Cisco Unified Communications Manager Security Guide, Release 10.0(1)

First Published: 2013-12-03

Last Modified: 2019-09-24

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

Text Part Number: OL-29848-01

CONTENTS

PREFACE

Preface xv

Purpose xv

Audience xvi

Organization xvi

Related Documentation xviii

Conventions xviii

Obtain Documentation, Support, and Security Guidelines xix

Cisco Product Security Overview xix

PART I

Security Basics 21

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 10

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 12

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, Reboot Servers and Clusters, and Restart 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 17
Support for Certificates from External CAs 18
Authentication, Integrity, and Authorization 19
Image Authentication 20
Device Authentication 20
File Authentication 20
Signaling Authentication 21
Digest Authentication 21
Authorization 23
Encryption 23
Signaling Encryption 24
Media Encryption 24
Configuration File Encryption 25
NMAP Scan Operation 26
Set Up Authentication and Encryption 26
Where to Find More Information 29

CHAPTER 2 **Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS)** 31
HTTPS 31
HTTPS for Cisco Unified IP Phone Services 33
Cisco Unified IP Phones that Support HTTPS 33
Features That Support HTTPS 33
Cisco Unified IP Phone Services Settings 34

Enterprise Parameter Settings for HTTPS Support 36
Save Certificate to Trusted Folder Using Internet Explorer 8 36
Copy Internet Explorer 8 Certificate to File 37
First-Time Authentication for Firefox with HTTPS 38
Save Certificate to Trusted Folder Using Firefox 3.x 38
Copy Firefox 3.x Certificate to File 39
First-Time Authentication for Safari with HTTPS 40
Save Certificate to Trusted Folder Using Safari 4.x 40
Copy Safari 4.x Certificate to File 41
Where to Find More Information About HTTPS Setup 42

CHAPTER 3 **Default Security Setup** 43
Default Security Features 43
Trust Verification Service 43
TVS Description 44
Initial Trust List 44
ITL Files 44
ITL File Contents 44
ITL and CTL File Interaction 45
Interactions and Restrictions 45
Update ITL File for IP Phones 45
Autoregistration 46
Obtain Cisco Unified IP Phone Support List 46
Certificate Regeneration 46
Regenerate CAPF Certificate 47
Regenerate TVS Certificate 47
Regenerate TFTP Certificate 47
Tomcat Certificate Regeneration 48
System Back-Up Procedure After TFTP Certificate Regeneration 48
Refresh Upgrade From Cisco Unified Communications Manager Release 7.x to Release 8.6 Or Later 49
Roll Back Cluster to a Pre-8.0 Release 50
Switch Back to Release 8.6 or Later After Revert 51
Migrate IP Phones Between Clusters with Cisco Unified Communications Manager and ITL Files 52

Bulk Certificate Export 53
Perform Bulk Reset of ITL File 53

CHAPTER 4 **Cisco CTL Client Setup** 55
About Cisco CTL Setup 55
Activate Cisco CTL Provider Service 56
Cisco CAPF Service Activation 57
Set up Secure Ports 57
Set Up Cisco CTL Client 58
Update CTL File 59
Update Cisco Unified Communications Manager Security Mode 60
Cisco CTL File Details 61
Verify Cisco Unified Communications Manager Security Mode 62
Set Up Smart Card Service to Started or Automatic 62
Verify or Uninstall Cisco CTL Client 63

CHAPTER 5 **Certificate Setup** 65
About Certificate Setup 65
Find Certificate 65
Certificate Settings 66

PART II **Security for Cisco IP Phone and Cisco Voice-Messaging Ports** 67

CHAPTER 6 **Phone Security** 69
Phone Security Overview 69
Trusted Devices 70
Cisco Unified Communications Manager Administration 70
Device Called Trust Determination Criteria 71
Phone Model Support 71
Preferred Vendor SIP Phone Security Set Up 71
Set Up Preferred Vendor SIP Phone Security Profile Per-Device Certificates 72
Set Up Preferred Vendor SIP Phone Security Profile Shared Certificates 72
View Phone Security Settings 73
Set Up Phone Security 73

Phone Security Interactions and Restrictions 74
Where to Find More Information About Phone Security 74

CHAPTER 7 **Phone Security Profile Setup** 75
Phone Security Profile Overview 75
Phone Security Profile Setup Prerequisites 75
Find Phone Security Profile 76
Set Up Phone Security Profile 77
Phone Security Profile Settings 77
Apply Security Profiles to Phone 86
Synchronize Phone Security Profile with Phones 87
Delete Phone Security Profile 87
Find Phones with Phone Security Profiles 88

CHAPTER 8 **Secure and Nonsecure Indication Tone Setup** 89
Secure and Non-Secure Indication Tone Overview 89
Protected Devices 89
Supported Devices 90
Secure and Non-Secure Indication Tone Tips 90
Secure and Non-Secure Indication Tone Configuration Tasks 91

CHAPTER 9 **Encryption to Analog Endpoint Setup** 93
Analog Phone Security Profile 93
Certificate Management for Secure Analog Phones 93

CHAPTER 10 **Certificate Authority Proxy Function** 95
About Certificate Authority Proxy Function 95
Cisco IP Phone and CAPF Interaction 96
CAPF Interaction with IPv6 Addressing 97
CAPF System Interactions and Requirements 100
CAPF in Cisco Unified Serviceability Setup 101
Set Up CAPF 101
Activate Certificate Authority Proxy Function Service 101
Update CAPF Service Parameters 102

Generate and Import Third Party CA-Signed LSCs 102
Install, Upgrade, Troubleshoot, or Delete Certificates From Phone Using CAPF 103
CAPF Settings 104
Find Phones by LSC Status or Authentication String 105
Generate CAPF Report 106
Enter Phone Authentication String 107
Verify Phone Authentication String 107

CHAPTER 11 **Encrypted Phone Configuration File Setup** 109
Encryption for Phone Configuration File Overview 109
Manual Key Distribution 110
Symmetric Key Encryption with Phone Public Key 111
Phone Models That Support Encryption 111
Encryption for Phone Configuration File Tips 112
Set Up Encryption Configuration File 113
Enable Phone Configuration File Encryption 114
Set Up Manual Key Distribution 114
Manual Key Distribution Settings 115
Enter Phone Symmetric Key 115
Verify LSC or MIC Certificate Installation 116
Disable Encryption for Phone Configuration File 117
Exclude Digest Credentials From Phone Configuration File Download 117

CHAPTER 12 **Digest Authentication for SIP Phones Setup** 119
Set up SIP Phone Digest Authentication 119
Set Up Digest Authentication Service Parameters 120
Set Up End User Digest Credentials 120
End User Digest Credential Settings 121
Set Up Digest User Using Phone 121

CHAPTER 13 **Phone Hardening** 123
Gratuitous ARP Disable 123
Web Access Disable 123
PC Voice VLAN Access Disable 124

Setting Access Disable 124
PC Port Disable 124
Set Up Phone Hardening 124
Where to Find More Information About Phone Hardening 125

CHAPTER 14 **Secure Conference Resources Setup** 127
Secure Conference 127
Conference Bridge Requirements 128
Secure Conference Icons 129
Secure Conference Status 129
Ad Hoc Conference Lists 130
Meet-Me Conference with Minimum Security Level 131
Cisco Unified IP Phone Secure Conference and Icon Support 132
Secure Conference CTI Support 132
Secure Conference Over Trunks and Gateways 132
CDR Data 133
Interactions and Restrictions 133
Cisco Unified Communications Manager Interactions with Secure Conference 133
Cisco Unified Communications Manager Restrictions with Secure Conference 134
Securing Conference Resources Tips 134
Set Up Secure Conference Bridge 135
Set Up Secure Conference Bridge in Cisco Unified Communications Manager Administration 136
Set Up Minimum Security Level for Meet-Me Conferences 137
Set Up Packet Capturing for Secure Conference Bridge 138
Where to Find More Information About Secure Conferences Resources 138

CHAPTER 15 **Voice-Messaging Ports Security Setup** 139
Voice-Messaging Security 139
Voice-Messaging Security Setup Tips 139
Set Up Secure Voice-Messaging Port 140
Apply Security Profile to Single Voice-Messaging Port 141
Apply Security Profile Using Voice Mail Port Wizard 142
Where to Find More Information About Voice-messaging Security 142

CHAPTER 16 **Call Secure Status Policy** 143

About Call Secure Status Policy 143

Setup Call Secure Status Policy 144

CHAPTER 17 **Secure Call Monitoring and Recording Setup** 145

About Secure Call Monitoring and Recording Setup 145

Set Up Secure Call Monitoring and Recording 145

PART III **Virtual Private Networks for Cisco Unified IP Phones** 147

CHAPTER 18 **Virtual Private Network Setup** 149

Virtual Private Network 149

Devices Supporting VPN 150

Set Up VPN Feature 150

Complete Cisco IOS Prerequisites 151

Configure Cisco IOS SSL VPN to Support IP Phones 151

Sample IOS Setup 153

Complete ASA Prerequisites for AnyConnect 157

Configure ASA for VPN Client on IP Phone 157

Sample ASA Setup 160

CHAPTER 19 **VPN Gateway Setup** 165

Upload VPN Concentrator Certificates 165

VPN Gateway Setup 166

Find VPN Gateway 166

Configure VPN Gateway 166

VPN Gateway Fields for VPN Client 167

CHAPTER 20 **VPN Group Setup** 169

Find VPN Group 169

Configure VPN Group 170

VPN Group Fields for VPN Client 170

CHAPTER 21 **VPN Profile Setup** 171

About VPN Profile Setup 171

Find VPN Profile 171

Configure VPN Profile 172

VPN Profile Fields for VPN Client 172

CHAPTER 22 **VPN Feature Setup** 175

About VPN Feature Setup 175

Configure VPN Feature Parameters 175

VPN Feature Parameters 176

PART IV **Cisco CTI, JTAPI, and TAPI Application Security** 179

CHAPTER 23 **Authentication and Encryption Setup for CTI, JTAPI, and TAPI** 181

Authentication for CTI, JTAPI, and TAPI Applications 181

Encryption for CTI, JTAPI, and TAPI Applications 183

CAPF Functions for CTI, JTAPI, and TAPI Applications 183

CAPF System Interactions and Requirements for CTI, JTAPI, and TAPI Applications 185

Securing CTI, JTAPI, and TAPI 185

Add Application and End Users to Security-Related Users Groups 186

Certificate Authority Proxy Function Service Activation 187

Update CAPF Service Parameters 188

Find Application User or End User CAPF Profile 188

Set Up Application User or End User CAPF Profile 189

CAPF Settings 190

Delete Application User CAPF or End User CAPF Profile 192

Set Up JTAPI/TAPI Security-Related Service Parameters 193

View Certificate Operation Status for Application or End User 193

CHAPTER 24 **Certificate Revocation/Expiry Status Verification** 195

Certificate Revocation/Expiry Status Verification 196

Verify Certificate Status 196

Support for Delegated Trust Model in OCSP Response 197

PART V Security for SRST References, Trunks, and Gateways 199

CHAPTER 25 Secure Survivable Remote Site Telephony (SRST) Reference 201

Securing SRST 201

Securing SRST Tips 202

Set Up Secure SRST 203

Set Up Secure SRST References 203

SRST Reference Security Settings 204

Delete Security From SRST Reference 206

SRST Certificate Deletion From Gateway 206

CHAPTER 26 Encryption Setup for Gateways and Trunks 207

Cisco IOS MGCP Gateway Encryption 207

H.323 Gateway and H.323/H.225/H.245 Trunk Encryption 208

SIP Trunk Encryption 209

Set Up Secure Gateways and Trunks 210

IPSec Setup Within Network Infrastructures 211

IPSec Setup Between Cisco Unified Communications Manager and Gateway or Trunks 211

Allow SRTP Using Cisco Unified Communications Manager Administration 211

Where to Find More Information About Gateway and Trunk Encryption 212

CHAPTER 27 SIP Trunk Security Profile Setup 213

About SIP Trunk Security Profile Setup 213

SIP Trunk Security Profile Setup Tips 213

Find SIP Trunk Security Profile 214

Set Up SIP Trunk Security Profile 214

SIP Trunk Security Profile Settings 215

Apply SIP Trunk Security Profile 221

Synchronize SIP Trunk Security Profile with SIP Trunks 222

Delete SIP Trunk Security Profile 222

Where to Find More Information About SIP Trunk Security Profiles 223

CHAPTER 28 Digest Authentication Setup for SIP Trunks 225

Set Up SIP Trunk Digest Authentication 225
Set Up Digest Authentication Enterprise Parameters 226
Set Up Digest Credentials 226
Application User Digest Credential Settings 226
Find SIP Realm 227
Configure SIP Realm 227
SIP Realm Settings 228
Delete SIP Realm 228

CHAPTER 29 **Cisco Unified Mobility Advantage Server Security Profile Setup** 231
About Cisco Unified Mobility Advantage Server Security Profile Setup 231
Find Cisco Unified Mobility Advantage Server Security Profile 232
Set Up Cisco Unified Mobility Advantage Server Security Profile 232
Cisco Unified Mobility Advantage Server Security Profile Settings 233
Cisco Unified Mobility Advantage Server Security Profile Client Application 234
Delete Cisco Unified Mobility Advantage Server Security Profile 234
Where to Find More Information About Cisco Unified Mobility Advantage Server Security Profile 235

CHAPTER 30 **FIPS 140-2 Mode Setup** 237
FIPS 140-2 Setup 237
Enable FIPS 140-2 Mode 238
Disable FIPS 140-2 Mode 239
Check FIPS 140-2 Mode Status 240
FIPS 140-2 Mode Server Reboot 240

Preface

- Purpose, on page xv
- Audience, on page xvi
- Organization, on page xvi
- Related Documentation, on page xviii
- Conventions, on page xviii
- Obtain Documentation, Support, and Security Guidelines, on page xix
- Cisco Product Security Overview, on page xix

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, on page 1	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), on page 31	Provides an overview of HTTPS and describes how to install the server authentication certificate in the trusted folder.
Default Security Setup, on page 43	Provides information about the Security by Default feature, which provides automatic security features for Cisco Unified IP Phones.
Cisco CTL Client Setup, on page 55	Describes how to configure authentication by installing and configuring the Cisco CTL Client.
Certificate Setup, on page 65	Describes how to manage certificates in the Certificate Configuration window.
Security for Phones and Voice Mail Ports	
Phone Security, on page 69	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, on page 75	Describes how to configure the security profile and apply it to the phones in Unified Communications Manager.
Secure and Nonsecure Indication Tone Setup, on page 89	Describes how to configure a phone to play a secure-indication tone.
Encryption to Analog Endpoint Setup, on page 93	Describes how to configure a secure SCCP connection to analog endpoints.

Chapter	Description
Certificate Authority Proxy Function, on page 95	Provides an overview of Certificate Authority Proxy Function and describes how to install, upgrade, delete, or troubleshoot locally significant certificates on supported phones.
Encrypted Phone Configuration File Setup, on page 109	Describes how to configure encrypted phone configuration files in Unified Communications Manager.
Digest Authentication for SIP Phones Setup, on page 119	Describes how to configure digest authentication on the phone that is running SIP in Unified Communications Manager Administration.
Phone Hardening, on page 123	Describes how to tighten the security on the phone by using Unified Communications Manager Administration.
Secure Conference Resources Setup, on page 127	Describes how to configure media encryption for secure conferences.
Voice-Messaging Ports Security Setup, on page 139	Describes how to configure security for voice mail ports in Unified Communications Manager Administration.
Secure Call Monitoring and Recording Setup, on page 145	Describes how to configure secure call monitoring and recording.
Virtual Private Networks for Cisco IP Phones	
Virtual Private Network, on page 149	Describes how to configure a virtual private network (VPN).
VPN Gateway Setup, on page 165	Describes how to configure a VPN gateway.
VPN Group Setup, on page 169	Describes how to configure a VPN group.
VPN Profile Setup, on page 171	Describes how to configure a VPN profile.
VPN Feature Setup, on page 175	Describes how to configure a VPN feature.
Security for CTI, JTAPI, and TAPI	
Authentication and Encryption Setup for CTI, JTAPI, and TAPI, on page 181	Describes how to configure the Application User CAPF Profile and End User CAPF Profiles in Unified Communications Manager.
Certificate Revocation/Expiry Status Verification, on page 195	Describes how to configure the Online Certificate Status Protocol (OCSP) to monitor the status of existing certificates and to revoke expired certificates automatically.
Security for SRST References, Gateways, Trunks, and Cisco Unified Mobility Advantage Servers	

Chapter	Description
Secure Survivable Remote Site Telephony (SRST) Reference, on page 201	Describes how to configure the SRST reference for security in Unified Communications Manager Administration.
Encryption Setup for Gateways and Trunks, on page 207	Describes how Unified Communications Manager communicates with a secure gateway or trunk; describes IPSec recommendations and considerations.
SIP Trunk Security Profile Setup, on page 213	Describes how to configure and apply the SIP trunk security profile in Unified Communications Manager Administration.
Digest Authentication Setup for SIP Trunks, on page 225	Describes how to configure digest authentication for the SIP trunk in Unified Communications Manager Administration.
Cisco Unified Mobility Advantage Server Security Profile Setup, on page 231	Describes how to configure a Cisco Unified Mobility Advantage server security profile in Unified Communications Manager Administration.
FIPS 140-2 Mode Setup, on page 237	Describes how to configure FIPS (Federal Information Processing Standard) 140-2 mode in Unified Communications Manager Administration.

Related Documentation

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

Refer to the following documents for further information about related Cisco IP 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 Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco Product Security Overview

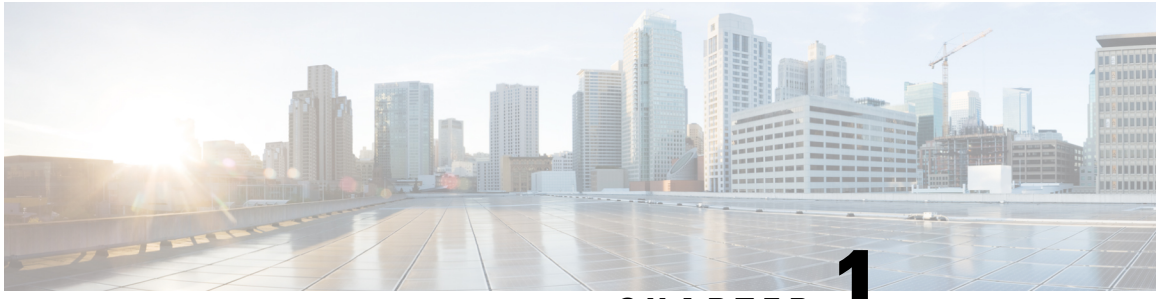
This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors 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 31
- Default Security Setup, on page 43
- Cisco CTL Client Setup, on page 55
- Certificate Setup, on page 65



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 Cisco IP 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 19
- Encryption, on page 23
- NMAP Scan Operation, on page 26
- Set Up Authentication and Encryption, on page 26
- Where to Find More Information, on page 29

Terms and Acronyms

The definitions in the following table apply when you configure authentication, encryption, and other security features for your Cisco IP telephony 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 IETF RFC 3711.
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 Cisco IP 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

To add presence group authorization for phones and trunks that are running SIP, configure presence groups to restrict presence requests to authorized users.

