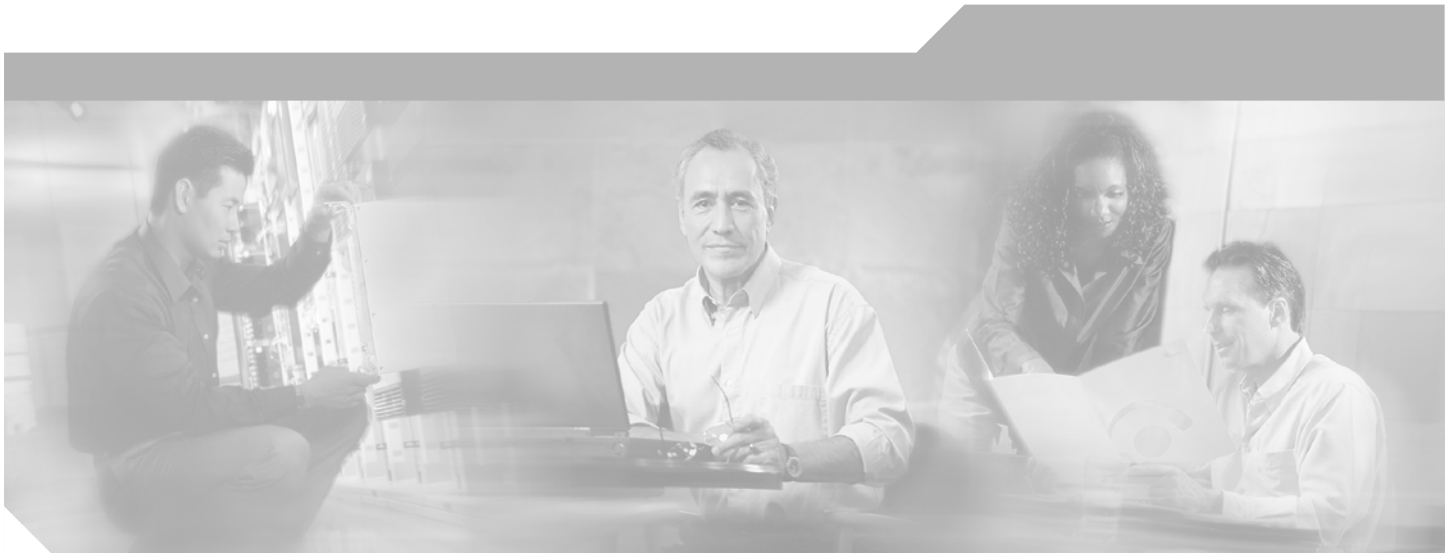


Cisco Unified CallManager Security Guide

Release 5.0(4)

Corporate 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: 408 526-4100

Text Part Number: OL-10051-01

Cisco Unified CallManager Security Guide

CONTENTS

Preface

This preface describes the purpose, audience, organization, and conventions of this guide and provides information on how to obtain related documentation.

The preface covers these topics:

Purpose

Cisco Unified CallManager 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 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.
- Troubleshoot issues.

Audience

This guide provides a reference and procedural guide for system and phone administrators who plan to configure the security features.

Organization

Table 1 lists the major sections of this guide:

Table 1 Guide Overview

Chapter	Description
Security Basics	
Chapter 1, "Security Overview"	Provides an overview of security terminology, system requirements, interactions and restrictions, installation requirements, and a configuration checklist; describes the different types of authentication and encryption.
Chapter 2, "Using Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)"	Provides an overview of HTTPS and describes how to install the server authentication certificate in the trusted folder.
Chapter 3, "Configuring the Cisco CTL Client"	Describes how to configure authentication by installing and configuring the Cisco CTL client.

Table 1 Guide Overview (continued)

Chapter	Description
Security for Phones and Voice Mail Ports	
Chapter 4, “Phone Security Overview”	Describes how Cisco Unified CallManager and the phone use security; provides a list of tasks that you perform to configure security for the phone.
Chapter 5, “Configuring a Phone Security Profile”	Describes how to configure the security profile and apply it to the phones in Cisco Unified CallManager Administration.
Chapter 6, “Using the Certificate Authority Proxy Function”	Provides an overview of Certificate Authority Proxy Function and describes how to install, upgrade, delete, or troubleshoot locally significant certificates on supported phones.
Chapter 7, “Configuring Encrypted Phone Configuration Files”	Describes how to configure encrypted phone configuration files in Cisco Unified CallManager Administration.
Chapter 8, “Configuring Digest Authentication for the SIP Phone”	Describes how to configure digest authenticationon the SIP phone in Cisco Unified CallManager Administration.
Chapter 9, “Phone Hardening”	Describes how to tighten the security on the phone by using Cisco Unified CallManager Administration.
Chapter 10, “Configuring Voice Messaging Ports for Security”	Describes how to configure security for voice mail ports in Cisco Unified CallManager Administration.
Security for CTI, JTAPI, and TAPI	
Chapter 11, “Configuring Authentication and Encryption for CTI, JTAPI, and TAPI”	Describes how to configure the Application User CAPF Profile and End User CAPF Profiles in Cisco Unified CallManager Administration.
Security for SRST References, Gateways, and Trunks	
Chapter 12, “Configuring a Secure Survivable Remote Site Telephony (SRST) Reference”	Describes how to configure the SRST reference for security in Cisco Unified CallManager Administration.
Chapter 13, “Configuring Encryption for Gateways and Trunks”	Describes how Cisco Unified CallManager communicates with a secure gateway or trunk; describes IPSec recommendations and considerations.
Chapter 14, “Configuring the SIP Trunk Security Profile”	Describes how to configure and apply the SIP trunk security profile in Cisco Unified CallManager Administration.
Chapter 15, “Configuring Digest Authentication for the SIP Trunk”	Describes how to configure digest authentication for the SIP trunk in Cisco Unified CallManager Administration.

Related 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 CallManager*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- Cisco Unified Survivable Remote Site Telephony (SRST) administration documentation that supports the SRST-enabled gateway
- The firmware release notes that support 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.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

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.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance please contact us by sending email to export@cisco.com.

