTI Manager port.

Restrictions

This section describes restrictions that apply to Cisco security features.

Authentication and Encryption

Consider the following restrictions before you install and configure authentication and encryption features:

- You cannot implement signaling or media encryption without device authentication. To install device authentication, enable the Cisco CTL Provider service and install and configure the Cisco CTL client.
- Cisco does not support Network Address Translation (NAT) with Unified Communications Manager if you configure mixed mode.

  You can enable UDP in the firewall to allow media stream firewall traversal. Enabling UDP 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.

Barge and Encryption

The following restrictions apply to barge and encryption:

- Due to bandwidth requirements, Cisco IP Phones 7942 and 7962 do not support barge from an encrypted device on an active encrypted call. The barge attempt will fail. A tone plays on the initiator phone to indicate that the barge failed.
- Encrypted Cisco IP Phones that are running release 8.2 or earlier can only barge an active call as authenticated or nonsecure participants.
- 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.
- If a caller barges a secure SIP call, the system provides tone-on-hold, and Unified Communications Manager classifies the call as nonsecure during the tone.

Note Nonsecure or authenticated Cisco IP Phones that are running release 8.3 or later can barge encrypted calls. The security icon indicates the security status for the conference.

Wideband Codecs and Encryption

The following information applies for Cisco Unified IP Phones 7962 or 7942 that are configured for encryption and associated with a wideband codec region. This only applies to Cisco Unified IP Phones 7962 or 7942 that are configured for TLS/SRTP.

To establish an encrypted call, Unified Communications Manager ignores the wideband codec and chooses another supported codec from the codec list that the phone presents. If the other devices in the call are not configured for encryption, Unified Communications Manager may establish the authenticated/nonsecure call by using the wideband codec.

Media Resources and Encryption

Unified Communications Manager supports authenticated and encrypted calls between secure Cisco Unified IP Phones (SCCP or SIP), secure CTI devices/route points, secure Cisco MGCP IOS gateways, secure SIP trunks, secure H.323 gateways, secure conference bridges, and secure H.323/H.245/H.225 trunks where no media resources are used. Unified Communications Manager does not provide media encryption in the following cases:

- Calls that involve transcoders
- Call that involve media termination points

Note MTP encryption is not supported only with the non-passthrough MTP.

Phone Support and Encryption

The following Cisco Unified IP Phones that are running SCCP support encryption: 6901, 6911, 6921, 6941, 6945, 6961,7906G, 7911G, 7925G, 7925G-EX, 7926G, 7931G, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7975G, 8941, 8945, and 9961.

The following Cisco Unified IP Phones that are running SIP support encryption: 6901, 6911, 6921, 6941, 6945, 6961, 7811, 7821, 7841, 7861, 7832, 7906G, 7911G, 7941G, 7941G-GE, 7942G, 7961G, 7961G-GE,7962G, 7965G, 7975G, 8811, 8821, 8821-EX, 8832, 8841, 8845, 8851, 8851NR, 8865, 8865NR, 8941, 8945, 8961, 9971, and 9971.

For more information, see the *System Configuration Guide for Cisco Unified Communications Manager* that support encryption and this version of Unified Communications Manager.

Warning To obtain the full benefit of security features, Cisco recommends that you upgrade Cisco IP Phones to firmware release 8.3 or later, which supports the encryption features in this Unified Communications Manager release. Encrypted phones that run earlier releases do not fully support these new features. These phones can participate in secure conference and barge calls only as authenticated or nonsecure participants.

Cisco IP Phones that are running on firmware release 8.3 with an earlier release of Unified Communications Manager will display their connection security status, not the conference security status, during a conference or barge call, and do not support secure conference features like conference list.

Phone Support and Encrypted Setup Files

Not all phones support encrypted configuration files. Some phones support encrypted configuration files but do not validate file signatures. All phones that support encrypted configuration files require firmware that is compatible with Unified Communications Manager Release 5.0 or later to receive full encrypted configuration files.

Security Icons and Encryption

The following restrictions apply to security icons and encryption:

- 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 nonsecure if the media streams that are associated with these tasks, such as MOH, are not encrypted.
- Unified Communications Manager does not display the shield icon for calls that are transiting H.323 trunks.
- For calls that involve the PSTN, the security icon shows the security status for only the IP domain portion of the call.
- A SIP trunk will report encrypted or not-authenticated security status when using the TLS transport type. When SRTP is negotiated, the security status will get encrypted; otherwise it will remain not-authenticated. This will allow Unified Communications Manager call control to determine the overall security level of a call that involves a SIP trunk.

  A SIP trunk will report authenticated status over the trunk if a party is authenticated during events such as a meet-me conference or a cbarge. (The SIP trunk will still be using TLS/SRTP.)
- For Secure Monitoring and Recording, a SIP trunk will utilize the existing Call Info header mechanism for transmitting the security icon status over the SIP trunk, as currently used by the SIP line. This enables the SIP trunk peer to monitor the overall security status of a call.
- Some phone models display only the lock icon, not the shield icon.

Cluster and Device Security Modes

Note Device security mode configures the security capability for a Cisco IP Phone or SIP trunk. Cluster security mode configures the security capability for your standalone server or a cluster.

When the cluster security mode equals nonsecure, the device security mode equals nonsecure in the phone configuration file. In these circumstances, the phone makes nonsecure connections with the SRST-enabled gateway and Unified Communications Manager, even if the device security mode specifies authenticated or encrypted. Security-related settings other than device security mode, such as the SRST Allowed check box, also get ignored. The security configuration does not get deleted in Unified Communications Manager Administration, but security does not get provided.

The phone attempts a secure connection to the SRST-enabled gateway only when the cluster security mode equals mixed, the device security mode in the phone configuration file is set to authenticated or encrypted, the SRST Allowed? check box is checked in the Trunk Configuration window, and a valid SRST certificate exists in the phone configuration file.

Digest Authentication and Encryption

Unified Communications Manager defines a SIP call as having two or more separate call legs. For a standard, two-party call between two SIP devices, two separate call legs exist: one leg between the originating SIP user agent and Unified Communications Manager (the originating call leg) and the other leg between Unified Communications Manager and destination SIP user agent (the terminating call leg). Each call leg represents a separate dialog. Because digest authentication is a point-to-point process, digest authentication on each call leg stays independent of the other call legs. SRTP capabilities can change for each call leg, depending on the capabilities that are negotiated between the user agents.

Packet Capturing and Encryption

When SRTP encryption is implemented, third-party sniffing tools do not work. Authorized administrators with appropriate authentication can initiate packet capturing with a configuration change in Unified Communications Manager Administration (for devices that support packet capturing). See the *Troubleshooting Guide for Cisco Unified Communications Manager* that supports this release for information about configuring packet capturing in Unified Communications Manager.

Best Practices

We recommend the following best practices while configuring security for Unified Communications Manager:

- Always install and configure security 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 If you fail to use IPSec, the session encryption keys get transmitted in cleartext.

- To prevent toll fraud, configure conference enhancements. For more information, see System Configuration Guide for Cisco Unified Communications Manager.

  To restrict external call transfers, perform configuration tasks. For more information, see Feature Configuration Guide for Cisco Unified Communications Manager.

Device Resets, Server and Cluster Reboots, and Service Restarts

This section describes when you need to reset the devices, to reboot the server/cluster, or to restart services in Cisco Unified Serviceability.

Consider the following guidelines:

- Reset a single device after you apply a different security profile in Cisco Unified Communications Manager Administration.
- Reset the devices if you perform phone-hardening tasks.
- Reset the devices after you change the cluster security mode from mixed to nonsecure mode (or vice versa).
- Restart all devices after you configure the Cisco CTL client or update the CTL file.
- Reset the devices after you update CAPF enterprise parameters.
- Restart the Cisco CTL Provider service after you update ports for the TLS connection.
- Restart the Cisco CallManager service after you change the cluster security mode from mixed to nonsecure mode (or vice versa).
- Restart the Cisco Certificate Authority Proxy Function service after you update associated CAPF service parameters.
- Restart all Cisco CallManager and Cisco TFTP services in Cisco Unified Serviceability after you configure the Cisco CTL Client or update the CTL file. Perform this task on all servers that run these services in the cluster.
- Restart all Cisco CallManager and Cisco TFTP services after you start or stop the CTL Provider service.

- Reset dependent devices after you configure secure SRST references.
- If you set the Smart Card service to Started and Automatic, reboot the PC where you installed the Cisco CTL client.
- Restart the Cisco IP Manager Assistant service, Cisco Web Dialer Web Service, and the Cisco Extended Functions service after you configure the security-related service parameters that are associated with the Application User CAPF Profile.

To restart the Cisco CallManager service, refer to *Cisco Unified Serviceability Administration Guide*.

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 parameter in the CTL client.
- 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.

CTL Client, SSL, CAPF, and Security Token Installation

To obtain authentication support, you can use one of the following options:

1. Install the Cisco CTL client, from Unified Communications Manager Administration. For the Cisco CTL client option, you must obtain at least two security tokens.
2. Use the CLI command set **utils ctl**, which does not require security tokens. For more information about this option, see the *Command Line Interface Guide for Cisco Unified Communications Solutions*.

Media and signaling encryption capabilities automatically install when you install Unified Communications Manager.

Unified Communications Manager automatically installs Secure Sockets Layer (SSL) for Unified Communications Manager virtual directories.

Cisco Certificate Authority Proxy Function (CAPF) installs automatically as a part of Unified Communications Manager Administration.

TLS and IPSec

Transport security handles the coding, packing, and sending of data. Unified Communications Manager provides the following secure transport protocols:

- Transport Layer Security (TLS) provides secure and reliable 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. Unified Communications Manager uses TLS to secure SCCP calls to phones that are running SCCP and SIP calls to phones or trunks that are running SIP.
- IP Security (IPSec) provides secure and reliable data transfer between Unified Communications Manager and gateways. IPSec implements signaling authentication and encryption to CiscoIOS MGCP and H.323 gateways.

You can add secure RTP (SRTP) to TLS and IPSec transport services for the next level of security on devices that support SRTP. SRTP authenticates and encrypts the media stream (voice packets) to ensure that voice conversations that originate at or terminate to CiscoUnifiedIPPhones and either TDM or analog voice gateway ports are protected from eavesdroppers who may have gained access to the voice domain. SRTP adds protection against replay attacks.

Cisco Unified Communications Manager 9.0 and later provides TLS/SRTP support for dual-mode smart phones. TLS establishes the same secure and reliable data transfer mode for mobile phones as for IP phones, and SRTP encrypts voice conversations.

Certificates

Certificates secure client and server identities. After root certificates are installed, certificates get added to the root trust stores to secure connections between users and hosts, including devices and application users.

Administrators can view the fingerprint of server certificates, regenerate self-signed certificates, and delete trust certificates at the Cisco Unified Communications Operating System GUI.

Administrators can also regenerate and view self-signed certificates at the command line interface (CLI).

For information on updating the CallManager trust store and managing certificates, refer to the *Administration Guide for Cisco Unified Communications Manager* that supports this Unified Communications Manager release.

Note

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

Note When you upload two certificates, ensure that they have same common name and same 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 SHA1 algorithm exists in Cisco 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 SHA256 algorithm, the certificate management happens in the following way:

1. The validity of incoming certificate is verified.
2. The certificate with same common name is searched in the Tomcat trust folder.
3. The serial numbers of the certificate existing in the Tomcat trust folder and the incoming certificate that you are uploading is checked. If the serial numbers are different, the validity start date of both the certificates is verified. If the validity start time stamp of incoming certificate is later than the validity start time stamp of the existing certificate, the existing certificate replaces the newer incoming certificate in the Tomcat trust folder. Else, the new incoming certificate is not uploaded.

Both SHA1 and SHA256 algorithms have same subject name or common name, which implies that they belong to the same entity. The Unified Communications Manager framework does not support both these algorithms on the Unified Communications Manager server simultaneously. Only one certificate that belongs to any entity is supported in a particular trust folder, irrespective of the signature algorithm.

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 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.

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.

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 This release of Unified Communications Manager doesn't provide SCEP interface support.

Note Be sure to run the CTL client after you upload a third-party, CA-signed certificate to the platform to update the CTL file.

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.

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.

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.

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.

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 80-bit or 32-bit authentication tag, the negotiation occurs over Real-Time Transport Protocol (RTP).

Note The SCCP phone supports only 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 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 8: 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

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

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.

Encrypted iX Channel

Unified Communications Manager supports an encrypted iX channel. The iX channel provides a reliable channel for multiplexing application media between SIP phones in a video conference. Encrypted iX Channel

uses DTLS to add security to your deployment and ensures that the application media is sent over the iX Channel is private and cannot be viewed by intermediate parties who attempt to intercept media.

IOS MTP and RSVP agents in pass through mode also support encrypted iX Channel.

Configuration

To enable an encrypted iX Channel on Unified Communications Manager, you must:

- Check the **Allow iX Application Media** check box in the SIP Profile Configuration that is used by any intermediate SIP trunks. This setting turns on the iX channel negotiation.
- Configure the **Secure Call Icon Display Policy** service parameter to enable a secure lock icon. By default, the setting is **All media except BFCP and iX transports must be encrypted**.

Encryption Modes

There are two types of Session Description Protocol (SDP) offers thatUnified Communications Manager supports for iX Channel encryption for encrypted phones. This encryption type is driven by what the endpoints support and is not a configurable item in the Unified Communications Manager.

- **Best Effort Encryption**—The SDP offer is for an encrypted iX Channel, but falls back to a non-encrypted iX Channel if the SIP peers do not support it. This approach can be used if encryption is not mandatory in the solution.

  For example, encryption is mandatory within the cloud, and not in a single enterprise.

  Best-Effort iX Encryption

  m=application 12345 **UDP/UDT/IX** *

  a=setup:actpass

  a=fingerprint: SHA-1 <key>

- **Forced Encryption**—The SDP offer is for an encrypted iX Channel only. This offer is rejected if the SIP peers do not support iX Channel encryption. This approach can be used in deployments where encryption is mandatory between endpoints.

  For example, encryption is mandatory between the two SIP devices.

  Forced iX Encryption

  m=application 12345 **UDP/DTLS/UDT/IX** *

  a=setup:actpass

  a=fingerprint: SHA-1 <key>

By default, all Cisco IP Phones are set to offer Best Effort iX Encryption. However, you can reset this to Forced Encryption by setting the **Encryption Mode** to **On** within the Product-Specific Configuration of Cisco TelePresence endpoints, or by reconfiguring settings on the Cisco Meeting Server.

Non-Encrypted Modes

Unified Communications Managerenables negotiation of secure active control messages in media path from endpoints in a meeting when the endpoint may not be deployed in a fully secure mode. For example, if the endpoint is Off-Net and is registered with Unified CM in Mobile and Remote Access mode.

Prerequisite

Before you start using this feature, make sure that:

- System adheres to the export compliance requirement
- SIP trunk to the conference bridge is secure

Unified CM can negotiate the DTLS information in secure active control messages for non-secure endpoints or softphones and receive messages in the following ways:

- **Best Effort Encryption iX** to On-Premise registered endpoints or softphones
- **Forced iX Encryption** to Off-Premise registered endpoints or softphones

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

Set Up Authentication and Encryption

Important This procedure applies to the CTL Client encryption option. You may also set up encryption by using the **utils ctl** CLI command set. 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.

Procedure

Step 1 Activate the Cisco CTL Provider service in Cisco Unified Serviceability

Be sure to activate the CiscoCTL Provider service on each Unified Communications Manager server in the cluster.

Tip If you activated this service prior to a Unified Communications Manager upgrade, you do not need to activate the service again. The service automatically activates after the upgrade.

Step 2 Activate the Cisco Certificate Authority Proxy service in Cisco Unified Serviceability to install, upgrade, troubleshoot, or delete locally significant certificates.

Activate the Cisco Certificate Authority Proxy service on the first node only.

Timesaver Performing this task before you install and configure the CiscoCTL client ensures that you do not have to update the CTL file to use CAPF.

Step 3 If you do not want to use the default port settings, configure ports for the TLS connection.

Tip If you configured these settings prior to a Unified Communications Manager upgrade, the settings migrate automatically during the upgrade.

Step 4 If using the Cisco CTL client for encryption, obtain at least two security tokens and the passwords, hostnames/IP addresses, and port numbers for the servers that you will configure for the CiscoCTL client.

Note You do not need hardware security tokens for the **utils ctl** CLI option.

Step 5 Install the CiscoCTL client.

Tip To update the CiscoCTL file after an upgrade to this Unified Communications Manager release, you must install the plug-in that is available in this Unified Communications Manager Administration release.

Step 6 Configure the CiscoCTL client.

Tip If you created the CiscoCTL file prior to a Unified Communications Manager upgrade, the CiscoCTL file migrates automatically during the upgrade. To update the CiscoCTL file after an upgrade to this Unified Communications Manager release, you must install and configure the latest version of the CiscoCTL client.

Step 7 Configure the phone security profiles.

Perform the following tasks when you configure the profiles:

a) Configure the device security mode.

Tip The device security mode migrates automatically during the Unified Communications Manager upgrade. If you want to configure encryption for devices that only supported authentication in a prior release, you must choose a security profile for encryption in the Phone Configuration window.

b) Configure CAPF settings (for some phones that are running SCCP and SIP).

Additional CAPF settings display in the Phone Configuration window.

c) If you plan to use digest authentication for phones that are running SIP, check the Enable Digest Authentication check box.
d) To enable encrypted configuration files (for some phones that are running SCCP and SIP), check the Encrypted Confide check box.
e) To exclude digest credentials in configuration file downloads, check the Exclude Digest Credential in Configuration File check box.

Step 8 Apply the phone security profiles to the phones.

The following steps are optional:

Step 9 (Optional) Verify that the locally significant certificates are installed on supported Cisco Unified IP Phones .

Step 10 (Optional) Configure digest authentication for phones that are running SIP.

Step 11 (Optional) Perform phone-hardening tasks.

Tip If you configured phone-hardening settings prior to a Unified Communications Manager upgrade, the device configuration settings migrate automatically during the upgrade.

Step 12 (Optional) Configure conference bridge resources for security.

Step 13 (Optional) Configure voice mail ports for security.

For more information, see the applicable Cisco Unity or Cisco Unity Connection integration guide for this Unified Communications Manager release.

Step 14 (Optional) Configure security settings for SRST references.

Tip If you configured secure SRST references in a previous Unified Communications Manager release, the configuration automatically migrates during the Unified Communications Manager upgrade.

Step 15 (Optional) Configure IPSec.

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

Step 16 (Optional) Configure the SIP trunk security profile.

If you plan to use digest authentication, check the Enable Digest Authentication check box in the profile.

For trunk-level authorization, check the authorization check boxes for the allowed SIP requests.

If you want application-level authorization to occur after trunk-level authorization, check the Enable Application Level Authorization check box.

You cannot check application-level authorization unless digest authentication is checked.

Step 17 (Optional) Apply the SIP trunk security profile to the trunk.

Step 18 (Optional) Configure digest authentication for the trunk.

Step 19 (Optional) If you checked the Enable Application Level Authorization check box in the SIP trunk security profile, configure the allowed SIP requests by checking the authorization check boxes in the Application User Configuration window.

Step 20 (Optional) Reset all phones.

Step 21 (Optional) Reboot all servers.

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

This section lists the recommended ciphers. Make sure that the ciphers configured are part of the recommended ciphers. Otherwise, you may encounter interoperability issues with other products over secure interfaces. After configuring the recommended ciphers, restart the affected services or reboot the server for the changes to take effect.

Warning Configuring hmac-sha2-512 in 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.

We recommend 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 for FIPS

```
ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256,
diffie-hellman-group14-sha1, diffie-hellman-group16-sha512, diffie-hellman-group14-sha256
```

SSH KEX for Non-FIPS

```
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 36.

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://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html.

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 9: 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.
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 Application Ciphers Support, on page 40 section for a list of ciphers supported by individual application interfaces.

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 10: 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: ECDHE-RSA-AES256-SHA: AES256-GCM-SHA384: AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: CAMELLIA128-SHA
DRS	TCP / TLS	4040	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA
Cisco Tomcat	TCP / TLS	8443 / 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-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: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA

Application / Process	Protocol	Port	Supported Ciphers
Cisco CallManager	TCP / TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-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:CAMELLIA128-SHA: ECDHE-ECDSA-DES-CBC3-SHA
Cisco CTL Provider	TCP / TLS	2444	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:
Cisco Certificate Authority Proxy Function	TCP / TLS	3804	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:
CTIManager	TCP / TLS	2749	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA
Cisco Trust Verification Service	TCP / TLS	2445	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA
Cisco Intercluster Lookup Service	TCP / TLS	7501	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:

Application / Process	Protocol	Port	Supported Ciphers
Secure Configuration download (HAPROXY)	TCP / TLS	6971, 6972	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA:
Authenticated Contact Search	TCP / TLS	9443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA:

Table 11: 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: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-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:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-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: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: CAMELLIA256-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:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA

Application / Process	Protocol	Port	Supported Ciphers
Cisco SIP Proxy	TCP / TLS	8083	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-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:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA
Cisco Tomcat	TCP / TLS	8443, 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-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: DHE-RSA-CAMELLIA128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-ECDSA-DES-CBC3-SHA

Application / Process	Protocol	Port	Supported Ciphers
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: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-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:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-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: ECDHE-RSA-AES256-SHA: ECDHE-ECDSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-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:CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: DES-CBC3-SHA

Table 12: 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-sha1`
	• Kex algorithms:
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`ecdh-sha2-nistp256`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group1-sha1`
	`diffie-hellman-group-exchange-sha256`
	`diffie-hellman-group-exchange-sha1`

SSH Client	• Ciphers:
	`aes128-ctr`
	`aes192-ctr`
	`aes256-ctr`
	`aes128-gcm@openssh.com`
	`aes256-gcm@openssh.com`
	• MAC algorithms:
	`hmac-sha2-256`
	`hmac-sha1`
	• Kex algorithms:
	`ecdh-sha2-nistp521`
	`ecdh-sha2-nistp384`
	`ecdh-sha2-nistp256`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group1-sha1`
	`diffie-hellman-group-exchange-sha256`
	`diffie-hellman-group-exchange-sha1`

Service	Ciphers/Algorithms

DRS Client	• Ciphers:
	`aes256-ctr`
	`aes256-cbc`
	`aes128-ctr`
	`aes128-cbc`
	`aes256-ctr`
	`blowfish-cbc`
	• MAC algorithms:
	`hmac-md5`
	`hmac-sha2-256`
	`hmac-sha1`
	`hmac-sha1-96`
	`hmac-md5-96`
	• Kex algorithms:
	`ecdh-sha2-nistp256`
	`ecdh-sha2-nistp384`
	`ecdh-sha2-nistp521`
	`diffie-hellman-group14-sha1`
	`diffie-hellman-group-exchange-sha256`
	`diffie-hellman-group-exchange-sha1`
	`diffie-hellman-group1-sha1`

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 (Linux OS)	`SHA-256 - 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
```

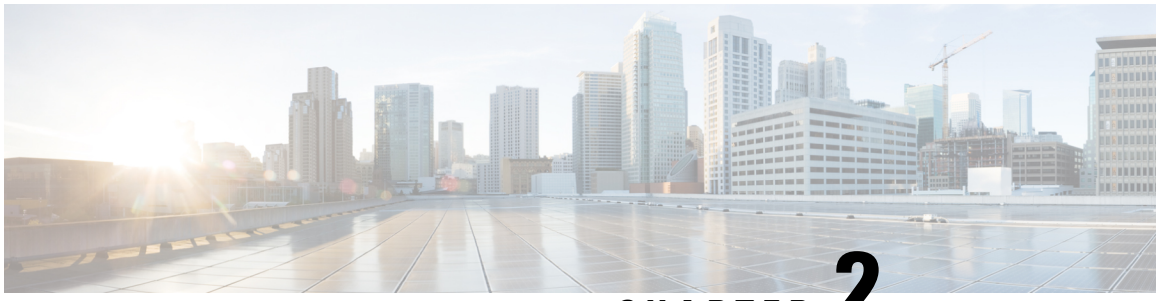
Where to Find More Information

Related Cisco Documentation

Refer to the following documents for further information about related CiscoIP telephony applications and products:

- *System Configuration Guide for Cisco Unified Communications Manager*
- *Administration Guide for Cisco Unified Communications Manager*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco Unified Communications Manager Integration Guide for Cisco Unity*
- *Cisco Unified Communications Manager Integration Guide for Cisco Unity Connection*

- *Cisco Unified Survivable Remote Site Telephony (SRST) Administration Guide* that supports the SRST-enabled gateway.
- *Administration Guide for Cisco Unified Communications Manager*
- *Cisco Unified Communications Manager Bulk Administration Guide*
- *Troubleshooting Guide for Cisco Unified Communications Manager*
- *Cisco IP Phone Administration Guide* that support your phone model



CHAPTER 2

Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS)

This chapter provides information about Hypertext Transfer Protocol over Secure Sockets Layer.