Note Refer to the *Cisco Unified Communications Manager Features and Services Guide* for more information about configuring presence groups.

To allow presence requests on SIP trunks, configure Unified Communications Manager to accept presence requests on the SIP trunk and, if required, configure Unified Communications Manager to accept and authenticate incoming presence requests from the remote device or application.

SIP Trunk

To use SIP-initiated transfer features and other advanced transfer-related features on SIP trunks, such as Web Transfer and Click to Dial, configure the SIP Trunk Security Profile to accept incoming Out of Dialog REFER requests.

To provide support for event reporting (such as MWI support) and to reduce per-call MTP allocations (from a voice-messaging server, for example), configure the SIP Trunk Security Profile to accept Unsolicited Notification SIP requests.

To allow Unified Communications Manager to transfer an external call on a SIP trunk to an external device or party (in attended transfer, for example), configure the SIP Trunk Security Profile to accept SIP requests with replaces header in REFERS and INVITES.

Extension Mobility

For extension mobility, the SIP digest credentials change when a user logs in and out because different credentials are configured for different end users.

CTI

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

When multiple instances of a CTI/JTAPI/TAPI application are running, CTI TLS support requires you to configure a unique instanceID (IID) for every application instance to secure 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:

- Auto-registration does not work when you configure mixed mode.
- 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, 7921G, 7925G, 7925G-EX, 7926G, 7931G, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7970G, 7971G, 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, 7970G, 7971G, 7975G, 8811, 8821, 8821-EX, 8832, 8841, 8845, 8851, 8851NR, 8865, 8865NR, 8941, 8945, 8961, 9971, and 9971.

For more information, see the Cisco Unified IP Phone administration guides for Cisco Unified IP Phones that support encryption and this version of Cisco 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

Cisco strongly recommends the following best practices while configuring security:

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

Warning The session encryption keys get transmitted in the clear if you fail to use IPSec.

- To prevent toll fraud, configure conference enhancements that are described in the *Cisco Unified Communications Manager System Guide*. Likewise, perform configuration tasks to restrict external transferring of calls. For information on how to perform this task, refer to the *Cisco Unified Communications Manager Features and Services Guide*.

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, Reboot Servers and Clusters, and Restart Services

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

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

Before you begin

Refer to the guidelines for device resets, server and cluster reboots, and service restarts before proceeding.

Procedure

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

The Find/List window displays.

Step 2 Click **Find**.

A list of configured Unified Communications Manager servers displays.

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

Step 4 Click **Reset**.

Step 5 Perform Step 2, on page 14 and Step 4, on page 14 for each server in the cluster.

Media Encryption with Barge Setup

When you attempt to configure barge for Cisco Unified IP Phones 7962 and 7942 that are configured for encryption, the following message displays:

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

The message displays when you perform the following tasks in Unified Communications Manager Administration:

- You update the Cluster Security Mode parameter in the CTL client.
- You update the Builtin Bridge Enable parameter in the Service Parameter window.

This message does not display in the Phone Configuration window when an encrypted security profile is configured for Cisco Unified IP Phones 7962 and 7942 and you choose **Default**for the Built In Bridge setting (or the default setting equals Default); however, the same restriction applies.

Tip For changes to take effect, you must reset the dependent Cisco IP devices.

For more information, see topics related to Barge and encryption.

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 Cisco IOS 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 Cisco Unified IP Phones 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 *Cisco Unified Communications Operating System Administration Guide* 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.

Phone Certificate Types

Cisco uses the following certificate types in phones:

- Manufacture-installed certificate (MIC)—Cisco Manufacturing automatically installs this certificate in supported phone models. Manufacturer-installed certificates authenticate to Cisco Certificate Authority Proxy Function (CAPF) for LSC installation. You cannot overwrite or delete the manufacture-installed certificate.
- Locally significant certificate (LSC)—This certificate type installs on supported phones after you perform the necessary 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.

Tip 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. Because 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.

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

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 CallManager trust store and managing certificates, refer to the *Cisco Unified Communications Operating System Administration Guide* that supports this release.

Server Certificate Types

Cisco uses the following self-signed (own) certificate types in Unified Communications Manager servers:

- HTTPS certificate (Tomcat)—A self-signed root certificate gets generated during the Unified Communications Manager installation for the HTTPS server. Cisco Unity Connection uses this certificate for SMTP and IMAP services.
- CallManager certificate—A self-signed root certificate automatically installs when you install Unified Communications Manager on the Unified Communications Manager server.
- CAPF certificate—The system copies this root certificate, which gets generated during Unified Communications Manager installation, to your server or to all servers in the cluster after you complete the Cisco CTL client configuration.
- IPSec certificate (ipsec_cert)—A self-signed root certificate gets generated during Unified Communications Manager installation for IPSec connections with MGCP and H.323 gateways.
- SRST-enabled gateway certificate—When you configure a secure SRST reference in Unified Communications Manager Administration, Unified Communications Manager retrieves the SRST-enabled gateway certificate from the gateway and stores it in the Unified Communications Manager database. After you reset the devices, the certificate gets added to the phone configuration file. Because the certificate is stored in the database, you cannot manage this certificate with the certificate management tool.
- TVS certificate—These are self-signed certificates that support the Trust Verification Service (TVS).

- Phone-VPN-trust certificate—This category allows the system to import Cisco Unified IP Phone VPN certificates. These certificates get stored in the Midlet trust store.
- Phone Certificates trust store (Phone-trust)—Unified Communications Manager uses this certificate type to support HTTPs access on phones. You can upload certificates to the Phone-trust store by using the Cisco Unified Communications Operating System GUI. Certificates in the Phone-CTL-trust are downloaded to the phone though the CTL file mechanism to support secure web access (HTTPS) from Cisco Unified IP Phones. Phone-trust certificates stay on the server and phones can request them through TVS.

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

- 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.
- 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.
- 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.

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

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 Cisco Unified Communications Operating System Certificate Manager GUI. Customers who currently use third-party CAs should use the CSR mechanism to issue certificates for Cisco CallManager, CAPF, IPSec, and Tomcat.

Note When using Multi-server (SAN) CA-signed certificates, the Multi-server certificate is only applied to nodes in the cluster at the time the certificate is uploaded to the Publisher. Therefore, anytime a node is rebuilt or a new node is added to the cluster, it is necessary to generate a new Multi-server certificate and upload it to the cluster.

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 does not provide SCEP interface support.

Be sure to run the CTL client after you upload a third-party, CA-signed certificate to the platform to update the CTL file. After running the CTL client, restart the appropriate service(s) for the update; for example, restart Cisco CallManager and Cisco TFTP services when you update the Unified Communications Manager certificate, restart CAPF when you update the CAPF certificate, and so on.

Note After uploading the Cisco CallManager 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, refer to the Cisco Unified Communications Operating System Administration Guide that supports this Cisco Unified Communications Manager release.

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 Table 2: Terminology, on page 1
- 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 Cisco CTL 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 *Cisco Unified Communications Operating System Administration Guide* 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 TFTP server 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:

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.

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. Cisco IOS gateways and trunks support media encryption without authentication. For Cisco IOS 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, Cisco strongly recommends that you configure IPSec because Cisco IOS 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.

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 or during auto-registration.

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.

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 Cisco CTL 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 Cisco CTL 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 Cisco CTL client.

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

Step 5 Install the Cisco CTL client.

Tip To update the Cisco CTL 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 Cisco CTL client.

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

Step 9 Configure CAPF to issue certificates to the phones.

Tip If you performed certificate operations before the upgrade to this Unified Communications Manager release and CAPF ran on a subscriber server, you must copy the CAPF data to the publisher database server before you upgrade a cluster to this Unified Communications Manager release.

Caution The CAPF data on the Unified Communications Manager subscriber server does not migrate to the Unified Communications Manager database, and a loss of data occurs, if you do not copy the data to the database. If a loss of data occurs, the locally significant certificates that you issued with the CAPF utility remain in the phones, but the CAPF utility for this release must reissue the certificates, which are no longer valid.

The following steps are optional:

Step 10 Verify that the locally significant certificates are installed on supported Cisco Unified IP Phones.

Step 11 Configure digest authentication for phones that are running SIP.

Step 12 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 13 Configure conference bridge resources for security.

Step 14 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 15 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 16 Configure IPSec.

For more information, see *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* and *Cisco Unified Communications Operating System Administration Guide*

Step 17 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 18 Apply the SIP trunk security profile to the trunk.

Step 19 Configure digest authentication for the trunk.

Step 20 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 21 Reset all phones.

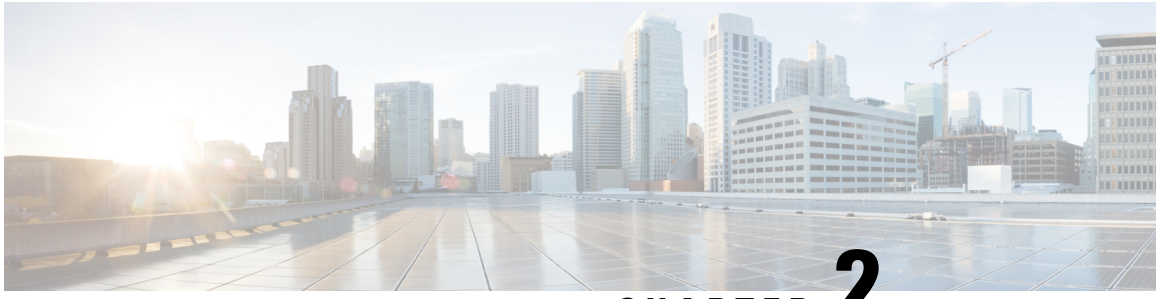
Step 22 Reboot all servers.

Where to Find More Information

Related Cisco Documentation

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

- *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*.
- *Cisco Unified Communications Operating System Administration Guide*
- *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.
- *Disaster Recovery System Administration Guide*
- *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 31
- HTTPS for Cisco Unified IP Phone Services, on page 33
- Save Certificate to Trusted Folder Using Internet Explorer 8, on page 36
- First-Time Authentication for Firefox with HTTPS, on page 38
- First-Time Authentication for Safari with HTTPS, on page 40
- Where to Find More Information About HTTPS Setup, on page 42

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 *Cisco Unified Communications Operating System Administration Guide* for more information.

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

Table 6: 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, 7970, 7971, 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 "Cisco Unified IP Phone Services Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*

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 7: 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.**

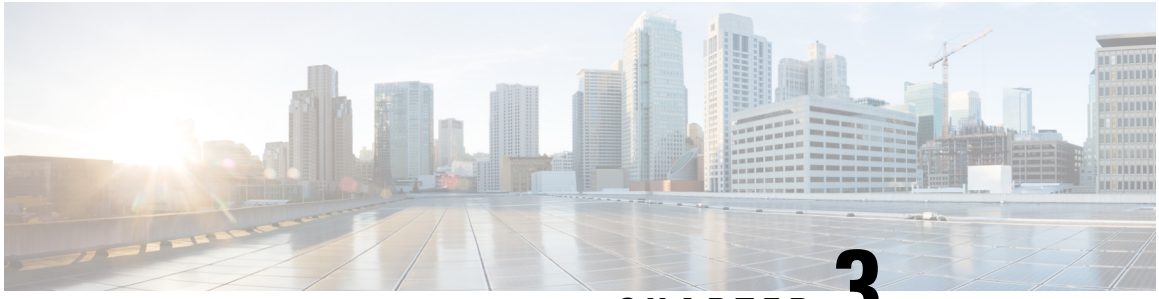
Step 8 Your file and settings display. Click **Finish**.

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*
- *Cisco Unified Communications Manager Administration Guide*
- 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 43
- Trust Verification Service, on page 43
- Initial Trust List, on page 44
- Update ITL File for IP Phones, on page 45
- Autoregistration, on page 46
- Obtain Cisco Unified IP Phone Support List, on page 46
- Certificate Regeneration, on page 46
- Tomcat Certificate Regeneration, on page 48
- System Back-Up Procedure After TFTP Certificate Regeneration, on page 48
- Refresh Upgrade From Cisco Unified Communications Manager Release 7.x to Release 8.6 Or Later, on page 49
- Roll Back Cluster to a Pre-8.0 Release, on page 50
- Migrate IP Phones Between Clusters with Cisco Unified Communications Manager and ITL Files, on page 52
- Perform Bulk Reset of ITL File, on page 53

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

Trust Verification Service (TVS) is the main component of SBD. TVS enables Cisco Unified IP Phones to authenticate application servers, such as EM services, directory, and MIDlet, during HTTPS establishment.

TVS provides the following features:

- Scalability— Cisco 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 do not require user intervention.

Note When you enable secure signaling and media, you must create a CTL file and set the cluster to mixed mode. You can use the CLI command **utils ctl set-cluster mixed-mode** to create the CTL file and change the security mode in one step.

TVS Description

The following basic concepts describe the Trust Verification Service:

- TVS runs on Unified Communications Manager server and authenticates certificates on behalf of the Cisco IP Phone.
- Instead of downloading all the trusted certificates, Cisco IP Phone only need to trust TVS.
- The TVS certificates and a few key certificates are bundled in a new file, that is the Initial Trust List file (ITL).
- The ITL file gets generated automatically without user intervention.
- The ITL file gets downloaded by Cisco IP Phones and trust flows from there.

Initial Trust List

ITL 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 gets 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 IP Phones download the ITL file during a boot up time or during a reset, 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 are available in 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 is not 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 look up 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 TFTP+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.

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 IP Phones

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

Note 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 versions 8.6 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 the "Roll Back Cluster to a Pre-8.0 Release" section in the *Cisco Unified Communications Manager Security Guide*.

Autoregistration

If the cluster is in nonsecure mode, the system supports autoregistration. 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.

Note In mixed mode, the system does not support autoregistration.

Obtain Cisco Unified IP Phone Support List

You can obtain a list of the Cisco IP Phones that support security by default by using Cisco Unified Reporting. To use Cisco Unified Reporting, follow this procedure:

Procedure

Step 1 From the Cisco Unified Reporting main window, click **System Reports**.

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

Step 3 Choose the appropriate feature from the **Feature** drop-down list.

Step 4 Click **Submit.**

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 *Cisco Unified Communications Operating System Administration Guide*.

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.

Procedure

Step 1 Regenerate the CAPF certificate.

See Chapter 6, "Security", in the *Cisco Unified Communications Operating System Administration Guide*.

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

See Chapter 4, "Configuring the Cisco CTL Client", in the *Cisco Unified Communications Operating System Administration Guide*.

Step 3 Restart the CAPF service.

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

Regenerate TVS Certificate

No manual steps are required to regenerate a 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.

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.

Procedure

Step 1 Regenerate the TFTP certificate.

See Chapter 6, “Security,” in the *Cisco Unified Communications Operating System Administration Guide*.

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, run the CTL client.

See Chapter 4, “Configuring the CTL Client,”.

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

See Chapter 6, “Security,” in the *Cisco Unified Communications Operating System Administration Guide*.

Tomcat Certificate Regeneration

To regenerate the CAPF certificate, perform the following steps:

Procedure

Step 1 Regenerate the Tomcat certificate.

See Chapter 6, “Security”, in the *Cisco Unified Communications Operating System Administration Guide*.

Step 2 Restart the Tomcat service.

See Chapter 6, “Security”, in the *Cisco Unified Communications Operating System Administration Guide*.

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

See Chapter 6, “Security,” in the *Cisco Unified Communications Operating System Administration Guide*.

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 8.0, 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 Disaster Recovery System Administration Guide.

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 Chapter 7, "Software Upgrades," in the *Cisco Unified Communications Operating System Administration Guide*.

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 *Disaster Recovery System Administration Guide*.

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 Administration, 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 Chapter 7, “Software Upgrades” in the *Cisco Unified Communications Operating System Administration Guide*.

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 ManagerRelease 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 *Cisco Unified Communications Operating System Administration Guide*.

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.

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.

Perform Bulk Reset of ITL File

When devices on a Unified Communications Manager cluster are locked and lose their trusted status, perform a bulk reset of the Identity Trust List (ITL) file with the CLI command **utils itl reset**. This command generates a new ITL recovery file.

Tip Whenever you perform a fresh installation of Unified Communications Manager, export the ITL key as soon as possible and perform a backup through the Disaster Recovery System.

The CLI command to export the ITL recovery pair is as follows:

file get tftp *ITLRecovery.p12*

You will be prompted to enter the SFTP server (where the key will be exported) and password.

Before you begin

Make sure that you perform this procedure on the Unified Communications Manager publisher.

If needed, export the key from the publisher.

Procedure

Step 1 Perform one of the following steps:

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

For **utils itl reset localkey**, the local key resides on the publisher. This step generates a new ITL file by taking the existing file on the system and replacing the signature of that file with the recovery key signature. The key is then copied to the TFTP servers in the cluster.

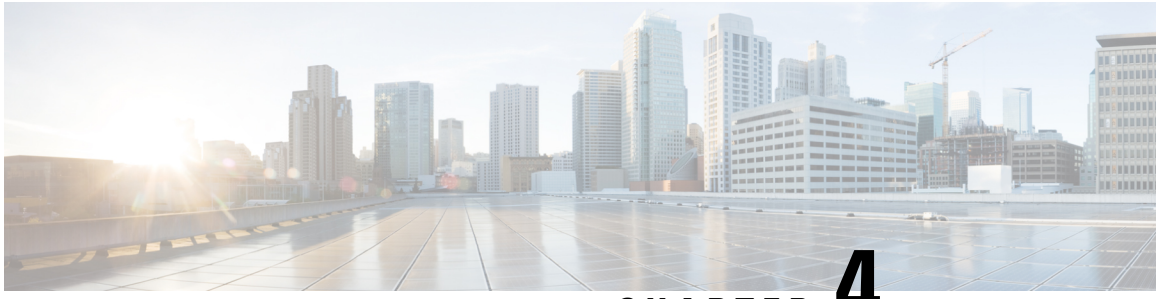
Step 2 Run **show itl** to verify that the reset was successful.

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

Step 4 Click **Reset**.