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

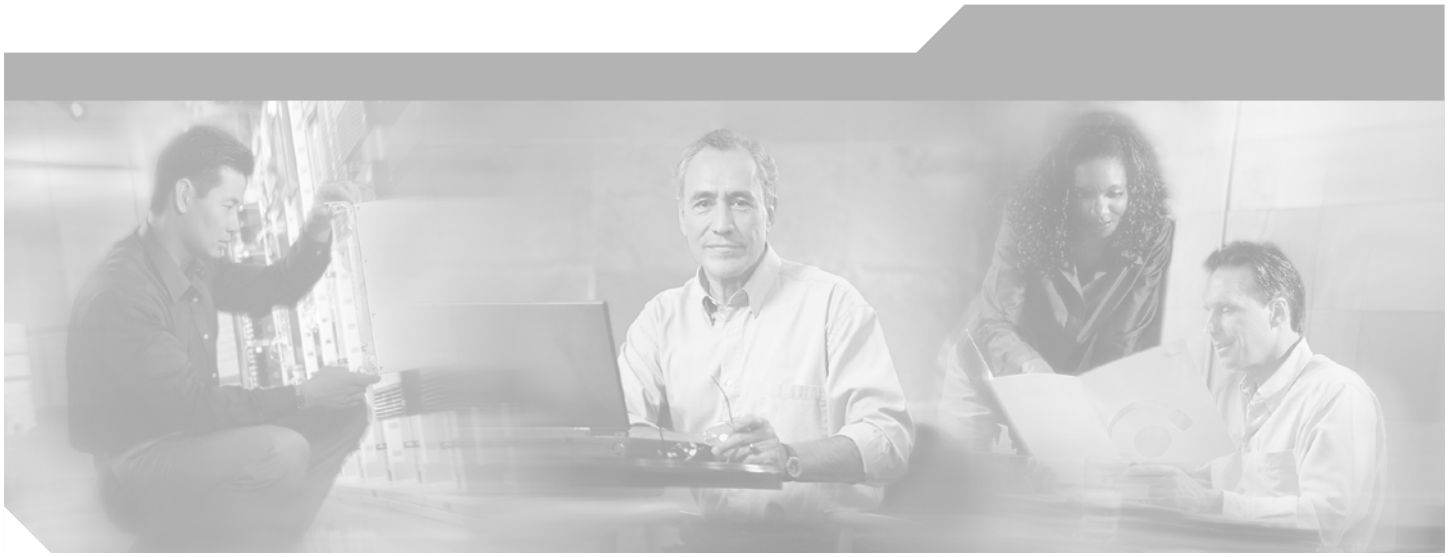
  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html



PART 1

Security Basics

CHAPTER 1

Security Overview

Implementing security mechanisms in the Cisco Unified CallManager system prevents identity theft of the phone/Cisco Unified CallManager 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.

This chapter provides information on the following topics:

Authentication and Encryption Terminology

The definitions in Table 1-1 apply when you configure authentication and encryption for your Cisco IP telephony network:

Table 1-1 Terminology

Term	Definition
Access control list (ACL)	List that defines rights and permissions to access system functions and resources. See Method List.
Authentication	Process that verifies the identity of an entity.
Authorization	Specifies whether an authenticated user, service, or application has the necessary permissions to perform a requested action; in Cisco Unified CallManager, security process that restricts SUBSCRIBE requests and certain trunk-side SIP requests to authorized users.
Authorization Header	A SIP user agent response to a challenge.
Certificate Authority (CA)	Entity that issues certificates; may be a Cisco or third-party entity.
Certificate Authority Proxy Function (CAPF)	Process by which supported devices can request locally significant certificates by using Cisco Unified CallManager Administration.
Certificate Trust List (CTL)	A file that contains a list of certificates that the phone is to trust. The Cisco Site Administrator Security Token (security token) signs the CTL file. The CTL file gets created automatically when the Cisco CTL client is used to transition the cluster to secure/mixed-mode.
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 signs the CTL file.
Device Authentication	Process that validates the identity of the device and ensures that the entity is what it claims to be before making a connection.
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 the authorization request that SIP phones or SIP trunks send.
Encryption	Process that ensures that only the intended recipient receives and reads the data; process that ensures the confidentiality of the information; process that translates data into ciphertext, which appears random and meaningless. 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.
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.

Table 1-1 Terminology (continued)

Term	Definition
Image Authentication	Process that prevents tampering with the binary image prior to loading it on the phone; process whereby a phone validates the integrity and source of an image.
Integrity	Process that ensures that data tampering has not occurred between entities.
IPSec	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 is installed on the phone or JTAPI/TAPI/CTI application; issued by a third-party certificate authority or CAPF.
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.
Man-in-the-Middle Attacks	Process that allows an attacker to observe and modify the information flow between Cisco Unified CallManager and the phone.
Media Encryption	Process whereby the confidentiality of the media is protected by use of 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 coming 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	Mode within a cluster that you configured for security; includes authenticated and nonauthenticated devices that connect to the Cisco Unified CallManager.
Nonce	A unique, random number that the server generates for each digest authentication request.
Nonsecure Call	Call in which at least one device is not authenticated or encrypted.
PKI	Public key infrastructure; the set of elements that is needed for public key encryption, including certificates and certificate authorities.
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.
System Administrator Security Token (SAST)	In CTI/JTAPI/TAPI applications, a token that is used to sign the CTL file for CTL download.
Simple Certificate Enrollment Protocol (SCEP)	An add-on that Microsoft Certificate Services Manager uses to generate certificates with CAPF function.
Secure Call	Call in which all devices are authenticated and the media stream is encrypted.
Signaling Authentication	Process that validates that no tampering occurred to signaling packets during transmission; uses the Transport Layer Security protocol.

Table 1-1 Terminology (continued)

Term	Definition
Signaling Encryption	Process that uses cryptographic methods to protect the confidentiality of all signaling messages that are sent between the device and the Cisco Unified CallManager server.
SIP Realm	A string (name) that specifies protected space in digest authentication; identifies the line or trunk side user agent for the SIP request.
SSL	Part of TLS infrastructure for transport security.
Transport Layer Security (TLS)	A security protocol that defines IETF and that provides integrity, authentication, and encryption and resides in the TCP layer in the IP communications stack.
Trust List	Certificate list without digital signatures.
Trust Store	Contains the list of trusted certificates and their public keys in Cisco Unified CallManager; CA, CAPF, root, and peer certificates get put in the trust store.
X.509	Binary format for importing digital user and CA certificates.