- HTTPS, on page 51
- HTTPS for Cisco Unified IP Phone Services, on page 53
- Save Certificate to Trusted Folder Using Internet Explorer 8, on page 56
- First-Time Authentication for Firefox with HTTPS, on page 58
- First-Time Authentication for Safari with HTTPS, on page 60
- Where to Find More Information About HTTPS Setup, on page 62

HTTPS

HTTPS, or Hypertext Transfer Protocol over Secure Sockets Layer (SSL), secures communication between a browser and a web server for Microsoft Windows users. HTTPS uses certificates to ensure server identities and to secure the browser connection. HTTPS uses a public key to encrypt the data, including the user login and password, during transport over the Internet.

Unified Communications Manager supports SSL and Transport Layer Security (TLS) for HTTPS connections. Cisco recommends using TLS for improved security if your web browser version supports TLS. Disable SSL on your web browser to use TLS for secure HTTPS communications.

To enable HTTPS, you must download a certificate that identifies the server during the connection process. You can accept the server certificate for the current session only, or you can download the certificate to a trust folder (file) to secure the current session and future sessions with that server. The trust folder stores the certificates for all your trusted sites.

Cisco supports these browsers for connection to the Cisco Tomcat web server application in Unified Communications Manager:

- Microsoft Internet Explorer (IE) 7 when running on Microsoft Windows XP SP3
- Microsoft Internet Explorer (IE) 8 when running on Microsoft Windows XP SP3 or Microsoft Vista SP2
- Firefox 3.x when running on Microsoft Windows XP SP3, Microsoft Vista SP2 or Apple MAC OS X
- Safari 4.x when running on Apple MAC OS X

Note When you install/upgrade Unified Communications Manager, an HTTPS self-signed certificate (Tomcat) is generated. The self-signed certificate migrates automatically during upgrades to Unified Communications Manager. A copy of this certificate is created in.DER and.PEM formats.

You can regenerate the self-signed certificate by using the Cisco Unified Communications Operating System GUI. Refer to the *Administration Guide for Cisco Unified Communications Manager* for more information.

The following table shows the applications that use HTTPS with Cisco Tomcat in Unified Communications Manager.

Table 13: Unified Communications Manager HTTPS Applications

Unified Communications Manager HTTPS Application	Web Application
ccmadmin	Unified Communications Manager Administration
ccmservice	Cisco Unified Serviceability
cmplatform	Operating System administration pages
cmuser	Cisco Personal Assistant
ast	Real Time Monitoring Tool
RTMTReports	Real Time Monitoring Tool reports archive
PktCap	TAC troubleshooting tools that are used for packet capturing
art	Unified Communications Manager CDR Analysis and Reporting
taps	Unified Communications Manager Auto-Register Phone Tool
dna	Dialed Number Analyzer
drf	Disaster Recovery System
SOAP	Simple Object Access Protocol API for reading from and writing to the Unified Communications Manager database **Note** For security, all Web applications that are using SOAP require HTTPS. Cisco does not support HTTP for SOAP applications. Existing applications that use HTTP will fail; they cannot be converted to HTTPS by changing directories.

HTTPS for Cisco Unified IP Phone Services

For Unified Communications Manager, Cisco IP Phones and Cisco Unified IP Phone Services support HTTPS, encryption, and secure identification of the server using port 8443.

TVS (Trust verification service) does not verify certificate chains. For TVS to verify the certificate, the same certificate that is presented to TVS by the phone must be in the Tomcat-trust certificate store.

TVS does verify root or intermediate certificates. Only the identity certificate is verified if it is not in the database. Even if the root and intermediate certificates are present,. verification fails.

Cisco Unified IP Phones that Support HTTPS

The following Cisco IP Phones support HTTPS:

- 6901, 6911, 6921, 6941, 6945, 6961
- 7811, 7821, 7832, 7841, 7861
- 7906, 7911, 7925, 7925-EX, 7926, 7931, 7941, 7941G-GE, 7942, 7945, 7961, 7962, 7961G-GE, 7965, 7975
- 8811, 8821, 8831, 8832, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR
- 8941, 8945, 8961
- 9951, 9971

Note The 69xx phones in this list can act as HTTPS clients, but cannot act as an HTTPS server. The remaining phones in this list can act as an HTTPS client or an HTTPS server.

Features That Support HTTPS

The following features support HTTPS:

- Cisco Extension Mobility (EM)
- Cisco Extension Mobility Cross Cluster (EMCC)
- Cisco Unified Communications Manager Manager Assistant (IPMA)
- Cisco Unified IP Phone Services
- Personal Directory
- Change Credentials

Cisco Unified IP Phone Services Settings

To support HTTPS in Unified Communications Manager Release 8.0(1) and later, the Phone Configuration Settings include the secure URL parameters shown in the following table.

To configure the secure URL parameters, choose **Device** > **Device Settings** > **Phone Services** from Unified Communications Manager Administration. For more information, see the *System Configuration Guide for Cisco Unified Communications Manager*

Note When you delete the Secured Phone URL Parameters in the Enterprise Parameter section of Cisco Unified Communications Manager Administration and then reboot, the URL Parameters are re-populated by default. After you reboot go to the Secured Phone URL Parameters section and make the correct modifications to the URL and reboot the phones.

Table 14: Phone Configuration Settings for Secure URLs

Field	Description
Secure Authentication URL	Enter the secure URL that the phone uses to validate requests that are made to the phone web server. **Note** If you do not provide a Secure Authentication URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. By default, this URL accesses a Cisco Unified Communications Self Care Portal window that was configured during installation. Leave this field blank to accept the default setting. Maximum length: 255
Secure Directory URL	Enter the secure URL for the server from which the phone obtains directory information. This parameter specifies the URL that secured Cisco IP Phones use when you press the Directory button. **Note** If you do not provide a Secure Directory URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. Leave this field blank to accept the default setting. Maximum length: 255

Field	Description
Secure Idle URL	Enter the secure URL for the information that displays on the Cisco IP Phone display when the phone is idle, as specified in Idle Timer field. For example, you can display a logo on the LCD when the phone has not been used for 5 minutes. **Note** If you do not provide a Secure Idle URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255
Secure Information URL	Enter the secure URL for the server location where the Cisco IP Phone can find help text information. This information displays when the user presses the information (i) button or the question mark (?) button. **Note** If you do not provide a Secure Information URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255
Secure Messages URL	Enter the secure URL for the messages server. The Cisco IP Phone contacts this URL when the user presses the Messages button. **Note** If you do not provide a Secure Messages URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255

Field	Description
Secure Services URL	Enter the secure URL for Cisco Unified IP Phone services. The is the location that the secure Cisco Unified IP Phone contacts when the user presses the Services button. **Note** If you do not provide a Secure Services URL, the device uses the nonsecure URL. If you provide both a secure URL and a nonsecure URL, the device chooses the appropriate URL, based on its capabilities. To accept the default setting, leave this field blank. Maximum length: 255

Enterprise Parameter Settings for HTTPS Support

To support HTTPS, Unified Communications Manager Release 8.0(1) and later supports the following new Enterprise Parameters:

- Secured Authentication URL
- Secured Directory URL
- Secured Idle URL
- Secured Information URL
- Secured Messaged URL
- Secured Services URL

Save Certificate to Trusted Folder Using Internet Explorer 8

Be sure to import the Unified Communications Manager certificate to Internet Explorer 8 to secure access without having to reload the certificate every time that you restart the browser. If you continue to a website that has a certificate warning and the certificate is not in the trust store, Internet Explorer 8 remembers the certificate for the current session only.

After you download the server certificate, Internet Explorer 8 continues to display certificate errors for the website. You can ignore the security warnings when the Trusted Root Certificate Authority trust store for the browser contains the imported certificate.

The following procedure describes how to import the Unified Communications Manager certificate to the root certificate trust store for Internet Explorer 8.

Procedure

Step 1 Browse to application on the Tomcat server (for example, enter the hostname, localhost, or IP address for Unified Communications Manager Administration in the browser).

The browser displays a Certificate Error: Navigation Blocked message to indicate that this website is untrusted.

Step 2 To access the server, click **Continue to this website (not recommended)**.

The Unified Communications Manager Administration window displays, and the browser displays the address bar and Certificate Error status in red.

Step 3 To import the server certificate, click the Certificate Error status box to display the status report. Click the **View Certificates** link in the report.

Step 4 Verify the certificate details.

Step 5 Select the **General** tab in the Certificate window and click **Install Certificate**.

The Certificate Import Wizard launches.

Step 6 To start the Wizard, click **Next**.

The Certificate Store window displays.

Step 7 Verify that the Automatic option, which allows the wizard to select the certificate store for this certificate type, is selected and click **Next**.

Step 8 Verify the setting and click **Finish**.

A security warning displays for the import operation.

Step 9 To install the certificate, click **Yes**.

The Import Wizard displays "The import was successful."

Step 10 Click **OK**. The next time that you click the **View certificates** link, the **Certification Path** tab in the Certificate window displays "This certificate is OK."

Step 11 To verify that the trust store contains the imported certificate, click **Tools** > **Internet Options** in the Internet Explorer toolbar and select the **Content** tab. Click **Certificates** and select the **Trusted Root Certifications Authorities** tab. Scroll to find the imported certificate in the list.

After importing the certificate, the browser continues to display the address bar and a Certificate Error status in red. The status persists even if you reenter the hostname, localhost, or IP address or refresh or relaunch the browser.

Copy Internet Explorer 8 Certificate to File

Copying the certificate to a file and storing it locally allows you to restore the certificate whenever necessary.

Performing the following procedure copies the certificate by using a standard certificate storage format. To copy the certificate contents to file, perform the following procedure:

Procedure

Step 1 Click the Certificate Error status box.

Step 2 Click **View Certificates**.

Step 3 Click the **Details** tab.

Step 4 Click the **Copy to File** button.

Step 5 The Certificate Export Wizard displays. Click **Next**.

Step 6 The following list defines the file formats from which you can choose. Choose the file format that you want to use for the exported file; click **Next**.

a) DER encoded binary X.509 (.CER)—Uses DER to transfer information between entities.

b) Base-64 encoded X.509 (.CER)—Sends secure binary attachments over the internet; uses ASCII text format to prevent corruption of file.

c) Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)—Exports the certificate and all certificates in the certification path to the chosen PC.

Step 7 Browse to the location to which you want to export the file copy and name the file. Click **Save**.

Step 8 The file name and path display in the Certificate Export Wizard pane. Click **Next**.

Step 9 Your file and settings display. Click **Finish**.

Step 10 When the successful export dialog box displays, click **OK**.

First-Time Authentication for Firefox with HTTPS

The first time that you (or a user) accesses Unified Communications Manager Administration or other Unified Communications Manager SSL-enabled virtual directories (after the Unified Communications Manager installation/upgrade) from a browser client, a Security Alert dialog box asks whether you trust the server.

When the dialog box displays, you must perform one of the following tasks:

- By clicking **I Understand The Risks**, you choose to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box displays each time that you access the application; that is, until you install the certificate in the trusted folder.
- By clicking **Get Me Out Of Here**, you cancel the action. No authentication occurs, and you cannot access the web application. To access the web application, you must click **I Understand The Risks**.

Save Certificate to Trusted Folder Using Firefox 3.x

Perform the following procedure to save the HTTPS certificate in the trusted folder in the browser client.

Procedure

Step 1 Access the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco Unified Communications Manager Administration in the browser).

Step 2 When the Security Alert dialog box displays, click **I Understand The Risks**.

Step 3 Click **Add Exception**.

The Add Exception dialog box displays.

Step 4 Click **Get Certificate**.

Step 5 Check the **Permanently store this exception** check box.

Step 6 Click **Confirm Security Exception**.

Step 7 To view the details of the certificate by performing the following steps:

a) From the Firefox browser, click **Tools** > **Options**.

The Options dialog box displays

b) Click **Advanced**.

c) Click **View Certificates**.

The Certificate Manager dialog box displays.

d) Highlight the certificate that you want to view and click **View**.

The Certificate Viewer dialog box displays.

e) Click the **Details** tab.

f) In the Certificate Fields field, highlight the field that you want to view.

Details display in the Field Values field.

g) From the Certificate Viewer dialog box, click **Close**.

h) From the Certificate Manager dialog box, click **OK**.

Copy Firefox 3.x Certificate to File

Copying the certificate to a file and storing it locally allows you to restore the certificate whenever necessary.

Performing the following procedure copies the certificate by using a standard certificate storage format. To copy the certificate contents to file, perform the following procedure:

Procedure

Step 1 From the Firefox browser, click **Tools** > **Options**.

The Options dialog box displays.

Step 2 If it is not already selected, click **Advanced**.

Step 3 Click the **Encryption** tab and click **View Certificates**.

The Certificate Manager dialog box displays.

Step 4 Click the **Servers** tab.

Step 5 Highlight the certificate you want to copy and click **Export**.

The Save Certificate to File dialog box displays.

Step 6 Browse to the location to which you want to copy the file.

Step 7 From the **Save as type** drop-down list, choose the file type from the following options:

a) X.509 Certificate (PEM)—Uses **PEM** to transfer information between entities.
b) X.509 Certificate with chain (PEM)—Uses Privacy Enhanced Mail to verify the certificate chain and transfer information between entities.

- X.509 Certificate (DER)—Uses **DER** to transfer information between entities.
- X.509 Certificate (PKCS#7)—PKCS#7 is a standard for signing or encrypting data. Since the certificate is needed to verify signed data, it is possible to include it in the SignedData structure. A.P7C-file is just a degenerated SignedData structure, without any data to sign.
- X.509 Certificate with chain (PKCS#7)—Uses PKCS#7 to verify the certificate chain and transfer information between entities.

Step 8 Click **Save**.

Step 9 Click **OK**.

First-Time Authentication for Safari with HTTPS

The first time that you (or a user) accesses Unified Communications Manager Administration or other Unified Communications Manager SSL-enabled virtual directories (after the Unified Communications Manager installation/upgrade) from a browser client, a Security Alert dialog box asks whether you trust the server.

When the dialog box displays, you must perform one of the following tasks:

- By clicking **Yes**, you choose to trust the certificate for the current web session only. If you trust the certificate for the current session only, the Security Alert dialog box displays each time that you access the application; that is, until you install the certificate in the trusted folder.
- By clicking **Show Certificate** > **Install Certificate**, you intend to perform certificate installation tasks, so you always trust the certificate. If you install the certificate in the trusted folder, the Security Alert dialog box does not display each time that you access the web application.
- By clicking **No**, you cancel the action. No authentication occurs, and you cannot access the web application. To access the web application, you must click **Yes** or install the certificate via the **Show Certificate** > **Install Certificate** options.

Note The address that you use to access Unified Communications Manager must match the name on the certificate, or a message will display by default. If you access the web application by using the localhost or IP address after you install the certificate in the trusted folder, a security alert indicates that the name of the security certificate does not match the name of the site that you are accessing.

Save Certificate to Trusted Folder Using Safari 4.x

Perform the following procedure to save the HTTPS certificate in the trusted folder in the browser client.

Procedure

Step 1 Access the Tomcat server (for example, enter the hostname, localhost, or IP address for Cisco Unified Communications Manager Administration in the browser).

Step 2 When the Security Alert dialog box displays, click **Show Certificate**.

You can click the **Details** tab to view the details of the certificate if you choose to verify the certificate data. To display a subset of settings, if available, choose one of the following options:

a) All—All options display in the Details pane.
b) Version 1 Fields Only—Version, Serial Number, Signature Algorithm, Issuer, Valid From, Valid To, Subject, and the Public Key options display.
c) Extensions Only—Subject Key Identifier, Key Usage, and the Enhanced Key Usage options display.
d) Critical Extensions Only—Critical Extensions, if any, display
e) Properties Only—Thumbprint algorithm and the thumbprint options display.

Step 3 In the Certificate pane, click **Install Certificate**.

Step 4 When the Certificate Import Wizard displays, click **Next**.

Step 5 Click the **Place all certificates in the following store** radio button; click **Browse**.

Step 6 Browse to **Trusted Root Certification Authorities**; select it and click **OK**.

Step 7 Click **Next**.

Step 8 Click **Finish**.

A Security Warning Box displays the certificate thumbprint for you.

Step 9 To install the certificate, click **Yes**.

A message states that the import was successful. Click **OK**.

Step 10 In the lower, right corner of the dialog box, click **OK**.

Step 11 To trust the certificate, so you do not receive the dialog box again, click **Yes**.

Tip You can verify the certificate was installed successfully by clicking the **Certification Path** tab in the Certificate pane.

Copy Safari 4.x Certificate to File

Copying the certificate to a file and storing it locally allows you to restore the certificate whenever necessary.

Performing the following procedure copies the certificate by using a standard certificate storage format. To copy the certificate contents to file, perform the following procedure:

Procedure

Step 1 In the Security Alert dialog box, click **Show Certificate**.

Tip In Safari, click the Certificate Error status box to display the Show Certificate option.

Step 2 Click the **Details** tab.

Step 3 Click the **Copy to File** button.

Step 4 The Certificate Export Wizard displays. Click **Next**.

Step 5 The following list defines the file formats from which you can choose. Choose the file format that you want to use for the exported file; click **Next**.

a) DER encoded binary X.509 (.CER)—Uses DER to transfer information between entities.

b) Base-64 encoded X.509 (.CER)—Sends secure binary attachments over the internet; uses ASCII text format to prevent corruption of file.

c) Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)—Exports the certificate and all certificates in the certification path to the chosen PC.

Step 6 Browse to the location to which you want to export the file copy and name the file. Click **Save**.

Step 7 The file name and path display in the Certificate Export Wizard pane. Click **Next.**

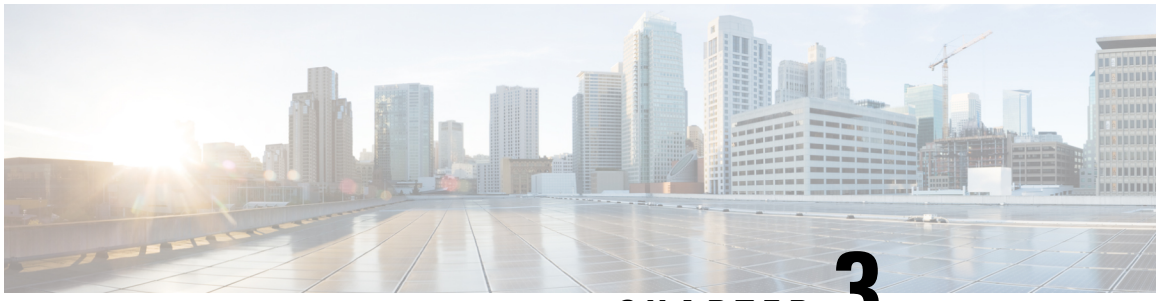
Step 8 Your file and settings display. Click **Finish**.

Step 9 When the successful export dialog box displays, click **OK**.

Where to Find More Information About HTTPS Setup

Related Cisco Documentation

- *Cisco Unified Serviceability Administration Guide*
- *Administration Guide for Cisco Unified Communications Manager*
- Microsoft documentation that is available on HTTPS



CHAPTER 3

Default Security Setup

This section provides information about the default security setup.

- Default Security Features, on page 63
- Trust Verification Service, on page 64
- Initial Trust List, on page 64
- Update ITL File for Cisco Unified IP Phones, on page 67
- Autoregistration, on page 67
- Obtain Cisco Unified IP Phone Support List, on page 67
- ECDSA Support for Common Criteria for Certified Solutions, on page 68
- Certificate Regeneration, on page 71
- Tomcat Certificate Regeneration, on page 74
- System Back-Up Procedure After TFTP Certificate Regeneration, on page 75
- Refresh Upgrade From Cisco Unified Communications Manager Release 7.x to Release 8.6 Or Later, on page 75
- Roll Back Cluster to a Pre-8.0 Release, on page 76
- Migrate IP Phones Between Clusters with Cisco Unified Communications Manager and ITL Files, on page 78
- Reset CTL Localkey, on page 85
- View the Validity Period of ITLRecovery Certificate, on page 86
- Contact Search Authentication Task Flow, on page 86

Default Security Features

Security by Default provides the following automatic security features for Cisco Unified IP Phones:

- Signing of the phone configuration files.
- Support for phone configuration file encryption.
- https with Tomcat and other Web services (Midlets)

For Unified Communications Manager Release 8.0 later, these security features are provided by default without running the CTL Client.

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.

TVS Description

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 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 IP Phone and trust flows from there.

Initial Trust List

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.

Initial Trust List Files

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 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.

ITL File Contents

The ITL file contains the following certificates:

- 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.

ITL and CTL File Interaction

The Cisco IP Phone relies on the CTL file to know about the cluster security mode (non-secure or mixed mode). The CTL File tracks the cluster security mode by including the Unified Communications Manager certificate in the Unified Communications Manager record.

The ITL File also contains the cluster security mode indication.

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 validity of ITLRecovery certificates continues to be 5 years if you upgrade Unified Communications Manager. While upgrading Unified Communications Manager, the certificates get copied to the later release. However, when you regenerate an ITLRecovery certificate or when you do a fresh install of Unified Communications Manager, the validity of ITLRecovery gets extended to 20 years.

- 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.

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.

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.

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.

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.

ECDSA Support for Common Criteria for Certified Solutions

Unified Communications Manager supports Elliptic Curve Digital Signature Algorithm (ECDSA) certificates. These certificates are stronger than the RSA-based certificates and are required for products that have Common Criteria (CC) certifications. The US government Commercial Solutions for Classified Systems (CSfC) program requires the CC certification and so, it is included in Unified Communications Manager.

The ECDSA certificates are available along with the existing RSA certificates in the following areas—Certificate Manager, SIP, Certificate Authority Proxy Function (CAPF), Transport Layer Security (TLS) Tracing, Entropy, HTTP, and computer telephony integration (CTI) Manager.

Note ECDSA is supported only for Unified Communications Manager and Tomcat.