Step 5 Restart the TFTP service and restart all devices.

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



CHAPTER 4

Cisco CTL Client Setup

This chapter provides information about Cisco CTL client setup.

- About Cisco CTL Setup, on page 55
- Activate Cisco CTL Provider Service, on page 56
- Cisco CAPF Service Activation, on page 57
- Set up Secure Ports, on page 57
- Set Up Cisco CTL Client, on page 58
- Update CTL File, on page 59
- Update Cisco Unified Communications Manager Security Mode, on page 60
- Cisco CTL File Details, on page 61
- Verify Cisco Unified Communications Manager Security Mode, on page 62
- Set Up Smart Card Service to Started or Automatic, on page 62
- Verify or Uninstall Cisco CTL Client, on page 63

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).

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

- System Administrator Security Token (SAST)
- Cisco CallManager and Cisco TFTP 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.

After you create the CTL file, you must restart the Cisco CallManager and Cisco TFTP services in Cisco Unified Serviceability on all nodes that run these services. 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 CallManager 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.

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 certificates to the CTL file. The service then transports the CTL file to all Unified Communications Manager and Cisco TFTP 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 Cisco CTL 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 **Cisco CTL 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 Cisco CTL 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 Cisco CallManager 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 58 through Step 6, on page 58.

b) To change the Ethernet Phone Port or SIP Phone Secure Port settings, perform Step 7, on page 58 through Step 11, on page 58.

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 Cisco CTL 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.

Step 6 Click **Save.**

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

Step 8 Find a server where the Cisco CallManager service runs, as described in the *Cisco Unified Communications Manager Administration Guide*; 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 Cisco CallManager 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.*

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 mainten
you must restart the TFTP services and then the CallMan
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.

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.

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 8: 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. **Note** Unified Communications Manager disables auto-registration if you configure mixed mode.
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. You can use auto-registration in this mode.
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.

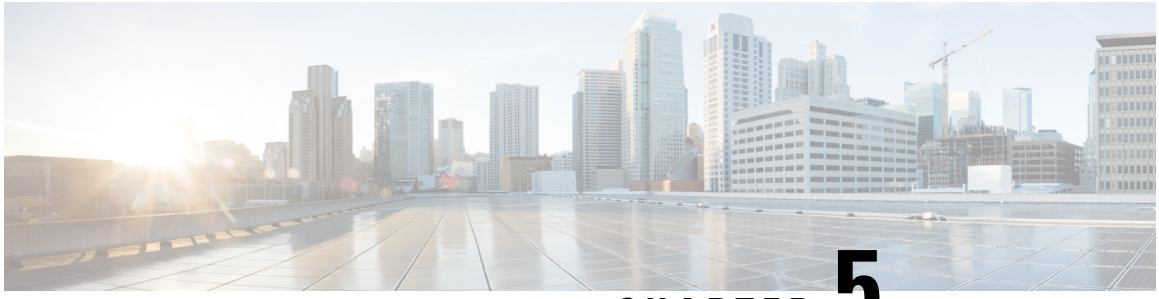
To verify that the Cisco CTL Client installed, perform the following procedure:

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

Certificate Setup

This chapter provides information about certificate setup.

- About Certificate Setup, on page 65
- Find Certificate, on page 65
- Certificate Settings, on page 66

About Certificate Setup

Use the Certificate Configuration window to view the certificates on your system. All fields on the Certificate Configuration window are read-only, except Duration in Cache.

Find Certificate

To find a certificate, perform the following procedure:

Procedure

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

The **Find and List Certificates** 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 66.

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.

Certificate Settings

All fields on the Certificate Management window are read-only, except Duration in Cache.

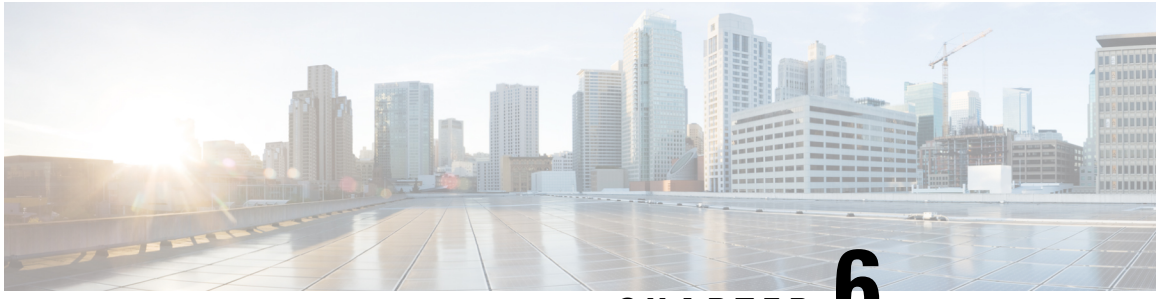
Table 9: VPN Profile Configuration Settings

Field	Definition
Subject Name (read only)	Displays the subject name for the certificate.
Issuer Name (read only)	Displays the issuer name for the certificate.
Serial Number (read only)	Displays the serial number (MAC address).
IPv4 Address (read only)	Displays the IPv4 address.
IPv6 Address (read only)	Displays the IPv6 address.
Duration in Cache	Enter the time, in hours, that the certificate can persist in the phone cache. A value of zero indicates that the certificate does not get cached. Leave blank to accept the system default value. Maximum: 720 hours
Selected Roles	Displays the roles currently associated with the certificate.
Selected Services	Displays the services currently associated with the certificate.

PART II

Security for Cisco IP Phone and Cisco Voice-Messaging Ports

- Phone Security, on page 69
- Phone Security Profile Setup, on page 75
- Secure and Nonsecure Indication Tone Setup, on page 89
- Encryption to Analog Endpoint Setup, on page 93
- Certificate Authority Proxy Function, on page 95
- Encrypted Phone Configuration File Setup, on page 109
- Digest Authentication for SIP Phones Setup, on page 119
- Phone Hardening, on page 123
- Secure Conference Resources Setup, on page 127
- Voice-Messaging Ports Security Setup, on page 139
- Call Secure Status Policy, on page 143
- Secure Call Monitoring and Recording Setup, on page 145



CHAPTER 6

Phone Security

This chapter provides information about phone security.

- Phone Security Overview, on page 69
- Trusted Devices, on page 70
- Phone Model Support, on page 71
- Preferred Vendor SIP Phone Security Set Up, on page 71
- View Phone Security Settings, on page 73
- Set Up Phone Security, on page 73
- Phone Security Interactions and Restrictions, on page 74
- Where to Find More Information About Phone Security, on page 74

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 consider 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 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 box, 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 box, 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 box, choose **Encrypted** or **Authenticated**.

Step 6 In the Transport type drop-down list box, 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 box, 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, refer to the *Cisco IP Phone Administration Guide* that supports your phone model.

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

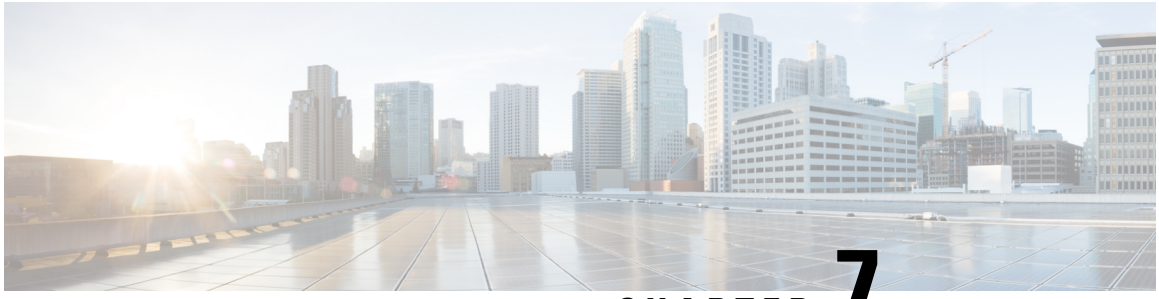
This section provides the interaction and restriction on Phone Security.

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

- *Cisco IP Phone Administration Guide* for your phone model
- *Troubleshooting Guide for Cisco Unified Communications Manager*



CHAPTER 7

Phone Security Profile Setup

This chapter provides information about security profile setup.

- Phone Security Profile Overview, on page 75
- Phone Security Profile Setup Prerequisites, on page 75
- Find Phone Security Profile, on page 76
- Set Up Phone Security Profile, on page 77
- Phone Security Profile Settings, on page 77
- Apply Security Profiles to Phone , on page 86
- Synchronize Phone Security Profile with Phones, on page 87
- Delete Phone Security Profile, on page 87
- Find Phones with Phone Security Profiles, on page 88

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 In Unified Communications Manager Administration, choose **System** > **Security Profile** > **Phone Security Profile**.

The **Find and List Phone 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 77.

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 Phone 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 > Phone Security Profile**.

Step 2 Perform one of the following tasks:

a) To add a new profile, click **Add New**.
The Phone Security Profile Configuration page appears.

b) To copy an existing security profile, locate the appropriate profile, click the **Copy** button 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 with the copied settings.

Step 3 Enter the appropriate settings for phones that are running SCCP or for phones that are running 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 10: 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 box 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 box, 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 Communication 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` **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. Medium- AES-256 AES-128 only: 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` **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.

Setting	Description
	Medium- AES-256 AES-128 only: 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` **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`
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. Cisco strongly recommends 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 Size	For this setting that is used for CAPF, choose the key size for the certificate from the drop-down list box. 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.

The following table describes the settings for the security profile for the phone that is running SIP.

Table 11: 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 box 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 box, 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**
Transport Type	When Device Security Mode is **Non Secure**, choose one of the following options from the drop-down list box (some options may not display): • **TCP**—Choose the Transmission Control Protocol to ensure that packets get received in the same order as the order in which they are sent. This protocol ensures that no packets get dropped, but the protocol does not provide any security. • **UDP**—Choose the User Datagram Protocol to ensure that packets are received quickly. This protocol, which can drop packets, does not ensure that packets are received in the order in which they are sent. This protocol does not provide any security. • **TCP + UDP**—Choose this option if you want to use a combination of TCP and UDP. This option does not provide any security. When Device Security Mode is **Authenticated** or **Encrypted**, TLS specifies the Transport Type. TLS provides signaling integrity, device authentication, and signaling encryption (encrypted mode only) for SIP phones. If Device Security Mode cannot be configured in the profile, the transport type specifies UDP.
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** Cisco recommends that you enable this option and configure a symmetric key to secure digest credentials and administrative passwords.

Setting	Description
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).
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 box, 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; Cisco strongly recommends 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 box. 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 IP Phones (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 begin

Before you apply a security profile that uses certificates for authentication of the phone, make sure that 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.

If the phone does not contain a certificate, perform the following steps:

1. In the **Phone Configuration** window, apply a non-secure profile.
2. In the **Phone Configuration** window, install a certificate by configuring the CAPF settings.
3. 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 From Cisco Unified CM Administration, choose **Device** > **Phone**.
The **Find and List Phones** window is displayed.

Step 2 Click **Find**.
A list of configured phones on the Unified Communications Manager is displayed.

Step 3 Choose the phone to which you want to apply the secure profile.
The **Phone Configuration** window is displayed.

Step 4 Go to the **Protocol Specific Information** section in the **Phone Configuration** window.

Step 5 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 6 Click **Save**.

Step 7 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 check box in the **Find and List** window, and click **Delete Selected**.

Synchronize Phone Security Profile with Phones

To synchronize phones with a phone security profile after configuration updates, perform the following procedure:

Procedure

Step 1 Choose **System** > **Security Profile** > **Phone Security Profile**.
The **Find and List Phone Security Profiles** window appears.

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.
The **Phone Security Profile Configuration** window appears.

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

This section describes how to delete a phone 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 **Security Profile Configuration** window 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, refer to the *Cisco Unified Communications Manager System Guide.*

Procedure

Step 1 Find the security profile to delete.

Step 2 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 3 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 4 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 In Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 From the first drop-down list box, choose the search parameter **Security Profile**.

a) From the drop-down list box, choose a search pattern.

b) 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.

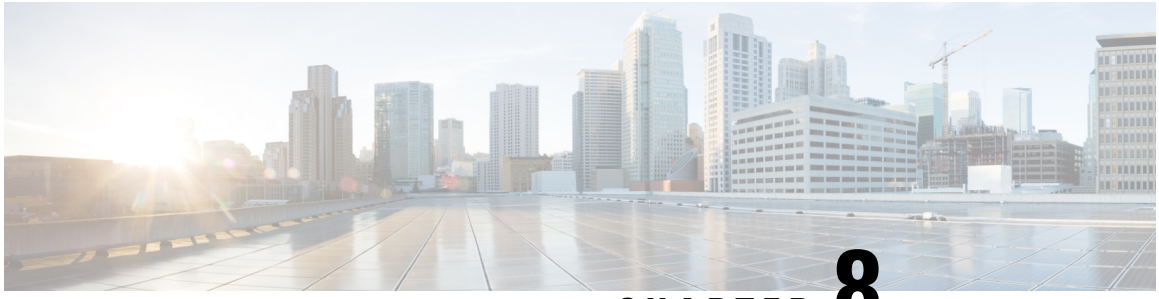
Step 3 Click **Find**.

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.



CHAPTER 8

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 89
- Secure and Non-Secure Indication Tone Tips, on page 90
- Secure and Non-Secure Indication Tone Configuration Tasks , on page 91

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**).

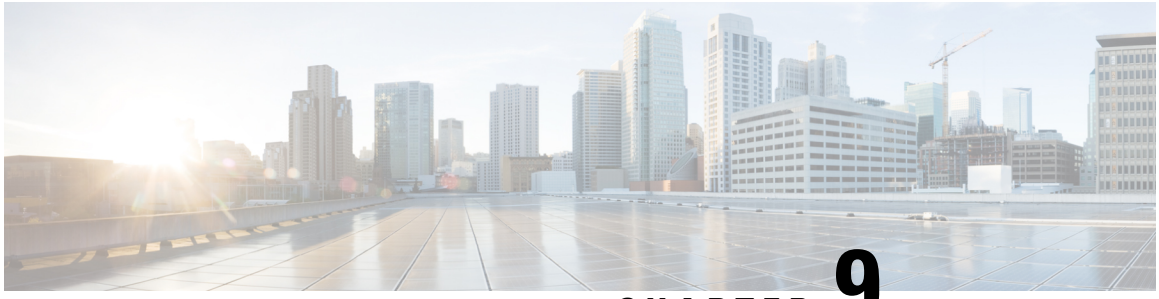
- Go to the **Directory Number Configuration** window that displays when you add a directory number from the **Phone Configuration** window. In the **Multiple Call/Call Waiting Settings on Device**

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 9

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 93
- Certificate Management for Secure Analog Phones, on page 93

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 *Cisco Unified Communications Operating System Administration Guide*.

CHAPTER 10

Certificate Authority Proxy Function

This chapter provides information about the certificate authority proxy function.

- About Certificate Authority Proxy Function, on page 95
- Cisco IP Phone and CAPF Interaction, on page 96
- CAPF Interaction with IPv6 Addressing, on page 97
- CAPF System Interactions and Requirements, on page 100
- CAPF in Cisco Unified Serviceability Setup, on page 101
- Set Up CAPF, on page 101
- Activate Certificate Authority Proxy Function Service, on page 101
- Update CAPF Service Parameters, on page 102
- Generate and Import Third Party CA-Signed LSCs, on page 102
- Install, Upgrade, Troubleshoot, or Delete Certificates From Phone Using CAPF, on page 103
- CAPF Settings, on page 104
- Find Phones by LSC Status or Authentication String, on page 105
- Generate CAPF Report, on page 106
- Enter Phone Authentication String, on page 107
- Verify Phone Authentication String, on page 107

About Certificate Authority Proxy Function

Certificate Authority Proxy Function (CAPF), which automatically installs with Cisco Unified Communications Manager, performs the following tasks, depending on your configuration:

- Authenticate via an existing Manufacturing Installed Certificate (MIC), Locally Significant Certificate (LSC), randomly generated authentication string, or optional less secure “null” authentication.
- Issues locally significant certificates to supported Cisco IP Phones.
- Upgrades existing locally significant certificates on the phones.
- Retrieves phone certificates for viewing and troubleshooting.

During installation, a certificate that is specific for CAPF gets generated. This CAPF certificate, which the Cisco CTL Client copies to all Cisco Unified Communications Manager servers in the cluster, uses the .0 extension.

Cisco IP Phone and CAPF Interaction

When the phone interacts with CAPF, the phone authenticates itself to CAPF by using an authentication string, existing MIC or LSC certificate, or "null," generates its public key and private key pair, and then forwards its public key to the CAPF server in a signed message. The private key remains in the phone and never gets exposed externally. CAPF signs the phone certificate and then sends the certificate back to the phone in a signed message.

Beginning from Cisco Unified Communications Manager Release 11.5(1) SU1, all the LSC certificates issued by CAPF service are signed with SHA-256 algorithm. Therefore, Cisco IP Phones 6900, 7800, 7900, 8800, 8900, and 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 We recommend to use the Cisco Unified Communications Manager prior to 11.5(1) SU1 release. If you use phone the models, which are in End of Software Maintenance or End of Life.

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.

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

Tip Key generation, which is set at low priority, allows the phone to function while the action occurs. You may notice that key generation takes up to 30 or more minutes to complete.

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.

Consider the following information about how CAPF interacts with the Cisco Unified IP Phone 7960G and 7940G when the phone is reset by a user or by Cisco 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 Cisco 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 Cisco 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 12: How IPv6 or IPv4 Phone Connects to CAPF

IP Mode of Phone	IP Addresses on Phone	CAPF IP Address	How Phone Connects to CAPF
Dual-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.
Dual-stack	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.

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

Table 13: 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.
IPv4 stack	IPv4	IPv4, IPv6	Phone uses an IPv4 address to connect to CAPF.
	IPv6	IPv4, 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	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.

CAPF System Interactions and Requirements

The following requirements exist for CAPF:

- Before you use CAPF, ensure that you performed all necessary tasks to install and configure the Cisco CTL Client. To use CAPF, you must activate the Cisco Certificate Authority Proxy Function service on the first node.
- During a certificate upgrade or install operation, if By Authentication String is the 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.
- Cisco strongly recommends that you use CAPF during a scheduled maintenance window because generating many certificates at the same time may cause call-processing interruptions.
- Ensure that the first node is functional and running during the entire certificate operation.
- Ensure that the phone is functional during the entire certificate operation.
- If a secure phone gets moved to another cluster, the Cisco 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.

Tip Cisco IP Telephony Backup and Restore System (BARS) backs up the CAPF data and reports because Cisco Unified Communications Manager stores the information in the Cisco Unified Communications Manager database.