System Requirements

The following system requirements exist for authentication or encryption:

- Cisco Unified CallManager 5.0(4) serves as the minimum requirement for the security features described in this document.
- The Administrator password can be different on every server in the cluster.
- The username and password used at the Cisco CTLclient (to log into the Cisco Unified CallManager server) is the same as Cisco Unified CallManager Administration username and password (the username and password used to log into the Cisco Unified CallManager Administration).
- For Certificate Authority Proxy Function (CAPF) information, see the "CAPF System Interactions and Requirements" section on page 6-3.
- Before you configure voice mail ports for security, verify that you installed a version of Cisco Unity that supports Cisco Unified CallManager 5.0.

Features List

Cisco Unified CallManager 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.

Table 1-2 provides a summary of security features that Cisco Unified CallManager can implement during a SIP or SCCP call, depending on the features supported and configured.

Table 1-2 Call Processing Security Features List

Security Feature	Line Side	Trunk Side
Transport/Connection/Integrity	Secure TLS port	IPSec associations Secure TLS port (SIP trunk only)
Device Authentication	TLS certificate exchange w/CAPF	IPSec certificate exchange or pre-shared key
Digest Authentication	SIP phone users only	SIP trunk users and SIP trunk application users
Signaling Authentication/Encryption	TLS Mode: authenticated or encrypted	IPSec [authentication header, encryption (ESP), or both] TLS Mode: authenticated or encrypted mode (SIP trunk only)
Media Encryption	SRTP	SRTP
Authorization	Presence requests	Presence requests Method list
Note: The features supported on a device vary by device type and protocol.		

Security Icons

Phones that support security icons display the Cisco Unified CallManager security level that is associated with a call.

- 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.
- The phone displays a lock icon for calls with encrypted media, meaning the media stream between the Cisco IP devices is encrypted.

Refer to "Phone Icons and Encryption" section on page 1-9, for restrictions that are associated with security icons.

Interactions and Restrictions

This section contains information on the following topics:

Interactions

This section describes how Cisco security features interact with Cisco Unified CallManager applications.

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

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

To allow presence requests on SIP trunks, you must authorize Cisco Unified CallManager to accept presence requests on the SIP trunk and, if required, configure end user clients in Cisco Unified CallManager Administration to allow Cisco Unified CallManager to accept and authenticate incoming presence requests from the remote device and application.

To use SIP-initiated transfer features and other advanced transfer-related features on SIP trunks, such as Web Transfer and Click to Dial, you must authorize Cisco Unified CallManager 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), you must authorize Cisco Unified CallManager to accept Unsolicited Notification SIP requests.

To allow Cisco Unified CallManager to transfer an external call on a SIP trunk to an external device or party (in attended transfer, for example) you must authorize Cisco Unified CallManager to accept SIP requests with replaces header in REFERS and INVITES.

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

Cisco Unified CallManager Assistant supports a secure connection to CTI (transport layer security connection); the administrator must configure a CAPF profile (one for each Cisco Unified CallManager Assistant node).

When multiple instance of a CTI/JTAPI/TAPI application are running, CTI TLS support requires administrators 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 Cisco Unified CallManager through the Cisco Unified CallManager TLS port. When the security mode equals nonsecure, the Cisco Unity TSP connects to Cisco Unified CallManager through the Cisco Unified CallManager port.

Restrictions

The following sections describe restrictions that apply to Cisco security features:

- Phone Icons and Encryption, page 1-9
- Cluster and Device Security Modes, page 1-9
- Packet Capturing and Encryption, page 1-9

Authentication and Encryption

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

- Auto-registration does not work when you configure the cluster for mixed mode.
- You cannot implement signaling or media encryption if device authentication does not exist in the cluster; that is, if you do not enable the CTL Provider service or install and configure the Cisco CTL client.
- Cisco does not support Network Address Translation (NAT) with Cisco Unified CallManager if you configure the cluster for 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 of the firewall.

  Signaling encryption does not support NAT traversal. Instead of using NAT, consider using LAN extension VPNs.
- SRTP encrypts voice packets only.

Barge and Encryption

The following restrictions apply to barge and encryption:

- A Cisco Unified IP Phone model 7960 (SCCP) and 7970 user cannot barge into an encrypted call if the Cisco Unified IP Phone model 7970 that is used to barge is not configured for encryption. When barge fails in this case, a busy tone plays on the phone where the user initiated the barge.

  If the initiator phone is configured for encryption, the barge initiator can barge into an authenticated or nonsecure call from the encrypted phone. After the barge occurs, Cisco Unified CallManager classifies the call as nonsecure.

  If the initiator phone is configured for encryption, the barge initiator can barge into an encrypted call, and the phone indicates that the call state equals encrypted.

  A user can barge into an authenticated call, even if the phone that is used to barge is nonsecure. The authentication icon continues to display on the authenticated devices in the call, even if the initiator phone does not support security.

Tip You can configure cbarge if you want barge functionality, but Cisco Unified CallManager automatically classifies the call as nonsecure.

- If you configure encryption for Cisco Unified IP Phone models 7960 and 7940, 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. A tone plays on the phone to indicate that the barge failed.

  A message displays in Cisco Unified CallManager Administration when you attempt the following configuration:

  – In the Phone Configuration window, you apply a security profile that supports encryption, you choose **On** for the Built In Bridge setting (or default setting equals On), and you click **Save** after you create this specific configuration.

  – In the Service Parameter window, you update the Builtin Bridge Enable parameter.

Wideband Codecs and Encryption

The following information applies for Cisco Unified IP Phone models 7960 or 7940 that are configured for encryption and associated with a wideband codec region. This only applies to Cisco Unified IP Phone models 7960 or 7940 that are configured for TLS/SRTP.

To establish an encrypted call, Cisco Unified CallManager 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, Cisco Unified CallManager may establish the authenticated/nonsecure call by using the wideband codec.

Media Resources and Encryption

Cisco Unified CallManager 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, and secure H.323/H.245/H.225 trunks where no media resources are used. For example, Cisco Unified CallManager 5.0 does not provide media encryption in the following cases:

- Calls that involve transcoders or media termination points
- Ad hoc or Meet Me conferences
- Calls that involve music on hold

Device Support and Encryption

Some Cisco Unified IP Phone models, such as CiscoUnified IP Phone model 7912, do not support encrypted calls. Some phones support encryption but do not validate certificate signatures. Refer to the Cisco Unified IP Phone administration guides for Cisco Unified IP Phone models that support encryption and this version of Cisco Unified CallManager for more information.