Certificate Manager ECDSA Support

In Unified Communications Manager Release 11.0, the certificate manager supports both generation of self-signed ECDSA certificates and the ECDSA certificate signing request (CSR). Earlier releases of Unified Communications Manager supported **RSA** certificate only. However, Unified Communications Manager Release 11.0 onwards, **CallManager-ECDSA** certificate has been added along with the existing **RSA** certificate.

Both the **CallManager** and **CallManager-ECDSA** certificates share the common certificate trust store—CallManager-Trust. Unified Communications Manager uploads these certificates to this trust store.

The certificate manager supports generation of ECDSA certificates having different values of key length.

When you update or install Unified Communications Manager, the self-signed certificate is generated. Unified Communications Manager Release 11.0 always has an ECDSA certificate and uses that certificate in its SIP interface. The secure Computer Telephony Integration (CTI) Manager interface also supports ECDSA certificates. As both the CTI Manager and SIP server use the same server certificate, both the interfaces work in synchronization.

SIP ECDSA Support

Unified Communications Manager Release 11.0 includes ECDSA support for SIP lines and SIP trunk interfaces. The connection between Unified Communications Manager and an endpoint phone or video device is a SIP line connection whereas the connection between two Unified Communications Managers is a SIP trunk connection. All SIP connections support the ECDSA ciphers and use ECDSA certificates.

Following are the scenarios when SIP makes (Transport Layer Security) TLS connections:

- When SIP acts as a TLS server—When the SIP trunk interface of Unified Communications Manager acts as a TLS server for incoming secure SIP connection, the SIP trunk interface determines if the CallManager-ECDSA certificate exists on disk. If the certificate exists on the disk, the SIP trunk interface uses the CallManager-ECDSA certificate if the selected cipher suite is

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 or **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**. The SIP trunk interface continues to support RSA TLS cipher suites for connections from clients that do not support ECDSA cipher suites. The **TLS Ciphers** drop-down list contains options that permit configuration of the supported cipher suites when Unified Communications Manager acts as a TLS server.

- When SIP acts as a TLS client—When the SIP trunk interface acts as a TLS client, the SIP trunk interface sends a list of requested cipher suites to the server based on the **TLS Ciphers** field (which also includes the **ECDSA ciphers** option) in the **Enterprise Parameters** window of Cisco Unified Communications Manager. The **TLS Ciphers**. This configuration determines the TLS client cipher suite list and the supported cipher suites in order of preference.

Note If you establish a TLS connection with an earlier release of the Unified Communications Manager that does not support ECDSA client certificate, the connection uses an RSA cipher suite. The client certificate sent in the TLS connection is not bound to the TLS Cipher you that you choose. Earlier releases of Unified Communications Manager also support that TLS servers receive and handle ECDSA client certificates.

Devices that use an ECDSA cipher to make a connection to Unified Communications Manager must have the CallManager-ECDSA certificate in their Identity Trust List (ITL) file. Then, the devices must incorporate the CallManager-ECDSA certificate into their local certificate store to trust the connection that is secured by the CallManager-ECDSA certificate.

CAPF ECDSA Support

Certificate Authority Proxy Function (CAPF) is a Cisco proprietary method for exchanging certificates between Cisco endpoints and Unified Communications Manager. Only Cisco endpoints use CAPF. To accomplish common criteria requirements, CAPF is updated to CAPF version 3 so that a client can be provided with ECDSA Locally Significant Certificate (LSC). A customer creates LSC locally. An LSC is an alternative to manufacturer installed certificate (MIC) that the manufacturer creates.

Use CAPF version 3 to allow Unified Communications Manager server to direct phone, CTI applications, and Jabber clients to generate EC keys to be used in their LSCs. After the EC Keys are generated, Unified Communications Manager either generates an ECDSA LSC and sends it to the Cisco endpoint or generates an ECDSA CSR.

In case the endpoint does not have CAPF version 3 support, you can configure the required EC key size and RSA key size and choose **EC Key Preferred, RSA Backup** option in **Phone Configuration** window from Cisco Unified CM Administration as a backup. This backup option is useful when CAPF server tries to send a request to EC key pair and the phone communicates to the server that it does not support EC key, the server sends the request to generate an RSA key pair instead of the EC key pair.

Note If Cisco endpoint supports CAPF version 3, and you choose **EC Preferred, RSA Backup** option in **Phone Configuration** without enabling **Endpoint Advanced Encryption Algorithm Support** parameter, then the ECDSA or RSA-based LSCs are not issued. If Cisco endpoint does not support CAPF version 3, and you enable or disable **Endpoint Advanced Encryption Algorithm Support** parameter then the RSA-based LSCs are issued.

Note The **Endpoint Advanced Encryption Algorithms Support** parameter indicates that phones download the TFTP configuration files using advanced TLS ciphers. By default, EC ciphers have the highest priority. This solution is only supported for an on-premises deployment without MRA.

Entropy

To have strong encryption, a robust source of entropy is required. Entropy is a measure of randomness of data and helps in determining the minimum threshold for common criteria requirements. Data conversion techniques, such as cryptography and encryption, rely on a good source of entropy for their effectiveness. If a strong encryption algorithm, such as ECDSA, uses a weak source of entropy, the encryption can be easily broken.

In Unified Communications Manager Release 11.0, the entropy source for Unified Communications Manager is improved. Entropy Monitoring Daemon is a built-in feature that does not require configuration. However, you can turn it off through the Unified Communications Manager CLI.

Use the following CLI commands to control the `Entropy Monitoring Daemon` service:

CLI Command	Description
utils service start Entropy Monitoring Daemon	Starts the `Entropy Monitoring Daemon` service.
utils service stop Entropy Monitoring Daemon	Stops the `Entropy Monitoring Daemon` service.
utils service active Entropy Monitoring Daemon	Activates the `Entropy Monitoring Daemon` service, which further loads the kernel module.
utils service deactive Entropy Monitoring Daemon	Deactivates the `Entropy Monitoring Daemon` service, which further unloads the kernel module.

HTTPS Support for Configuration Download

For secure configuration download, Unified Communications Manager Release 11.0 is enhanced to support HTTPS in addition to the HTTP and TFTP interfaces that were used in the earlier releases. Both client and server use mutual authentication, if required. Clients that are enrolled with ECDSA LSCs and Encrypted TFTP configurations are required to present their LSC.

The HTTPS interface uses both the CallManager and the CallManager-ECDSA certificates as the server certificates.

Note When you update CallManager, CallManager ECDSA, or Tomcat certificates, you must deactivate and reactivate the TFTP service. Port 6971 is used for authentication of the CallManager and CallManager-ECDSA certificates whereas port 6972 is used for the authentication of the Tomcat certificates.

CTI Manager Support

The computer telephony integration (CTI) interface is enhanced to support four new ciphers. The ciphers suites are **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256**, **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**, **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** and **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**. By supporting these cipher suites, the CTI Manager interface needs to have the **CallManager-ECDSA** certificate, if it exists in Unified Communications Manager. Similar to the SIP interface, the Enterprise Parameter **TLS Ciphers** option in Unified Communications Manager is used to configure the TLS ciphers that are supported on the CTI Manager secure interface.

Certificate Regeneration

If you regenerate one of the Unified Communications Manager certificates, you must perform the steps in this section.

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

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 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 Certificate*, section in the Cisco Unified Communications Manager Security Guide.

Step 3 CAPF service is automatically restarted when 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

Step 1 Regenerate the TVS certificate.

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

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

Step 3 TVS service is automatically restarted when TVS certificate is regenerated.

Regenerate TFTP Certificate

To regenerate a TFTP certificate, follow these steps:

Note If you plan to regenerate multiples 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 is applicable when the Phone interaction on Certificate Update parameter is automatically reset.

Procedure

Step 1 Regenerate the TFTP 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* .

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

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* .

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* .

Refresh Upgrade From Cisco Unified Communications Manager Release 7.x to Release 8.6 Or Later

To upgrade your cluster from Release 7.x to Release 8.6 or later, follow this procedure:

Procedure

Step 1 Follow the normal procedure for upgrading a cluster. For more information, see *Administration Guide for Cisco Unified Communications Manager* .

Tip After you finish upgrading all nodes in the cluster to Unified Communications Manager Release 8.6 or later, you must also follow all the steps in this procedure to ensure that your Cisco Unified IP Phones register with the system.

Step 2 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 Chapter 4, “Configuring the CTL Client,”.

Step 3 Wait ten minutes for the Cisco IP Phones to automatically restart and register with Unified Communications Manager.

Caution You must back up your cluster using the Disaster Recovery System (DRS) to be able to recover the cluster.

Step 4 Back Up Your Cluster.

To backup your cluster using DRS, see the *Administration Guide for Cisco Unified Communications Manager* .

What to do next

Once the publisher is up after the upgrade, do not reboot until the CAR migration completes. You are not allowed to switch to old version or perform a DRS backup in this phase. You can monitor the CAR migration status by navigating to **Cisco Unified Serviceability** > **Tools** > **CDR Analysis and Reporting**.

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.

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.

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.

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 80

Self-signed Certificate Fields

Table 15: 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**. • 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.

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 **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 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.

Generate Certificate Signing Request

If you generate a new certificate signing request for a specific certificate type, the application overwrites the existing certificate signing request for that certificate type.

You can upload the CA signed certificates by generating CSR from Cisco Unified Operating System Administration and present to the CA. Whenever you generate a CSR, a new private key is generated along with CSR.

A private key is a file that is unique to a server and service, which you have selected while generating CSR. Do not share this private key with anyone for security compliance. If you provide a private key to someone, it compromises the security that the certificate provides. Also, do not regenerate a new CSR for the same service if you are using the old CSR to create a certificate. Unified Communications Manager deletes the old CSR and private key, replaces both of them with new one and makes the old CSR unserviceable.

Note Unified Communications Manager Release 11.0 onwards, when you choose the bulk operation units—TFTP or all, the ECDSA certificates get included with the RSA certificates.

Procedure

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

Step 2 Click **Generate CSR**.
The **Generate Certificate Signing Request** window appears.

Step 3 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 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 Certificate Signing Request** window. See the Related Topics section for more information about the fields and their configuration options.

Step 6 Click **Generate**.

Related Topics

Certificate Signing Request Fields, on page 83

Certificate Signing Request Fields

Table 16: Certificate Signing Request Fields

Field	Description
Certificate Purpose	From the drop-down box, select a value: • **CallManager** • **CallManager-ECDSA**

Field	Description

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>`

	Shows the name of the Unified Communications Manager application that you selected in the **Distribution** field by default.
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 box, 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 are not 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.
Hash Algorithm	Select a value from the **Hash Algorithm** drop-down box to have stronger hash algorithm as the elliptical curve key length. From the **Hash Algorithm** drop-down box, 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 is mandatory that you select SHA256 as the hashing algorithm.

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**.

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.

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 86	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 87	Configure Unified Communications Manager for Contact Search Authentication.
Step 3	Configure Secure Directory Server for Contact Search, on page 87	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.

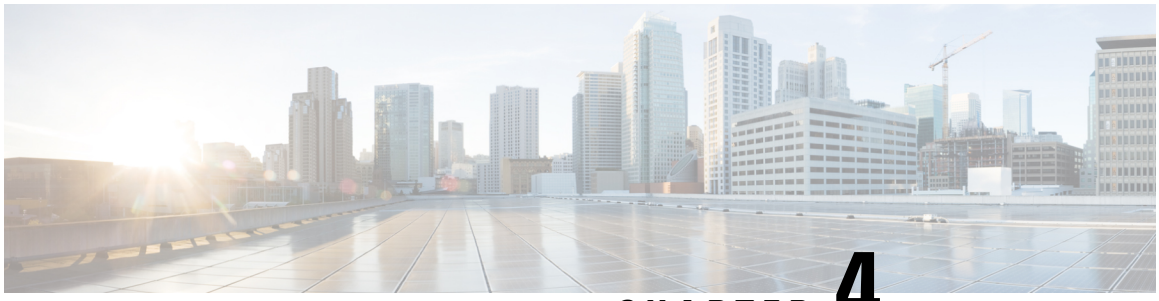
Procedure

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**.



CHAPTER 4

Cisco CTL Client Setup

This chapter provides information about Cisco CTL client setup.

- About Cisco CTL Setup, on page 89
- Addition of Second SAST Role in the CTL File for Recovery, on page 91
- SIP OAuth Configuration Through CLI, on page 91
- Activate Cisco CTL Provider Service, on page 92
- Cisco CAPF Service Activation, on page 93
- Set up Secure Ports, on page 93
- Set Up Cisco CTL Client, on page 94
- SAST Roles of CTL File, on page 96
- Migrate Phones from One Cluster to Another Cluster, on page 97
- Migration from eToken-based CTL File to Tokenless CTL File, on page 98
- Update CTL File, on page 98
- Update Cisco Unified Communications Manager Security Mode, on page 99
- Cisco CTL File Details, on page 100
- Verify Cisco Unified Communications Manager Security Mode, on page 101
- Set Up Smart Card Service to Started or Automatic, on page 101
- Verify or Uninstall Cisco CTL Client, on page 102

About Cisco CTL Setup

Device, file, and signaling authentication rely on the creation of the Certificate Trust List (CTL) file, which is created when you install and configure the Cisco Certificate Trust List (CTL).

Note

- To enable mixed-mode or to update the CTL File, ensure that the Smart Licensing registration is completed in Unified Communications Manager by using the Registration Token received from the Smart account or Virtual account that has Allow export-controlled functionality enabled. For details on how to configure Cisco Smart Software Licensing, see the "Smart Software Licensing" chapter of the *System Configuration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.
- An alarm named *ClusterModeSecurityFailedExportControlNotAllow* is sent when you are running CTL Client but Unified Communications Manager is not enabled for export-controlled functionality.

The CTL file contains entries for the following servers or security tokens:

- System Administrator Security Token (SAST)
- CiscoCallManager and CiscoTFTP services that are running on the same server
- Certificate Authority Proxy Function (CAPF)
- TFTP server(s)
- ASA firewall
- ITLRecovery

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.

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.

After the Cisco CTL Client adds a server certificate to the CTL file, you can update the CTL file by running the following CLI 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.

When you configure a firewall in the CTL file, you can secure a Cisco ASA Firewall as part of a secure Unified Communications Manage system. It displays the firewall certificate as a "CCM" certificate.

Note

- You must run the CLI commands on the publisher node.
- Be aware that regenerating the ITLRecovery certificate changes the signer of the file. Phones that do not support Security by Default will not accept the new CTL file unless CTL files are manually deleted from the phone. For information on deleting the CTL files on the phone, see the *Cisco IP Phone Administration Guide* for your phone model.

Addition of Second SAST Role in the CTL File for Recovery

Earlier releases of Unified Communications Manager has tokenless approach where endpoints trusted only one Cisco site administrator security token (SAST). This SAST is the CallManager certificate. In this approach, the certificate trust list (CTL) file contained only one SAST record that was used to sign the CTL file. As only one SAST was used, any update in the SAST signer caused the endpoints to get locked out. Following points list the scenarios when endpoints or devices locked out due to update in SAST signer:

- The endpoints accepted the CTL file that is signed by using the CallManager certificate during registration.
- An administrator regenerated the CallManager certificate and updated the CTL file. This regeneration implied that the updated CTL file was signed by updated CallManager certificate instead of the existing CallManager certificate.
- The endpoints did not trust the updated CallManager certificate because the updated certificate was unavailable in the endpoints trust list. So, the endpoints rejected the CTL file instead of downloading it.
- The endpoints tried to connect with the ccm service securely over Transport Layer Security (TLS), ccmservice offered its updated CallManager certificate to the endpoints as part of TLS exchange. Because the updated certificate was unavailable in the endpoints trust list, endpoints rejected the CTL file instead of downloading it.
- The endpoints no longer talk to ccmservice and get locked out as a result.

For easier recovery from the endpoint lock out, the tokenless approach for endpoints is enhanced by addition of second SAST in the CTL File for recovery. In this feature, the tokenless CTL file contains two SAST tokens—the CallManager record and the ITLRecovery record.

The ITLRecovery certificate is chosen over other certificates because of the following reasons:

- Does not change because of secondary reasons, such as change in hostname.
- Already being used in the ITL file.

SIP OAuth Configuration Through CLI

Through the CLI, 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 12.5(1)*.

Consider the following points:

- When Cluster SIP OAuth mode is enabled, Cisco 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 Cisco Unified Communications Manager user interface.

  - **SIP OAuth Port**

- **SIP OAuth MRA Port**

  You can configure the ports from Cisco Unified CM Administration, choose **System** > **Cisco Unified CM** > **CallManager** page.

- Restart the Cisco CallManager service in all the nodes for the parameter change to take effect.

The encryption option consists of the following CLI commands:

admin:utils sipOAuth-mode
Check the status of SIP OAuth mode in the cluster.
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.

Activate Cisco CTL Provider Service

After you configure the Cisco CTL Client, the Cisco CTL Provider service changes the security mode from nonsecure to mixed mode and transports the server certcertificates to the CTL file. The service then transports the CTL file to all Unified Communications Manager and CiscoTFTP servers.

If you activate this service and then upgrade Unified Communications Manager, Unified Communications Manager automatically reactivates the service after the upgrade.

Tip You must activate the CiscoCTL Provider service on all servers in the cluster.

To activate the service, perform the following procedure:

Procedure

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

Step 2 In the Servers drop-down list box, choose a server where you have activated the Cisco CallManager or Cisco TFTP services.

Step 3 Click the **CiscoCTL Provider** service radio button.

Step 4 Click **Save.**

Tip Perform this procedure on all servers in the cluster.

Note You can enter a CTL port before you activate the CiscoCTL Provider service. If you want to change the default port number, see topics related to setting up ports for a TLS connection.

Step 5 Verify that the service runs on the servers. In Cisco Unified Serviceability, choose **Tools** > **Control Center - Feature Services** to verify the state of the service.

Cisco CAPF Service Activation

Warning Activating the Cisco certificate authority proxy function service before you install and configure the Cisco CTL Client ensures that you do not have to update the CTL file to use CAPF.

Set up Secure Ports

You may have to configure a different TLS port number if the default port is currently being used or if you use a firewall and you cannot use the port within the firewall.

- The Cisco CTL Provider default port for the TLS connection equals 2444. The Cisco CTL Provider port monitors requests from the Cisco CTL Client. This port processes Cisco CTL Client requests, such as retrieving the CTL file, setting the cluster security mode, and saving the CTL file to the TFTP server.

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

- The Ethernet Phone Port monitors registration requests from the phone that is running SCCP. In nonsecure mode, the phone connects through port 2000. In mixed mode, the Unified Communications Manager port for TLS connection equals the value for the Unified Communications Manager port number added to (+) 443; therefore, the default TLS connection for Unified Communications Manager equals 2443. Update this setting only if the port number is in use or if you use a firewall and you cannot use the port within the firewall.
- The SIP Secure Port allows Unified Communications Manager to listen for SIP messages from phones that are running SIP. The default value equals 5061. If you change this port, you must restart the CiscoCallManager service in Cisco Unified Serviceability and reset the phones that are running SIP.

Tip After you update the port(s), you must restart the Cisco CTL Provider service in Cisco Unified Serviceability.

Tip You must open the CTL ports to the data VLAN from where the CTL Client runs.

To change the default setting, perform the following procedure:

Procedure

Step 1 Perform the following tasks, depending on the port that you want to change:

a) To change the Port Number parameter for the Cisco CTL Provider service, perform Step 2, on page 94 through Step 6, on page 94.

b) To change the Ethernet Phone Port or SIP Phone Secure Port settings, perform Step 7, on page 94 through Step 11, on page 94.

Step 2 To change the Cisco CTL Provider port, choose **System** > **Service Parameters** in Unified Communications Manager Administration.

Step 3 In the Server drop-down list, choose a server where the CiscoCTL Provider service runs.

Step 4 In the Service drop-down list box, choose Cisco CTL Provider service.

Tip For information on the service parameter, click the question mark or the link name.

Step 5 To change the value for the Port Number parameter, enter the new port number in the Parameter Value field.

Note Starting 12.X onwards, you cannot change the value for the Port Number parameter in the Parameter Value field.

Step 6 Click **Save.**

Step 7 To change the Ethernet Phone Port or SIP Phone Secure Port settings, choose **System** > **CiscoUnifiedCM** in Unified Communications Manager Administration.

Step 8 Find a server where the CiscoCallManager service runs, as described in the *Administration Guide for Cisco Unified Communications Manager*; after the results display, click the **Name** link for the server.

Step 9 After the Unified Communications Manager Configuration window displays, enter the new port numbers in the Ethernet Phone Port or SIP Phone Secure Port fields.

Step 10 Reset the phones and restart the CiscoCallManager service in Cisco Unified Serviceability.

Step 11 Click **Save**.

Set Up Cisco CTL Client

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

Note

- The CLI command **utils ctl set-cluster mixed-mode**, sets the cluster in mixed-mode. To enable mixed-mode, ensure that the Unified Communications Manager is registered with the Cisco Smart Software Manager or Cisco Smart Software Manager satellite and the Registration Token received from the Smart account or Virtual account has Allow export-controlled functionality enabled while registering with this cluster.
- The CLI command **utils ctl update CTLFile**, updates the CTLFile. To update the CTLFile in mixed-mode, ensure that the Unified Communications Manager is registered with the Cisco Smart Software Manager or Cisco Smart Software Manager satellite and the Registration Token received from the Smart account or Virtual account has Allow export-controlled functionality enabled while registering with this cluster.
- When the Unified Communications Manager is not registered with the Registration Token that has Allow export-controlled functionality enabled and you run the **utils ctl set-cluster mixed-mode** and **utils ctl update CTLFile** commands, the following error message is displayed:

  ```
  Command cannot be executed because the Unified Communications Manager
  cluster is not registered to a Smart/Virtual Account with Allow
  export-controlled functionality. Please ensure Product Token received
  from the Smart/Virtual Account has Allow export-controlled functionality
  checked when registering the UCM Cluster.
  ```

The Cisco CTL CLI performs the following tasks:

- Sets the Unified Communications Manager security mode for a cluster or standalone server.

Note You cannot set the Unified Communications Manager cluster security parameter to mixed mode through the Enterprise Parameters Configuration window of Unified Communications Manager Administration. You can set the cluster security mode through the Cisco CTL Client or the CLI command set **utils ctl**.

- Creates the Certificate Trust List (CTL), which is a file that contains certificate entries for security tokens, Unified Communications Manager, ASA firewall, and CAPF server.

  The CTL file indicates the servers that support TLS for the phone connection. The client automatically detects the Unified Communications Manager, Cisco CAPF, and ASA firewall and adds certificate entries for these servers.

Note The Cisco CTL Client also provides supercluster support: up to 16 call processing servers, 1 publisher, 2 TFTP servers, and up to 9 media resource servers.

Tip You can update the CTL file during a scheduled maintenanc you must restart the TFTP services and then the CallManage that run these services in the cluster.

After you complete the Cisco CTL configuration, the CTL performs the following tasks:

- Writes the CTL file to the Unified Communications Manager server(s).
- Writes CAPF capf.cer to all Unified Communications Manager subsequent nodes (not first node) in the cluster.
- Writes CAPF certificate file in PEM format to all Unified Communications Manager subsequent nodes (not first node) in the cluster.
- Writes the file to all configured TFTP servers.
- Writes the file to all configured ASA firewalls.
- Signs the CTL file with the private key of the security token that exists in the USB port at the time you create the CTL file.

SAST Roles of CTL File

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

Table 17: 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

Cisco Unified Communications Manager Version	SAST Roles in Token-based CTL File	SAST Roles in Tokenless CTL File
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

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.

Migration from eToken-based CTL File to Tokenless CTL File

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.