CAPF in Cisco Unified Serviceability Setup

You perform the following tasks in Cisco Unified Serviceability:

- Activate the Cisco Certificate Authority Proxy Function service.
- Configure trace settings for CAPF.

Refer to the *Cisco Unified Serviceability Administration Guide*s for more information.

Set Up CAPF

Perform the following tasks to install, upgrade, or troubleshoot locally significant certificates.

Procedure

Step 1 Determine whether a locally significant certificate exists in the phone.

Determine whether you need to copy CAPF data to the Unified Communications Manager publisher database server. For more information, see the *Cisco IP Phone Administration Guide* for your phone model.

.

Tip If you used the CAPF utility with Unified Communications Manager 4.0 and verified that the CAPF data exists in the Unified Communications Manager database, you can delete the CAPF utility that you used with Unified Communications Manager 4.0.

Step 2 Verify that the Cisco Certificate Authority Proxy Function service is running.

Tip This service must run during all CAPF operations. It must also run for the Cisco CTL Client to include the CAPF certificate in the CTL file.

Step 3 Verify that you performed all necessary tasks to install and configure the Cisco CTL Client. Ensure that the CAPF certificate exists in the Cisco CTL file.

Step 4 If necessary, update CAPF service parameters.

Step 5 To install, upgrade, or troubleshoot locally significant certificates in the phone, use Unified Communications Manager Administration.

Step 6 If it is required for certificate operations, enter the authentication string on the phone.

Activate Certificate Authority Proxy Function Service

Cisco Unified Communications Manager does not automatically activate the Certificate Authority Proxy Function service in Cisco Unified Serviceability.

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

To activate the service, perform the following procedure:

Procedure

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

Step 2 From the **Servers** drop-down list box, choose the server on which you want to activate the Certificate Authority Proxy Function service.

Step 3 Check the **Certificate Authority Proxy Function** check box.

Step 4 Click **Save**.

Update CAPF Service Parameters

The CAPF Service Parameter window provides information on the number of years that the certificate is valid, the maximum number of times that the system retries to generate the key, and so on.

For the CAPF service parameters to show Active status in Cisco Unified Communications Manager Administration, you must activate the Certificate Authority Proxy Function service.

To update the CAPF service parameters, perform the following procedure:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list box, choose the server.

Tip You must choose the first node in the cluster.

Step 3 From the **Service** drop-down list box, choose the **Cisco Certificate Authority Proxy Function** service.

Step 4 Update the CAPF service parameters, as described in help that displays for the parameter.

Note To display help for the CAPF service parameters, click the question mark or the parameter name links.

Step 5 For the changes to take effect, restart the Cisco Certificate Authority Proxy Function service.

Generate and Import Third Party CA-Signed LSCs

CAPF LSCs are locally signed. However, you may require phones to use third party CA signed LSCs.

Note Perform Steps 1 and 2 once and repeat the remaining steps until you configure all require phone LSC operations.

Procedure

Step 1 Import the third party CA certificate into the Unified Communications Manager trust store.

Step 2 Follow these steps to configure the service parameter Certificate Issuer to Endpoint:

a) In Cisco Unified CM Administration, select **System** > **Service Parameter**.
b) Select your Unified Communications Manager server frop the drop-down list box.
c) Under the service drop-down list box, select **Cisco Certificate Authority Proxy Function**.
d) For the service parameter Certificate Issuer to Endpoint, select **Offline CA**.

Step 3 Check CSR generation progress. After the phones reregister, use the CLI command **utils capf csr count**to check whether the CSRs are generated.

Step 4 Dump the CSRs to the desired location (local directory or remote directory through FTP or TFTP) by using the CLI command **utils capf csr dump**.
The CLI tars and zip the CSRs into a single file (`.tgz`) before uploading.

Step 5 When all the signed certificates are provided by the CA, you need to tar and zip all the certificates into a single file using the Linux command **`tar cvzf <filename.tgz> *.der`**.

Step 6 Use the CLI command **utils capf cert import** to import the certificates into Unified Communications Manager.

Note The imported certificate must be in DER format, and they must be tarred in a flat file structure.

The CLI command untars the file, and parses and verifies each certificate. If the certificates are valid, they are sent to the phones, and the corresponding CSR is deleted.

What to do next

To remove all the CSRs and certificates that were previously built and imported, you can use the command **utils capf csr delete**.

Install, Upgrade, Troubleshoot, or Delete Certificates From Phone Using CAPF

Perform the following procedure to use the Certificate Authority Proxy Function:

Procedure

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

Step 2 After the search results display, locate the phone where you want to install, upgrade, delete, or troubleshoot the certificate and click the **Device Name (Line)** link for that phone.

Step 3 Enter the configuration settings, as described in Table 14: CAPF Configuration Settings, on page 104.

Step 4 Click **Save**.

Step 5 Click **Reset**.

CAPF Settings

The following table describes the CAPF settings in the **Phone Configuration** window in Cisco Unified Communications Manager Administration.

Table 14: CAPF Configuration Settings

Setting	Description
Certificate Operation	From the drop-down list box, 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 in the phone. • **Delete**—Deletes the locally significant certificate that exists in the phone. • **Troubleshoot**—Retrieves the locally significant certificate (LSC) or the manufacture-installed certificate (MIC), so you can view the certificate credentials in the CAPF trace file. If both certificate types exist in the phone, Cisco Unified Communications Manager creates two trace files, one for each certificate type. **Tip** By choosing the Troubleshoot option, you can verify that an LSC or MIC exists in the phone. The Delete and Troubleshoot options do not display if a certificate does not exist in the phone.
Authentication String	If you chose the By Authentication String option, this field applies. Manually enter a string or generate a string by clicking the Generate String button. Ensure that the string contains 4 to 10 digits. To install, upgrade, or troubleshoot a locally significant certificate, the phone user or administrator must enter the authentication string on the phone.
Generate String	If you want CAPF to automatically generate an authentication string, click this button. The 4- to 10-digit authentication string displays in the Authentication String field.

Setting	Description
Operation Completes by	This field, which supports all certificate operation options, specifies the date and time by which you must complete the operation. The values that display apply for the first node.
Operation Status	This field displays the progress of the certificate operation; for example, <operation type> pending, failed, or successful, where operating type equals the Install/Upgrade, Delete, or Troubleshoot certificate operation options. You cannot change the information that displays in this field.

Find Phones by LSC Status or Authentication String

To find phones on the basis of certificate operation status or the authentication string, perform the following procedure:

Procedure

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

The Find and List window displays. Records from an active (prior) query may also display in the window.

Step 2 From the first drop-down list box, choose one of the following options:

a) **LSC Status**— Choosing this option returns a list of phones that use CAPF to install, upgrade, delete, or troubleshoot locally significant certificates.

b) **LSC Expires**- Choosing this option returns a list of phones based on the specified lsc expiration search criteria.

c) **LSC Issued by** - Choosing this option returns a list of phones based on the specified lsc issued by search criteria.

d) **LSC Issuer Expires by** - Choosing this option returns a list of phones based on the specified lsc issuer expires by search criteria.

e) **Authentication String**—Choosing this option returns a list of phones with an authentication string that is specified in the Authentication String field.

Step 3 From the second drop-down list box, choose a search pattern.

Step 4 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 5 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 6 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.

Generate CAPF Report

If you want to do so, you can generate a CAPF report to view the status of the certificate operation, the authentication string, security profile, authentication mode, and so on. The report includes information such as device name, device description, security profile, authentication string, authentication mode, LSC status, and so on.

To generate a CAPF report, perform the following procedure:

Procedure

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

The **Find/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 106.

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 In the Related Links drop-down list box, choose **CAPF Report in File**; then, click **Go**.

Step 5 Save the file to a location that you will remember.

Step 6 Use Microsoft Excel to open the .csv file.

Enter Phone Authentication String

If you chose the By Authentication String mode and generated an authentication string, you must enter the authentication string on the phone to install the locally significant certificate.

Tip The authentication string applies for one-time use only. Obtain the authentication string that displays in the **Phone Configuration** window or in the CAPF report.

Before you begin

Before you enter the authentication string on the phone, verify that the following conditions are met:

- The CAPF certificate exists in the CTL file.
- You activated the Cisco Certificate Authority Proxy Function service.
- The first node functions and runs. Ensure that the server runs for each certificate installation.
- The device has registered.
- A signed image exists on the phone; refer to the Cisco IP Phone Administration Guide.

Procedure

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

Step 2 If the configuration is locked, press ****#** (asterisk, asterisk, pound sign) to unlock it.

Step 3 Scroll down the **Settings** menu. Highlight “Security Configuration” and press the **Select** softkey.

Step 4 Scroll down the **Security Configuration** menu. Highlight “LSC” and press the **Update** softkey.

Step 5 When prompted for the authentication string, enter the string that the system provides and press the **Submit** softkey.

The phone installs, updates, deletes, or fetches the certificate, depending on the current CAPF configuration.

You can monitor the progress of the certificate operation by viewing the messages that display on the phone. After you press **Submit**, the message “Pending” displays under the LSC option. The phone generates the public and private key pair and displays the information on the phone. When the phone successfully completes the process, the phone displays a successful message. If the phone displays a failure message, you entered the wrong authentication string or did not enable the phone for upgrade.

You can stop the process by choosing the Stop option at any time.

Verify Phone Authentication String

You can verify that the certificate is installed on the phone by pressing the **Applications** button and selecting the **Model Information** menu.

CHAPTER 11

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.

- Encryption for Phone Configuration File Overview, on page 109
- Phone Models That Support Encryption, on page 111
- Encryption for Phone Configuration File Tips, on page 112
- Set Up Encryption Configuration File, on page 113
- Enable Phone Configuration File Encryption, on page 114
- Set Up Manual Key Distribution, on page 114
- Manual Key Distribution Settings, on page 115
- Enter Phone Symmetric Key, on page 115
- Verify LSC or MIC Certificate Installation, on page 116
- Disable Encryption for Phone Configuration File, on page 117
- Exclude Digest Credentials From Phone Configuration File Download, on page 117

Encryption for Phone Configuration File Overview

The TFTP configuration file contains confidential information such as username, password, IP addresses, port details, phone SSH credentials, WLAN sensitive data, and so on. By default, the confidential information is available in cleartext. We recommend that you encrypt the TFTP configuration file, to protect your data.

To encrypt the TFTP configuration file, navigate to Cisco Unified CM Administration, choose **System** > **Security** > **Phone Security Profile** and check the **TFTP Encrypted Config** check box.

After you enable the TFTP Encrypt Config option, configure the required parameters in Unified Communications Manager Administration and the phone, and then restart the required services in Cisco Unified Serviceability, the TFTP server:

1. Deletes all the plaintext configuration files on disk
2. Generates encrypted versions of the configuration files

If the phone supports encrypted phone configuration files and if you have performed the necessary tasks for phone configuration file encryption, the phone requests an encrypted version of the configuration file.

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.

Some phones do not 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 does not 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.

To ensure that you maintain the privacy of the key information, Cisco strongly recommends 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 parameter in Unified Communications Manager 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 111.

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

Phone Model and Protocol	Encryption Method
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.
Cisco Unified IP Phone 6901, 6911, 6921, 6941, 6945, and 6961 Cisco Unified IP Phone 7970G, 7971G, 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 7971G-GE, 7961G-GE, 7941G-GE Cisco Unified IP Phone 7931G, 7921G, (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: AES 128Key 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).

Encryption for Phone Configuration File Tips

We recommend that you enable the TFTP Encrypted Config flag to secure confidential data in phone downloads. For phones that do not 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 Config flag is set, the phone cannot register.

Consider the following information when you configure encrypted configuration files in Unified Communications Manager Administration:

- Only phones that support encrypted configuration files display the TFTP Encrypted Config flag in the phone security profile. You cannot configure encrypted configuration files for Cisco Unified IP Phones

7800, 7942, and 7962 (SCCP only) because these phones do not receive confidential data in the configuration file download.

- The default setting for TFTP Encrypted Config is False (unchecked). If you apply the default setting, the non-secure profile to the phone, the digest credentials and secured passwords are sent in the clear.
- For Cisco 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 do not recommend that you use this method.
- For Cisco Unified IP Phones 7800, 7942, and 7962 (SIP only), Unified Communications Manager Administration 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 does not 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 keep the TFTP file encryption setting disabled and enable the Exclude Digest Credential in Configuration File flag on the security profile window, which will exclude digest credentials from future downloads.

After digest credentials exist in these phones and an incoming file does not 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 Credentials flag on the corresponding security profile window to download the new digest credentials to the phone.

Set Up Encryption Configuration File

The following procedure provides the tasks used to configure encrypted configuration files inUnified Communications Manager Administration.

Procedure

Step 1 Verify that the Cluster Security Mode is configured for Mixed Mode.

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

Step 2 Check the **TFTP Encrypted Config** check box in the Phone Security Profile. Be sure to apply the profile to the phone.

Step 3 Determine which phones support manual key distribution and which phones support symmetric key encryption with phone public key (PKI encryption).

Step 4 If your phone supports manual key distribution, perform the manual key distribution tasks.

Step 5 If your phone supports manual key distribution, enter the symmetric key on the phone; reset the phone.

Step 6 If your phone supports the method, symmetric key encryption with phone public key (PKI encryption), verify that a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone.

Enable Phone Configuration File Encryption

The TFTP server queries the database when it builds the configuration file. If the phone security profile that is applied to the phone has the TFTP encrypted configuration flag set, the TFTP server builds an encrypted configuration file.

Procedure

Step 1 Find the appropriate device security profile for the phone to access the TFTP encryption flag.

Step 2 Check the **TFTP Encrypted Config** check box to enable configuration file encryption.

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 Choose the phone and click **Next**.

Step 4 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 5 Click **Save**.

Step 6 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 15: 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

Follow this procedure to enter the symmetric key on the phone after you configure manual key distribution in Unified Communications Manager Administration.

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

This procedure applies to Cisco Unified IP Phones that use PKI encryption. To determine, if your phone supports PKI encryption, see Phone Models Supporting Encrypted Configuration File section.

Before you begin

The following procedure assumes that:

- The phone exists in Unified Communications Manager database
- You have enabled the TFTP Encrypted Config parameter in Unified Communications Manager Administration

Procedure

Step 1 Verify that a Manufacture-Installed Certificate (MIC) or a Locally Significant Certificate (LSC) exists in the phone.

Tip Choose the **Troubleshoot** option in the CAPF settings section of the Phone Configuration window, to verify whether an LSC or MIC exists in the phone in Unified Communications Manager. The Delete and Troubleshoot options do not display if a certificate does not 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, refer to the Cisco Unified IP Phone administration guides for Cisco Unified IP Phones that support this version of Unified Communications Manager.

Step 2 If a certificate does not 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 3 After you configure the CAPF settings, click **Save**.

Step 4 In the **Phone Configuration** window, click **Reset**. The phone requests an encrypted configuration file from the TFTP server after the phone resets.

Disable Encryption for Phone Configuration File

To disable encryption for the phone configuration files, you must uncheck the TFTP Encrypted Config check box in the phone security profile in Unified Communications Manager Administration and save your change.

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 Manager database.

Cisco Unified IP Phones 7911G, 7931G (SCCP only), 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7971G, 7971G-GE, and 7975G request an encrypted file (.enc.sgn file) when the encrypted configuration setting gets updated to false, the phone requests an unencrypted, signed file (.sgn file).

If Cisco Unified IP Phones that are running SCCP: 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7921G, 7925G, 7925G-EX, 7926G, 7931G, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7971G, 7971G-GE, 7975G, 8941, 8945 and Cisco Unified IP Phones that are running SIP: 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7941G, 7941G-GE, 7942G, 7961G, 7961G-GE,7962G, 7965G, 7970G, 7971G, 7971G-GE, 7975G, 8941, 8945, 8961, 9971, 7811, 78321, 7841, 7861, 7832, 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NE, 8821, 8831, 8832, 8832NR. Request an encrypted file when the encryption configuration setting gets updated to False, 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.

Tip 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 GUI to disable encryption. For Cisco Unified IP Phones (SIP only), delete the symmetric key at the phone GUI to disable encryption. For information on how to perform these tasks, refer to 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 12

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 *Cisco Unified Communications Manager Administration Guide*.

- Set up SIP Phone Digest Authentication, on page 119
- Set Up Digest Authentication Service Parameters, on page 120
- Set Up End User Digest Credentials, on page 120
- End User Digest Credential Settings, on page 121
- Set Up Digest User Using Phone, on page 121

Set up SIP Phone Digest Authentication

The following procedure provides the tasks used to configure digest authentication for phones that are running SIP.

Procedure

Step 1 Configure the security profiles for phones that are running SIP; make sure that you check the **Enable Digest Authentication** check box.

Step 2 Apply a security profile to the phone that is running SIP.

Step 3 If you want to update the default setting, configure service parameters that are related to digest authentication; for example, configure the SIP Station Realm service parameter.

Step 4 Configure the digest credentials in the **End User Configuration** window.

Step 5 Choose the **Digest User** in the **Phone Configuration** window.

Choosing a digest user for these phones that are running SIP ensures that the digest credentials get included in the phone configuration file.

Step 6 On Cisco Unified IP Phones 7942 or 7962 (SIP only), enter the digest credentials that you configured in the **End User Configuration** window.

For information on how to enter the authentication name and password on the phone, refer to the *Cisco Unified IP Phone Administrator Guide* for your phone.

Set Up Digest Authentication Service Parameters

You configure the SIP Realm for challenges to phones with the service parameter SIP Station Realm. At installation, Unified Communications Manager provides a default setting, ccmsipline. For additional information on the parameter, click the question mark or the parameter name link that displays in the **Service Parameter Configuration** window.

To update digest authentication service parameters, for example, the SIP Realm Station parameter, perform the following procedure:

Procedure

Step 1 In Unified Communications Manager, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list box, choose a node where you activated the Cisco CallManager service.

Step 3 From the **Service** drop-down list box, choose the Cisco CallManager 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 parameter, click the question mark or the parameter name link.

Step 5 Click **Save**.

Set Up End User Digest Credentials

The following procedure assumes that the end user exists in the Unified Communications Manager database. To configure digest credentials for the end user, perform the following procedure:

Procedure

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

Step 2 After the specific **End User Configuration** window displays, enter the appropriate settings.

Step 3 Click **Save**.

Step 4 To configure digest credentials for additional end users, repeat the procedure.

What to do next

After you configure digest credentials in the **End User Configuration** window, choose the digest user for the phone by accessing the **Phone Configuration** window.

After you choose the digest user, enter the digest authentication credentials that you get from the **End User Configuration** window on the Cisco Unified IP Phone 7962 or 7942 (SIP only).