Note In this release, the following Cisco Unified SCCP IP Phone models support encryption: 7906, 7911, 7940, 7941, 7941G-GE, 7960, 7961, 7961G-GE, 7970, 7971. The following Cisco Unified SIP IP Phone models support encryption: 7906, 7911, 7941, 7941G-GE, 7961, 7961G-GE, 7970, 7971.

Cisco Unified SIP IP Phone models 7940/7960 support signaling encryption with TLS.

SIP trunks do not support SRTP encryption; Cisco Unified CallManager secures calls on SIP trunks with TLS.

Note Cisco Unified CallManager supports SRTP primarily for IOS gateways and Cisco Unified CallManager H.323 trunks on gatekeeper-controlled and non-gatekeeper-controlled trunks. If SRTP cannot be engaged for a call, Cisco Unified CallManager engages RTP.

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 new firmware (except for Cisco Unified IP Phone models 7905 and 7912) that is compatible with this release to receive full encrypted configuration files. Cisco Unified IP Phone models 7905 and7912 use existing security mechanisms and do not require new firmware for this feature.

Refer to "Supported Phone Models" section on page 7-4, for phone support of encrypted configuration files.

Phone Icons and Encryption

The encryption lock icon indicates that the media stream between the Cisco IP devices is encrypted.

The encryption lock icon may not display on the phone when you perform tasks such as conferencing, transferring, or putting a call on hold; the status changes from encrypted to nonsecure if the media streams that are associated with these tasks are not encrypted.

Cisco Unified CallManager does not display the lock icon for calls that originate at or terminate to SIP trunk-side connections. Cisco Unified CallManager does not display the shield icon for calls that are transiting H.323 trunks.

Cluster and Device Security Modes

When the cluster security mode equals nonsecure, the device security mode is nonsecure in the phone configuration file, even though Cisco Unified CallManager 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 the Cisco Unified CallManager servers in the cluster.

When the cluster security mode equals nonsecure, the security-related configuration in Cisco Unified CallManager Administration gets ignored; for example, the device security mode, the SRST Allowed check box, and so on. The configuration does not get deleted in Cisco Unified CallManager Administration, but security is not provided.

The phone attempts a secure connection to the SRST-enabled gateway only when the cluster security mode equals secure, 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.

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 in Cisco Unified CallManager Administration with a configuration change in Cisco Unified CallManager Administration (for devices that support packet capturing).

Best Practices

Cisco strongly recommends the following best practices:

- Always perform installation and configuration tasks in a secure lab environment before you deploy to a wide-scale network.
- Use IPSec for gateways and other application servers at remote locations; for example, Cisco Unity, or Cisco Unified Contact Center, or other Cisco Unified CallManager servers.

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

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

Resetting the Devices, Restarting Services, or Rebooting the Server/Cluster

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

Consider the following guidelines:

- Reset a single device after you apply a different security profile in Cisco Unified CallManager Administration.
- Reset the devices if you perform phone-hardening tasks.
- Reset the devices after you change the clusterwide 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 clusterwide 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 CallManager Serviceability after you configure the Cisco CTL client or update the CTL file. Perform this task on all servers that run these services.
- 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 CallManager IP Manager Assistant Service, Cisco WebDialer 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 the *Cisco Unified CallManager Serviceability Administration Guide*.

To reset a single device after updating the configuration, see the "Applying a Phone Security Profile" section on page 5-9.

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

Procedure

Step 1 In Cisco Unified CallManager Administration, choose **System > Cisco Unified CallManager**.

The Find/List window displays.

Step 2 Click **Find**.

A list of configured Cisco Unified CallManager servers displays.

Step 3 Choose the Cisco Unified CallManager on which you want to reset devices.

Step 4 Click **Reset**.

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

Configuring Media Encryption with Barge

Use the following information with the "Barge and Encryption" section on page 1-7.

When you attempt to configure barge for Cisco Unified IP Phone models 7960 and 7940 that are configured for encryption, the following message displays:

If you configure encryption for Cisco Unified IP Phone models 7960 and 7940, 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 Cisco Unified CallManager Administration:

- In the Phone Configuration window, you choose **Encrypted** for the Device Security Mode (or System Default equals Encrypted), and **On** for the Built In Bridge setting (or default setting equals On), and you click **Insert** or **Update** after you create this specific configuration.
- In the Enterprise Parameter window, you update the Device Security Mode parameter.
- In the Service Parameter window, you update the Built In Bridge Enable parameter.

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

Installation

To obtain authentication support, you install a plug-in, the Cisco CTL client, from Cisco Unified CallManager Administration. To install the Cisco CTL client, you must obtain at least two security tokens.

Media and signaling encryption capabilities automatically install when you install Cisco Unified CallManager.

Cisco Unified CallManager automatically installs Secure Sockets Layer (SSL) for Cisco Unified CallManager virtual directories.

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

TLS and IPSec

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

- Transport Layer Security (TLS) provides secure and reliable data transfer between two systems or devices, using secure ports and certificate exchange. TLS secures and controls connections between Cisco Unified CallManager-controlled systems, devices, and processes to prevent access to the voice domain. Cisco Unified CallManager uses TLS to secure SCCP calls to SCCP phones and SIP calls to SIP phones or trunks.
- IP Security (IPSec) provides secure and reliable data transfer between Cisco Unified CallManager and gateways. IPSec implements signaling authentication and encryption to Cisco IOS MGCP and H.323 gateways. IPSec uses real-time protocol (RTP) for message authentication and to transport the actual date stream in a connection.

Secure RTP (SRTP) can be added 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 originating at or terminating 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.

Certificate Types

Certificates secure client and server identities. Cisco uses the following certificate types in phones:

- Manufacture-installed certificate (MIC)—Cisco manufacturing automatically installs this certificate in supported phone models. With certain phone models, one MIC and one locally significant certificate can exist in the same phone, in which case, the LSC takes precedence over the MIC for authentication to the Cisco Unified CallManager after you configure the device security mode for authentication or encryption.

  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). With certain phone models, one LSC and one MIC can exist in the same phone, in which case, the LSC takes precedence over the MIC for authentication to the Cisco Unified CallManager after you configure the device security mode for authentication or encryption.

The Certificate Management Tool does not manage these certificates that are stored in the phone.

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

- HTTPS certificate (tomcat_cert)—This self-signed root certificate gets generated during the Cisco Unified CallManager installation for the HTTPS server.