Update CTL File

Note This procedure is not required if you manage cluster security through the CLI command set **utils ctl**.

You must update the CTL file if the following scenarios occur:

- If you add a new Unified Communications Manager server to the cluster

  Note To add a node to a secure cluster, see *Installing Unified Communications Manager*, which describes how to add a node and how to configure security for the new node.

- If you change the name or IP address of a Unified Communications Manager server
- If you change the IP address or hostname for any configured TFTP servers
- If you change the IP address or hostname for any configured ASA firewall
- If you enabled the Cisco Certificate Authority Function service in Cisco Unified Serviceability
- If you need to add or remove a security token
- If you need to add or remove a TFTP server
- If you need to add or remove a Unified Communications Manager server
- If you need to add or remove an ASA firewall
- If you restore a Unified Communications Manager server or Unified Communications Manager data

- If you manually regenerate CallManager, CAPF, or ITL Recovery certificate on any node on the Cisco Unified Communications Manager cluster that contains a CTL file, you must re-run the CTL wizard. This step is not required for the generation of other certificates.
- If you update from a Unified Communications Manager version prior to 7.1.5 to a version 7.1.5 or later.
- If you update from a Unified Communications Manager version prior to 10.5 to a version 10.5 or later, refer to the migration section from Hardware eTokens to Tokenless Solution.
- After you upload a third-party, CA-signed certificate to the platform.

Note When a domain name is added or changed on a Unified Communications Manager cluster in mixed mode, you must update the CTL file for the phone configuration files to take effect.

Tip Cisco strongly recommends that you update the file when minimal call-processing interruptions will occur.

Caution If Unified Communications Manager is integrated with Unity Connection 10.5 or later using secure SIP or SCCP, then the secure calls may stop working with Unity Connection. You must reset the corresponding port groups on Unity Connection to resolve this issue.

To reset the port group through the Unity Connection Administration interface, navigate to **Telephony Integrations** > **Port Group**, select the port group that you want to reset, and click **Reset** on the **Port Group Basics** page.

Update Cisco Unified Communications Manager Security Mode

You must use the Cisco CTL to configure the cluster security mode. You cannot change the Unified Communications Manager security mode from the Enterprise Parameters Configuration window in Unified Communications Manager Administration.

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

To change the cluster security mode after the initial configuration of the Cisco CTL Client, you must update the CTL file.

Procedure

Step 1 Run the CLI command `utils ctl set-cluster mixed-mode` to change the cluster security mode to secure.

Step 2 Run the CLI command `utils ctl set-cluster non-secure-mode` to change the cluster security mode to non-secure.

Cisco CTL File Details

Note You can set up encryption by using the **utils ctl** CLI command set, which does not require security tokens. For more information about this option, see the *Command Line Interface Guide for Cisco Unified Communications Solutions.*

You can set the cluster security mode to nonsecure or mixed mode, as described in the following table. Only mixed mode supports authentication, encrypted signaling, and encrypted media.

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

Table 18: CTL Configuration Settings

Setting	Description
Unified Communications Manager Server	
Security Mode	
Set Unified Communications Manager Cluster to Mixed Mode	Mixed mode allows authenticated, encrypted, and nonsecure Cisco IP Phones to register with Unified Communications Manager. In this mode, Unified Communications Manager ensures that authenticated or encrypted devices use a secure port.
Set Unified Communications Manager Cluster to Non-Secure Mode	If you configure nonsecure mode, all devices register as unauthenticated, and Unified Communications Manager supports image authentication only. When you choose this mode, the Cisco CTL Client removes the certificates for all entries that are listed in the CTL file, but the CTL file still exists in the directory that you specified. The phone requests unsigned configuration files and registers as nonsecure with Unified Communications Manager. **Tip** To revert the phone to the default nonsecure mode, you must delete the CTL file from the phone and all Unified Communications Manager servers.
CTL Entries	

Setting	Description
Tokens	If you have not already done so, remove the token that you initially inserted into the server or workstation. When the application prompts you to do so, insert the next token and click **OK**. When the security token information for the additional token displays, click **Add**. For all security tokens, repeat these tasks.
Add TFTP Server	Click this button to add an Alternate TFTP server to the certificate trust list. For information on the settings, click the **Help** button after the Alternate TFTP Server tab settings display. After you enter the settings, click **Next**.
Add Firewall	Click this button to add an ASA firewall to the certificate trust list. For information on the settings, click the **Help** button after the Firewall tab settings display. After you enter the settings, click **Next**.

Verify Cisco Unified Communications Manager Security Mode

To verify the cluster security mode, perform the following procedure:

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

Procedure

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

Step 2 Locate the **Cluster Security Mode** field. If the value in the field displays as **1**, you correctly configured Unified Communications Manager for mixed mode. (Click the field name for more information.)

Tip You cannot configure this value in Unified Communications Manager Administration. This value displays after you configure the Cisco CTL Client.

Set Up Smart Card Service to Started or Automatic

If the Cisco CTL Client installation detects that the Smart Card service is disabled, you must set the Smart Card service to automatic and started on the server or workstation where you are installing the Cisco CTL Client plug-in.

Tip You cannot add the security tokens to the CTL file if the service is not set to started and automatic.

Tip After you upgrade the operating system, apply service releases, upgrade Cisco Unified Communications Manager, and so on, verify that the Smart Card service is started and automatic.

To set the service to started and automatic, perform the following procedure:

Procedure

Step 1 On the server or workstation where you installed the Cisco CTL Client, choose **Start** > **Programs** > **Administrative Tools** > **Services** or **Start** > **Control Panel** > **Administrative Tools** > **Services**.

Step 2 From the Services window, right-click the **Smart Card** service and choose Properties.

Step 3 In the Properties window, verify that the **General** tab displays.

Step 4 From the Startup type drop-down list box, choose **Automatic**.

Step 5 Click **Apply**.

Step 6 In the Service Status area, click **Start**.

Step 7 Click **OK**.

Step 8 Reboot the server or workstation and verify that the service is running.

Verify or Uninstall Cisco CTL Client

Uninstalling the Cisco CTL Client does not delete the CTL file. Likewise, the cluster security mode and the CTL file do not change when you uninstall the client. If you choose to do so, you can uninstall the Cisco CTL using the CLI option.

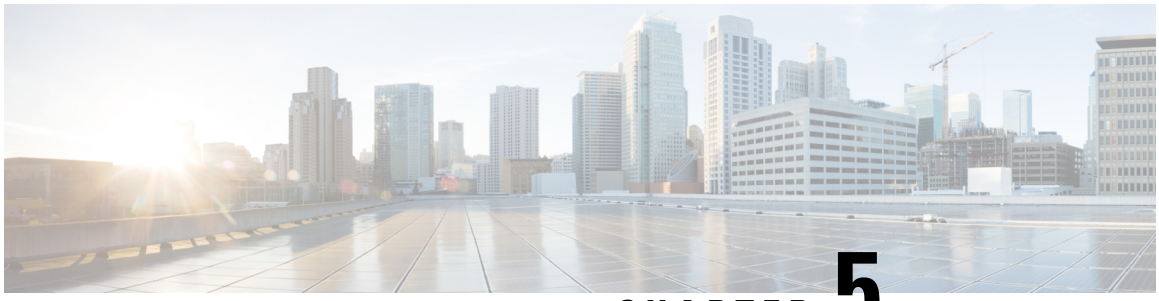
To verify that the Cisco CTL Client installed, perform the following procedure:

Procedure

Step 1 Choose **Start** > **Control Panel** > **Add Remove Programs**.

Step 2 To verify that the client installed, locate **Cisco CTL Client**.

Step 3 To uninstall the client, click **Remove**.



CHAPTER 5

TLS Setup

- TLS Overview, on page 103
- TLS Prerequisites, on page 103
- TLS Configuration Task Flow, on page 104
- TLS Interactions and Restrictions, on page 108

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, and Prime Collaboration Provisioning.

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 105.	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 105.	Configure the TLS cipher options that Unified Communications Manager supports.
Step 3	Configure TLS in a SIP Trunk Security Profile, on page 105.	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 106.	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 106.	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 107.	Assign the TLS-enabled profile that you created to a phone.
Step 7	Add Secure Phone Profile to a Universal Device Template, on page 108.	Assign a TLS-enabled phone security profile to a universal device template. If you have the 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 103.

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.

Step 4 Perform Step 3 on all Unified Communications Managerand 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**.

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 19: 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 20: 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.
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.

Feature	Restriction
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 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).
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.

Feature	Restriction
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 21: Cisco Unified Communications Manager Ports Affected by 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
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

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
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 with trunk)	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
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 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:

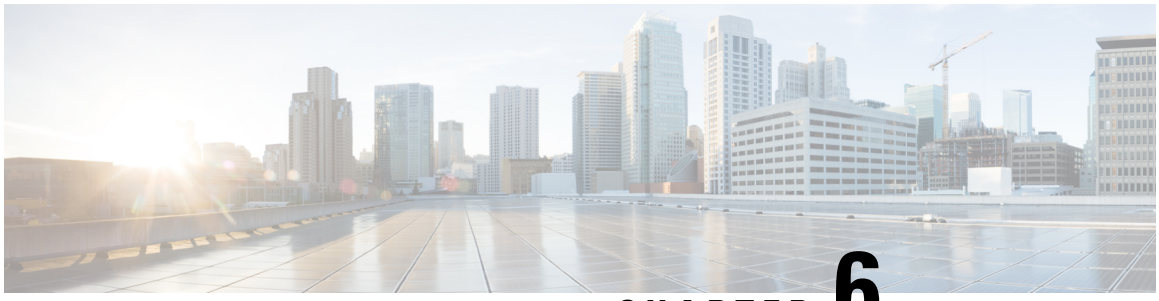
Table 22: Instant Messaging & Presence Ports Affected by Transport Layer Security Version 1.2

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
7335	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 II

Certificates

- Certificate Overview, on page 117
- Certificate Authority Proxy Function, on page 129
- Certificate Monitoring and Revocation, on page 145



CHAPTER 6

Certificate Overview

- Certificates Overview, on page 117
- Administration Tasks for Certificates, on page 121

Certificates Overview

A certificate is a file that contains the certificate holder name, public key and digital signature of the certificate authority that is issuing the certificate. A certificate proves the identity of the owner of the certificate.

Unified Communications Manager uses certificates that use the public-key infrastructure (PKI) in order to validate server and client identity and to enable encryption. When another system (for example, a phone or media server) tries to connect to Unified Communications Manager, it presents its certificate to Unified Communications Manager in order to verify its identity. Unified Communications Manager will not trust the other system, and will deny access, unless it has a matching certificate in the appropriate trust store.

Unified Communications Manager uses two broad classes of certificates:

- Self-signed Certificates—By default, Unified Communications Manager uses self-signed certificates. These are certificates where Unified Communications Manager itself signs the certificate in order to confirm the identity of the server or client. Unified Communications Manager can issue self-signed certificates for itself, or for LSC certificates on behalf of phones via the Certificate Authority Proxy Function.
- CA-signed certificates—You can also configure Unified Communications Manager to use certificates that are signed by a third-party certificate authority (CA). You must complete a Certificate Signing Request (CSR) to have the CA sign a certificate on behalf of Unified Communications. The CA receives the request and issues CA-signed certificates. To use CA-signed certificates, you must first install the CA root certificate chain on Unified Communications Manager.

Note Typically, self-signed certificates are accepted for internal connections that do not cross a company firewall. However, for WAN connections, or for connections that use the public internet, you should use CA-signed certificates.

Note Generalized Time values for X.509 PKI certificates must be expressed in Greenwich Mean Time (GMT) and must include seconds (**YYYYMMDDHHMMSSZ**). Fractional seconds are not allowed. Certificates that violate this rule, whether offered from a peer entity, or loaded in the trust store, may fail the certificate verification process.

CTL File

The Cisco Certificate Trust List is a file that is created when you enable mixed mode by the Cisco CTL Client or by running one of the utils ctl CLI commands (for example, utils ctl update CTLFile). When mixed mode is enabled, the CTL file gets installed on Cisco IP Phones via the TFTP server. The CTL file contains a list of certificates for phones to trust, including the Certificate Authority Proxy Function system certificate and other certificates.

For details on how to configure the CTL File, see the CTL Client Setup chapter.

TLS

Transport Line Signaling (TLS) uses CA-signed certificates. When TLS is configured, the other system presents its certificate to Unified Communications Manager as part of the initial connection setup. If Unified Communications Manager has the other system's certificate installed, it trusts the other system, and communication occurs. If the other system's certificate is not present, the other system is untrusted, and communication fails.

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.

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 23: 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	Y	Y		
CAPF (publisher only)	N	Y			Y	Y		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		
TVS	Y	Y	Y		Y	Y	Y		

Table 24: 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	Y	Y		Y
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		Y
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

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 25: 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.

Administration Tasks for Certificates

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.

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 deactivated and later activated when a Tomcat certificate is uploaded. Else, the TFTP continues to offer the old cached self-signed tomcat certificate.

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.
- If you import a certificate into the CAPF-trust, it is enabled only on that particular node and is not replicated across the cluster.

Regenerate a Certificate

We recommend you to 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 phones and reboot 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 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 certificate details page, a self-signed certificate with the same key length is regenerated.

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.

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.

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 26: Certificate Names and Descriptions

Name	Description	Related Services
tomcat tomcat-ECDSA	This certificate is used by WebServices and Cisco CallManager services when SIP Oauth mode is enabled.	Cisco Tomcat Services, Cisco CallManager Service.
CallManager CallManager-ECDSA	This is used for SIP, SIP trunk, SCCP, TFTP etc.	CallManager - NA CallManager-ECDSA - Cisco CallManager Service
CAPF	Used by the CAPF service running on the Unified Communications Manager Publisher. This certificate is used to issue LSC to the endpoints (except online and offline CAPF mode)	N/A
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

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.

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 Restart the Cisco CallManager Service on all nodes in the cluster after the keys are reassigned.

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**.

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**.

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.

Troubleshoot Certificate Errors

Before you begin

If you encounter an error when you attempt to access Unified Communications Manager services from an IM and Presence Service node or IM and Presence Service functionality from a Unified Communications Manager node, the source of the issue is the tomcat-trust certificate. The error message `Connection to the Server cannot be established (unable to connect to Remote Node)` appears on the following Serviceability interface windows:

- **Service Activation**
- **Control Center - Feature Services**
- **Control Center - Network Services**

Use this procedure to help you resolve the certificate error. Start with the first step and proceed, if necessary. Sometime, you may only have to complete the first step to resolve the error; in other cases, you have to complete all the steps.

Procedure

Step 1 From Cisco Unified OS Administration, verify that the required tomcat-trust certificates are present: **Security** > **Certificate Management**.

If the required certificates are not present, wait 30 minutes before checking again.

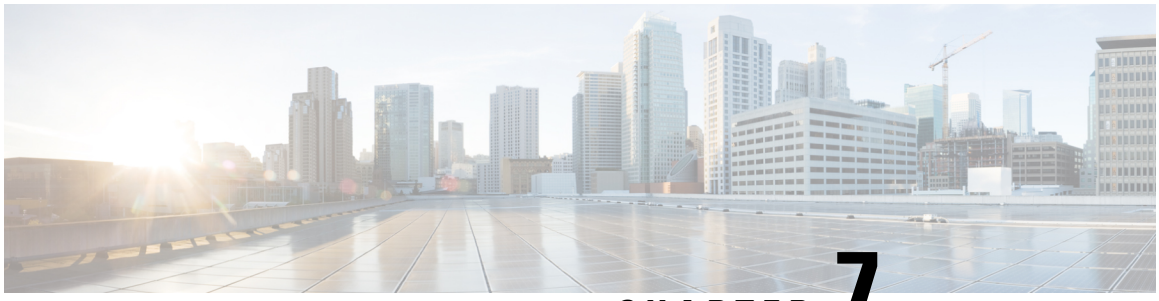
Step 2 Choose a certificate to view its information. Verify that the content matches with the corresponding certificate on the remote node.

Step 3 From the CLI, restart the Cisco Intercluster Sync Agent service: **utils service restart Cisco Intercluster Sync Agent**.

Step 4 After the Cisco Intercluster Sync Agent service restarts, restart the Cisco Tomcat service: **utils service restart Cisco Tomcat**.

Step 5 Wait 30 minutes. If the previous steps do not address the certificate error and a tomcat-trust certificate is present, delete the certificate. After you delete the certificate, you must manually exchange it by downloading the Tomcat and Tomcat-ECDSA certificate for each node and uploading it to its peers as a tomcat-trust certificate.

Step 6 After the certificate exchange is complete, restart Cisco Tomcat on each affected server: **utils service restart Cisco Tomcat**.



CHAPTER 7

Certificate Authority Proxy Function

- Certificate Authority Proxy Function (CAPF) Overview, on page 129
- CAPF Prerequisites, on page 131
- Certificate Authority Proxy Function Configuration Task Flow, on page 132
- CAPF Administration Tasks, on page 139
- CAPF System Interactions and Restrictions, on page 140

Certificate Authority Proxy Function (CAPF) Overview

The Cisco Certificate Authority Proxy Function (CAPF) is a Cisco proprietary service that issues Locally Significant Certificates (LSCs) and authenticates Cisco endpoints. The CAPF service runs on Unified Communications Manager and performs the following tasks:

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

CAPF Running Modes

You can configure CAPF to operate in the following modes:

- Cisco Authority Proxy Function—The CAPF service on Unified Communications Manager issues LSCs that are signed by CAPF service itself. This is the default mode.
- 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 CSR is submitted, the CA signs and returns the CA-signed LSC automatically.
- Offline CA—Use this option if you want to use an offline external CA to sign LSC for phones. This option requires you to manually download the LSC, submit them to the CA, and then upload the CA-signed certificates after they are ready.

Note Cisco recommends that if you want to use a third-party CA to sign LSC, use the **Online CA** option instead of **Offline CA** as the process is automated, much quicker, and less likely to encounter problems.

CAPF Service Certificate

When Unified Communications Manager is installed, CAPF service is installed automatically and a CAPF-specific system certificate is generated. When security is applied, Cisco CTL Client copies the certificate to all cluster nodes.

Phone Certificate Types

Cisco uses the following X.509v3 certificate types for phones:

- Locally Significant Certificates (LSC)—A certificate that installs on supported phones after you perform the necessary configuration tasks that are associated with the Cisco Certificate Authority Proxy Function (CAPF). The LSC secures the connection between Unified Communications Manager and the phone after you configure the device security mode for authentication or encryption.

  Note For Online CA, the LSC validity is based on the CA and can be used as long as the CA allows it.

- Manufacture Installed Certificates (MIC)—Cisco Manufacturing installs MICs automatically in supported phone models. Manufacturer-installed certificates authenticate to Cisco Certificate Authority Proxy Function (CAPF) for LSC installation. You cannot overwrite or delete manufacture-installed certificate.

Note Cisco recommends that you use Manufacturer Installed Certificates (MICs) for LSC installation only. Cisco supports LSCs to authenticate the TLS connection with Unified Communications Manager. Since MIC root certificates can be compromised, customers 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.

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

CAPF Prerequisites

Before configuring the Certificate Authority Proxy Function for LSC generation, perform the following:

- If you want to use a third-party CA to sign your LSCs, configure your CA externally.
- Plan how you are going to authenticate your phones.
- Before you generate LSCs, ensure that you have the following:
  - Unified Communications Manager Release 12.5 or later.
  - Endpoints that use CAPF for certificates (includes Cisco IP Phones and Jabber).
  - Microsoft Windows Server 2012 and 2016.
  - Domain Name Service (DNS) is configured.
- You must upload the CA root and HTTPS certificates before generating LSCs. During a secure SIP connection, HTTPS certificate goes through the CAPF-trust and the CA root certificate goes through the CAPF-trust and the CallManager-trust. The Internet Information Services (IIS) hosts the HTTPS certificate. The CA root certificate is used to sign the Certificate Signing Requests (CSR).

  Following are the scenarios when you have to upload the certificates:

Table 27: Upload Certificate Scenarios

Scenarios	Results
CA root and HTTPS certificates are same.	Upload the CA root certificate.
CA root and HTTPS certificates are different and if HTTPS certificates are issued by the same CA root certificate.	Upload the CA root certificate.
The intermediate CA and HTTPS certificates are different and are issued by the CA root certificate.	Upload the CA root certificate.
CA root and HTTPS certificates are different and are issued by the same CA root certificate.	Upload CA root and HTTPS certificate.

Note Cisco strongly recommends that you use CAPF during a scheduled maintenance window because generating multiple certificates simultaneously may cause call-processing interruptions.

Certificate Authority Proxy Function Configuration Task Flow

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

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 to the CAPF-trust store. Otherwise, you can skip this task.
Step 2	Upload Certificate Authority (CA) Root Certificate , on page 133	Upload the CA root certificate to the Unified Communications Manager Trust store.
Step 3	Configure Online Certificate Authority Settings, on page 133	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 136 • Update CAPF Settings via Bulk Admin, on page 137 • Configure CAPF Settings for a Phone, on page 138	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 139	(Optional) 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

Upload the cluster-wide certificate, to distribute it to all the servers within the cluster.

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**.

Configure Online Certificate Authority Settings

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

Note FIPS enabled mode doesn't support Online CAPF and CAPFv3.

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 in order 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 HTTPS certificate.

  Note The hostname configured is the same as the Common Names (CN) of the HTTPs 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.
- Online CA Type—Choose the default type, Microsoft CA.
- Online CA Username—Enter the username of the CA server.
- Online CA Password—Enter the password for the username of the CA server.

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

- For Online CA operation, EST servers use TVS certificates from CUCM and if the TVS certificate is CA signed, then the Online CA will not work.
- 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
- Device secure registration fails if LSC certificate is not provided with 'Digital signature' and 'key encipherment' while using Online CA for LSC operation.

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 136
b) Update CAPF Settings via Bulk Admin, on page 137
c) Configure CAPF Settings for a Phone, on page 138

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 137.

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 login to the publisher node.

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

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

CAPF Administration Tasks

After you configure CAPF and issue LSC certificates, use the following tasks to administer LSC certificates on an ongoing basis.

Certificate Status Monitoring

You can configure the system to monitor certificate status automatically. The system will email you when certificates are approaching expiration, and then revoke the certificates after expiration.

For details on how to configure certificate monitoring checks, see the Certificate Monitoring and Revocation Task Flow in the "Manage Certificates" chapter.

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**.

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 and Restrictions

Feature	Interaction
Authentication String	CAPF authentication method for the phone, you must enter the same authentication string on the phone after the operation, or the operation will fail. If TFTP Encrypted Configuration enterprise parameter is enabled and you fail to enter the authentication string, the phone may fail and may not recover until the matching authentication string is entered on the phone
Cluster Server Credentials	All servers in the Unified Communications Manager cluster must use the same administrator username and password, so CAPF can authenticate to all servers in the cluster

Feature	Interaction
Migrating secure phone	If a secure phone gets moved to another cluster, the Unified Communications Manager will not trust the LSC certificate that the phone sends because it was issued by another CAPF, whose certificate is not in the CTL file. To enable the secure phone to register, delete the existing CTL file. You can then use the Install/Upgrade option to install a new LSC certificate with the 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 series, 7900 series, 8900 series, and 9900	Cisco recommends upgrading Cisco Unified IP Phones 6900 series, 7900 series, 8900 series, and 9900 series to use LSCs for TLS connection to Unified Communications Manager and removing MIC root certificates from the CallManager trust store to avoid possible future compatibility issues. Be aware that 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 CallManager trust store: • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048
Power Failures	The following information applies when a communication or power failure occurs. • If a communication failure occurs while the certificate installation is taking place on the phone, the phone will attempt to obtain the certificate three more times in 30-second intervals. You cannot configure these values. • If a power failure occurs while the phone attempts a session with CAPF, the phone will use the authentication mode that is stored in flash; that is, if the phone cannot load the new configuration file from the TFTP server after the phone reboots. After the certificate operation completes, the system clears the value in flash.