End User Digest Credential Settings

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

Table 16: 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.

Set Up Digest User Using Phone

To associate a digest user with a phone, perform the following procedure:

Procedure

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

Step 2 After the specific **Phone Configuration** window displays, locate the **Digest User** setting and choose the end user that you want to associate with the phone.

Step 3 Click **Save**.

Step 4 Click **Reset**.

After you associate the end user with the phone, save the configuration and reset the phone.

CHAPTER 13

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 123
- Web Access Disable, on page 123
- PC Voice VLAN Access Disable, on page 124
- Setting Access Disable, on page 124
- PC Port Disable, on page 124
- Set Up Phone Hardening, on page 124
- Where to Find More Information About Phone Hardening, on page 125

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 Cisco Quality Report Tool, do not function properly without access to the phone web pages. Disabling the web server also affects any serviceability application, such as CiscoWorks, that relies on web access.

To determine whether the web services are disabled, the phone parses a parameter in the configuration file that indicates whether the services are disabled or enabled. If the web services are disabled, the phone does not open the HTTP port 80 for monitoring purposes and blocks access to the phone internal web pages.

PC Voice VLAN Access Disable

By default, Cisco IP Phones forward all packets that are received on the switch port (the one that faces the upstream switch) to the PC port. If you choose to disable the PC Voice VLAN Access setting in the Phone Configuration window, packets that are received from the PC port that use voice VLAN functionality will drop. Various Cisco IP Phones use this functionality differently.

- Cisco Unified IP Phones 7942 and 7962 drop any packets that are tagged with the voice VLAN, in or out of the PC port.
- Cisco Unified IP Phone 7970G drops any packet that contains an 802.1Q tag on any VLAN, in or out of the PC port.

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

To increase the phone security, disable functionalities such as PC Port, Setting Access, Gratuitous ARP, PC Voice VLAN Access, and Web Access on the phone.

To disable the functionalities on the phone, perform the following procedure:

Procedure

Step 1 From 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.
The **Phone Configuration** window appears.

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 14

Secure Conference Resources Setup

This chapter provides information about secure conference resources setup.

- Secure Conference, on page 127
- Conference Bridge Requirements, on page 128
- Secure Conference Icons, on page 129
- Secure Conference Status, on page 129
- Cisco Unified IP Phone Secure Conference and Icon Support, on page 132
- Secure Conference CTI Support, on page 132
- Secure Conference Over Trunks and Gateways, on page 132
- CDR Data, on page 133
- Interactions and Restrictions, on page 133
- Securing Conference Resources Tips, on page 134
- Set Up Secure Conference Bridge, on page 135
- Set Up Secure Conference Bridge in Cisco Unified Communications Manager Administration, on page 136
- Set Up Minimum Security Level for Meet-Me Conferences, on page 137
- Set Up Packet Capturing for Secure Conference Bridge, on page 138
- Where to Find More Information About Secure Conferences Resources, on page 138

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 *Cisco Unified Communications Manager System Guide* for more information.

Secure Conference Icons

Cisco IP Phones display a conference security icon for the security level of the entire conference. These icons match the status icons for a secure two-party call, as described in the user documentation for your phone.

The audio and video portions of the call provide the basis for the conference security level. The call gets considered secure only if both the audio and video portions are secure.

For ad hoc and meet-me secure conferences, the security icon for the conference displays next to the conference softkey in the phone window for conference participants. The icon that displays depends on the security level of the conference bridge and all participants:

- A lock icon displays if the conference bridge is secure and all participants in the conference are encrypted.
- A shield icon displays if the conference bridge is secure and all participants in the conference are authenticated. Some phone models do not display the shield icon.
- When the conference bridge or any participant in the conference is nonsecure, the call state icon (active, hold, and so on) displays, or, on some older phone models, no icon displays.

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

When an encrypted phone connects to a secure conference bridge, the media streaming between the device and the conference bridge gets encrypted; however, the icon for the conference can be encrypted, authenticated, or nonsecure depending on the security levels of the other participants. A nonsecure status indicates that one of the parties is not secure or cannot be verified.

When a user presses Barge, the icon that displays next to the Barge softkey provides the security level for the barge conference. If the barging device and the barged device support encryption, the system encrypts the media between the two devices, but the barge conference status can be nonsecure, authenticated, or encrypted, depending on the security levels of the connected parties.

Secure Conference Status

Conference status can change as participants enter and leave the conference. An encrypted conference can revert to a security level of authenticated or nonsecure if an authenticated or nonsecure participant connects to the call. Likewise, the status can upgrade if an authenticated or nonsecure participant drops off the call. A nonsecure participant that connects to a conference call renders the conference nonsecure.

Conference status can also change when participants chain conferences together, when the security status for a chained conference changes, when a held conference call is resumed on another device, when a conference call gets barged, or when a transferred conference call completes to another device.

Note The Advanced Ad Hoc Conference Enabled service parameter determines whether ad hoc conferences can be linked together by using features such as conference, join, direct transfer, and transfer.

Unified Communications Manager provides these options to maintain a secure conference:

- Ad hoc conference lists
- Meet-Me conference with minimum security level

Ad Hoc Conference Lists

A conference list displays on participating phones when the ConfList softkey is pressed during a conference call. The conference list provides the conference status as well as the security status for each participant to identify participants that are not encrypted.

Conference list displays these security icons: nonsecure, authenticated, encrypted, held. The conference initiator can use the conference list to eject participants with a low security status.

Note The Advanced Ad Hoc Conference Enabled service parameter determines whether conference participants other than the conference initiator can eject conference participants.

As participants join the conference, they get added to the top of the conference list. To remove nonsecure participants from a secure conference with the ConfList and RmLstC softkeys, refer to the user documentation for your phone.

The following sections describe secure ad hoc conference interactions with other features.

Secure Ad Hoc Conference and Conference Chaining

When an ad hoc conference is chained to another ad hoc conference, the chained conference displays in the list as member “Conference” with its own security status. Unified Communications Manager includes the security level for the chained conference to determine the overall conference security status.

Secure Ad Hoc Conference and cBarge

When a user presses the cBarge softkey to join an active conference, Unified Communications Manager creates an ad hoc conference and allocates a conference bridge according to the security level and MRGL of the barged device. The cbarge member names display in the conference list.

Secure Ad Hoc Conference and Barge

If a participant in a secure ad hoc conference gets barged, the barge call security status shows in the conference list next to the barge target. The security icon for the barge target may show authenticated when, in fact, the media is encrypted between the barge target and the conference bridge, because the barge caller has an authenticated connection.

If the barge target is secure but in an unsecured ad hoc conference, if the ad hoc conference status later changes to secure, the barge caller icon will update as well.

Secure Ad Hoc Conference and Join

Authenticated or encrypted phone users can use the Join softkey at a Cisco Unified IP Phone (only phones that are running SCCP) to create or join a secure ad hoc conference. If a user presses Join to add a participant with an unknown security status to an existing conference, Unified Communications Manager downgrades the conference status to unknown. A participant who adds a new member with Join becomes the conference initiator and can eject the new member or any other participant from the conference list (if the Advanced Ad Hoc Conference Enabled setting is True).

Secure Ad Hoc Conference and Hold/Resume

When a conference initiator puts the conference call on hold to add a participant, the conference status remains unknown (nonsecure) until the added participant answers the call. After the new participant answers, conference status updates in the conference list.

If a caller on a shared line resumes a held conference call at another phone, the conference list updates when the caller presses Resume.

Meet-Me Conference with Minimum Security Level

As administrator, you can specify a minimum security level for a conference when you configure a meet-me pattern or number as nonsecure, authenticated, or encrypted. Participants must meet the minimum security requirement, or the system blocks the participant and drops the call. This action applies to meet-me conference call transfers, resumed meet-me conference calls on shared lines, and chained Meet-Me conferences.

The phone that initiates the meet-me conference must meet the minimum security level, or the system rejects the attempt. When the minimum security level specifies authenticated or encrypted and a secure conference bridge is not available, the call fails.

If you specify nonsecure as the minimum level for the conference bridge, the conference bridge accepts all calls, and the conference status is nonsecure.

The following sections describe secure meet-me conference interactions with other features.

Meet-Me Conference and Ad Hoc Conference

To add a meet-me conference to an ad hoc conference or add an ad hoc conference to a meet-me conference, the ad hoc conference must meet the minimum security level for the meet-me conference, or the call is dropped. The conference icon can change when the conference gets added.

Meet-Me Conference and Barge

Unless a barge caller meets the minimum security requirement when the caller barges a meet-me conference participant, the security level of the barged device downgrades, and both the barge caller and the barged call get dropped.

Meet-Me Conference and Hold/Resume

A phone on a shared line cannot resume a meet-me conference unless the phone meets the minimum security level. If a phone does not meet the minimum security level, all phones on the shared line get blocked when the user presses Resume.

Cisco Unified IP Phone Secure Conference and Icon Support

These Cisco Unified IP Phones support secure conference and secure conference icons:

- Cisco Unified IP Phones 7942 and 7962 (SCCP only, authenticated secure conference only)
- Cisco Unified IP Phones 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7921G, , 7931G, 7942, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7970G, 7971G, 7971G-GE, 7975G, 8941, and 8945. (SCCP only)
- Cisco Unified IP Phones 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7941G, 7941G-GE, 7942G, 7961G, 7961G-GE,7962G, 7965G, 7970G, 7971G, 7971G-GE, 7975G, 8941, 8945, 8961, 9971, and 9971.

  Cisco IP Phones 7811, 7821, 7841, 7861, Cisco IP Conference Phone7832, Cisco IP Phones 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR, Cisco Wireless IP Phone 8821, Cisco Unified IP Conference Phone 8831, Cisco IP Conference Phone 8832.

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

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

See topics related to Unified Communications Manager secure conference restrictions for more restrictions that apply to Cisco Unified IP Phones.

For additional information about secure conference calls and security icons, refer to the *Cisco IP Phone Administration Guide and Cisco IP Phone User Guide* for your phone.

Secure Conference CTI Support

Unified Communications Manager supports secure conference over licensed CTI devices. Refer to the *Unified Communications Manager JTAPI Developers Guide* and *Unified Communications Manager TAPI Developers Guide* for this release for more information.

Secure Conference Over Trunks and Gateways

Unified Communications Manager supports secure conference over intracluster trunks (ICTs), H.323 trunks/gateways, and MGCP gateways; however, encrypted phones that are running release 8.2 or earlier will revert to RTP for ICT and H.323 calls, and the media does not get encrypted.

If a conference involves a SIP trunk, the secure conference status is nonsecure. In addition, SIP trunk signaling does not support secure conference notifications to off-cluster participants.

CDR Data

CDR data provides the security status of each call leg from the phone endpoint to the conference bridge as well as the security status of the conference itself. The two values use two different fields inside the CDR database.

CDR data provides termination cause code 58 (Bearer capability not presently available) when a meet-me conference rejects a join attempt that does not meet the minimum security level requirement. See the *CDR Analysis and Reporting Administration Guide* for more information.

Interactions and Restrictions

This section contains information on the following topics:

- Cisco Unified Communications Manager Interactions with Secure Conference, on page 133
- Cisco Unified Communications Manager Restrictions with Secure Conference, on page 134

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 must contain the Unified Communications Manager certificate, and Unified Communications Manager must contain certificates for the DSP farm system and the DSP connection. To ensure the conference bridge passes authentication, the X509 certification name must contain the conference bridge name.
- If conference bridge certificates expire or change for any reason, use the certificate management feature in Cisco Unified Communications Operating System Administration to update the certificates in the trusted store. The TLS authentication fails when certificates do not match, and conference bridge does not work because it cannot register to Unified Communications Manager.
- The secure conference bridge registers to Unified Communications Manager through TLS connection at port 2443; a nonsecure conference bridge registers to Unified Communications Manager through TCP connection at port 2000.
- Changing the device security mode for the conference bridge requires a reset of Unified Communications Manager devices and a restart of the Cisco CallManager service.

Set Up Secure Conference Bridge

The following procedure provides the tasks used to add secure conferencing to your network.

Procedure

Step 1 Verify that you installed and configured the Cisco CTL 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 Cisco CallManager service on the server.

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

Tip Be sure to copy the certificate to each server in the cluster and restart the Cisco CallManager 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 Cisco CallManager 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 135.

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 136.

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 *Cisco Unified Communications Manager Administration Guide*.

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 135.

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 137.

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 *Cisco Unified Communications Manager Administration Guide*.

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 26

CHAPTER 15

Voice-Messaging Ports Security Setup

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

- Voice-Messaging Security, on page 139
- Voice-Messaging Security Setup Tips, on page 139
- Set Up Secure Voice-Messaging Port, on page 140
- Apply Security Profile to Single Voice-Messaging Port, on page 141
- Apply Security Profile Using Voice Mail Port Wizard, on page 142
- Where to Find More Information About Voice-messaging Security, on page 142

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 Cisco CallManager 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 *Cisco Unified Communications Operating System Administration Guide* 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 Cisco CTL 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 Cisco CallManager service.

For more information, see the *Cisco Unified Communications Operating System Administration Guide* 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 Cisco CallManager 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 *Cisco Unified Communications Manager Administration Guide*.

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 *Cisco Unified Communications Manager Administration Guide*. Click **Next**.

Step 6 Continue the configuration process, as described in the *Cisco Unified Communications Manager Administration Guide*. 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 26
- Certificates, on page 16

CHAPTER 16

Call Secure Status Policy

- About Call Secure Status Policy, on page 143
- Setup Call Secure Status Policy, on page 144

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 *Cisco Unified Communications Manager Administration Guide*.

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 17

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 145
- Set Up Secure Call Monitoring and Recording, on page 145

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 The system does not support secure or nonsecure recording on authenticated phones.

-
-

Set Up Secure Call Monitoring and Recording

To configure Secure Call Monitoring and Recording, use the following procedure:

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 DN page on the agent phone.
c) Create a route pattern for the recorder.
d) Add a call recording profile to the DN.
e) Provision monitoring and recording tones as needed.

For more information and detailed procedures, see the "Monitoring and Recording" chapter in the *Cisco Unified Communications Manager Features and Services Guide*.

PART III

Virtual Private Networks for Cisco Unified IP Phones

- Virtual Private Network Setup, on page 149
- VPN Gateway Setup, on page 165
- VPN Group Setup, on page 169
- VPN Profile Setup, on page 171
- VPN Feature Setup, on page 175

CHAPTER 18

Virtual Private Network Setup

This chapter provides information about virtual private network setup.

- Virtual Private Network, on page 149
- Devices Supporting VPN, on page 150
- Set Up VPN Feature, on page 150
- Complete Cisco IOS Prerequisites, on page 151
- Configure Cisco IOS SSL VPN to Support IP Phones , on page 151
- Sample IOS Setup, on page 153
- Complete ASA Prerequisites for AnyConnect, on page 157
- Configure ASA for VPN Client on IP Phone, on page 157
- Sample ASA Setup, on page 160

Virtual Private Network

Note The VPN menu and its options are not available in the U.S. export unrestricted version of Cisco Unified Communications Manager.

The Cisco VPN Client for Cisco Unified IP Phones adds another option for customers attempting to solve the remote telecommuter problem by complementing other Cisco remote telecommuting offerings.

- Easy to Deploy—All settings configured via CUCM administration.
- Easy to Use—After configuring the phone within the Enterprise, the user can take it home and plug it into their broadband router for instant connectivity, without any difficult menus to configure.
- Easy to Manage—Phone can receive firmware updates and configuration changes remotely.
- Secure—VPN tunnel only applies to voice and Cisco Unified IP Phone services. A PC connected to the PC port is responsible for authenticating and establishing it own tunnel with VPN client software.

Devices Supporting VPN

You can use Cisco Unified Reporting to determine which Cisco Unified IP Phones support the VPN client. From Cisco Unified Reporting, click **Unified CM Phone Feature List**. For the Feature, choose **Virtual Private Network Client** from the pull-down menu. 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*.

Set Up VPN Feature

The following procedure provides the tasks to configure the VPN feature for supported Cisco Unified IP Phones.

For VPN concentrator configuration information, refer to the documentation for the VPN concentrator; such the following:

- SSL VPN Client (SVC) on ASA with ASDM Configuration Example

  The ASA software must be version 8.0.4 or later, and the “AnyConnect Cisco VPN Phone” license must be installed in conjunction with an "AnyConnect Premium" license.

  To avoid long delays when the user upgrades the firmware or configuration information on a remote phone, Cisco recommends that you set up the VPN concentrator close in the network to the TFTP or Cisco Unified Communications Manager server. If this is not feasible in your network, you can set up an alternate TPTP or load server that is next to the VPN concentrator.

- SSL VPN Client (WebVPN) on IOS with SDM Configuration Example

  The IOS software must be versions 15.1(2)T or later. Feature Set/License:" Universal (Data & Security & UC)" for the 2900 models and “Advanced Security” for the 2800 models with SSL VPN licenses activated.

  To avoid long delays when the user upgrades the firmware or configuration information on a remote phone, Cisco recommends that you set up the VPN concentrator close in the network to the TFTP or Cisco Unified Communications Manager server. If this is not feasible in your network, you can set up an alternate TPTP or load server that is next to the VPN concentrator.

Procedure

Step 1 Set up the VPN concentrators for each VPN Gateway.

Step 2 Upload the VPN concentrator certificates.

Step 3 Configure the VPN Gateways.

Step 4 Create a VPN Group using the VPN Gateways.

Step 5 Configure the VPN Profile.

Step 6 Add the VPN Group and VPN Profile to a Common Phone Profile. In Cisco Unified Communications Manager Administration, choose **Device** > **Device Settings** > **Common Phone Profile**.

For more information, see the "Common Phone Profile Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*.

Note If you do not associate a VPN Profile with the Common Phone Profile, VPN uses the default settings defined in the **VPN Feature Configuration** window.

Step 7 Upgrade the firmware for Cisco Unified IP Phones 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 firmware, see the *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager* for your Cisco Unified IP Phone model.

Note Before you can upgrade to firmware release 9.0(2), supported Cisco Unified IP Phones must be running firmware release 8.4(4) or later.

Step 8 Using a supported Cisco Unified IP Phone, establish a VPN connection.

For more information about configuring a Cisco Unified IP Phone and establishing a VPN connection, see the *Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager* for your Cisco Unified IP Phone model.

Complete Cisco IOS Prerequisites

Before you create Cisco IOS configuration for VPN client on an IP Phone, complete the following steps:

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

Feature Set/License: Advanced Security for IOS ISR

Step 2 Activate the SSL VPN License.