- Cisco Unified CallManager node certificate—This self-signed root certificate automatically installs when you install Cisco Unified CallManager 5.0 for the Cisco Unified CallManager server. Cisco Unified CallManager certificates provide server identification, including the Cisco Unified CallManager server name and the Global Unique Identifier (GUID).
- CAPF certificate—The system copies this root certificate to all servers in the cluster after you complete the Cisco CTL client configuration.
- IPSec certificate (ipsec_cert)—This self-signed root certificate gets generated during Cisco Unified CallManager installation for IPSec connections with MGCP and H.323 gateways.
- SRST-enabled gateway certificate—When you configure a secure SRST reference in Cisco Unified CallManager Administration, Cisco Unified CallManager retrieves the SRST-enabled gateway certificate from the gateway and stores it in the Cisco Unified CallManager database. After you reset the devices, the certificate gets added to the phone configuration file. Because the certificate is stored in the database, this certificate does not get integrated into the certificate management tool.

After root certificates are installed, certificates get added to the root trust stores to secure connections between users and hosts, integrate application devices, and so on.

Cisco Unified CallManager imports the following certificate types to the Cisco Unified CallManager trust store:

- Cisco Unity server certificate—Cisco Unity uses this self-signed root certificate to sign the Cisco Unity SCCP device certificates. The Cisco Unity Telephony Integration Manager manages this certificate.
- Cisco Unity SCCP device certificates—Cisco Unity SCCP devices use this signed certificate to establish a TLS connection with the Cisco Unified CallManager. Every Unity device (or port) gets issued a certificate that is rooted at the Unity root certificate. The Unity certificate name is a hash of the certificate's subject name, which is based on the Unity machine name.
- SIP Proxy server certificate—A SIP user agent that connects via a SIP trunk authenticates to Cisco Unified CallManager if the Cisco Unified CallManager trust store contains the SIP user agent certificate and if the SIP user agent contains the Cisco Unified CallManager certificate in its trust store.

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

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

Note Cisco Unified CallManager supports only PEM (.pem) and DER (.der) formatted certificates.

For information on updating the Cisco Unified CallManager trust store, generating Certificate Signing Requests (CSRs), and managing certificates, refer to the *Cisco Unified Communications Operating System Administration Guide.*

Authentication, Integrity, and Authorization Overview

Integrity and authentication protect against the following threats:

- TFTP file manipulation (integrity)
- Modification of call-processing signaling between the phone and Cisco Unified CallManager (authentication)
- Man-in-the-middle attacks (authentication), as defined in Table 1-1
- 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.

See the following sections for information on authentication, integrity, and authorization:

- Image Authentication, page 1-14
- Device Authentication, page 1-14
- File Authentication, page 1-15
- Signaling Authentication, page 1-15
- Digest Authentication, page 1-16
- Authorization, page 1-17

Image Authentication

This process prevents tampering with the binary image, that is, 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 are automatically installed when you install Cisco Unified CallManager. Likewise, firmware updates that you download from the web also provide signed binary images.

Device Authentication

This process validates the identity of the device and ensures that the entity is who it claims to be. For a list of devices that are supported, see the "Supported Phone Models" section on page 4-2.

Device authentication occurs between the Cisco Unified CallManager 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. This process of mutual certificate exchange is called mutual authentication.

Device authentication relies on the creation of the Cisco CTL file (for authenticating Cisco Unified CallManager server node and applications), as described in "Configuring the Cisco CTL Client" section on page 3-1, and the Certificate Authority Proxy Function (for authenticating phones and JTAPI/TAPI/CTI applications), as described in "Using the Certificate Authority Proxy Function" section on page 6-1.

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

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 the "Supported Phone Models" section on page 4-2.

The TFTP server does not sign any files if you configure the cluster for nonsecure mode. 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 Cisco Unified CallManager Administration.

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 Cisco Unified CallManager entry and certificate must exist in the file.
- You configured the device for authentication or encryption.

Note File authentication relies on the creation of the Certificate Trust List (CTL) file, which the "Configuring the Cisco CTL Client" section on page 3-1 describes.

Signaling Authentication

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

Signaling authentication relies on the creation of the Certificate Trust List (CTL) file, which the "Configuring the Cisco CTL Client" section on page 3-1 describes

Digest Authentication

This process for SIP trunks and phones allows Cisco Unified CallManager to challenge the identity of a SIP user agent (UA) when the UA sends a request to Cisco Unified CallManager. (A SIP user agent represents a device or application that originates a SIP message.)

Cisco Unified CallManager acts as a user agent server (UAS) for SIP calls originated by line-side phones or devices 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, Cisco Unified CallManager acts primarily as B2BUA connecting SCCP and SIP endpoints.

Cisco Unified CallManager can challenge SIP phones or SIP devices connecting through a SIP trunk (as a UAS) and can respond to challenges received on its SIP trunk interface (as a UAC). When digest authentication is enabled for a phone, Cisco Unified CallManager challenges all SIP phone requests except keepalive messages.

Note Cisco Unified CallManager does not respond to challenges from line-side phones.

Cisco Unified CallManager 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 UA and Cisco Unified CallManager (the originating call leg) and the other leg between Cisco Unified CallManager and destination SIP UA (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 negotiated between the user agents.

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.

Cisco Unified CallManager server uses a SIP 401 (Unauthorized) message to initiate a challenge, which includes the nonce and the realm in the header. (The nonce specifies a random number that gets used to calculate the MD5 hash.) When a SIP user agent challenges the identity of Cisco Unified CallManager, Cisco Unified CallManager responds to SIP 401 and SIP 407 (Proxy Authentication Required) messages.

After you enable digest authentication for a SIP phone or trunk and configure digest credentials, Cisco Unified CallManager calculates a credentials checksum that includes a hash of the username, password, and the realm. Cisco Unified CallManager encrypts the values and stores the username and the checksum in the database. Each digest user can have one set of digest credentials per realm.

Tip SIP phones can only exist in the Cisco Unified CallManager realm. For SIP trunks, the realm represents the domain that connects through the SIP trunk, such as xyz.com, which helps to identify the source of the request.

When Cisco Unified CallManager challenges a user agent, Cisco Unified CallManager indicates the realm and nonce value for which the user agent must present its credentials. After receiving a response, Cisco Unified CallManager validates the checksum for the username that is stored in the database against the credentials received in the response header from the UA. If the credentials match, digest authentication succeeded, and Cisco Unified CallManager processes the SIP request.