Feature	Interaction
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, IP Phones 7900/8900/9900 series models 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.

CAPF Examples with 7942 and 7962 Phones

Consider the following information about how CAPF interacts with the Cisco Unified IP Phone 7962 and 7942 when the phone is reset by a user or by Unified Communications Manager.

Note In the following examples, if the LSC does not already exist in the phone and if **By Existing Certificate** is chosen for the CAPF Authentication Mode, the CAPF certificate operation fails.

Example-Nonsecure Device Security Mode

In this example, 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 LSC, configure the Device Security Mode to Authenticated or Encrypted.

Example-Authenticated/Encrypted Device Security Mode

In this example, 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 does not 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 cannot configure **By Authentication String** in this example because the phone does not automatically contact the CAPF server; the registration fails if the phone does not have a valid LSC.

CAPF Interaction with IPv6 Addressing

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

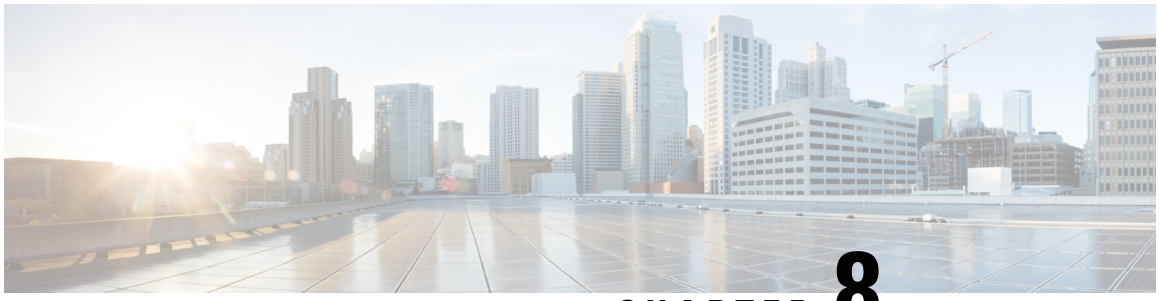
When the phone connects to CAPF to get a certificate, CAPF uses the configuration from the Enable IPv6 enterprise parameter to determine whether to issue or upgrade the certificate to the phone. If the enterprise parameter is set to **False**, CAPF ignores/rejects connections from phones that use IPv6 addresses, and the phone does not receive the certificate.

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

Table 28: 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 cannot connect via 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 cannot connect to CAPF.
Two stack	IPv6	IPv4	Phone cannot connect to CAPF.
Two stack	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects 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 cannot connect to CAPF.
IPv6 stack	IPv6	IPv6	Phone uses an IPv6 address to connect to CAPF.
IPv6 stack	IPv6	IPv4	Phone cannot connect to CAPF.



CHAPTER 8

Certificate Monitoring and Revocation

- Certificate Monitoring Overview, on page 145
- Certificate Monitoring Task Flow, on page 146

Certificate Monitoring Overview

Administrators must be able to keep track of certificates. Part of this is knowing which certificates need to be renewed and when. Cisco Unified Communications Manager contains automated systems that help administrators to know which certificates are approaching renewal and when. You can configure the system to do the following:

- Monitor certificate statuses on an ongoing basis and email you when a certificate is approaching expiration.
- Use the Online Certificate Status Protocol (OCSP) to check certificate status regularly and revoke certificates as they expire.

Certificate Revocation through Online Certificate Status Protocol

Unified Communications Manager provisions the OCSP for monitoring certificate revocation. System checks for the certificate status to confirm validity at scheduled intervals and every time there is, a certificate uploaded.

The Online Certificate Status Protocol (OCSP) helps administrators manage their system's certificate requirements. When OCSP is configured, it provides a simple, secure, and automated method to check certificate validity and revoke expired certificates in real-time.

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

Validation Checks

Unified Communications Manager checks the certificate status and confirms validity.

The certificates are validated 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, Unified Communications Manager falls back to the Trust Responder Model (TRP) and 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.

- Enable OCSP option in the **Certificate Revocation** window to provide the most secure means of checking certificate revocation in real-time. Choose from options to use the OCSP URI from a certificate or from the configured OCSP URI. For more information on manual OCSP configuration, see Configure Certificate Revocation via OCSP.

Note In case of leaf certificates, TLS clients like syslog, FileBeat, SIP, ILS, LBM, and so on send OCSP requests to the OCSP responder and receives the certificate revocation response in real-time from the OCSP responder.

One of the following status is returned for the certificate once the validations are performed and the Common Criteria mode is ON.

- **Good** --The **good** state indicates a positive response to the status inquiry. At a minimum, this positive response indicates that the certificate is not revoked, but does not necessarily mean that the certificate was ever issued or that the time at which the response was produced is within the certificate's validity interval. Response extensions may be used to convey additional information on assertions made by the responder regarding the status of the certificate such as positive statement about issuance, validity, etc.
- **Revoked** --The **revoked** state indicates that the certificate has been revoked (either permanantly or temporarily (on hold)).
- **Unknown** -- The **unknown** state indicates that the OCSP responder doesn't know about the certificate being requested.

Note In Common Criteria mode, the connection fails in both **Revoked** as well as **Unknown** case whereas the connection would succeed in **Unknown** response case when Common Criteria is not enabled.

Certificate Monitoring Task Flow

Complete these tasks to configure the system to monitor certificate status and expiration automatically.

- Email you when certificates are approaching expiration.
- Revoke expired certificates.

Procedure

	Command or Action	Purpose
Step 1	Configure Certificate Monitor Notifications, on page 147	Configure automatic certificate monitoring. The system periodically checks certificate statuses

	Command or Action	Purpose
		and emails you when a certificate is approaching expiration.
Step 2	Configure Certificate Revocation via OCSP, on page 148	Configure the OCSP so that the system revokes expired certificates automatically.

Configure Certificate Monitor Notifications

Configure automated certificate monitoring for Unified Communications Manager or the IM and Presence Service. The system periodically checks the status of certificates and emails you when a certificate is approaching expiration.

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

Procedure

Step 1 Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate monitoring) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate monitoring).

Step 2 Choose **Security** > **Certificate Monitor**.

Step 3 In the **Notification Start Time** field, enter a numeric value. This value represents the number of days before certificate expiration where the system starts to notify you of the upcoming expiration.

Step 4 In the **Notification Frequency** fields, enter the frequency of notifications.

Step 5 Optional. Check the **Enable E-mail notification** check box to have the system send email alerts of upcoming certificate expirations..

Step 6 Check the **Enable LSC Monitoring** check box to include LSC certificates in the certificate status checks.

Step 7 In the **E-mail IDs** field, enter the email addresses where you want the system to send notifications. You can enter multiple email addresses separated by a semicolon.

Step 8 Click **Save**.

Note The certificate monitor service runs once every 24 hours by default. 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 does not change even when the certificate is close to the expiry date of seven days. It runs every 1 hour when the certificate either has expired or is going to expire in one day.

What to do next

Configure the Online Certificate Status Protocol (OCSP) so that the system revokes expired certificates automatically. For details, seeConfigure Certificate Revocation via OCSP, on page 148

Configure Certificate Revocation via OCSP

Enable the Online Certificate Status Protocol (OCSP) to check certificate status regularly and to revoke expired certificates automatically.

Before you begin

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

Procedure

Step 1 Log in to Cisco Unified OS Administration (for Unified Communications Manager certificate revocation) or Cisco Unified IM and Presence Administration (for IM and Presence Service certificate revocation).

Step 2 Choose **Security** > **Certificate Revocation**.

Step 3 Check the **Enable OCSP** check box, and perform one of the following tasks:

- If you want to specify an OCSP responder for OCSP checks, select the **Use configured OCSP URI** button and enter the URI of the responder in the **OCSP Configured URI** field.
- If the certificate is configured with an OCSP responder URI, select the **Use OCSP URI from Certificate** button.

Step 4 Check the **Enable Revocation Check** check box.

Step 5 Complete the **Check Every** field with the interval period for revocation checks.

Step 6 Click **Save**.

Step 7 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-lived connections:

a) From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.
b) Under **Certificate Revocation and Expiry**, set the **Certificate Validity Check** parameter to **True**.
c) Configure a value for the **Validity Check Frequency** parameter.

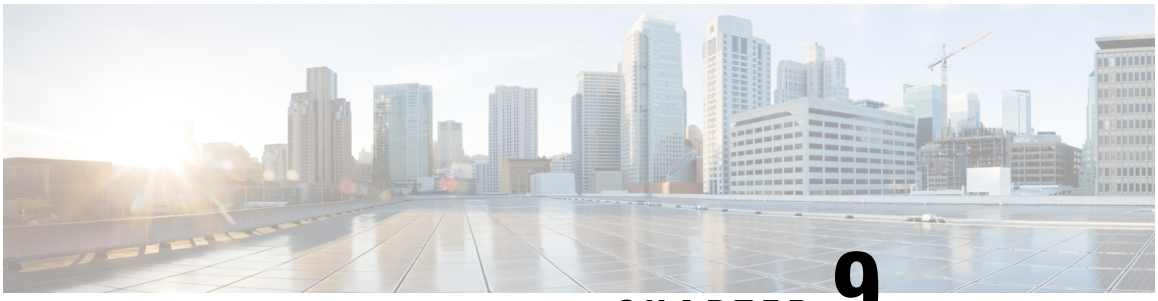
Note The interval value of the **Enable Revocation Check** parameter in the **Certificate Revocation** window takes precedence over the value of the **Validity Check Frequency** enterprise parameter.

d) Click **Save**.

PART III

Security for Cisco IP Phone and Cisco Voice-Messaging Ports

- Phone Security, on page 151
- Phone Security Profile Setup, on page 157
- Secure and Nonsecure Indication Tone Setup, on page 173
- Encryption to Analog Endpoint Setup, on page 177
- Encrypted Phone Configuration File Setup, on page 179
- Digest Authentication for SIP Phones Setup, on page 191
- Phone Hardening, on page 195
- Secure Conference Resources Setup, on page 199
- Voice-Messaging Ports Security Setup, on page 211
- Call Secure Status Policy, on page 215
- Secure Call Monitoring and Recording Setup, on page 217



CHAPTER 9

Phone Security

This chapter provides information about phone security.

- Phone Security Overview, on page 151
- Trusted Devices, on page 152
- Phone Model Support, on page 153
- Preferred Vendor SIP Phone Security Set Up, on page 153
- View Phone Security Settings, on page 155
- Set Up Phone Security, on page 155
- Phone Security Interactions and Restrictions, on page 156
- Where to Find More Information About Phone Security, on page 156

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 create a new CTL file 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.

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.

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.

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, configure the Cisco CTL Client 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 to the *Cisco IP Phone Administration Guide* that supports your phone model.

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.

Step 7 Encrypt the phone configuration file, if the phone supports this functionality.

Step 8 To harden the phone, disable phone settings.

Phone Security Interactions and Restrictions

This section provides the interaction and restriction on Phone Security.

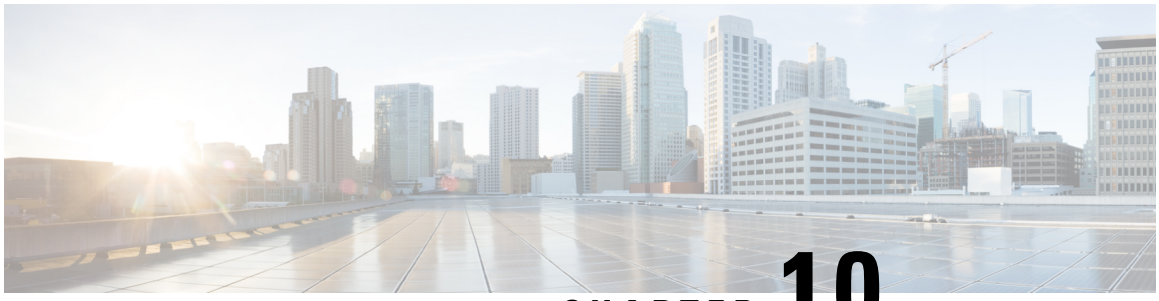
Table 29: Phone Security Interactions and Restrictions

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.

Where to Find More Information About Phone Security

Related Cisco Documentation

- *Administration Guide for Cisco Unified Communications Manager*
- *Troubleshooting Guide for Cisco Unified Communications Manager*



CHAPTER 10

Phone Security Profile Setup

This chapter provides information about security profile setup.

- Phone Security Profile Overview, on page 157
- Phone Security Profile Setup Prerequisites, on page 157
- Find Phone Security Profile, on page 158
- Set Up Phone Security Profile, on page 159
- Phone Security Profile Settings, on page 159
- Apply Security Profiles to Phone , on page 169
- Synchronize Phone Security Profile with Phones, on page 170
- Delete Phone Security Profile, on page 170
- Find Phones with Phone Security Profiles, on page 171

Phone Security Profile Overview

Unified Communications Manager Administration groups security-related settings for a phone type and protocol into security profiles to allow you to assign a single security profile to multiple phones. Security-related settings include device security mode, digest authentication, and some CAPF settings. You apply the configured settings to a phone when you choose the security profile in the Phone Configuration window.

Installing Unified Communications Manager provides a set of predefined, nonsecure security profiles for auto-registration. 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.

Only the security features that the selected device and protocol support display in the security profile settings window.

Phone Security Profile Setup 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.

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 159.

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**.

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 30: 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 31: 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 SIPphones. 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.

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.

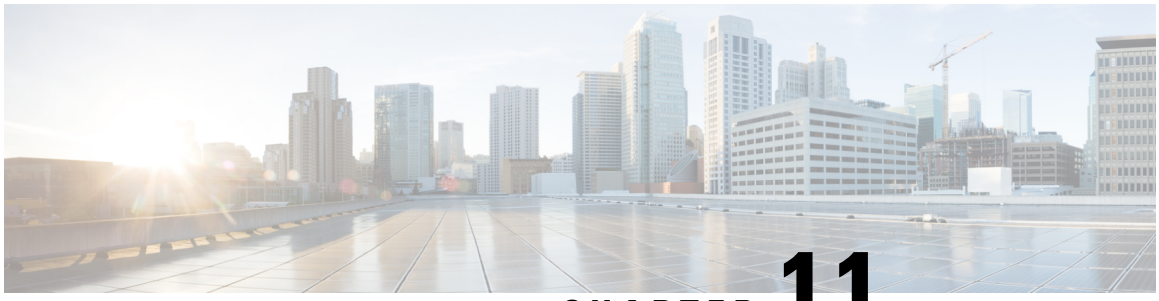
Step 3 Click **Find**.

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.



CHAPTER 11

Secure and Nonsecure Indication Tone Setup

This chapter provides information about secure and nonsecure indication tone setup. The system plays secure and nonsecure indication tones on a protected phone to indicate whether a call is encrypted.

- Secure and Non-Secure Indication Tone Overview, on page 173
- Secure and Non-Secure Indication Tone Tips, on page 174
- Secure and Non-Secure Indication Tone Configuration Tasks , on page 175

Secure and Non-Secure Indication Tone Overview

The Secure Tone feature can configure a phone to play a secure indication tone when a call is encrypted. The tone indicates that the call is protected and that confidential information may be exchanged. The 2-second tone comprises three long beeps. If the call is protected, the tone begins to play on a protected phone as soon as the called party answers.

When the call is not protected, the system plays a non-secure indication tone, which comprises six short beeps, on a protected phone. For video calls, you might first hear secure indication tone for the audio portion of the call and then non-secure indication tone for overall non-secure media.

The secure and non-secure indication tones are supported on the following types of calls:

- Intracluster to IP-to-IP calls
- Intercluster protected calls
- IP-to-Time-Division-Multiplexing (TDM) calls through a protected MGCP E1 PRI gateway

Note Only callers on protected phones can hear secure and non-secure indication tones. Callers on phones that are not protected never hear these tones. For video calls, the system plays secure and non-secure indication tones on protected devices.

Protected Devices

Configuration designates a protected device in Unified Communications Manager. 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 nonsecure indication tones when the system determines the protected status of a call.

You can make the following types of calls that can use the secure and nonsecure 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

Supported Devices

You can use Cisco Unified Reporting to determine which Cisco IP Phone models support secure and nonsecure indication tones. From Cisco Unified Reporting, click **Unified CM Phone Feature List**. For the Feature pull-down menu, choose **Secure Tone**. The system displays a list of products that support the feature.

For more information about using Cisco Unified Reporting, see the *Cisco Unified Reporting Administration Guide*.

Secure and Non-Secure Indication Tone Tips

This section provides information that pertains to the impact of using the secure indication tone feature:

- Following are the facts about protected devices:
  - You can configure phones that are running SCCP or SIP as protected devices.
  - Protected devices that call non-protected devices that are encrypted play the secure tone, while protected devices that call non-protected and non-encrypted devices play a non-secure tone.
  - When a protected phone calls another protected phone, and the media is not encrypted, the call does not drop. The system plays non-secure indication tone to the phones on the call.
- For video calls, the system plays secure and non-secure indication tones on protected devices.

Note For video calls, the user may first hear secure indication tone for the audio portion of the call and then non-secure indication tone for overall non-secure media.

- A lock icon that displays on a Cisco IP Phone indicates that the media is encrypted, but does not necessarily mean that the phone has been configured as a protected device. However, the lock icon must be present for a protected call to occur.
- The following services and features are impacted:
  - Multiline supplementary services (such as call transfer, conference, and call waiting) are supported on protected phones. When the user invokes a supplementary service on a protected phone, the system plays secure or non-secure indication tone to reflect the updated status of the call.
  - Cisco Extension Mobility and Join Across Line services are disabled on protected phones.
  - Shared-line configuration is not available on protected phones.

- Hold/Resume and Call Forward All are supported for protected calls.

- 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 Managerkey 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, refer to *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* for the version of Cisco IOS software that you are using.

Secure and Non-Secure Indication Tone Configuration Tasks

Make sure that you configure the following items for the secure tone to play:

- In the **Phone Configuration** window, which you can navigate to by choosing **Device** > **Phone** in Unified Communications Manager Administration, configure the following items:
  - From the **Softkey Template** drop-down list in the **Device Information** portion of the window, choose **Standard Protected Phone**.

Note You must use a new softkey template without supplementary service softkeys for a protected phone.

  - For the **Join Across Lines** option (also in the **Device Information** portion of the window), choose **Off**.
  - Check the **Protected Device** check box (also in the **Device Information** portion of the window).
  - From the **Device Security Profile** drop-down list (in the **Protocol Specific Information** portion of the window), choose a secure phone profile that is already configured in the **Phone Security Profile Configuration** window (**System** > **Security Profile** > **Phone Security Profile**).

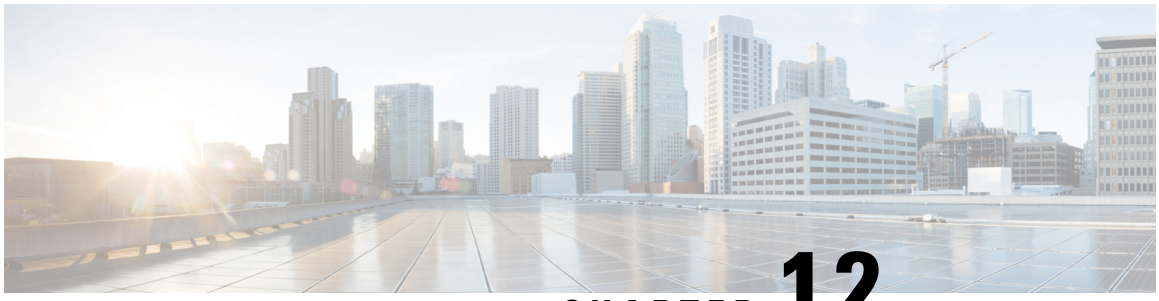
- Go to the **Directory Number Configuration** window that displays when you add a directory number from the **Phone Configuration** window. In the **Multiple Call/Call Waiting Settings on Device**

DeviceName area of the **Directory Number Configuration** window, set the following options to a value of 1:

- Maximum Number of Calls
- Busy Trigger

- In Unified Communications Manager Administration, choose **System** > **Service Parameters**. In the first **Service Parameter Configuration** window, choose your server and choose the Cisco CallManager service. In the second **Service Parameter Configuration** window, locate the **Clusterwide Parameters (Feature - Secure Tone)** area, and set the **Play Secure Indication Tone** option to **True**. (The default value specifies False.)
- If you are configuring a protected MGCP E1 PRI gateway, choose **Device** > **Gateway** > **Add New** in Unified Communications Manager Administration and choose a supported gateway. Choose **MCGP** as the protocol. When the **Gateway Configuration** window displays, specify the following configuration choices:
  - Set **Global ISDN Switch Type** to **Euro**.
  - After you complete the rest of the MGCP Gateway configuration, click **Save**; then, click the endpoint icon that appears to the right of subunit 0 in the window. The **Enable Protected Facility IE** check box displays. Check this check box.

    This configuration allows the system to pass protected status of the call between Cisco Unified IP Phone endpoints and the protected PBX phones that connect to the MGCP gateway.



CHAPTER 12

Encryption to Analog Endpoint Setup

This chapter provides information about encryption to analog endpoint setup. This feature enables you to create a secure SCCP connection for analog phones to a Cisco VG2xx Gateway. The gateway uses Transport Layer Security (TLS) with Unified Communications Manager for SCCP signaling communication and uses SRTP for voice communication. The existing Unified Communications Manager TLS functionality, including certificate management, is used for secure SCCP communication.

- Analog Phone Security Profile, on page 177
- Certificate Management for Secure Analog Phones, on page 177

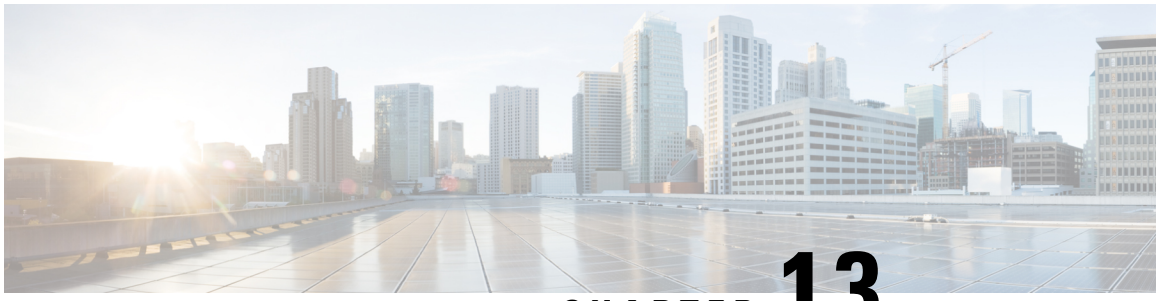
Analog Phone Security Profile

To establish an encrypted connection to analog phones, you must create a Phone Security Profile for analog phones with the Device Security Mode parameter set to **Authenticated** or **Encrypted**. To create a Phone Security Profile, navigate to **System** > **Security Profile** > **Phone Security Profile** in Unified Communications Manager Administration.