Configure 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> 1024 1024
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 Cisco 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
```

Sample IOS Setup

You can use the following sample IOS configuration for VPN client on IP phone as a general guideline to creating your own configurations. The configuration entries can change over time.

```
Current configuration: 4648 bytes
!
! Last configuration change at 13:48:28 CDT Fri Mar 19 2010 by test
!
version 15.2
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
no service password-encryption
!
! hostname of the IOS
hostname vpnios
!
boot-start-marker

! Specifying the image to be used by IOS - boot image
boot system flash c2800nm-advsecurityk9-mz.152-1.4.T
boot-end-marker
!
!
logging buffered 21474836
!
aaa new-model
!
!
 aaa authentication login default local
 aaa authentication login webvpn local
 aaa authorization exec default local
 !
 aaa session-id common
 !
```

```
 clock timezone CST -6
 clock summer-time CDT recurring
 !
 crypto pki token default removal timeout 0
 !

! Define trustpoints
 crypto pki trustpoint iosrcdnvpn-cert
  enrollment selfsigned
  serial-number
  subject-name cn=iosrcdnvpn-cert
  revocation-check none
  rsakeypair iosrcdnvpn-key 1024
 !
 crypto pki trustpoint CiscoMfgCert
  enrollment terminal
  revocation-check none
  authorization username subjectname commonname
 !
 crypto pki trustpoint CiscoRootCA
  enrollment terminal
  revocation-check crl
  authorization username subjectname commonname
 !
 !
! Certificates
 crypto pki certificate chain iosrcdnvpn-cert
  certificate self-signed 04
 crypto pki certificate chain CiscoMfgCert
  certificate ca 6A6967B3000000000003
 crypto pki certificate chain CiscoRootCA
  certificate ca 5FF87B282B54DC8D42A315B568C9ADFF
 crypto pki certificate chain test
  certificate ca 00
 dot11 syslog
 ip source-route
 !
 !
 ip cef
 !
 !
 !
 ip domain name nw048b.cisco.com
 no ipv6 cef
 !
 multilink bundle-name authenticated
 !
!
 voice-card 0
 !
 !
 !
 license udi pid CISCO2821 sn FTX1344AH76
 archive
  log config
   hidekeys
 username admin privilege 15 password 0 vpnios
 username test privilege 15 password 0 adgjm
 username usr+ privilege 15 password 0 adgjm
 username usr# privilege 15 password 0 adgjm
 username test2 privilege 15 password 0 adg+jm
 username CP-7962G-SEP001B0CDB38FE privilege 15 password 0 adgjm
 !
 redundancy
```

```
 !
!
!--- Configure interface. Generally one interface to internal network and one outside
 interface GigabitEthernet0/0
  description "outside interface"
  ip address 10.89.79.140 255.255.255.240
  duplex auto
  speed auto
 !
 interface GigabitEthernet0/1
  description "Inside Interface"
  ip address dhcp
  duplex auto
  speed auto
 !
!--- Define IP local address pool
 ip local pool webvpn-pool 10.8.40.200 10.8.40.225
 ip default-gateway 10.89.79.129
 ip forward-protocol nd
 ip http server
 ip http authentication local
 ip http secure-server
 ip http timeout-policy idle 60 life 86400 requests 10000
 !
 !
!--- Define static IP routes
ip route 0.0.0.0 0.0.0.0 10.89.79.129
ip route 10.89.0.0 255.255.0.0 10.8.40.1
 !
 no logging trap
 access-list 23 permit 10.10.10.0 0.0.0.7
!
 control-plane
 !
line con 0
  exec-timeout 15 0
 line aux 0
! telnet access
 line vty 0 4
  exec-timeout 30 0
  privilege level 15
  password vpnios
  transport input telnet
 line vty 5 15
  access-class 23 in
  privilege level 15
  transport input all
 !
 exception data-corruption buffer truncate
 scheduler allocate 20000 1000
 !

! webvpn gateway configuration
 webvpn gateway VPN_RCDN_IOS
  hostname vpnios
  ip address 10.89.79.140 port 443
! ssl configuration
  ssl encryption aes128-sha1
  ssl trustpoint iosrcdnvpn-cert
  inservice
  !
! webvpn context for User and Password authentication
 webvpn context UserPasswordContext
  title "User-Password authentication"
```

```
 ssl authenticate verify all
 !
 !
 policy group UserPasswordGroup
   functions svc-enabled
   hide-url-bar
   timeout idle 3600
   svc address-pool "webvpn-pool"
   svc default-domain "nw048b.cisco.com"
   svc split include 10.89.75.0 255.255.255.0
   svc dns-server primary 64.101.128.56
   svc dtls
 default-group-policy UserPasswordGroup
 gateway VPN_RCDN_IOS domain UserPasswordVPN
 inservice
!
!
! webvpn context for Certificate (username pre-filled) and Password authentication
webvpn context CertPasswordContext
 title "certificate plus password"
 ssl authenticate verify all
 !
 !
 policy group CertPasswordGroup
   functions svc-enabled
   hide-url-bar
   timeout idle 3600
   svc address-pool "webvpn-pool"
   svc default-domain "nw048b.cisco.com"
   svc dns-server primary 64.101.128.56
   svc dtls
 default-group-policy CertPasswordGroup
 gateway VPN_RCDN_IOS domain CertPasswordVPN
 authentication certificate aaa
 username-prefill
 ca trustpoint CiscoMfgCert
 inservice
!
!
! webvpn context for certificate only authentication
webvpn context CertOnlyContext
 title "Certificate only authentication"
 ssl authenticate verify all
 !
 !
 policy group CertOnlyGroup
   functions svc-enabled
   hide-url-bar
   timeout idle 3600
   svc address-pool "webvpn-pool"
   svc default-domain "nw048b.cisco.com"
   svc dns-server primary 64.101.128.56
   svc dtls
 default-group-policy CertOnlyGroup
 gateway VPN_RCDN_IOS domain CertOnlyVPN
 authentication certificate
 ca trustpoint CiscoMfgCert
 inservice
!
end
```

Complete ASA Prerequisites for AnyConnect

Before you create an ASA configuration for VPN client on an IP phone, complete the following steps:

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

Note Replacing ASA certificates results in non-availability of Cisco Unified Communications Manager.

Perform the following steps to configure ASA for VPN client on IP phone.

Procedure

Step 1 Local configuration

a) Configure 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 routes and default routes.

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
```

c) Configure the DNS.

Example:

```
hostname(config)# dns domain-lookup inside
hostname(config)# dns server-group DefaultDNS
hostname(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 Cisco Unified Communications Manager and IOS.

The following certificates need to be imported from the Cisco 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 Cisco Unified Communications Manager certificates, do the following:

a) From the Cisco Unified Communications Manager OS Administration web page.
b) Choose **Security** > **Certificate Management**. (Note: This location may change based on the UCM version)
c) Find the certificates Cisco_Manufacturing_CA and CAPF. Download the .pem file and save as .txt file.
d) Create trustpoint on the ASA.

Example:

```
hostname(config)# crypto pki trustpoint trustpoint_name
hostname(config-ca-trustpoint)# enrollment terminal
hostname(config)# crypto pki authenticate trustpoint
```

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.

e) You should generate the following IOS self-signed certificates and register them with Cisco Unified Communications Manager, or replace with a certificate that you import from a CA.

- Generate a self-signed certificate.

  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(ca-trustpoint)# rsakeypair <name> 1024 1024
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 Cisco 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 Cisco 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 Managing Certificate part of the CUCM.

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:

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
username CP-7975G-SEP001AE2BC16CB attributes vpn-group-policy GroupPhoneWebvpn
service-type remote-access
```

ASA Certificate Configuration

For more information on ASA certificate configuration, refer to http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example09186a0080bef910.shtml

Sample ASA Setup

You can use the following sample ASA configuration for VPN client on IP phone as a general guideline to creating your own configurations. The configuration entries can change over time.

```
ciscoasa(config)# show running-config
: Saved
:

!--- ASA version
ASA Version 8.2(1)
!
!--- Basic local config on ASA
hostname ciscoasa
domain-name nw048b.cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
dns-guard

!--- Configure interface. Generally one interface to internal network and one outside
!--- Ethernet0/0 is outside interface with security level 0
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 10.89.79.135 255.255.255.0

!--- Ethernet0/1 is inside interface with security level 100
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address dhcp
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 security-level 100
 no ip address
!
interface Management0/0
 shutdown
 nameif management
 security-level 100
 no ip address
 management-only
!

!--- Boot image of ASA
boot system disk0:/asa821-k8.bin
ftp mode passive

!--- Clock settings
clock timezone CST -6
clock summer-time CDT recurring
```

```
!--- DNS configuration
dns domain-lookup outside
dns server-group DefaultDNS
 name-server 64.101.128.56
 domain-name nw048b.cisco.com


!--- Enable interface on the same security level so that they can communicate to each other
same-security-traffic permit inter-interface
!--- Enable communication between hosts connected to same interface
same-security-traffic permit intra-interface
pager lines 24

!--- Logging options
logging enable
logging timestamp
logging console debugging
no logging message 710005
mtu outside 1500
mtu inside 1500
mtu management 1500

!--- Define IP local address pool
ip local pool Webvpn_POOL 10.8.40.150-10.8.40.170 mask 255.255.255.192
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside

!--- ASDM image
asdm image disk0:/asdm-623.bin
no asdm history enable
arp timeout 14400

!--- Static routing
route outside 0.0.0.0 0.0.0.0 10.89.79.129 1
route inside 10.89.0.0 255.255.0.0 10.8.40.1 1
route inside 0.0.0.0 0.0.0.0 10.8.40.1 tunneled

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.1.0 255.255.255.0 inside
http redirect outside 80
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000

!--- ASA certs
!--- trustpoints and certificates
crypto ca trustpoint ASA_VPN_Cert
 enrollment self
 keypair ASA_VPN_Cert_key
 crl configure
crypto ca trustpoint CiscoMfgCert
 enrollment terminal
 crl configure
```

```
crypto ca trustpoint UCM_CAPF_Cert
 enrollment terminal
 no client-types
 crl configure
crypto ca certificate chain ASA_VPN_Cert
 certificate 02d5054b
  quit

crypto ca certificate chain CiscoMfgCert
 certificate ca 6a6967b3000000000003
  quit

crypto ca certificate chain UCM_CAPF_Cert
 certificate ca 6a6967b3000000000003
  quit
telnet timeout 5
ssh scopy enable
ssh timeout 5
console timeout 0

!--- configure client to send packets with broadcast flag set
dhcp-client broadcast-flag
!--- specifies use of mac-addr for client identifier to outside interface
dhcp-client client-id interface outside
!
tls-proxy maximum-session 200
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

!--- configure ssl
ssl encryption aes128-sha1
ssl trust-point ASA_VPN_Cert
ssl certificate-authentication interface outside port 443

!--- VPN config
!--- Configure webvpn
webvpn
 enable outside
 default-idle-timeout 3600
 svc image disk0:/anyconnect-win-2.1.0148-k9.pkg 1
 svc enable

!--- Group-policy
group-policy GroupPhoneWebvpn internal
group-policy GroupPhoneWebvpn attributes
 banner none
 vpn-simultaneous-logins 10
 vpn-idle-timeout none
 vpn-session-timeout none
 vpn-tunnel-protocol IPSec svc webvpn
 default-domain value nw048b.cisco.com
 address-pools value Webvpn_POOL
 webvpn
  svc dtls enable
  svc keep-installer installed
  svc keepalive 120
  svc rekey time 4
  svc rekey method new-tunnel
  svc dpd-interval client none
  svc dpd-interval gateway 300
  svc compression deflate
  svc ask none default webvpn
```

```
!--- Configure user attributes
username test password S.eA5Qq5kwJqZ3QK encrypted
username test attributes
 vpn-group-policy GroupPhoneWebvpn
 service-type remote-access

!—Configure username with Phone MAC address for certificate+password method
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
username CP-7975G-SEP001AE2BC16CB attributes
 vpn-group-policy GroupPhoneWebvpn
 service-type remote-access

!--- Configure tunnel group for username-password authentication
tunnel-group VPNphone type remote-access
tunnel-group VPNphone general-attributes
 address-pool Webvpn_POOL
 default-group-policy GroupPhoneWebvpn
tunnel-group VPNphone webvpn-attributes
 group-url https://10.89.79.135/VPNphone enable

!--- Configure tunnel group with certificate only authentication
tunnel-group CertOnlyTunnelGroup type remote-access
tunnel-group CertOnlyTunnelGroup general-attributes
 default-group-policy GroupPhoneWebvpn
tunnel-group CertOnlyTunnelGroup webvpn-attributes
 authentication certificate
 group-url https://10.89.79.135/CertOnly enable

!--- Configure tunnel group with certificate + password authentication
tunnel-group CertPassTunnelGroup type remote-access
tunnel-group CertPassTunnelGroup general-attributes
 authorization-server-group LOCAL
 default-group-policy GroupPhoneWebvpn
 username-from-certificate CN
tunnel-group CertPassTunnelGroup webvpn-attributes
 authentication aaa certificate
 pre-fill-username ssl-client
 group-url https://10.89.79.135/CertPass enable

!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
```

```
service-policy global_policy global
prompt hostname context
Cryptochecksum:cd28d46a4f627ed0fbc82ba7d2fee98e
: end
```

CHAPTER 19

VPN Gateway Setup

This chapter provides information about VPN gateway setup. To configure a VPN gateway, you must first upload the VPN concentrator certificates and then configure the VPN gateway.

Note The VPN menu and its options are not available in the U.S. export unrestricted version of Cisco Unified Communications Manager.

- Upload VPN Concentrator Certificates, on page 165
- VPN Gateway Setup, on page 166

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.

The Cisco Unified IP Phone sends its Manufacturer Installed Certificate (MIC) by default. If you configure the CAPF service, the Cisco Unified IP Phone sends its Locally Significant Certificate (LSC).

To use device level certificate authentication, install the root MIC or CAPF certificate in the ASA, so that the Cisco Unified IP Phones 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**.

The **Certificate List** window appears.

Step 2 Click **Upload Certificate**.

The **Upload Certificate** dialog box appears.

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**.

VPN Gateway Setup

Find VPN Gateway

Procedure

Step 1 In Cisco Unified CM Administration, choose **Advanced Features** > **VPN** > **VPN Gateway**.

The **Find and List VPN Gateways** window appears. Records from an active (prior) query may also display in the window.

Step 2 To find all records in the database, do not enter any search criteria.

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 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 appear. You can change the number of items that appear on each page by choosing a different value from the **Rows per Page** drop-down list.

Step 4 From the list of records that appears, 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.

Configure VPN Gateway

To add, update, or copy a VPN gateway, perform the following procedure:

Before you begin

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 165.

Procedure

Step 1 In 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 167.

Step 4 Click **Save**.

VPN Gateway Fields for VPN Client

Field	Description
VPN Gateway Name	Enter the name of the VPN gateway.
VPN Gateway Description	Enter a description of the VPN gateway.
VPN Gateway URL	Enter the URL for the main VPN concentrator in the gateway. **Note** You must configure the VPN concentrator with a group URL and use this URL as the gateway URL. For configuration information, refer to the documentation for the VPN concentrator, such as the following: • *SSL VPN Client (SVC) on ASA with ASDM Configuration Example*
VPN Certificates in this Gateway	Use the up and down arrow keys to assign certificates to the gateway. If you do not assign a certificate for the gateway, the VPN client will fail 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.

CHAPTER 20

VPN Group Setup

Note This chapter provides information about creating a VPN group. After you create a VPN group, you can add one of the VPN gateways you just configured to it.

The VPN menu and its options are not available in the U.S. export unrestricted version of Cisco Unified Communications Manager.

- Find VPN Group, on page 169
- Configure VPN Group, on page 170
- VPN Group Fields for VPN Client, on page 170

Find VPN Group

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Advanced Features** > **VPN** > **VPN Group**.

The **Find and List VPN Groups** window appears. Records from an active (prior) query may also appear in the window.

Step 2 To find all records in the database, do not enter any search criteria.

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 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 appear. 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 appear, 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.

Configure VPN Group

User this procedure to add, update, or copy a VPN group.

Procedure

Step 1 In Unified Communications Manager 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 167 for the field description details.

Step 4 Click **Save**.

VPN Group Fields for VPN Client

Field	Definition
VPN Group Name	Enter the name of the VPN group.
VPN Group Description	Enter a description of the VPN group.
All Available VPN Gateways	Scroll to see all available VPN gateways.
Selected VPN Gateways in this VPN Group	Use the up and down arrow buttons to move available VPN gateways into and out of this VPN group. If the VPN client encounters a 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.

CHAPTER 21

VPN Profile Setup

This chapter provides information about VPN profile setup.

Note The VPN menu and its options are not available in the U.S. export unrestricted version of Cisco Unified Communications Manager.

- About VPN Profile Setup, on page 171
- Find VPN Profile, on page 171
- Configure VPN Profile, on page 172
- VPN Profile Fields for VPN Client, on page 172

About VPN Profile Setup

Use the VPN Profile window to create a profile that you assign to the Cisco Unified IP Phone by using the **Common Phone Profile Configuration** window.

Find VPN Profile

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Advanced Features** > **VPN** > **VPN Profile**.

The **Find and List VPN Profiles** window appears. Records from an active (prior) query may also appear in the window.

Step 2 To find all records in the database, do not enter any search criteria.

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 the **Clear Filter** button to remove all added search criteria.

Step 3 Click **Find**.

All matching records appear. You can change the number of items that appear on each page by choosing a different value from the **Rows per Page** drop-down list.

Step 4 From the list of records that appears, 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.

Configure VPN Profile

Use this procedure to add, update, or copy a VPN group.

Procedure

Step 1 From Unified Communications Manager 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 172 for the field description details.

Step 4 Click **Save**.

VPN Profile Fields for VPN Client

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 login attempt occurs, a user manually clears the password, or the phone resets or loses power.

CHAPTER 22

VPN Feature Setup

This chapter provides information about the VPN feature configuration parameters.

Note The VPN menu and its options are not available in the U.S. export unrestricted version of Cisco Unified Communications Manager.

- About VPN Feature Setup, on page 175
- Configure VPN Feature Parameters, on page 175
- VPN Feature Parameters, on page 176

About VPN Feature Setup

The **VPN Feature Configuration** window contains the common configuration settings for the VPN feature that the system uses when you do not associate a VPN Profile with a Common Phone Profile. If you define a VPN Profile as part of configuring a Common Phone Profile, the VPN Profile settings take precedence over the VPN Feature Configuration settings.

Configure VPN Feature Parameters

Procedure

Step 1 From Unified Communications Manager 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 176.

Step 3 Click **Save**.