When responding to a challenge from a user agent that is connected through the SIP trunk, Cisco Unified CallManager responds with the Cisco Unified CallManager username and password that are configured for the realm, that is specified in the challenge message header. When Cisco Unified CallManager gets challenged, the Cisco Unified CallManager looks up the username and encrypted password based on the realm that the challenge message specifies. Cisco Unified CallManager decrypts the password, calculates the digest, and presents it in the response message.

Administrators configure SIP digest credentials for a phone user or application user. For applications, you specify digest credentials in the Applications User Configuration window in Cisco Unified CallManager Administration. For SIP phones, you specify the digest authentication credentials, which are then applied to a phone, in the End User window in Cisco Unified CallManager Administration.

To associate the credentials with the phone after you configure the user, you choose a Digest User, an 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.

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 Cisco Unified CallManager still initiates challenges.

Administrators configure the SIP realm for challenges to the phone and for challenges that are received through the SIP trunk.The SIP Realm GUI provides the trunk-side credentials for UAC mode. You configure the SIP realm for phones with the service parameter SIP Station Realm. You must configure a SIP realm and username and password in Cisco Unified CallManager Administration for each SIP trunk user agent that can challenge Cisco Unified CallManager.

Administrators configure the minutes that the nonce value stays valid for the external device before getting rejected and a new number gets generated by Cisco Unified CallManager..

Authorization

Cisco Unified CallManager uses the authorization process to restrict certain categories of messages from SIP phones, from SIP trunks, and from SIP application requests on SIP trunks.

For SIP INVITE messages and in-dialog messages, and for SIP phones, Cisco Unified CallManager provides authorization through calling search spaces and partitions.

For SIP SUBSCRIBE requests from phones, Cisco Unified CallManager provides authorization for user access to presence groups.

For SIP trunks, Cisco Unified CallManager 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 window when you check the related check boxes in the window.

Authorization occurs for the SIP trunk first (as configured in the SIP Trunk Security Profile) and then for the SIP application user agent on the SIP trunk (as configured in the Application User Configuration), when application-level authorization is configured. For the trunk, Cisco Unified CallManager downloads the trunk 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, Cisco Unified CallManager 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, Cisco Unified CallManager processes the request. If digest authentication is enabled, Cisco Unified CallManager 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, Cisco Unified CallManager challenges the device with a 401 message.

To enable SIP application authorization on the SIP trunk, you must check the Enable Application Level Authorization check box in the SIP Trunk Security Profile window. Before an application-level ACL gets applied, Cisco Unified CallManager authenticates the SIP trunk user agent through digest authentication. Therefore, you must enable digest authentication in the SIP Trunk Security Profile for application-level authorization to occur.

Encryption Overview

Tip Encryption installs automatically when you install Cisco Unified CallManager 5.0 on each server in the cluster.

Cisco Unified CallManager supports the following types of encryption:

- Signaling Encryption, page 1-18
- Media Encryption, page 1-19
- Configuration File Encryption, page 1-20

Signaling Encryption

Signaling encryption ensures that all SIP and SCCP signaling messages that are sent between the device and the Cisco Unified CallManager 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 Cisco Unified CallManager 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.

SIP trunks support signaling encryption but do not support media encryption.

Media Encryption

Media encryption, which uses SRTP, ensures that only the intended recipient can interpret the media streams between supported devices. Support includes audio streams only. 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.

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

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 may occur for transfers from a secure device to a non-secure device, conferencing, 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).

Tip 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, H.323/H.245/H.225 trunks, and SIP trunks rely on IPSec configuration to ensure that security-related information does not get sent in the clear. Cisco Unified CallManager does not verify that you configured IPSec correctly. If you do not configure IPSec correctly, security-related information may get exposed.

Secure SIP trunks can support secure calls over TLS; be aware, though, that the trunk supports signaling encryption but does not support media encryption (SRTP). Because the trunk does not support media encryption, the shield icon may display on the phones during the call; that is, if all devices in the call support authentication or signaling encryption.

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 Cisco Unified CallManager.
2. When Device A places a call to Device B, Cisco Unified CallManager 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 SIP phones and H.323 trunks/gateways generate their own cryptographic parameters and send them to Cisco Unified CallManager.

Configuration File Encryption

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

Cisco Unified CallManager 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 Unified IP Phones that support this option (see "Supported Phone Models" section on page 7-4).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.

Cisco Unified CallManager 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, Cisco Unified CallManager 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 Cisco Unified CallManager and in the phone.

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

See Chapter 7, "Understanding Encryption of the Phone Configuration File", for more information.

Configuration Checklist Overview

Table 1-3 describes tasks that you must perform to implement authentication and encryption. Each chapter may also contain a checklist for the tasks that you must perform for the specified security feature.

Table 1-3 Configuration Checklist for Authentication and Encryption

Configuration Steps		Related Procedures and Topics
Step 1	On each server in the cluster, activate the Cisco CTL Provider service in Cisco Unified CallManager Serviceability. **Tip** If you activated this service prior to a Cisco Unified CallManager upgrade, you do not need to activate the service again. The service automatically activates after the upgrade.	Activating the Cisco CTL Provider Service, page 3-3

Table 1-3 Configuration Checklist for Authentication and Encryption (continued)

Configuration Steps		Related Procedures and Topics
Step 2	On the first node, activate the Cisco Certificate Authority Proxy service in Cisco Unified CallManager Serviceability to install, upgrade, troubleshoot, or delete locally significant certificates. **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.	Activating the Certificate Authority Proxy Function Service, page 6-5
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 Cisco Unified CallManager upgrade, the settings migrate automatically during the upgrade.	Configuring Ports for the TLS Connection, page 3-4
Step 4	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.	Configuring the Cisco CTL Client, page 3-7
Step 5	Install the Cisco CTL client. **Tip** You cannot use the Cisco CTL client that was available with Cisco Unified CallManager 4.0. To update the Cisco CTL file after an upgrade to Cisco Unified CallManager 5.0(4), you must install the plug-in that is available in Cisco Unified CallManager Administration 5.0(4).	• System Requirements, page 1-4 • Installation, page 1-11 • Installing the Cisco CTL Client, page 3-6
Step 6	Configure the Cisco CTL client. **Tip** If you created the Cisco CTL file prior to a Cisco Unified CallManager upgrade, the Cisco CTL file migrates automatically during the upgrade. To update the Cisco CTL file after an upgrade to Cisco Unified CallManager 5.0(4), you must install and configure the 5.0(4) version of the Cisco CTL client.	Configuring the Cisco CTL Client, page 3-7