When you configure an analog phone attached to a Cisco VG2xx gateway, choose the secure analog profile you created for the Device Security Profile parameter. To configure the Device Security Profile parameter, navigate to **Device** > **Phone** in Unified Communications Manager Administration and scroll down to the Protocol Specific Information section for the phone you want to configure.

Certificate Management for Secure Analog Phones

For secure analog phones to function, you must import the same CA-signed certificate into Cisco Unified Communications Manager that is being used by the Cisco VG2xx Gateway. For more information about importing certificates, see Chapter 6, “Security,” in the *Administration Guide for Cisco Unified Communications Manager* .



CHAPTER 13

Encrypted Phone Configuration File Setup

This chapter provides information about encrypted phone configuration files setup. After you configure security-related settings, the phone configuration file contains sensitive information, such as digest passwords and phone administrator passwords. To ensure privacy of the configuration file, you must configure the configuration files for encryption.

- TFTP Encrypted Configuration Files Overview, on page 179
- Phone Models That Support Encryption, on page 181
- TFTP Encrypted Configuration Files Tips, on page 182
- Encryption for Phone Configuration File Task Flow, on page 183
- Disable TFTP Encrypted Configuration Files, on page 188
- Exclude Digest Credentials From Phone Configuration File Download, on page 189

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 configured mixed mode and enabled the **TFTP Encrypted Config** option in Cisco Unified CM Administration.

Manual Key Distribution

With manual key distribution, a 128- or 256-bit symmetric key, which is stored in the Unified Communications Manager database, encrypts the phone configuration file after the phone resets. To determine the key size for your phone model.

To encrypt the configuration file, the administrator can either manually enter the key into or prompt Unified Communications Manager to generate the key in the **Phone Configuration** window. After the key exists in the database, the administrator or user must enter the key into the phone by accessing the user interface on the phone; the phone stores the key in flash as soon as you press the **Accept** softkey. After the key is entered, the phone requests an encrypted configuration file after it is reset. After the required tasks occur, the symmetric key uses RC4 or AES 128 encryption algorithms to encrypt the configuration file. To determine which phones use the RC4 or AES 128 encryption algorithms, see Phone Models That Support Encryption, on page 181.

When the phone contains the symmetric key, the phone always requests the encrypted configuration file.Unified Communications Manager downloads the encrypted configuration file to the phone, which the TFTP server signs. Not all phone types validate the signer of the configuration file.

The phone decrypts the file contents by using the symmetric key that is stored in flash. If decryption fails, the configuration file does not get applied to the phone.

Tip If the TFTP Encrypted Config setting gets disabled, administrators must remove the symmetric key from the phone GUI, so the phone requests an unencrypted configuration file the next time that it is reset.

Symmetric Key Encryption with Phone Public Key

If the phone contains a manufacturing-installed certificate (MIC) or a locally significant certificate (LSC), the phone contains a public and private key pair, which are used for PKI encryption.

If you are using this method for the first time, the phone compares the MD5 hash of the phone certificate in the configuration file to the MD5 hash of the LSC or MIC. If the phone does not identify a problem, the phone requests an encrypted configuration file from the TFTP server after the phone resets. If the phone identifies

a problem, for example, the hash does not match, the phone does not contain a certificate, or the MD5 value is blank, the phone attempts to initiate a session with CAPF unless the CAPF authentication mode equals By Authentication String (in which case, you must manually enter the string). The Certificate Authority Proxy Function (CAPF) authenticates Cisco IP Phones to Unified Communications Manager and issues phone certificates (LSCs). CAPF extracts the phone public key from the LSC or MIC, generates a MD5 hash, and stores the values for the public key and certificate hash in the Unified Communications Manager database. After the public key gets stored in the database, the phone resets and requests a new configuration file.

After the public key exists in the database and the phone resets, the symmetric key encryption process begins after the database notifies TFTP that the public key exists for the phone. The TFTP server generates a 128-bit symmetric key, which encrypts the configuration file with the Advanced Encryption Standard (AES)128 encryption algorithm. Then, the phone public key encrypts the symmetric key, which it includes in the signed envelope header of the configuration file. The phone validates the file signing, and, if the signature is valid, the phone uses the private key from the LSC or MIC to decrypt the encrypted symmetric key. The symmetric key then decrypts the file contents.

Every time that you update the configuration file, the TFTP server automatically generates a new key to encrypt the file.

Tip For phones that support this encryption method, the phone uses the encryption configuration flag in the configuration file to determine whether to request an encrypted or unencrypted file. If the TFTP Encrypted Config setting is disabled, and Cisco IP Phones that support this encryption method request an encrypted file (.enc.sgn file), Unified Communications Manager sends a 'file not found error' to the phone. The phone then requests an unencrypted, signed file (.sgn file).

If the TFTP Encrypted Config setting is enabled but the phone requests an unencrypted configuration file for some reason, the TFTP server offers an unencrypted file that contains minimal configuration settings. After the phone receives the minimum configuration, the phone can detect error conditions, such as key mismatch, and may start a session with CAPF to synchronize the phone public key with the Unified Communications Manager database. If the error condition is resolved, the phone requests an encrypted configuration file the next time that it resets.

Phone Models That Support Encryption

You can encrypt the phone configuration file for the following Cisco Unified IP Phones:

Phone Model and Protocol	Encryption Method
Cisco Unified IP Phone 7800 or 6921	Manual key distribution—Encryption algorithm: RC4Key size: 256 bits File signing support: No
Cisco Unified IP Phone 7942 or 7962 (SIP only)	Manual key distribution—Encryption algorithm: Advanced Encryption Standard (AES)128Key size: 128 bits File signing support: These phones that are running SIP receive signed, encrypted configuration files but ignore the signing information.

Phone Model and Protocol	Encryption Method
Cisco Unified IP Phone 6901, 6911, 6921, 6941, 6945, and 6961 Cisco Unified IP Phone 7975G; Cisco Unified IP Phone 7961G, 7962G, or 7965G;Cisco Unified IP Phone 7941G, 7942G, or 7945G;Cisco Unified IP Phone 7911G; Cisco Unified IP Phone 7906G Cisco Unified IP Phone , 7961G-GE, 7941G-GE Cisco Unified IP Phone 7931G, (SCCP only) Cisco Unified Wireless IP Phone 7925G, 7925G-EX, 7926G Cisco Unified IP Phone 8941 and 8945 Cisco Unified IP Phone 8961, 9951, and 9971 Cisco IP Phone 7811, 7821, 7841, 7861 Cisco IP Conference Phone 7832 Cisco IP Phone 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR Cisco Unified Conference Phone 8831 Cisco Conference Phone 8832 Cisco Wireless IP Phone 8821	Symmetric key encryption with phone public key (PKI encryption)—Encryption algorithm: AES128Key size: 128 bits File signing support: Yes **Note** Cisco Unified IP Phones 6901 and 6911 do not request for the ITL file as they do not support security by default. Therefore, the Unified Communications Manager cluster should be set to secure (Mixed) mode for the Cisco Unified IP Phones 6901 and 6911 to get the Cisco CTL file containing Cisco Certificate Authority Proxy Function (CAPF) details for the encrypted configuration file to work on the Cisco Unified IP Phones (6901 and 6911).

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, make sure that the cluster security is in mixed mode, verify phones in your cluster that support manual key encryption and public key encryption, verify the phones that support SHA-1 and SHA-512 and complete the tasks below.

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 184	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 184	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 187	For phones that use public keys, verify the certificate installation.
Step 4	Update CTL File, on page 187	After you complete your TFTP config file updates, regenerate the CTL file.
Step 5	Restart Services, on page 188	Restart the Cisco CallManager and Cisco TFTP services.

	Command or Action	Purpose
Step 6	Reset Phones, on page 188	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.

Set Up Manual Key Distribution

For phones that use manual keys, you must set up manual key distribution.

Before you begin

The following procedure assumes that:

- Your phone exists in the Unified Communications Manager database.
- A compatible firmware load exists on the TFTP server.
- You have enabled the TFTP Encrypted Config parameter in Unified Communications Manager Administration.
- Your phone supports manual key distribution.

Procedure

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

Step 2 Click **Find**.

Step 3 After the **Phone Configuration** window displays, configure the manual key distribution settings.

Note After you have configured the settings, you should not change the key.

Step 4 Click **Save**.

Step 5 Enter the symmetric key on the phone and then reset the phone.

For information on how to perform these tasks, refer to the phone administration guide that supports your phone model.

Manual Key Distribution Settings

The following table describes the manual distribution configuration settings in the **Phone Configuration** window.

Table 32: Manual Key Distribution Configuration Settings

Setting	Description
Symmetric Key	Enter a string of hexadecimal characters that you want to use for the symmetric key. Valid characters include numerals, 0-9, and uppercase/lowercase characters, A-F (or a-f). Make sure that you enter the correct bits for the key size; otherwise, Cisco Unified Communications Manager rejects the value. Cisco Unified Communications Manager supports the following key sizes: • Cisco Unified IP Phones 7800 and (SIP only)—256 bits • Cisco Unified IP Phones 7942 and 7962 (SIP only)—128 bits After the key is configured, you should not change it.
Generate String	If you want Cisco Unified Communications Manager Administration to generate a hexadecimal string for you, click the **Generate String** button. After the key is configured, you should not change it.
Revert to Database Value	If you want to restore the value that exists in the database, click this button.

Enter Phone Symmetric Key

If you used the previous procedure to configure a manual key for your phone in Unified Communications Manager, use this procedure to enter the key on the phone.

Procedure

Step 1 Press the **Settings** button on the phone.

Step 2 If the configuration is locked, scroll down the **Settings** menu, highlight **Unlock Phone** and press the **Select** softkey. Enter the phone password and press the **Accept** softkey.

The phone accepts the password.

Step 3 Scroll down the **Settings** menu, highlight **Security Configuration**, and press the **Select** softkey.

Step 4 In the **Security Configuration** menu, highlight the **Set Cfg Encrypt Key** option and press the **Select** softkey.

Step 5 When prompted for the encryption key, enter the key (in hex). If you need to clear the key, enter 32 zero digits.

Step 6 After you have finished entering the key, press the **Accept** softkey.

The phone accepts the encryption key.

Step 7 Reset the phone.

After the phone resets, the phone requests encrypted configuration files.

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**..

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, 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, 7925G, 7925G-EX, 7926G, 7931G, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 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, 7975G, 8941, 8945, 8961, 9971, 7811, 78321, 7841, 7861, 7832, 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NE, 8821, 8831, 8832, 8832NR.

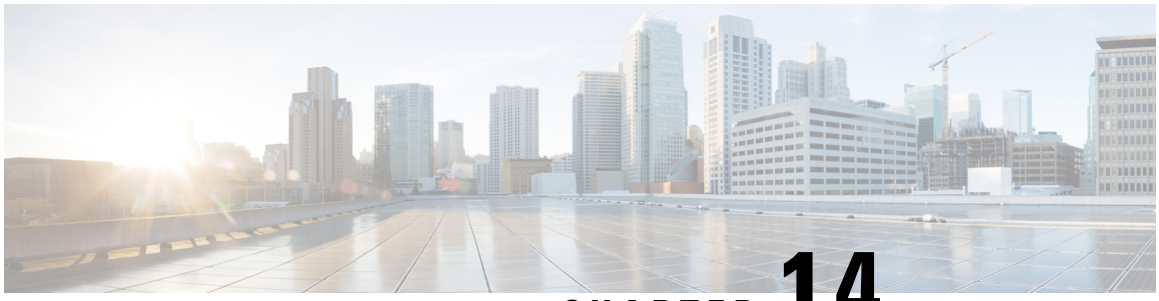
Procedure

	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.

Exclude Digest Credentials From Phone Configuration File Download

To exclude digest credentials from the configuration file that is sent to phones after the initial configuration, check the Exclude Digest Credentials in Configuration File check box for the security profile that is applied to the phone. Only Cisco Unified IP Phones 7800, 7942, and 7962 (SIP only) support this option.

You may need to uncheck this check box to update the configuration file for changes to digest credentials.



CHAPTER 14

Digest Authentication for SIP Phones Setup

This chapter provides information about digest authentication for SIP phones setup. For additional information on how digest authentication works for phones that are running SIP, see Digest Authentication, on page 21.

When you enable digest authentication for a phone, Unified Communications Manager challenges all requests except keepalive messages for phones that are running SIP. Unified Communications Manager uses the digest credentials for 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.

For information about configuring digest authentication for non-Cisco phones that are running SIP, refer to Appendix C in the *Administration Guide for Cisco Unified Communications Manager*.

- Enable Digest Authentication in Phone Security Profile, on page 191
- Configure SIP Station Realm, on page 192
- Assign Digest Credentials to Phone User, on page 192
- End User Digest Credential Settings, on page 192
- Assign Digest Authentication to the Phone, on page 193

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**.

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**.

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**.

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 33: 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.

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.

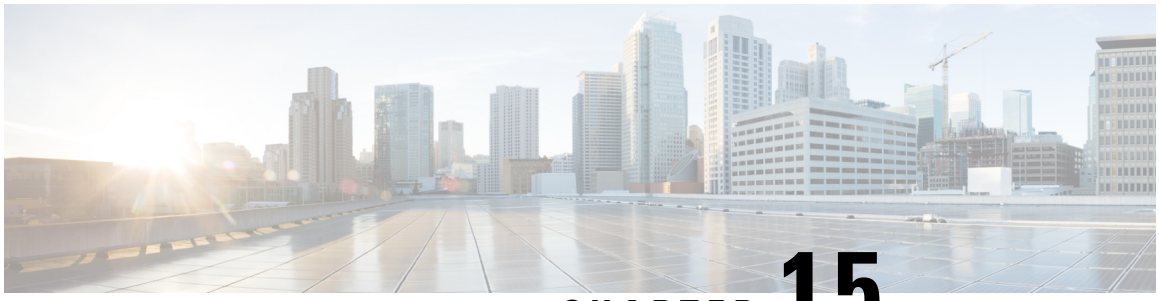
Step 3 From the **Digest User** drop-down list, assign the end user for whom you assigned digest credentials.

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.



CHAPTER 15

Phone Hardening

This chapter provides information about phone hardening. To tighten security on the phone, you can perform phone hardening tasks in the **Phone Configuration** window in Unified Communications Manager Administration.

- Gratuitous ARP Disable, on page 195
- Web Access Disable, on page 195
- PC Voice VLAN Access Disable, on page 196
- Setting Access Disable, on page 196
- PC Port Disable, on page 196
- Set Up Phone Hardening, on page 196
- Where to Find More Information About Phone Hardening, on page 197

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.

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.

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.

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

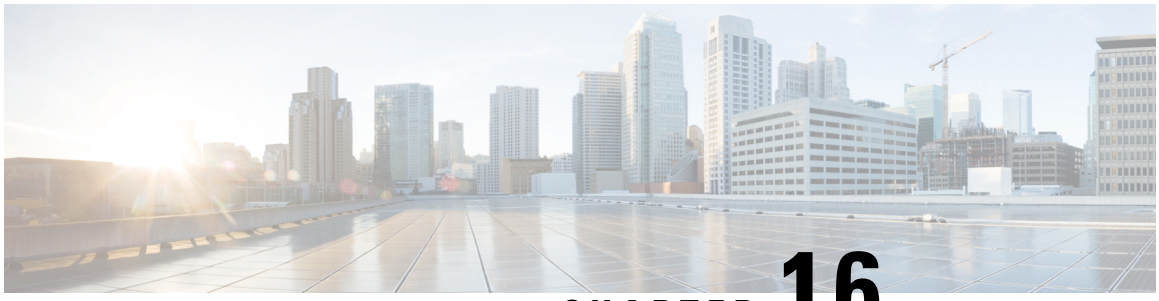
Tip To review information on these settings, click the help icon that appears next to the parameters in the **Phone Configuration** window.

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**.

Where to Find More Information About Phone Hardening



CHAPTER 16

Secure Conference Resources Setup

This chapter provides information about secure conference resources setup.

- Secure Conference, on page 199
- Conference Bridge Requirements, on page 200
- Secure Conference Icons, on page 201
- Secure Conference Status, on page 201
- Cisco Unified IP Phone Secure Conference and Icon Support, on page 204
- Secure Conference CTI Support, on page 204
- Secure Conference Over Trunks and Gateways, on page 204
- CDR Data, on page 205
- Interactions and Restrictions, on page 205
- Securing Conference Resources Tips, on page 206
- Set Up Secure Conference Bridge, on page 207
- Set Up Secure Conference Bridge in Cisco Unified Communications Manager Administration, on page 208
- Set Up Minimum Security Level for Meet-Me Conferences, on page 209
- Set Up Packet Capturing for Secure Conference Bridge, on page 210
- Where to Find More Information About Secure Conferences Resources, on page 210

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, , 7931G, 7942, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 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, 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 205
- Cisco Unified Communications Manager Restrictions with Secure Conference, on page 206

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.
- 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 CiscoCallManager 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 207.

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 208.

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 207.

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 209.

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.

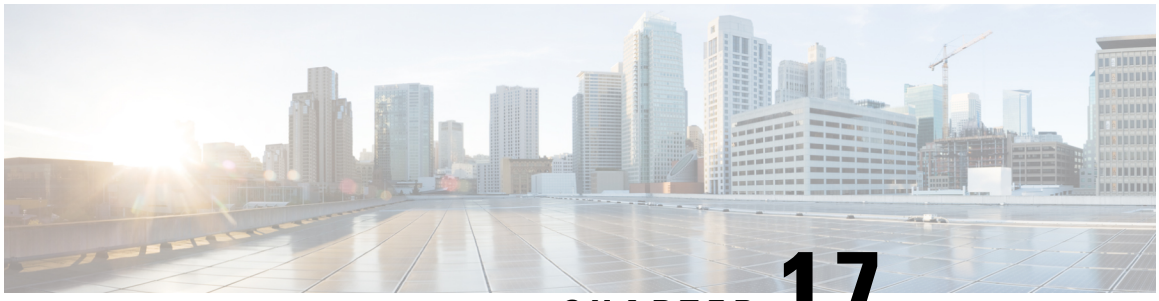
Set Up Packet Capturing for Secure Conference Bridge

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.

Where to Find More Information About Secure Conferences Resources

- System Requirements, on page 6
- Interactions and Restrictions, on page 8
- Certificates, on page 16
- Set Up Authentication and Encryption, on page 32



CHAPTER 17

Voice-Messaging Ports Security Setup

This chapter provides information about voice-messaging ports security setup.

- Voice-Messaging Security, on page 211
- Voice-Messaging Security Setup Tips, on page 211
- Set Up Secure Voice-Messaging Port, on page 212
- Apply Security Profile to Single Voice-Messaging Port, on page 213
- Apply Security Profile Using Voice Mail Port Wizard, on page 214
- Where to Find More Information About Voice-messaging Security, on page 214

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 you installed and configured the CiscoCTL Client for Mixed Mode.

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*.

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**.

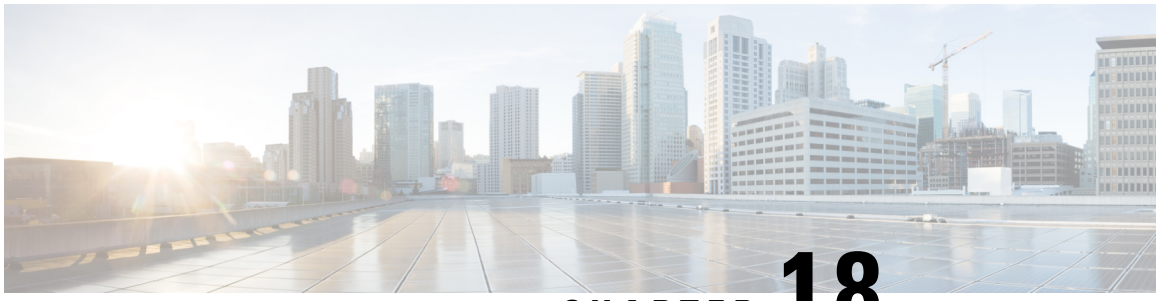
Step 4 In the **Cisco Voice Mail Device Information** window, choose a **Device Security Mode** from the drop-down list box. The database predefines these options. The default value specifies **Not Selected**.

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**.

Where to Find More Information About Voice-messaging Security

- System Requirements, on page 6
- Set Up Authentication and Encryption, on page 32
- Certificates, on page 16



CHAPTER 18

Call Secure Status Policy

- About Call Secure Status Policy, on page 215
- Setup Call Secure Status Policy, on page 216

About Call Secure Status 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.

Setup Call Secure Status Policy

Procedure

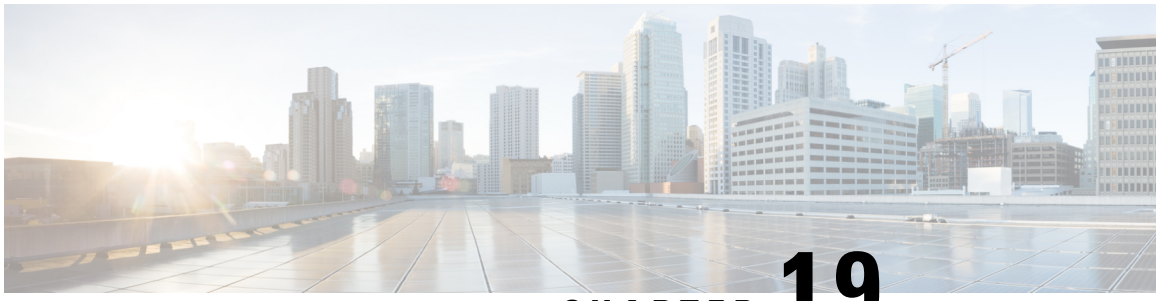
Step 1 Find the Call Secure Status Policy service parameter, as described in the "Configure Service Parameters" section of the *System Configuration Guide for Cisco Unified Communications Manager* .

Step 2 From the **Secure Call Icon Display Policy** drop-down list, choose a policy option.

A warning message with the impact on video calls and secure tone is displayed.

Step 3 Click **Save**.

The window refreshes, and Unified Communications Manager updates the service parameter with your changes.



CHAPTER 19

Secure Call Monitoring and Recording Setup

This chapter provides information about secure call monitoring and recording setup.

- About Secure Call Monitoring and Recording Setup, on page 217
- Set Up Secure Call Monitoring and Recording, on page 218

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.
- Ensure that the **Cluster SIPOAuth Mode** field a Cisco CallManager enterprise parameter, is set to **Enabled**.

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.

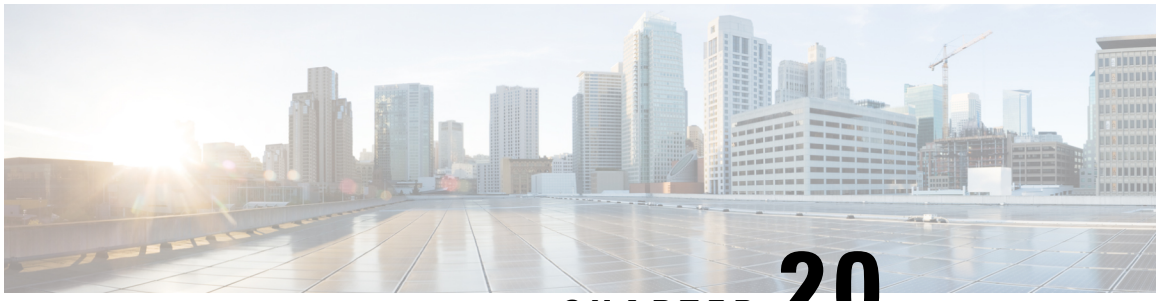
a) Configure a built-in bridge for the agent phone.
b) Configure the Recording Option (**Automatic Call Recording Enabled and Application Invoked Call Recording Enabled**.) using the **Directory Number** page on the agent phone.
c) Create a **route pattern** for the recorder.
d) Add a **call recording 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.