What to do next

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 the *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

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 , the keep alive setting in the VPN concentrator overwrites this setting. Default: 60 seconds Minimum: 0 Maximum: 120 seconds
Fail to Connect	This field specifies the amount of time to wait for login or connect operations to complete while the system creates the VPN tunnel. Default: 30 seconds Minimum: 0 Maximum: 600 seconds
Client Authentication Method	From the drop-down list, choose the client authentication method: • User and password • Password only • Certificate (LSC or MIC) Default: User And Password

Field	Default
Enable Password Persistence	When True, a user password gets saved in the phone until either a failed login attempt occurs, a user manually clears the password, or the phone resets or loses power. 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

PART IV

Cisco CTI, JTAPI, and TAPI Application Security

- Authentication and Encryption Setup for CTI, JTAPI, and TAPI, on page 181
- Certificate Revocation/Expiry Status Verification, on page 195

CHAPTER 23

Authentication and Encryption Setup for CTI, JTAPI, and TAPI

This chapter provides a brief overview of how to secure the CTI, JTAPI, and TAPI applications. It also describes the tasks that you must perform in Unified Communications Manager Administration to configure authentication and encryption for CTI/TAPI/JTAPI applications.

This document does not describe how to install the Cisco JTAPI 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 181
- Encryption for CTI, JTAPI, and TAPI Applications, on page 183
- CAPF Functions for CTI, JTAPI, and TAPI Applications, on page 183
- CAPF System Interactions and Requirements for CTI, JTAPI, and TAPI Applications, on page 185
- Securing CTI, JTAPI, and TAPI, on page 185
- Add Application and End Users to Security-Related Users Groups, on page 186
- Certificate Authority Proxy Function Service Activation, on page 187
- Update CAPF Service Parameters, on page 188
- Find Application User or End User CAPF Profile, on page 188
- Set Up Application User or End User CAPF Profile, on page 189
- CAPF Settings, on page 190
- Delete Application User CAPF or End User CAPF Profile, on page 192
- Set Up JTAPI/TAPI Security-Related Service Parameters, on page 193
- View Certificate Operation Status for Application or End User, on page 193

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 The following information assumes that you configured security settings during the Cisco JTAPI/TSP plug-in installation. It also assumes 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, port 2748.

CTIManager and the application verify the identity of the other party through a mutually authenticated TLS handshake (certificate exchange). When a TLS connection occurs, CTIManager and the application exchange QBE messages via the TLS port, port 2749.

To authenticate with the application, CTIManager uses the Unified Communications Manager certificate — either the self-signed certificate that installs automatically on the Unified Communications Manager server during installation or a third-party, CA-signed certificate that you uploaded to the platform.

After you generate the CTL file through the CLI command set **utils ctl** or the Cisco CTL Client, this certificate is added automatically to the CTL file. Before the application attempts to connect to CTIManager, the application downloads the CTL file from the TFTP server.

The first time that the JTAPI/TSP client downloads the CTL file from the TFTP server, the JTAPI/TSP client trusts the CTL file. Because the JTAPI/TSP client does not validate the CTL file, Cisco strongly recommends that the download occur in a secure environment. 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 where Cisco IP 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 Unified Communications Manager Administration, as described in Table 17: Application and End User CAPF Profile Configuration Settings , on page 190.

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 Administration 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 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.

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 Administration. 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 CTI ports and route points, you must configure the application to support secure calls because the application handles the media parameters.

CTI ports/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 CTI ports/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 application users 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 two 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 you performed all necessary tasks to install and configure the Cisco CTL Client. 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 first node.
- Because generating many certificates at the same time may cause call-processing interruptions, Cisco strongly recommends that you use CAPF during a scheduled maintenance window.
- Ensure that the first node is functional and running during the entire certificate operation.
- Ensure that the CTI/ JTAPI/TAPI application is functional during the entire certificate 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:

- *Computer Telephony Integration, Cisco Unified Communications Manager System Guide*
- *Cisco JTAPI Installation Guide for Unified Communications Manager*
- *Cisco TAPI Installation Guide for Unified Communications Manager*
- *Cisco Unified Communications Manager Administration Guide*

Step 2 Verify that the following Unified Communications Managersecurity features are installed (if not installed, install and configure these features):

- Verify that you installed the CTL Client and the CTL file has run, so the CTL file is created.
- Verify that you installed the CTL provider service and that the service is activated.
- Verify that you installed the CAPF service and that the service is activated. If necessary, update CAPF service parameters.

  Tip The CAPF service must run for the Cisco CTL 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 that 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.

See the *Cisco Unified Communications Manager Administration Guide* for more information.

Step 3 If you want CTIManager and the application to use a TLS connection, add the application user or end users to the Standard CTI Secure Connection user group.

Tip A CTI application can be assigned to either an application user or an end user, but not both.

Step 4 If you want to use SRTP, add the application user or end user to the Standard CTI Allow Reception of SRTP Key Material user group.

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 role configuration in the *Administration Guide for Cisco Unified Communications Manager* .

Note 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 5 Configure the Application User CAPF Profile or End User CAPF Profile in Unified Communications Manager Administration.

Step 6 Enable the corresponding security-related parameters in the CTI/JTAPI/TAPI application.

Add Application and End Users to Security-Related Users 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 Administration 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.

Because Unified Communications Manager Assistant, Cisco QRT, and Cisco Web Dialer do not support encryption, 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.

Tip For information on deleting an application or end user from a user group, refer to the *Cisco Unified Communications Manager Administration Guide*. For information about security-related settings in the **Role Configuration** window, refer to the *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 In 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 Step 5, on page 187 through Step 7, on page 187.

Step 5 Click the **Add Application Users to Group** button.

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 display in the **User Group** window.

Step 8 To add end users to the group, perform Step 9, on page 187 through Step 11, on page 187.

Step 9 Click the **Add Users to Group** button.

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 display in the **User Group** window.

Certificate Authority Proxy Function Service Activation

Unified Communications Manager does 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. To verify that the CAPF certificate exists, display the CAPF certificate at the Cisco Unified Communications Operating System GUI.

Update CAPF Service Parameters

The CAPF Service Parameter window provides information on the number of years that the certificate is valid, the maximum number of times that the system retries to generate the key, and so on

For the CAPF service parameters to display as Active in Unified Communications Manager Administration, you must 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 In Unified Communications Manager Administration, choose **System** > **Service Parameters**.

Step 2 From the Server drop-down list box, choose the server.

Tip You must choose the first node in the cluster.

Step 3 From the Service drop-down list box, choose the Cisco Certificate 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 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.

Find Application User or End User CAPF Profile

To find an application or end user CAPF profile, perform the following procedure:

Procedure

Step 1 In Unified Communications Manager Administration, choose one of the following options, depending on which profile you want to access:

a) **User Management** > **Application User CAPF Profile**

b) **User Management** > **End User CAPF 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 189.

To filter or search records

- From the first drop-down list box, choose a search parameter

a) From the second drop-down list box, choose a search pattern.
b) 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 Application User or End User CAPF Profile

Use Table 17: Application and End User CAPF Profile Configuration Settings , on page 190 as a reference when you install/upgrade/troubleshoot locally significant certificates for JTAPI/TAPI/CTI applications.

Tip Cisco recommends that you configure Application User CAPF Profiles before you configure End User CAPF Profiles.

Procedure

Step 1 In Unified Communications Manager Administration, choose one of the following options:

a) **User Management** > **Application User CAPF Profile**.
b) **User Management** > **End User CAPF Profile**.

The **Find and List** window displays.

Step 2 Perform one of the following tasks:

a) To add a new CAPF profile, 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 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 with the settings from the displayed profile.

c) To update an existing entry, locate and display the appropriate profile. The configuration window displays with the current settings.

Step 3 Enter the appropriate settings as described in Table 17: Application and End User CAPF Profile Configuration Settings , on page 190.

Step 4 Click **Save**.

Step 5 Repeat the procedure for each application and end user that you want to use security.

What to do next

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 17: Application and End User CAPF Profile Configuration Settings

Setting	Description
Application User	From the drop-down list box, 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 box, 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.

Setting	Description
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 box, 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, the administrator must enter the authentication string in the JTAPI/TSP preferences GUI on the application PC. 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 this button. The 4-to10-digit authentication string displays in the Authentication String field.

Setting	Description
Key Size (bits)	From the drop-down list box, choose the key size for the certificate. The default setting equals 1024. The other option for key size is 512. Key generation, which is set at low priority, allows the application to function while the action occurs. Key generation may take up to 30 or more minutes to complete.
Operation Completes by	This field, which supports all certificate operations, specifies the date and time by which you must complete the operation. The values that display 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.

Delete Application User CAPF or End User CAPF Profile

This section describes how to delete an Application User CAPF Profile or End User CAPF Profile from the Unified Communications Manager database.

Before you begin

Before you can delete an Application User CAPF Profile or End User CAPF 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 **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 *Cisco Unified Communications Manager System Guide*.

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.

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 In Unified Communications Manager Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list box, choose the server where the Cisco IP Manager Assistant service is activated.

Step 3 From the **Service** drop-down list box, choose the **Cisco IP Manager Assistant** service.

Step 4 After the parameters display, locate the CTIManager Connection Security Flag and CAPF Profile Instance ID for Secure Connection to CTIManager parameters.

Step 5 Update the parameters, as described in the help that displays when you click the question mark or parameter name link.

Step 6 Click **Save**.

Step 7 Repeat the procedure on each server where the service is activated.

View Certificate Operation Status for Application or End User

You can view the certificate operation status in a specific Application User or **End User CAPF Profile configuration** window (not the Find/List window) or in the **JTAPI/TSP Preferences** GUI window.

CHAPTER 24

Certificate Revocation/Expiry Status Verification

This chapter provides a brief overview of how to check the status of the certificates generated for sessions in Unified Communications Manager Administration. The certificate service periodically checks for long lived sessions between Unified Communications Manager and other services. Long lived sessions have duration of six hours or more. The check is performed for the following long lived sessions:

- CTI Connections with JTAPI /TAPI applications.
- LDAP Connection between Unified Communications Manager and SunOne servers.
- IPSec Connections

It also describes how to configure the enterprise parameter for verifying certificate revocation and expiry.

The enterprise parameter **Certificate Revocation and Expiry** allows you to control the certificate validation checks. The revocation and expiry check parameter is enabled on the **Enterprise Parameter** page of Unified Communications Manager. The certificate expiry for the long lived sessions is not verified, when the enterprise parameter value is disabled.

The certificate revocation service is active for LDAP and IPSec connections, when the **Enable Revocation** is selected on the Operating System Administration of Unified Communications Manager and revocation and expiry check parameter is set to enabled. The periodicity of the check for IPSec connections are based on the **Check Every** value. The revocation check for the certificate is not performed, if the **Enable Revocation** check box is unchecked.

Note The GeneralizedTime values for X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) profile must be expressed in Greenwich Mean Time (GMT) and must include seconds (i.e., times are **YYYYMMDDHHMMSSZ**), even when the number is zero. GeneralizedTime values must not include the fractional seconds. If the peer entity offers a certificate which violates this rule or a certificate is loaded in the trust stores from the peer entities, then it could possibly fail the certificate verification process.

- Certificate Revocation/Expiry Status Verification, on page 196
- Verify Certificate Status, on page 196
- Support for Delegated Trust Model in OCSP Response, on page 197

Certificate Revocation/Expiry Status Verification

This chapter provides a brief overview of how to check the status of the certificates generated for sessions in Unified Communications Manager Administration. The certificate service periodically checks for long lived sessions between Unified Communications Manager and other services. Long lived sessions have duration of six hours or more. The check is performed for the following long lived sessions:

- CTI Connections with JTAPI /TAPI applications.
- LDAP Connection between Unified Communications Manager and SunOne servers.
- IPSec Connections

It also describes how to configure the enterprise parameter for verifying certificate revocation and expiry.

The enterprise parameter **Certificate Revocation and Expiry** allows you to control the certificate validation checks. The revocation and expiry check parameter is enabled on the **Enterprise Parameter** page of Unified Communications Manager. The certificate expiry for the long lived sessions is not verified, when the enterprise parameter value is disabled.

The certificate revocation service is active for LDAP and IPSec connections, when the **Enable Revocation** is selected on the Operating System Administration of Unified Communications Manager and revocation and expiry check parameter is set to enabled. The periodicity of the check for IPSec connections are based on the **Check Every** value. The revocation check for the certificate is not performed, if the **Enable Revocation** check box is unchecked.

Note The GeneralizedTime values for X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) profile must be expressed in Greenwich Mean Time (GMT) and must include seconds (i.e., times are **YYYYMMDDHHMMSSZ**), even when the number is zero. GeneralizedTime values must not include the fractional seconds. If the peer entity offers a certificate which violates this rule or a certificate is loaded in the trust stores from the peer entities, then it could possibly fail the certificate verification process.

Verify Certificate Status

The following procedure provides the tasks that you perform to enable or disable the certificate validity check.

Procedure

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

The Enterprise Parameters Configuration window displays.

Step 2 Under **Certificate Revocation and Expiry** section,

a) From the **Certificate Validity Check** drop-down list box, select Enabled to enable the validity check.

b) Enter the **Validity Check Frequency (hours)** value.

The default value is 24 hours. The minimum value is 6 hours and the maximum value is 576 hours.

Step 3 Click Save.

Step 4 Click Apply Config.

The Apply Configuration Information dialog displays.

Step 5 Click Ok.

The timers for DIRSYNC and CTI are restarted.

Support for Delegated Trust Model in OCSP Response

Online Certificate Status Protocol (OCSP) allows a device to obtain real-time information about the status of a given certificate. Examples of certificate status are Good, Revoked, and Unknown.

Unified Communications Manager uses OCSP to validate third-party certificates that are uploaded into the Unified Communications Manager trust store. Unified Communications Manager requires an OCSP Responder URL to connect to the OCSP responder server over HTTP. It sends an HTTP request to the responder to validate a certificate.

Unified Communications Manager currently supports the Trusted Responder Model of OCSP, where the OCSP response is signed by a self-signed certificate of the OCSP server. This self-signed certificate is uploaded to the trust store before initiating an OCSP request. This certificate is used to verify the signature on the OCSP response.

Unified Communications Manager 11.0 and later support the Delegated Trust Model (DTM) of the OCSP responder, where the OCSP responses are no longer approved by the self-signed certificate but are issued by a Certificate Authority (Root CA or Subordinate CA). The CA certificate validates the OCSP responder certificates. The CA certificate that issued the OCSP responder certificate in Unified Communications Manager trust store is required, instead of OCSP response signing certificate. When you receive an OCSP response, the CA's certificate is used to validate the signature in the response.

Note In case of a DTM execution failure, the OCSP response is verified using the self-signed certificate.

PART V

Security for SRST References, Trunks, and Gateways

- Secure Survivable Remote Site Telephony (SRST) Reference, on page 201
- Encryption Setup for Gateways and Trunks, on page 207
- SIP Trunk Security Profile Setup, on page 213
- Digest Authentication Setup for SIP Trunks, on page 225
- Cisco Unified Mobility Advantage Server Security Profile Setup, on page 231
- FIPS 140-2 Mode Setup, on page 237

CHAPTER 25

Secure Survivable Remote Site Telephony (SRST) Reference

This chapter provides information about SRST references.

- Securing SRST, on page 201
- Securing SRST Tips, on page 202
- Set Up Secure SRST, on page 203
- Set Up Secure SRST References, on page 203
- SRST Reference Security Settings, on page 204
- Delete Security From SRST Reference, on page 206
- SRST Certificate Deletion From Gateway, on page 206

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 *Cisco IOS 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 Cisco CTL 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 18: Configuration Settings for Secure SRST References , on page 205.
- 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 *Cisco Unified Communications Manager Administration Guide*.

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 *Cisco Unified Communications Manager Administration Guide*, 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 *Cisco Unified Communications Manager Administration Guide*.

The configuration window displays with the current settings.

Step 3 Enter the security-related settings as described in Table 18: Configuration Settings for Secure SRST References , on page 205.

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

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 18: 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 Cisco CTL Provider service authenticates to the Certificate Provider service on the SRST-enabled gateway. The Cisco CTL 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 Cisco SRST 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 Cisco CTL 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 26

Encryption Setup for Gateways and Trunks

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

- Cisco IOS MGCP Gateway Encryption, on page 207
- H.323 Gateway and H.323/H.225/H.245 Trunk Encryption, on page 208
- SIP Trunk Encryption, on page 209
- Set Up Secure Gateways and Trunks, on page 210
- IPSec Setup Within Network Infrastructures, on page 211
- IPSec Setup Between Cisco Unified Communications Manager and Gateway or Trunks, on page 211
- Allow SRTP Using Cisco Unified Communications Manager Administration, on page 211
- Where to Find More Information About Gateway and Trunk Encryption, on page 212

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 clear 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.

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 *Cisco Unified Communications Operating System Administration Guide*.

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 *Cisco Unified Communications Manager Administration Guide*.

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, Cisco strongly recommends 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 Cisco IOS MGCP gateways for security.

Procedure

Step 1 Verify that you installed and configured the Cisco CTL Client; verify that the cluster security mode equals 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 Administration.

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 *Cisco Unified Communications Manager Administration Guide*.

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, Cisco strongly recommends 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 document 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 *Cisco IOS Security Configuration Guide, Release 12.2* (or later).
- Terminate the remote end of the IPSec connection in the secure Cisco IOS 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 may compromise privacy of the media streams.

IPSec Setup Between Cisco 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 *Cisco Unified Communications Operating System Administration Guide*.

Allow SRTP Using Cisco Unified Communications Manager Administration

The SRTP Allowed check box displays in the following configuration windows in Unified Communications Manager Administration:

- 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 *Cisco Unified Communications Manager Administration Guide*.

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, Cisco strongly recommends 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 19
- Encryption, on page 23

CHAPTER 27

SIP Trunk Security Profile Setup

This chapter provides information about SIP trunk security profile setup.

- About SIP Trunk Security Profile Setup, on page 213
- SIP Trunk Security Profile Setup Tips, on page 213
- Find SIP Trunk Security Profile, on page 214
- Set Up SIP Trunk Security Profile, on page 214
- SIP Trunk Security Profile Settings, on page 215
- Apply SIP Trunk Security Profile, on page 221
- Synchronize SIP Trunk Security Profile with SIP Trunks, on page 222
- Delete SIP Trunk Security Profile, on page 222
- Where to Find More Information About SIP Trunk Security Profiles, on page 223

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 214.

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 In 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 with 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 with 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 214.

The configuration window displays with the current settings.

Step 3 Enter the appropriate settings as described in Table 19: SIP Trunk Security Profile Configuration Settings, on page 215.

Step 4 Click **Save**.