Table 1-3 Configuration Checklist for Authentication and Encryption (continued)

Configuration Steps		Related Procedures and Topics
Step 7	Configure the phone security profiles. Perform the following tasks when you configure the profiles: • Configure the device security mode (for SCCP and SIP phones). The device security mode migrates automatically during the Cisco Unified CallManager upgrade. If you want to configure encryption for devices that only supported authentication in Cisco Unified CallManager 4.0, you must choose a security profile for encryption in the Phone Configuration window. • Configure CAPF settings (for some SCCP and SIP phones). Additional CAPF settings display in the Phone Configuration window. • If you plan to use digest authentication for SIP phones, check the Enable Digest Authentication check box. • To enable encrypted configuration files (for some SCCP and SIP phones), check the TFTP Encrypted Confide check box. • To exclude digest credentials in configuration file downloads, check the TFTP Exclude Digest Credential in Configuration File check box.	Configuring a Phone Security Profile, page 5-1 Configuration Tips for Phone Security Profiles, page 5-1 Configuring Encrypted Phone Configuration Files, page 7-1 Configuration Tips for Encrypted Configuration Files, page 7-4
Step 8	Apply the phone security profiles to the phones.	Applying a Phone Security Profile, page 5-9
Step 9	Configure CAPF to issue certificates to the phones. If you performed certificate operations before the upgrade to Cisco Unified CallManager 5.0 and CAPF ran on a subscriber server, you must copy the CAPF data to the 4.0 publisher database server before you upgrade the cluster to Cisco Unified CallManager 5.0. **Caution** The CAPF data on the Cisco Unified CallManager 4.0 subscriber server does not migrate to the Cisco Unified CallManager 5.0 database, and a loss of data occurs if you do not copy the data to the 5.0 database. If a loss of data occurs, the locally significant certificates that you issued with CAPF utility 1.0(1) remain in the phones, but CAPF 5.0 must reissue the certificates, which are no longer valid.	• System Requirements, page 1-4 • CAPF Configuration Checklist, page 6-4
Step 10	Verify that the locally significant certificates are installed on supported Cisco Unified IP Phones.	• System Requirements, page 1-4 • Entering the Authentication String on the Phone, page 6-9
Step 11	Configure digest authentication for SIP phones.	Configuring Digest Authentication for the SIP Phone, page 8-1

Table 1-3 Configuration Checklist for Authentication and Encryption (continued)

Configuration Steps		Related Procedures and Topics
Step 12	Perform phone-hardening tasks. **Tip** If you configured phone-hardening settings prior to a Cisco Unified CallManager upgrade, the device configuration settings migrate automatically during the upgrade.	Phone Hardening, page 9-1
Step 13	Configure voice mail ports for security.	• Configuring Voice Messaging Ports for Security, page 10-1 • *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*
Step 14	Configure security settings for SRST references. **Tip** If you configured secure SRST references in a previous Cisco Unified CallManager release, the configuration automatically migrates during the Cisco Unified CallManager upgrade.	Configuring a Secure Survivable Remote Site Telephony (SRST) Reference, page 12-1
Step 15	Configure IPSec.	• Configuring Encryption for Gateways and Trunks, page 13-1 • Considerations for Configuring IPSec in the Network Infrastructure, page 13-5 • *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* • *Cisco Unified Communications Operating System Administration Guide*
Step 16	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.	• Configuring the SIP Trunk Security Profile, page 14-2 • Configuring Digest Authentication Enterprise Parameters, page 15-2
Step 17	Apply the SIP trunk security profile to the trunk.	Applying a SIP Trunk Security Profile, page 14-7
Step 18	Configure digest authentication for the trunk.	Configuring Digest Authentication for the SIP Trunk, page 15-1
Step 19	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.	• Configuring the SIP Trunk Security Profile, page 14-2 • See also application user authorization in the *Cisco Unified CallManager Administration Guide*

Table 1-3 Configuration Checklist for Authentication and Encryption (continued)

Configuration Steps		Related Procedures and Topics
Step 20	Reset all phones in the cluster.	Resetting the Devices, Restarting Services, or Rebooting the Server/Cluster, page 1-10
Step 21	Reboot all servers in the cluster.	Resetting the Devices, Restarting Services, or Rebooting the Server/Cluster, page 1-10

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 CallManager*
- *Cisco Unified Communications Operating System Administration Guide*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*
- *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- Cisco Unified Survivable Remote Site Telephony (SRST) administration documentation that supports the SRST-enabled gateway
- *Cisco IP Telephony Disaster Recovery Framework Administration Guide*
- *Cisco Unified CallManager Bulk Administration Guide*
- *Troubleshooting Guide for Cisco Unified CallManager, Release 5.0(4)*
- The firmware release notes that support your phone model

Using Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)

This chapter contains information on the following topics:

HTTPS Overview

Hypertext Transfer Protocol over Secure Sockets Layer (SSL), which secures communication between the browser client and the tomcat server, uses a certificate and a public key to encrypt the data that is transferred over the Internet. HTTPS also ensures that the user login password transports securely via the web. The following Cisco Unified CallManager applications support HTTPS, which ensures the identity of the server: Cisco Unified CallManager Administration, Cisco Unified CallManager Serviceability, the Cisco Unified IP Phone User Option Pages, TAPS, Cisco Unified CallManager CDR Analysis and Reporting, Cisco Unified Dialed Number Analyzer, and the Cisco Unified CallManager Real Time Monitoring Tool.

When you install/upgrade Cisco Unified CallManager, the HTTPS self-signed certificate (tomcat_cert) generates in the platform. The self-signed certificate migrates during upgrades. A copy of the certificate gets made in .DER and .PEM formats. Table 2-1 shows the applications that use HTTPS in Cisco Unified CallManager.