PART IV

Virtual Private Networks for Cisco Unified IP Phones

- VPN Client, on page 221



CHAPTER 20

VPN Client

- VPN Client Overview, on page 221
- VPN Client Configuration Task Flow, on page 221

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 222	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 223	Configure Cisco IOS for VPN client on an IP Phone. Perform this action if you want to configure Cisco IOS VPN.
Step 3	Complete ASA Prerequisites for AnyConnect, on page 224	Complete ASA prerequisites for AnyConnect. Perform this action if you want to configure ASA VPN.

	Command or Action	Purpose
Step 4	Configure ASA for VPN Client on IP Phone, on page 225	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 227	Upload the VPN concentrator certificates.
Step 7	Configure VPN Gateway, on page 228	Configure the VPN gateways.
Step 8	Configure VPN Group, on page 229	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 230 • Configure VPN Feature Parameters, on page 231	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 233	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 227.

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 228.

Step 4 Click **Save**.

VPN Gateway Fields for VPN Client

The table describes the VPN Gateway fields for VPN Client.

Table 34: 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.

Field	Description
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 228 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 35: 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.

Field	Definition
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 230 for the field description details.

Step 4 Click **Save**.

VPN Profile Fields for VPN Client

The table describes the VPN profile field details.

Table 36: 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.

Field	Definition
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 231.

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 37: 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
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**.

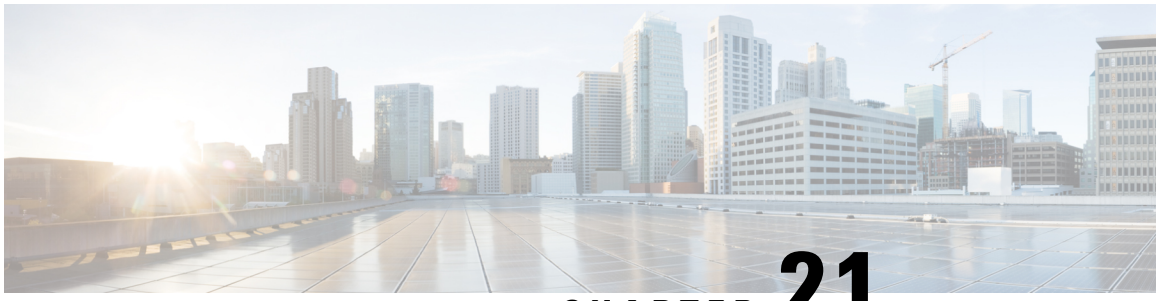
Step 4 Click **Save** and then **Apply Config**.

Step 5 Click **OK** in apply configuration window.

PART V

Cisco CTI, JTAPI, and TAPI Application Security

- Authentication and Encryption Setup for CTI, JTAPI, and TAPI, on page 237



CHAPTER 21

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 237
- Encryption for CTI, JTAPI, and TAPI Applications, on page 238
- CAPF Functions for CTI, JTAPI, and TAPI Applications, on page 239
- Securing CTI, JTAPI, and TAPI, on page 245
- Add Application and End Users to Security-Related Access Control Groups, on page 246
- Set Up JTAPI/TAPI Security-Related Service Parameters, on page 247
- View Certificate Operation Status for Application or End User, on page 247

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.

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, Port2749.

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 CAPF 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.

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.

If you did not activate this service before you installed and configured the Cisco CTL Client, you must update the CTL file.

After you activate the Cisco Certificate Authority Proxy Function service, CAPF automatically generates a key pair and certificate that is specific for CAPF. The CAPF certificate, which the Cisco CTL Client copies to your standalone server or all server(s) in the cluster, uses the .0 extension. The CAPF certificate is then displayed at 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 CAPF 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 CAPF 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 CTL Client is installed and run the CTL file to create it.
- Verify if the CTL provider service is installed and that the service is activated.
- 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 CiscoCTL Client 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.

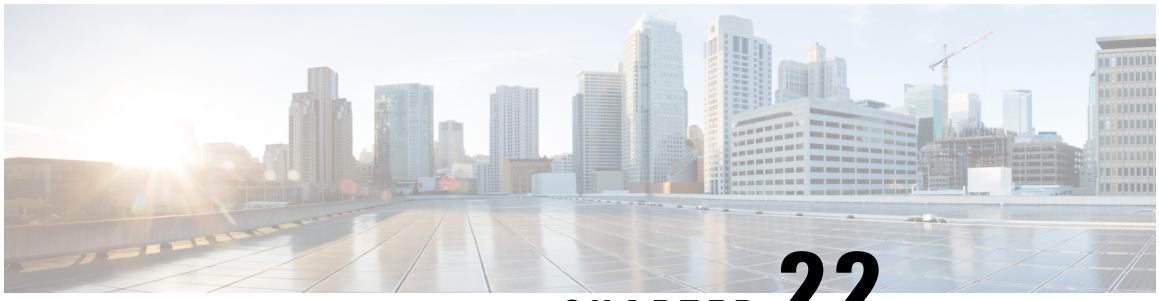
View Certificate Operation Status for Application or End User

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.

PART VI

Security for SRST References, Trunks, and Gateways

- Secure Survivable Remote Site Telephony (SRST) Reference, on page 251
- Encryption Setup for Gateways and Trunks, on page 257
- SIP Trunk Security Profile Setup, on page 263
- Digest Authentication Setup for SIP Trunks, on page 273
- Cisco Unified Mobility Advantage Server Security Profile Setup, on page 279
- FIPS 140-2 Mode Setup, on page 285
- Cisco V.150 Minimum Essential Requirements (MER), on page 287



CHAPTER 22

Secure Survivable Remote Site Telephony (SRST) Reference

This chapter provides information about SRST references.

- Securing SRST, on page 251
- Securing SRST Tips, on page 252
- Set Up Secure SRST, on page 253
- Set Up Secure SRST References, on page 253
- SRST Reference Security Settings, on page 254
- Delete Security From SRST Reference, on page 256
- SRST Certificate Deletion From Gateway, on page 256

Securing SRST

A SRST-enabled gateway provides limited call-processing tasks if the Unified Communications Manager cannot complete the call.

Secure SRST-enabled gateways contain a self-signed certificate. After you perform SRST configuration tasks in Unified Communications Manager Administration, Unified Communications Manager uses a TLS connection to authenticate with the Certificate Provider service in the SRST-enabled gateway. Unified Communications Manager then retrieves the certificate from the SRST-enabled gateway and adds the certificate to the Unified Communications Manager database.

After you reset the dependent devices in Unified Communications Manager Administration, the TFTP server adds the SRST-enabled gateway certificate to the phone cnf.xml file and sends the file to the phone. A secure phone then uses a TLS connection to interact with the SRST-enabled gateway.

Tip The phone configuration file only contains a certificate from a single issuer. Consequently, the system does not support HSRP.

Securing SRST Tips

Ensure that the following criteria are met to secure the connection between the secure phone and the SRST-enabled gateway:

- The SRST reference contains a self-signed certificate.
- You configured Mixed Mode through the Cisco CTL Client.
- You configured the phone for authentication or encryption.
- You configured the SRST reference in Unified Communications Manager Administration.
- You reset the SRST-enabled gateway and the dependent phones after the SRST configuration.

Note Unified Communications Manager provides the PEM format files that contain phone certificate information to the SRST-enabled gateway.

Note For LSC authentication, download the CAPF root certificate (CAPF.der). This root certificate allows the secure SRST to verify the phone LSC during the TLS handshake.

- When the cluster security mode equals nonsecure, the device security mode remains nonsecure in the phone configuration file, even though Unified Communications Manager Administration may indicate that the device security mode is authenticated or encrypted. Under these circumstances, the phone attempts nonsecure connections with the SRST-enabled gateway and Unified Communications Manager.

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

- When the cluster security mode equals nonsecure, the system ignores the security-related configuration; for example, the device security mode, the Is SRST Secure? check box, and so on. The configuration does not get deleted in from the database, but security is not provided.
- The phone attempts a secure connection to the SRST-enabled gateway only when the cluster security mode equals Mixed Mode, the device security mode in the phone configuration file is set to authenticated or encrypted, the Is SRST Secure? check box is checked in the **SRST Configuration** window, and a valid SRST-enabled gateway certificate exists in the phone configuration file.
- If you configured secure SRST references in a previous Unified Communications Manager release, the configuration automatically migrates during the upgrade.
- If phones in encrypted or authenticated mode fail over to SRST, and, during the connection with SRST, the cluster security mode switches from Mixed Mode to Nonsecure Mode, these phones will not fall back to Unified Communications Manager automatically. You must power down the SRST router to force these phones to reregister to Unified Communications Manager. After phones fall back to Unified Communications Manager, you can power up SRST, and failover and fallback will be automatic again.

Set Up Secure SRST

The following procedure provides the tasks to perform the SRST configuration process for security.

Procedure

Step 1 Verify that you performed all necessary tasks on the SRST-enabled gateway, so the device supports Unified Communications Manager and security.

For more information, see the *CiscoIOS SRST Version System Administrator Guide* that supports this version of Unified Communications Manager.

Step 2 Verify that you performed all necessary tasks to install and configure the CiscoCTL Client.

Step 3 Verify that a certificate exists in the phone.

For more information, refer to the Cisco Unified IP Phone documentation for your phone model.

Step 4 Verify that you configured the phones for authentication or encryption.

Step 5 Configure the SRST reference for security, which includes enabling the SRST reference in the Device Pool Configuration window.

Step 6 Reset the SRST-enabled gateway and phones.

Set Up Secure SRST References

Consider the following information before you add, update, or delete the SRST reference in Cisco Unified Communications Manager AdministrationUnified Communications Manager Administration:

- Adding a Secure SRST Reference—The first time that you configure the SRST reference for security, you must configure all settings that are described in Table 39: Configuration Settings for Secure SRST References, on page 255.
- Updating a Secure SRST Reference—Performing SRST updates in Unified Communications Manager Administration does not automatically update the SRST-enabled gateway certificate. To update the certificate, you must click the **Update Certificate** button; after you click the button, the contents of the certificate display, and you must accept or reject the certificate. If you accept the certificate, Unified Communications Manager replaces the SRST-enabled gateway certificate in the trust folder on the Unified Communications Manager server or on each Unified Communications Manager server in the cluster.
- Deleting a Secure SRST Reference—Deleting a secure SRST reference removes the SRST-enabled gateway certificate from the Unified Communications Manager database and the cnf.xml file in the phone.

  For information on how to delete SRST references, refer to the *Administration Guide for Cisco Unified Communications Manager* .

To configure a secure SRST reference, perform the following procedure:

Procedure

Step 1 In Unified Communications Manager Administration, choose **System** > **SRST**.

The **Find and List** window displays.

Step 2 Perform one of the following tasks:

a) To add a new SRST reference, click **Add New** in the **Find** window. (You can also display a profile and then click **Add New**.) The configuration window displays with the default settings for each field.

b) To copy an existing SRST reference, locate the appropriate SRST reference as described in the *Administration Guide for Cisco Unified Communications Manager*, 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 with the configured settings.

c) To update an existing SRST reference, locate the appropriate SRST reference as described in the *Administration Guide for Cisco Unified Communications Manager*.

The configuration window displays with the current settings.

Step 3 Enter the security-related settings as described in Table 39: Configuration Settings for Secure SRST References, on page 255.

For descriptions of additional SRST reference configuration settings, refer to the *Administration Guide for Cisco Unified Communications Manager*.

The **Find and List** window displays.

Step 4 After you check the Is SRST Secure? check box, a dialog box displays a message that you must download the SRST certificate by clicking the Update Certificate button. Click **OK**.

Step 5 Click **Save**.

Step 6 To update the SRST-enabled gateway certificate in the database, click the **Update Certificate** button.

Tip This button displays only after you check the Is SRST Secure? check box and click **Save**.

Step 7 The fingerprint for the certificate displays. To accept the certificate, click **Save**.

Step 8 Click **Close**.

Step 9 In the SRST Reference Configuration window, click **Reset**.

What to do next

Verify that you enabled the SRST reference in the **Device Pool Configuration** window.

SRST Reference Security Settings

The following table describes the available settings for secure SRST references in Unified Communications Manager Administration.

Table 39: Configuration Settings for Secure SRST References

Setting	Description
Is SRST Secure?	After you verify that the SRST-enabled gateway contains a self-signed certificate, check this check box. After you configure the SRST and reset the gateway and dependent phones, the CiscoCTL Provider service authenticates to the Certificate Provider service on the SRST-enabled gateway. The CiscoCTL Client retrieves the certificate from the SRST-enabled gateway and stores the certificate in the Unified Communications Manager database. **Tip** To remove the SRST certificate from the database and phone, uncheck this check box, click **Save**, and reset the dependent phones.
SRST Certificate Provider Port	This port monitors requests for the Certificate Provider service on the SRST-enabled gateway. Unified Communications Manager uses this port to retrieve the certificate from the SRST-enabled gateway. The CiscoSRST Certificate Provider default port equals 2445. After you configure this port on the SRST-enabled gateway, enter the port number in this field. **Tip** You may need to configure a different port number if the port is currently used or if you use a firewall and you cannot use the port within the firewall.The port number must exist in the range of 1024 and 49151; otherwise, the following message displays: Port Numbers can only contain digits.
Update Certificate	**Tip** This button displays only after you check the Is SRST Secure? check box and click Save. After you click this button, the CiscoCTL Client replaces the existing SRST-enabled gateway certificate that is stored in the Unified Communications Manager database, if a certificate exists in the database. After you reset the dependent phones, the TFTP server sends the cnf.xml file (with the new SRST-enabled gateway certificate) to the phones.

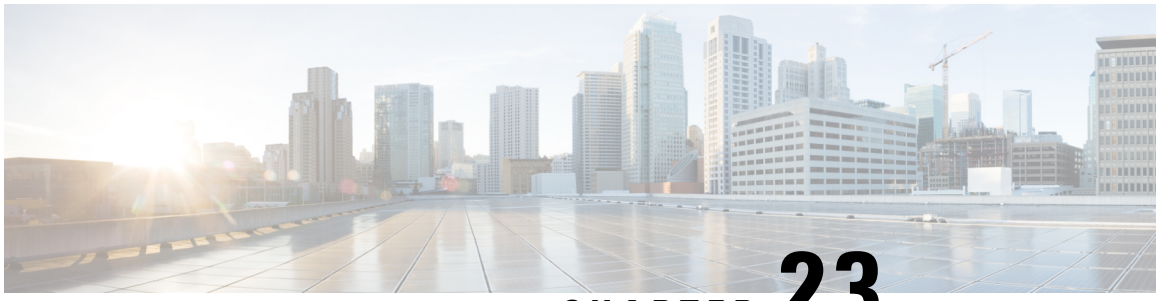
Delete Security From SRST Reference

To make the SRST reference nonsecure after you configure security, uncheck the Is SRTS Secure? check box in the SRST Configuration window. A message states that you must turn off the credential service on the gateway.

SRST Certificate Deletion From Gateway

If the SRST certificate no longer exists in the SRST-enabled gateway, you must remove the SRST certificate from the Unified Communications Manager database and the phone.

To perform this task, uncheck the **Is SRST Secure?** check box and click **Update** in the SRST Configuration window; then, click **Reset Devices**.



CHAPTER 23

Encryption Setup for Gateways and Trunks

This chapter provides information about encryption setup for gateways and trunks.

- Cisco IOS MGCP Gateway Encryption, on page 257
- H.323 Gateway and H.323/H.225/H.245 Trunk Encryption, on page 258
- SIP Trunk Encryption, on page 259
- Set Up Secure Gateways and Trunks, on page 260
- IPsec Setup Within Network Infrastructures, on page 261
- IPsec Setup Between Unified Communications Manager and Gateway or Trunks, on page 261
- Allow SRTP Using Unified Communications Manager Administration, on page 262
- Where to Find More Information About Gateway and Trunk Encryption, on page 262

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* .

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.

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*.

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:

- Cisco recommends that you 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.

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 in this chapter, refer to the *Administration Guide for Cisco Unified Communications Manager* .

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.

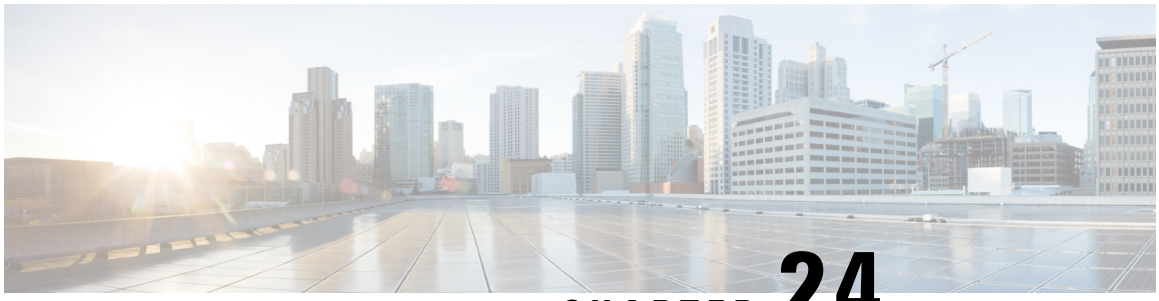
Step 3 Click **Save**.

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.)

Where to Find More Information About Gateway and Trunk Encryption

- Authentication, Integrity, and Authorization, on page 20
- Encryption, on page 24



CHAPTER 24

SIP Trunk Security Profile Setup

This chapter provides information about SIP trunk security profile setup.

- About SIP Trunk Security Profile Setup, on page 263
- SIP Trunk Security Profile Setup Tips, on page 263
- Find SIP Trunk Security Profile, on page 264
- Set Up SIP Trunk Security Profile, on page 264
- SIP Trunk Security Profile Settings, on page 265
- Apply SIP Trunk Security Profile, on page 270
- Synchronize SIP Trunk Security Profile with SIP Trunks, on page 271
- Delete SIP Trunk Security Profile, on page 271
- Where to Find More Information About SIP Trunk Security Profiles, on page 272

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.

Find SIP Trunk Security Profile

To find a SIP trunk security profile, perform the following procedure:

Procedure

Step 1 Choose **System** > **Security Profile** > **SIP Trunk Security Profile**.

The **Find and List** window displays. 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 264.

To filter or search records

a) From the drop-down list box, choose a search parameter.
b) Then from the drop-down list box, 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 the **Clear Filter** button 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 box.

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 item that you choose.

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, on page 264.

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 40: 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. **Tip** You must use UDP as the outgoing transport type when connecting SIP trunks between Unified Communications Manager systems and IOS gateways that do not support TCP connection reuse.

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 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.
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.

Setting	Description
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.
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.

Setting	Description
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**.

Delete SIP Trunk Security Profile

This section describes how to delete a SIP trunk security profile from the Unified Communications Manager database.

Before you begin

Before you can delete a security profile from 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 box in the **SIP Trunk 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* .

Procedure

Step 1 Find the SIP trunk security profile to delete.

Step 2 Perform one of the following tasks:

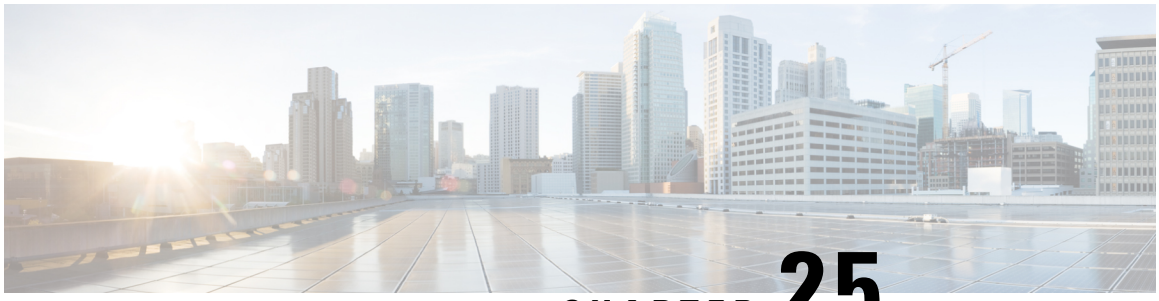
a) To delete multiple security profiles, perform one of these tasks in the **Find and List** window:
   - Check the check boxes next to the security profiles that you want to delete; then, click **Delete Selected**.
   - You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

b) To delete a single security profile, perform one of these tasks in the **Find and List** window:
   - Check the check box next to the security profile that you want to delete; then, click **Delete Selected**.
   - Click the **Name** link for the security profile. After the specific Security Profile Configuration window displays, click **Delete Selected**.

Step 3 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Where to Find More Information About SIP Trunk Security Profiles

- Authorization, on page 23
- Interactions, on page 9
- Digest Authentication, on page 21



CHAPTER 25

Digest Authentication Setup for SIP Trunks

This chapter provides information about digest authentication setup for SIP trunks. When you configure digest authentication for SIP trunks, Unified Communications Manager challenges the identity of the SIP user agent when it receives a SIP request on the SIP trunk. The SIP user agent, in turn, can challenge the identity of Unified Communications Manager when Unified Communications Managersends a SIP request to the trunk. For additional information on how digest authentication works for SIP trunks, see Digest Authentication, on page 21.

- Set Up SIP Trunk Digest Authentication, on page 273
- Set Up Digest Authentication Enterprise Parameters, on page 274
- Set Up Digest Credentials, on page 274
- Application User Digest Credential Settings, on page 274
- Find SIP Realm, on page 275
- Configure SIP Realm, on page 275
- SIP Realm Settings, on page 276
- Delete SIP Realm, on page 276

Set Up SIP Trunk Digest Authentication

The following procedure describes the tasks to configure digest authentication for SIP trunks.

Procedure

Step 1 Configure the SIP trunk security profiles; make sure that you check the **Enable Digest Authentication** check box.

Step 2 Apply a SIP trunk security profile to the trunk.

Step 3 Configure the enterprise parameter, Cluster ID, if not configured.

This parameter supports Unified Communications Manager challenges to the identity of the SIP user agent that is sending a SIP request on the SIP trunk.

Step 4 If Unified Communications Manager challenges the identity of SIP user agents that are sending SIP requests on the SIP trunk, configure the digest credentials for the application user in the **Application User Configuration** window.

Step 5 If Unified Communications Manager responds to challenges from a trunk peer, configure the SIP realm.

Set Up Digest Authentication Enterprise Parameters

To configure the enterprise parameter, Cluster ID, for digest authentication, choose **System** > **Enterprise Parameters** in Unified Communications Manager Administration. Locate the Cluster ID parameter and update the value, as described in the Help for the parameter. This parameter supports Unified Communications Manager challenges to the identity of the SIP user agent that is sending a SIP request on the SIP trunk.

Tip To access the Help for the parameter, click the question mark that displays in the **Enterprise Parameters Configuration** window or click the parameter link.

Set Up Digest Credentials

If Unified Communications Manager challenges the identity of a SIP user agent, you must configure the digest credentials for the application user in the Application User Configuration window in Unified Communications Manager Administration. Unified Communications Manager uses these credentials to verify the identity of SIP user agents that are sending requests through the SIP trunk.

To configure the digest credentials for an application user, perform the following procedure:

Procedure

Step 1 Find the application user, as described in the *Administration Guide for Cisco Unified Communications Manager* .

Step 2 Click the application user link.

Step 3 After the specific **Application User Configuration** window displays, enter the appropriate settings, as described in Table 42: SIP Realm Security Profile, on page 276.