What to do next

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 19: 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 box in the **Trunk Configuration** window.

Setting	Description
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 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**
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 box, 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.

Setting	Description
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.

Setting	Description
Accept Unsolicited Notification	If you want Unified Communications Manager to accept incoming non-INVITE, unsolicited notification messages that come via the SIP trunk, check this check box. If you checked the **Enable Application Level Authorization** check box, go to the **Application User Configuration** window and check the **Accept Unsolicited Notification** check box for any application users that are authorized for this method.
Accept Replaces Header	If you want Unified Communications Manager to accept new SIP dialogs, which have replaced existing SIP dialogs, check this check box. If you checked the **Enable Application Level Authorization** check box, go to the **Application User Configuration** window and check the **Accept Header Replacement** check box for any application users that are authorized for this method.
Transmit Security Status	If you want Unified Communications Manager to transmit the security icon status of a call from the associated SIP trunk to the SIP peer, check this check box. Default: This box is not checked.

Setting	Description
SIP V.150 Outbound SDP Offer Filtering	From the drop-down list box, 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 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.

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 *Cisco Unified Communications Manager Administration Guide*.

Step 2 After the **Trunk Configuration** window displays, locate the **SIP Trunk Security Profile** setting.

Step 3 From the security profile drop-down list box, choose the security profile that applies to the device.

Step 4 Click **Save**.

Step 5 To reset the trunk, click **Apply Config**.

What to do next

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**.

The **Find and List SIP Trunk Security Profiles** window displays.

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. The **SIP Trunk Security Profile Configuration** window displays.

Step 5 Make any additional configuration changes.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

The **Apply Configuration Information** dialog displays.

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 *Cisco Unified Communications Manager System Guide*.

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 28

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 225
- Set Up Digest Authentication Enterprise Parameters, on page 226
- Set Up Digest Credentials, on page 226
- Application User Digest Credential Settings, on page 226
- Find SIP Realm, on page 227
- Configure SIP Realm, on page 227
- SIP Realm Settings, on page 228
- Delete SIP Realm, on page 228

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 *Cisco Unified Communications Manager Administration Guide*.

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 21: SIP Realm Security Profile, on page 228.

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 20: 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 227.

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 21: SIP Realm Security Profile, on page 228.

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 21: 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 29

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 231
- Find Cisco Unified Mobility Advantage Server Security Profile, on page 232
- Set Up Cisco Unified Mobility Advantage Server Security Profile, on page 232
- Cisco Unified Mobility Advantage Server Security Profile Settings, on page 233
- Cisco Unified Mobility Advantage Server Security Profile Client Application, on page 234
- Delete Cisco Unified Mobility Advantage Server Security Profile, on page 234
- Where to Find More Information About Cisco Unified Mobility Advantage Server Security Profile, on page 235

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 232.

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 231.
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 231.
c) To update an existing profile, locate the appropriate security profile and continue with Cisco Unified Mobility Advantage Server Security Profile Setup, on page 231.

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 22: Security Profile Settings, on page 233

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 22: 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 30

FIPS 140-2 Mode Setup

This chapter provides information about FIPS 140-2 mode setup.

• FIPS 140-2 Setup, on page 237

FIPS 140-2 Setup

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

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

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

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

When you enable FIPS 140-2 mode, Unified Communications Manager reboots, runs certification self-tests at startup, performs the cryptographic modules integrity check, and then regenerates the keying materials. At this point, Unified Communications Manager operates in FIPS 140-2 mode.

FIPS requirements include the following: performance of startup self-tests and restriction to a list of approved cryptographic functions.

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

- CiscoSSL 1.0.2n.6.2.194 with FIPS Module CiscoSSL FOM 6_2_0
- CiscoJ 5.2.1
- RSA CryptoJ 6_2_3
- openssh 7.5.9
- NSS

You can perform the following FIPS-related tasks:

- Enable FIPS 140-2 mode
- Disable FIPS 140-2 mode
- Check the status of FIPS 140-2 mode

Note

- By default, your system is in non-FIPS mode, you must enable it.

Enable FIPS 140-2 Mode

You can enable FIPS 140-2 through the CLI. For more information, see the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Consider the following information before you enable FIPS 140-2 mode on Unified CM:

- When you switch from non-FIPS to FIPS mode, the MD5 and DES protocols will not be functional.
- In single server clusters, because certificates are regenerated, you need to run the CTL Client or apply the Prepare Cluster for Rollback to pre-8.0 enterprise parameter before you enable FIPS mode. If you do not perform either of these steps, you must manually delete the ITL file after you enable FIPS mode.
- After you enable FIPS mode on a server, please wait until the server reboots and the phones re-register successfully before enabling FIPS on the next server.

Caution Before you enable FIPS mode, we strongly recommend that you perform a system backup. If FIPS checks fail at start-up, the system halts and requires a recovery CD to be restored.

Procedure

Step 1 Start a CLI session.

For more information, see “Start CLI Session” in the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Step 2 In the CLI, enter **utils fips enable**

The following prompts appear:

```
Security Warning: The operation will regenerate certificates for1)
CallManager

2)Tomcat
3)IPsec
4)TVS
5)CAPF
6)SSH
Any third party CA signed certificates that have been uploaded for the above
components will need to be re-uploaded. If the system is operating in mixed
mode, then the CTL client needs to be run again to update the CTL file.
```

```
*******************************************************************************
This will change the system to FIPS mode and will reboot.
*******************************************************************************
Do you want to continue (yes/no)?
```

Step 3 Enter **yes**.

The following message appears:

```
Generating certificates...Setting FIPS mode in operating system.
FIPS mode enabled successfully.
*******************************************************
It is highly recommended that after your system restarts
that a system backup is performed.
*******************************************************
The system will reboot in a few minutes.
```

Unified CM reboots automatically.

Note Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.

Note If you have a single server cluster and applied the **Prepare Cluster for Rollback to pre 8.0** enterprise parameter before you enabled FIPS 140-2 mode, you must disable this enterprise parameter after making sure that all the phones registered successfully to the server.

Note In FIPS mode, Unified CM uses RedHat Openswan (FIPS validated) in place of Racoon (non-FIPS validated). If the security policies in Racoon contain functions that are not FIPS approved, the CLI command will ask you to redefine the security policies with FIPS approved functions and abort. For more information, see topics related to IPsec Management in the *Cisco Unified Communications Operating System Administration Guide*.

Disable FIPS 140-2 Mode

FIPS 140-2 is disabled through the CLI. For more information, see the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Consider the following information before you disable FIPS 140-2 mode on Unified Communications Manager (Unified CM):

- In single or multiple server clusters, we strongly recommend that you run the CTL Client. If the CTL Client is not run on a single server cluster, you must manually delete the ITL File after disabling FIPS mode.
- In multiple server clusters, each server must be disabled separately, because FIPS mode is not disabled cluster-wide but rather on a per-server basis.

To disable FIPS 140-2 mode, perform the following procedure:

Procedure

Step 1 Start a CLI Session.

For more information, see the Starting a CLI Session section in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Step 2 In the CLI, enter **utils fips disable**

Unified CM reboots and is restored to non-FIPS mode.

Note Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.

Check FIPS 140-2 Mode Status

To confirm that FIPS 140-2 mode is enabled, check the mode status from the CLI.

To check the status of FIPS 140-2 mode, perform the following procedure:

Procedure

Step 1 Start a CLI Session.

For more information, see the Starting a CLI Session section in the *Command Line Interface Reference Guide for Cisco Unified Communications Solutions*.

Step 2 In the CLI, enter **utils fips status**

The following message appears to confirm that FIPS 140-2 mode is enabled.

```
admin:utils fips status
The system is operating in FIPS mode. Self test status:

- S T A R T --------------------
Executing FIPS selftests
runlevel is N 3
Start time: Thu Apr 28 15:59:24 PDT 2011
NSS self tests passed.
Kernel Crypto tests passed.
Operating System OpenSSL self tests passed.
Openswan self tests passed.
OpenSSL self tests passed.
CryptoJ self tests passed...
```

FIPS 140-2 Mode Server Reboot

When a Unified Communications Manager (Unified CM) server reboots in FIPS 140-2 mode, it triggers FIPS startup self-tests in each of the FIPS 140-2 modules after rebooting.

Caution If any of these self-tests fail, the Unified CM server halts.

Note A Unified CM server is automatically rebooted when FIPS is enabled or disabled with the corresponding CLI command. A user can also initiate a reboot.

Caution If the startup self-test failed because of a transient error, restarting the Unified CM server fixes the issue. However, if the startup self-test error persists, it indicates a critical problem in the FIPS module and the only option is to use a recovery CD.

INDEX

A

authentication 8, 9, 10, 19, 181
- device 19
- digest 19
- interactions 8, 9
- overview 19
- restrictions 8, 10
- with CTI/JTAPI/TAPI applications 181

authentication string 95, 105, 107, 183
- entering on phone 107
- finding phones using 105
- with CAPF 95
- with CTI/JTAPI/TAPI applications 183

authorization 9, 19, 214, 215
- configuration settings (table) 215
  - for SIP trunk 215
- configuring for SIP trunk 214
- interactions 9
- overview 19

B

barge 14, 127, 129
- encryption restrictions with 14
- security 127
- security icons 129

C

Certificate Authority Proxy Function (CAPF) 15, 57, 95, 96, 97, 100, 101, 102, 103, 104, 105, 106, 107, 183, 185, 188, 189, 190, 192, 193
- activating service 101
- authentication string 107
  - entering on phone 107
- CAPF service 57
- configuration checklist (table) 101
- configuration settings (table) 104, 190
  - for CTI/JTAPI/TAPI applications 190
  - for phones 104
- configuring an application user or end user CAPF profile 189
- configuring in Cisco Unified Serviceability 101
- deleting an application user or end user CAPF profile 192
- finding an application user or end user CAPF profile 188
- finding phones using LSC or authentication string 105

Certificate Authority Proxy Function (CAPF) *(continued)*
- generating CAPF report 106
- installing 15
- interaction with Cisco Unified IP Phone 96
- interaction with IPv6 addressing 97
- interactions and requirements 100
- overview 95
- updating service parameters 102
- using for phone certificate operations 103
- viewing certificate operation status for application user or end user 193
- with CTI/JTAPI/TAPI applications 183, 185, 188
  - interactions and requirements 185
  - overview 183
  - updating service parameters 188

Certificate Signing Requests (CSRs) 16

certificates 16, 38, 40
- external CAs 16
- Firefox certificate 38
- Safari certificate 40
- types 16

Cisco Unified IP Phone 7, 69, 73, 75, 96, 104, 107, 109, 124, 132
- authentication string 107
  - entering on phone 107
- configuration checklist (table) for security 73
- configuration settings (table) 104
  - for CAPF 104
- configuration tips for phone security profiles 75
- disabling the PC Port setting 124
- disabling the PC Voice VLAN Access setting 124
- disabling the Setting Access setting 124
- encrypted configuration file 109
- interaction with CAPF 96
- secure conference support 132
- security icons 7
- understanding security 69
- viewing security settings 73

computer telephony integration (CTI) 185, 186
- configuration checklist (table) for securing 185
- secure user groups 186
  - adding application users and end users 186

conference bridge 127, 128, 129, 133, 134, 135, 136, 137, 138
- conference list 129
- configuration checklist (table) for security 135
- configuration tips for security 134

conference bridge *(continued)*
configuring minimum Meet-Me security 137
configuring packet capture on a secure conference bridge 138
configuring security 136
minimum Meet-Me security level 129
security 127
security icons 129
security interactions 133
security requirements 128
security restrictions 133
configuration file 23
encryption 23
CTL client 15, 55, 56, 57, 58, 60, 61, 62, 63
CAPF service 57
cluster security mode 60
updating 60
configuration settings (table) 61
configuring 57, 58
CTL client 58
TLS port 57
CTL Provider service 56
installing 15
overview 55
security mode 62
verifying 62
security token 58
configuring CTL client 58
setting the Smart Card service 62
uninstalling 63
verifying 63
CTL file 59
updating 59
CTL Provider 56
activating service 56

D

device authentication 19, 77, 214, 215
configuration settings (table) 77, 215
for phone that is running SCCP 77
for phone that is running SIP 77
for SIP trunk 215
configuring for phones 77
configuring for SIP trunk 214
overview 19
digest authentication 19, 77, 119, 120, 121, 214, 215, 225, 226, 227, 228
associating digest user with a phone 121
cluster ID 226
configuration checklist (table) 119, 225
for phones 119
for SIP trunk 225
configuration settings (table) 77, 121, 215, 226, 228
for application user digest credentials 226
for end user 121
for phone that is running SIP 77
for SIP realm 228
digest authentication *(continued)*
configuration settings (table) *(continued)*
for SIP trunk 215
configuring a SIP realm 227
configuring digest credentials 120, 226
for application user 226
for end user 120
configuring for phones 77
configuring for SIP trunk 214
configuring service parameters 120
deleting a SIP realm 228
finding a SIP realm 227
overview 19

E

encrypted configuration file 109, 110, 111, 112, 113, 114, 115, 116, 117
configuration checklist (table) 113
configuration settings (table) 115
for manual key 115
configuration tips 112
configuring manual key distribution 114
disabling 117
enabling 114
entering symmetric key 115
manual key configuration checklist (table) 115
manual key distribution 110
phone support 111
symmetric key encryption with public key 111
understanding 109
using symmetric key encryption w/public key 116
encryption 8, 9, 10, 14, 15, 23, 77, 133, 183, 207, 208, 209, 210, 211, 214, 215
configuration checklist (table) for gateways and trunks 210
configuration settings (table) 77, 215
for phone that is running SCCP 77
for phone that is running SIP 77
for SIP trunk 215
configuring for phones 77
configuring SRTP allowed check box 211
configuring with barge 14
for H.323 gateway 208
for H.323/H.225/H.245 trunk 208
for MGCP gateway 207
for SIP trunk 209
installing 15
interactions 8, 9, 133
overview 23
restrictions 8, 10, 133
signaling 77, 214
configuring for phones 77
configuring for SIP trunk 214
with CTI/JTAPI/TAPI applications 183
etoken 58
configuring CTL client 58

F

file authentication 19, 77
configuring for phones 77
overview 19

H

HTTPS 31, 38, 40
overview 31
virtual directories (table) 31
with Firefox 38
with Safari 40

I

image authentication 19
overview 19
integrity 19
overview 19
IPSec 15, 210, 211
configuration checklist (table) for IPSec 210
configuring 211
gateway or trunk considerations 211
infrastructure considerations 211
recommendations 211

J

JTAPI 185, 193
configuration checklist (table) for securing 185
configuring security service parameters 193

L

locally significant certificate (LSC) 105, 183
finding phones using 105
with CTI/JTAPI/TAPI applications 183

M

media encryption, *See* encryption
MGCP gateway 210, 211
configuration checklist (table) for security 210
configuring 211

N

NMAP scans 26
running 26

P

phone hardening 124
configuring 124
disabling the PC Port setting 124
disabling the PC Voice VLAN Access setting 124
disabling the Setting Access setting 124
phone security profile 87
synchronizing configuration to applicable phones 87
port 57
CTL Provider 57
Ethernet phone 57
SIP secure 57
protected call 89

S

secure conference 127, 128, 129, 132, 133, 134, 135, 136, 137, 138
Cisco Unified IP Phone support 132
conference bridge requirements 128
conference list 129
configuration checklist (table) 135
configuration tips 134
configuring minimum Meet-Me security 137
configuring packet capture 138
configuring secure conference bridge 136
CTI support 132
interactions 133
minimum Meet-Me security level 129
restrictions 133
security icons 129
security overview 127
trunks and gateways 132
secure indication tone 89
secure sockets layer (SSL) 15, 31
installing 15
with HTTPS 31
security 1, 6, 8, 9, 10, 13, 14, 15, 16, 19, 23, 26, 29, 31, 55, 58, 59, 133
authentication overview 19
authorization overview 19
best practices 13
certificate types 16
configuration checklist for authentication and encryption (table) 26
CTL client overview 55
encryption overview 23
external CAs 16
features list 6
HTTPS 31
installing 15
interactions 8, 9, 133
rebooting the cluster 14
rebooting the server 14
resetting devices 14
restarting Cisco Unified Communications Manager service 14
restrictions 8, 10, 133

security *(continued)*
SCCP calls (table) 6
SIP calls (table) 6
system requirements 6
terminology (table) 1
tokens 55, 58, 59
using barge with encryption 14
where to find more information 29
security mode 60, 62
cluster 60, 62
configuring 60
verifying 62
security profile 75, 76, 77, 86, 87, 88, 213, 214, 215, 221, 222, 231, 232, 234
applying for SIP trunk 221
applying to Cisco Unified Mobility Advantage Server 234
applying to phones 86
configuration settings (table) 77, 215
for phone that is running SCCP 77
for phones that is running SIP 77
for SIP trunk 215
configuration tips for phones 75
configuring for phones 77
configuring for SIP trunk 214
deleting for Cisco Unified Mobility Advantage server 234
deleting for phones 87
deleting for SIP trunk 222
finding for Cisco Unified Mobility Advantage servers 232
finding for phones 76
finding for SIP trunk 214
finding phones that use 88
overview for Cisco Unified Mobility Advantage 231
overview for phones 75
overview for SIP trunk 213
security token 58
configuring CTL client 58
signaling authentication 19
overview 19
signaling encryption 23
overview 23
SIP Trunk security profile 222
synchronizing configuration to applicable SIP trunks 222
Site Administrator Security Token (SAST) 55
SRST 201, 202, 203, 206, 237
configuration checklist (table) for securing 203
SRST *(continued)*
configuration tips for securing 202
overview for securing 201, 237
troubleshooting 206
certificate deleted on gateway 206
SRST reference 203, 204, 206, 238, 239
configuration settings (table) for security 204
configuring 203, 238, 239
troubleshooting 206
deleting secured reference 206

T

TAPI 185, 193
configuration checklist (table) for securing 185
configuring security service parameters 193
Tftp service 55
TLS Proxy server 55
transport layer security (TLS) 15, 57
port 57
transport security 15, 77, 214, 215
and real-time protocol (RTP) 15
and secure real-time protocol (SRTP) 15
configuration settings (table) 77, 215
for phone that is running SCCP 77
for phone that is running SIP 77
for SIP trunk 215
configuring for phones that are running SIP 77
configuring for SIP trunk 214
IPSec 15
TLS 15
troubleshooting 206
SRST certificate deleted on gateway 206

V

voice messaging 139, 140
configuration checklist (table) for security 140
security overview 139
security requirements 139
voice messaging port 139, 140, 141, 142
applying a security profile 141
applying a security profile using the Wizard 142
configuration checklist (table) for security 140
security overview 139