Step 4 Click **Save**.

Application User Digest Credential Settings

The following table describes the settings for the digest credential settings in the **Application User Configuration** window in Unified Communications Manager Administration.

Table 41: Digest Authentication Credentials

Setting	Description
Digest Credentials	Enter a string of alphanumeric characters.

Setting	Description
Confirm Digest Credentials	To confirm that you entered the digest credentials correctly, enter the credentials in this field.

Find SIP Realm

To find a SIP Realm, perform the following procedure:

Procedure

Step 1 In Unified Communications Manager Administration, choose **User Management** > **SIP Realm**.

The **Find and List** window displays. 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 275.

To filter or search records

a) From the first drop-down list box, choose a search parameter.
b) From the second drop-down list box, 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 the **Clear Filter** button 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 box.

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 item that you choose.

What to do next

If you have not already done so, configure the Cluster ID enterprise parameter.

Configure SIP Realm

If Unified Communications Manager responds to challenges from one or more trunk peers, you must configure SIP Realm for each SIP trunk user agent that can challenge Unified Communications Manager.

To add or update a SIP Realm, perform the following procedure:

Procedure

Step 1 In Unified Communications Manager Administration, choose **User Management** > **SIP Realm**.
Step 2 Enter the appropriate settings as described in Table 42: SIP Realm Security Profile, on page 276.
Step 3 Click **Save**.
Step 4 Perform the procedure for all realms that you must add or update.

What to do next

To ensure that digest authentication is successful, verify that the same settings that you configured in Unified Communications Manager are configured on the SIP user agent.

SIP Realm Settings

The SIP Realm provides the trunk-side credentials when Unified Communications Manager gets challenged by a trunk peer.

The following table describes the settings for the SIP Realm.

Table 42: SIP Realm Security Profile

Setting	Description
Realm	Enter the domain name for the realm that connects to the SIP trunk; for example, SIPProxy1_xyz.com. You can use alphanumeric characters, period, dash, underscore, and space.
User	Enter the user name for the SIP user agent in this realm; for example, enter the Unified Communications Manager server name. The SIP trunk uses this user name to challenge this Unified Communications Manager.
Digest Credentials	Enter the password that Unified Communications Manager uses to respond to a challenge for this realm and user.
Confirm Digest Credentials	Re-enter the password for verification.

Delete SIP Realm

This section describes how to delete a SIP Realm from the Unified Communications Manager database.

Procedure

Step 1 Find the SIP Realm to delete.

Step 2 Perform one of the following tasks:

a) To delete multiple SIP Realms, perform one of these tasks in the **Find and List** window:

- Check the check boxes next to the realms that you want to delete; then, click **Delete Selected**.

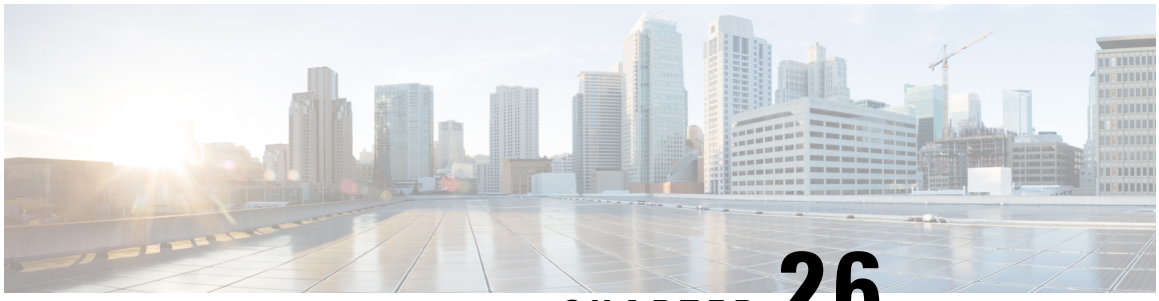
  You can delete all configurable records for this selection by clicking **Select All** and then clicking **Delete Selected**.

b) To delete a single SIP Realm, perform one of these tasks in the **Find and List** window:

- Check the check box next to the realm that you want to delete; then, click **Delete Selected**.

  Click the **Name** link for the realm. After the specific **SIP Realm Configuration** window displays, click **Delete Selected**.

Step 3 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.



CHAPTER 26

Cisco Unified Mobility Advantage Server Security Profile Setup

This chapter provides information about Cisco Unified Mobility Advantage server security profile setup.

- About Cisco Unified Mobility Advantage Server Security Profile Setup, on page 279
- Find Cisco Unified Mobility Advantage Server Security Profile, on page 280
- Set Up Cisco Unified Mobility Advantage Server Security Profile, on page 280
- Cisco Unified Mobility Advantage Server Security Profile Settings, on page 281
- Cisco Unified Mobility Advantage Server Security Profile Client Application, on page 282
- Delete Cisco Unified Mobility Advantage Server Security Profile, on page 282
- Where to Find More Information About Cisco Unified Mobility Advantage Server Security Profile, on page 283

About Cisco Unified Mobility Advantage Server Security Profile Setup

Unified Communications Manager Administration groups security-related settings to allow you to assign a single security profile to multiple Mobile Communicator clients. Security-related settings include device security mode, incoming transport type, and X.509 subject name. Configuring a Cisco Unified Mobility Advantage server security profile in Unified Communications Manager Administration automatically applies this profile to all configured Mobile Communicator clients on that Unified Communications Manager.

Only the security features that the Cisco Unified Mobility Advantage server supports display in the security profile settings window.

Note You cannot configure Cisco Unified Mobility Advantage servers in Unified Communications Manager Assistant Administration. For information on setting up a security profile for a Cisco Unified Mobility Advantage server, refer to your Cisco Unified Mobility Advantage documentation. Make sure that the Cisco Unified Mobility Advantage Security Profile you configure on Unified Communications Manager matches the security profile on the Cisco Unified Mobility Advantage servers. For information on configuring a Cisco Unity Cisco Unified Mobility Advantage server security profile, see the *Cisco Unified Communications Manager Security Guide*.

Find Cisco Unified Mobility Advantage Server Security Profile

To find a Cisco Unified Mobility Advantage server security profile, perform the following procedure:

Procedure

Step 1 In Unified Communications Manager Administration, choose **System > Security Profile** > **CUMA Server Security Profile**.

The Find and List CUMA Server Security Profile window displays. 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 280.

To filter or search records

a) From the first drop-down list box, choose a search parameter.
b) From the second drop-down list box, 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 the **Clear Filter** button 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 box.

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 item that you choose.

Set Up Cisco Unified Mobility Advantage Server Security Profile

To add, update, or copy a security profile, perform the following procedure:

Procedure

Step 1 In Unified Communications Manager Administration, choose **System** > **Security Profile** > **CUMA Server Security Profile**.

Step 2 Perform one of the following tasks:

a) To add a new profile, click **Add New** in the **Find** window and continue with Cisco Unified Mobility Advantage Server Security Profile Setup, on page 279.
b) To copy an existing security profile, locate the appropriate profile and click the **Copy** button next to the security profile that you want to copy, and continue with Cisco Unified Mobility Advantage Server Security Profile Setup, on page 279.
c) To update an existing profile, locate the appropriate security profile and continue with Cisco Unified Mobility Advantage Server Security Profile Setup, on page 279.

When you click **Add New**, the configuration window displays with the default settings for each field. When you click **Copy**, the configuration window displays with the copied settings.

Step 3 Enter the appropriate settings as described in Table 43: Security Profile Settings, on page 281

Step 4 Click **Save**.

Cisco Unified Mobility Advantage Server Security Profile Settings

The following table describes the settings for the Cisco Unified Mobility Advantage Server security profiles.

Table 43: Security Profile Settings

Setting	Description
Name	Enter a name for the security profile. **Tip** Include the device model 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. 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 (<>).
Device Security Mode	From the drop-down list box, choose one of the following options: • **Non Secure**—No security features except image authentication exist for the Cisco Unified Mobility Advantage server. A TCP connection opens to Unified Communications Manager. • **Authenticated**—Unified Communications Manager provides integrity and authentication for the Cisco Unified Mobility Advantage server. A TLS connection that uses NULL/SHA opens for signaling. • **Encrypted**—Unified Communications Manager provides integrity, authentication, and encryption for the Cisco Unified Mobility Advantage server. A TLS connection that uses AES128/SHA opens for signaling, and SRTP carries the media for all mobile calls.

Setting	Description
Transport Type	When Device Security Mode is **Non Secure**, choose the following option from the drop-down list box: • **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. 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).
Secure Certificate Subject or Subject Alternate Name	(Required for Authenticated or Encrypted Device Security Mode setting.) This field applies if you configured TLS as the transport type. Secure Certificate Subject or Subject Alternate Name is an ITU Telecommunication Standardization Sector standard for Public Key Infrastructure in cryptography. The subject name corresponds to the source connection TLS certificate. 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.

Cisco Unified Mobility Advantage Server Security Profile Client Application

No “Device Security Profile” field exists on the device configuration window for a Mobile Communicator client, which means that you do not have to manually apply the Cisco Unified Mobility Advantage Server Security profile to a client.

Configuring a Cisco Unified Mobility Advantage server security profile in Unified Communications Manager Administration automatically applies this profile to all configured Mobile Communicator clients on that Unified Communications Manager.

Delete Cisco Unified Mobility Advantage Server Security Profile

This section describes how to delete a Cisco Unified Mobility Advantage server security profile from the Unified Communications Manager database.

Procedure

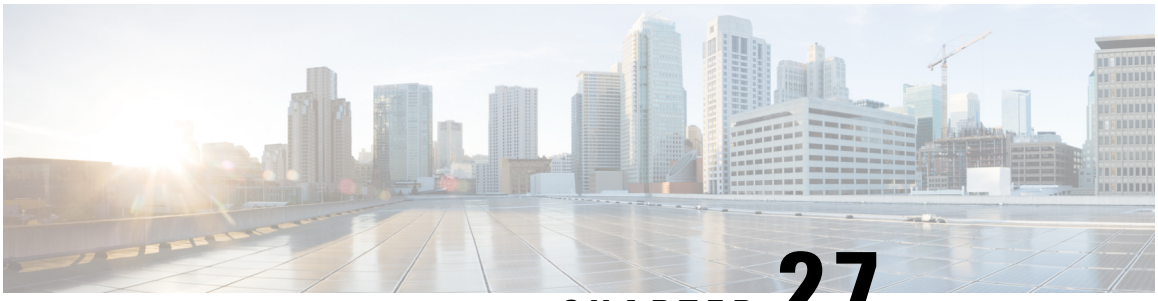
Step 1 Find the security profile to delete.

Step 2 To delete a security profile, perform the following task:

a) In the **Find and List** window, check the check box next to the appropriate security profile; then, click **Delete Selected**.

Step 3 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Where to Find More Information About Cisco Unified Mobility Advantage Server Security Profile



CHAPTER 27

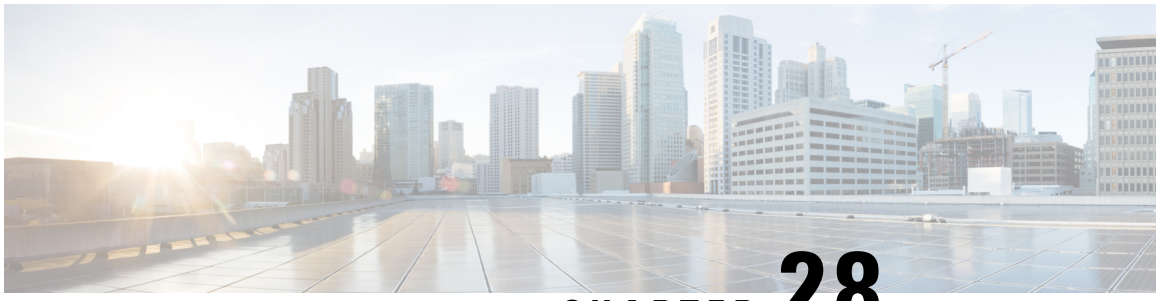
FIPS 140-2 Mode Setup

This chapter provides information about FIPS 140-2 mode setup.

- FIPS Mode Not Supported in Some 12.x Versions, on page 285

FIPS Mode Not Supported in Some 12.x Versions

FIPS mode is supported with 12.5(1)SU1. However, FIPS mode is not supported with Releases 12.0(x) and 12.5(1) of Cisco Unified Communications Manager and the IM and Presence Service. If you are upgrading from an earlier release with FIPS mode, Enhanced Security Mode, or Common Criteria Mode enabled, you must disable them prior to the upgrade to these releases, or upgrade to 12.5(1)SU1 instead. TFTP and other services will not work in 12.0(x) or 12.5(1) with FIPS mode enabled.



CHAPTER 28

Cisco V.150 Minimum Essential Requirements (MER)

- V.150 Overview, on page 287
- Prerequisites for Cisco V.150.1 MER, on page 287
- Configure V.150 Task Flow, on page 288

V.150 Overview

The V.150 Minimum Essential Requirements feature allows you to make secure calls in a modem over 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)

Prerequisites for Cisco V.150.1 MER

Your system should already be set up with basic call control functionality. For instructions on how to set up the call control system, refer to theSystem 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 available in Spring 2016
- 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.

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 289, perform the following subtasks: • Configure Media Resource Group for Non-V.150 Endpoints, on page 290 • Configure a Media Resource Group List for Non-V.150 Endpoints, on page 290 • Configure Media Resource Group for V.150 Endpoints, on page 290 • Configure a Media Resource Group List for V.150 Endpoints, on page 291	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 291	Add V.150 functionality to a gateway.
Step 3	Configure V.150 MGCP Gateway Port Interface, on page 292	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 292	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 293	Add V.150 support to the phones that will be placing V.150 calls.
Step 6	To Configure SIP Trunk Task Flow, on page 294, perform one or any of the following subtasks: • Configure SIP Profile for V.150, on page 294 • Set the Clusterwide V.150 Filter, on page 294	Add V.150 support to the SIP trunk that will be used for V.150 calls.

	Command or Action	Purpose
	• Add V.150 Filter to SIP Trunk Security Profile, on page 295 • Configure SIP Trunk for V.150, on page 296	
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 290	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 290	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 290	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 291	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 290

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 290

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 294	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 294	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 295	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 296	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**.

INDEX

A

authentication 8, 9, 20, 237
  device 20
  digest 20
  interactions 8, 9
  overview 20
  restrictions 8, 9
  with CTI/JTAPI/TAPI applications 237
authentication string 239
  with CTI/JTAPI/TAPI applications 239
authorization 9, 20, 264, 265
  configuration settings (table) 265
    for SIP trunk 265
  configuring for SIP trunk 264
  interactions 9
  overview 20

B

barge 14, 199, 201
  encryption restrictions with 14
  security 199
  security icons 201

C

Certificate Authority Proxy Function (CAPF) 15, 93, 142, 239, 240, 241, 242, 243, 244, 247
  CAPF service 93
  configuration settings (table) 242
    for CTI/JTAPI/TAPI applications 242
  configuring an application user or end user CAPF profile 241
  deleting an application user or end user CAPF profile 244
  installing 15
  interaction with IPv6 addressing 142
  viewing certificate operation status for application user or end user 247
  with CTI/JTAPI/TAPI applications 239, 240, 243
    interactions and requirements 240
    overview 239
    updating service parameters 243
Certificate Signing Requests (CSRs) 16
certificates 16, 58, 60
  external CAs 16
certificates *(continued)*
  Firefox certificate 58
  Safari certificate 60
  types 16
Cisco Unified IP Phone 7, 151, 155, 157, 179, 196, 204
  configuration checklist (table) for security 155
  configuration tips for phone security profiles 157
  disabling the PC Port setting 196
  disabling the PC Voice VLAN Access setting 196
  disabling the Setting Access setting 196
  encrypted configuration file 179
  secure conference support 204
  security icons 7
  understanding security 151
  viewing security settings 155
computer telephony integration (CTI) 245, 246
  configuration checklist (table) for securing 245
  secure user groups 246
    adding application users and end users 246
conference bridge 199, 200, 201, 205, 206, 207, 208, 209, 210
  conference list 201
  configuration checklist (table) for security 207
  configuration tips for security 206
  configuring minimum Meet-Me security 209
  configuring packet capture on a secure conference bridge 210
  configuring security 208
  minimum Meet-Me security level 201
  security 199
  security icons 201
  security interactions 205
  security requirements 200
  security restrictions 205
configuration file 24
  encryption 24
Configuration Task Flow 86
Contact Search Authentication 86, 87
CTL client 15, 89, 92, 93, 94, 99, 100, 101, 102
  CAPF service 93
  cluster security mode 99
    updating 99
  configuration settings (table) 100
  configuring 93, 94
    CTL client 94
    TLS port 93
  CTL Provider service 92

CTL client *(continued)*
installing 15
overview 89
security mode 101
verifying 101
security token 94
configuring CTL client 94
setting the Smart Card service 101
uninstalling 102
verifying 102
CTL file 98
updating 98
CTL Provider 92
activating service 92

D

device authentication 20, 159, 264, 265
configuration settings (table) 159, 265
for phone that is running SCCP 159
for phone that is running SIP 159
for SIP trunk 265
configuring for phones 159
configuring for SIP trunk 264
overview 20
digest authentication 20, 159, 191, 192, 193, 264, 265, 273, 274, 275, 276
associating digest user with a phone 193
cluster ID 274
configuration checklist (table) 191, 273
for phones 191
for SIP trunk 273
configuration settings (table) 159, 192, 265, 274, 276
for application user digest credentials 274
for end user 192
for phone that is running SIP 159
for SIP realm 276
for SIP trunk 265
configuring a SIP realm 275
configuring digest credentials 192, 274
for application user 274
for end user 192
configuring for phones 159
configuring for SIP trunk 264
configuring service parameters 192
deleting a SIP realm 276
finding a SIP realm 275
overview 20

E

Enable 87
encrypted configuration file 179, 180, 181, 182, 185, 186, 187, 188
configuration settings (table) 185
for manual key 185
configuration tips 182
encrypted configuration file *(continued)*
configuring manual key distribution 185
disabling 188
entering symmetric key 186
manual key configuration checklist (table) 185
manual key distribution 180
phone support 181
symmetric key encryption with public key 180
understanding 179
using symmetric key encryption w/public key 187
encryption 8, 9, 14, 15, 24, 159, 205, 238, 257, 258, 259, 260, 262, 264, 265
configuration checklist (table) for gateways and trunks 260
configuration settings (table) 159, 265
for phone that is running SCCP 159
for phone that is running SIP 159
for SIP trunk 265
configuring for phones 159
configuring SRTP allowed check box 262
configuring with barge 14
for H.323 gateway 258
for H.323/H.225/H.245 trunk 258
for MGCP gateway 257
for SIP trunk 259
installing 15
interactions 8, 9, 205
overview 24
restrictions 8, 9, 205
signaling 159, 264
configuring for phones 159
configuring for SIP trunk 264
with CTI/JTAPI/TAPI applications 238
etoken 94
configuring CTL client 94

F

file authentication 20, 159
configuring for phones 159
overview 20

H

HTTPS 51, 58, 60
overview 51
virtual directories (table) 51
with Firefox 58
with Safari 60

I

image authentication 20
overview 20
integrity 20
overview 20

IPSec 15, 260, 261
configuration checklist (table) for IPSec 260
configuring 261
gateway or trunk considerations 261
infrastructure considerations 261
recommendations 261

J

JTAPI 245, 247
configuration checklist (table) for securing 245
configuring security service parameters 247

L

locally significant certificate (LSC) 239
with CTI/JTAPI/TAPI applications 239

M

media encryption, *See* encryption
MGCP gateway 260, 261
configuration checklist (table) for security 260
configuring 261

N

NMAP scans 32
running 32

P

phone hardening 196
configuring 196
disabling the PC Port setting 196
disabling the PC Voice VLAN Access setting 196
disabling the Setting Access setting 196
phone security profile 170
synchronizing configuration to applicable phones 170
Phone Support 86
port 93
CTL Provider 93
Ethernet phone 93
SIP secure 93
protected call 173

S

secure conference 199, 200, 201, 204, 205, 206, 207, 208, 209, 210
Cisco Unified IP Phone support 204
conference bridge requirements 200
conference list 201
configuration checklist (table) 207
configuration tips 206
configuring minimum Meet-Me security 209
secure conference *(continued)*
configuring packet capture 210
configuring secure conference bridge 208
CTI support 204
interactions 205
minimum Meet-Me security level 201
restrictions 205
security icons 201
security overview 199
trunks and gateways 204
Secure Directory Server URL 87
secure indication tone 173
secure sockets layer (SSL) 15, 51
installing 15
with HTTPS 51
security 1, 6, 8, 9, 13, 14, 15, 16, 20, 24, 32, 49, 51, 89, 94, 98, 205
authentication overview 20
authorization overview 20
best practices 13
certificate types 16
configuration checklist for authentication and encryption (table) 32
CTL client overview 89
encryption overview 24
external CAs 16
features list 6
HTTPS 51
installing 15
interactions 8, 9, 205
rebooting the cluster 14
rebooting the server 14
resetting devices 14
restarting Cisco Unified Communications Manager service 14
restrictions 8, 9, 205
SCCP calls (table) 6
SIP calls (table) 6
system requirements 6
terminology (table) 1
tokens 89, 94, 98
using barge with encryption 14
where to find more information 49
security mode 99, 101
cluster 99, 101
configuring 99
verifying 101
security profile 157, 158, 159, 169, 170, 171, 263, 264, 265, 270, 271, 279, 280, 282
applying for SIP trunk 270
applying to Cisco Unified Mobility Advantage Server 282
applying to phones 169
configuration settings (table) 159, 265
for phone that is running SCCP 159
for phones that is running SIP 159
for SIP trunk 265
configuration tips for phones 157
configuring for phones 159

security profile *(continued)*
configuring for SIP trunk 264
deleting for Cisco Unified Mobility Advantage server 282
deleting for phones 170
deleting for SIP trunk 271
finding for Cisco Unified Mobility Advantage servers 280
finding for phones 158
finding for SIP trunk 264
finding phones that use 171
overview for Cisco Unified Mobility Advantage 279
overview for phones 157
overview for SIP trunk 263
security token 94
configuring CTL client 94
signaling authentication 20
overview 20
signaling encryption 24
overview 24
SIP Trunk security profile 271
synchronizing configuration to applicable SIP trunks 271
Site Administrator Security Token (SAST) 89
SRST 251, 252, 253, 256
configuration checklist (table) for securing 253
configuration tips for securing 252
overview for securing 251
troubleshooting 256
certificate deleted on gateway 256
SRST reference 253, 254, 256
configuration settings (table) for security 254
configuring 253
troubleshooting 256
deleting secured reference 256

T

TAPI 245, 247
configuration checklist (table) for securing 245
configuring security service parameters 247
Tftp service 89
TLS Proxy server 89
transport layer security (TLS) 15, 93
port 93
transport security 15, 159, 264, 265
and real-time protocol (RTP) 15
and secure real-time protocol (SRTP) 15
configuration settings (table) 159, 265
for phone that is running SCCP 159
for phone that is running SIP 159
for SIP trunk 265
configuring for phones that are running SIP 159
configuring for SIP trunk 264
IPSec 15
TLS 15
troubleshooting 256
SRST certificate deleted on gateway 256

V

voice messaging 211, 212
configuration checklist (table) for security 212
security overview 211
security requirements 211
voice messaging port 211, 212, 213, 214
applying a security profile 213
applying a security profile using the Wizard 214
configuration checklist (table) for security 212
security overview 211