Table 2-1 Cisco Unified CallManager HTTPS Applications

Cisco Unified CallManager HTTPS Application	Web Application
CMAdmin	Cisco Unified CallManager Administration
CMService	Cisco Unified CallManager Serviceability
CMUser	Cisco Personal Communications Assistant

Table 2-1 Cisco Unified CallManager HTTPS Applications (continued)

Cisco Unified CallManager HTTPS Application	Web Application
AST	Cisco Unified CallManager Real-Time Monitoring Tool
RTMTReports	Cisco Unified CallManager Real Time Monitoring Tool reports archive
CMTraceAnalysis	Trace Analysis Tool
PktCap	TAC troubleshooting tools that are used for packet capturing
ART	Cisco Unified CallManager CDR Analysis and Reporting
TAPS	Tool for Auto-Registration Phone Support (TAPS)
dna	Cisco Unified Dialed Number Analyzer
drf	Disaster Recovery System
SOAP	Simple Object Access Protocol API for reading from and writing to the Cisco Unified CallManager database **Note** For security, all Web applications using SOAP require HTTPS. HTTP is not supported for SOAP applications. Existing applications that use HTTP will fail; they cannot be converted to HTTPS by changing directories.

Note If you access the web application by using the hostname and install the certificate in the trusted folder and then try to access the application by using the localhost or IP address, the Security Alert dialog box displays to indicate that the name of the security certificate does not match the name of the site.

If you use the localhost, the IP address, or the hostname in the URL to access the application that supports HTTPS, you must save the certificate in the trusted folder for each of type of URL (with the local host, IP address, and so on); otherwise, the Security Alert dialog box displays for each type.

Using Internet Explorer with HTTPS

This section provides details on the following topics about using HTTPS with Internet Explorer:

- Using Internet Explorer to Save the Certificate to the Trusted Folder, page 2-3
- Viewing Details of the Certificate, page 2-4
- Copying the Certificate to File, page 2-4

The first time that you (or a user) accesses Cisco Unified CallManager Administration or other Cisco Unified CallManager SSL-enabled virtual directories (after the Cisco Unified CallManager 5.0 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 **View 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 **View Certificate > Install Certificate** options.

Using Internet Explorer to Save the Certificate to the Trusted Folder

To save the HTTPS certificate in the trusted folder on the browser client, so the Security Alert dialog box does not display each time that you access the web application, perform the following procedure:

Procedure

Step 1 Browse to the application on the tomcat server (for example, Cisco Unified CallManager Administration).

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

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**.

Step 9 A Security Warning Box displays the certificate thumbprint for you.

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** to proceed.

Note If you use the localhost, the IP address, or the hostname in the URL to access the application that supports HTTPS, you must save the certificate in the trusted folder for each of type of URL (with the local host, IP address, and so on); otherwise, the Security Alert dialog box displays for each type.

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

Additional Information

See the "Related Topics" section on page 2-6.

Viewing Details of the Certificate

When the Security Alert dialog box displays, click the **View Certificate** button and then the **Details** tab to view the details of the certificate.

Tip You cannot change any data that displays for the settings in the pane.

The following certificate settings may display:

- Version
- Serial Number
- Signature Algorithm
- Issuer
- Valid From
- Valid To
- Subject
- Public key
- Subject Key Installer
- Key Usage
- Enhanced Key Usage
- Thumbprint Algorithm
- Thumbprint

To display a subset of settings, if available, choose one of the following options:

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

Note You can regenerate the self-signed certificate by using the Cisco Unified Communications Platform Administration GUI.

Copying the 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 **View Certificate**.

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**.

- **DER encoded binary X.509 (.CER)**—Uses DER to transfer information between entities.
- **Base-64 encoded X.509 (.CER)**—Sends secure binary attachments over the internet; uses ASCII text format to prevent corruption of file.
- **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**.

Additional Information

See the "Related Topics" section on page 2-6.

Using Netscape with HTTPS

This section provides details on the following topics about using HTTPS with Netscape.

When you use HTTPS with Netscape, you can view the certificate credentials, trust the certificate for one session, trust the certificate until it expires, or not trust the certificate at all.

Netscape does not provide a certificate export utility for copying certificates to a file.

Tip If you trust the certificate for one session only, you must repeat the "Using Netscape to Save the Certificate to the Trusted Folder" procedure each time that you access the HTTPS-supported application. If you do not trust the certificate, you cannot access the application.

Using Netscape to Save the Certificate to the Trusted Folder

Perform the following procedure to save the certificate to the trusted folder:

Procedure

Step 1 Access the application, for example, Cisco Unified CallManager Administration, by using Netscape.

The certificate authority dialog box displays.

Step 2 Click one of the following radio buttons:

- Accept this certificate for this session
- Do not accept this certificate and do not connect
- Accept this certificate forever (until it expires)

Note If you choose Do not accept, the application does not display.

Note To view the certificate credentials before you continue, click **Examine Certificate**. Review the credentials, and click **Close**.

Step 3 Click **OK**.

The Security Warning dialog box displays.

Step 4 Click **OK**.

Note You can regenerate the self-signed certificate by using the Cisco Unified Communications Platform Administration GUI.

Additional Information

See the "Related Topics" section on page 2-6.

Where to Find More Information

Related Topics

Certificate Types, page 1-12

Related Cisco Documentation

- *Cisco Unified CallManager Serviceability Administration Guide*
- *Cisco Unified CallManager Administration Guide*
- Microsoft documentation that is available on HTTPS

Configuring the Cisco CTL Client

This chapter contains information on the following topics:

Cisco CTL Client Overview

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) client on a single Windows workstation or server that has a USB port.

Note Supported Windows versions for CTL client include Windows 2000 and Windows XP.

Tip Do not use Terminal Services to install the Cisco CTL client. Cisco installs Terminal Services, so Cisco Technical Assistance Center (TAC) can perform remote troubleshooting and configuration tasks.

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

- Site Administrator Security Token (SAST)
- Cisco Unified CallManager and Cisco TFTP running on the same server
- Certificate Authority Proxy Function (CAPF)

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 of the servers. After you create the CTL file, you must restart the Cisco CallManager and Cisco TFTP services in Cisco Unified CallManager Serviceability on all servers in the cluster 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 none of the TFTP servers contains a certificate, the phone requests an unsigned file.

Cisco Unified CallManager Administration uses an etoken to authenticate the TLS connection between the CTL client and provider.

Configuration Tips for Cisco CTL Client Configuration

Consider the following information when you configure the CTL client in Cisco Unified CallManager Administration:

- Ensure that Cisco Unified CallManager node hostnames are resolvable on the remote PC where the CTL client is installed, or the CTL client will not function correctly.
- You must activate the Cisco CTL provider service on all servers in the cluster.
- After you create the CTL file, you must restart the Cisco CallManager and Cisco TFTP services in Cisco Unified CallManager Serviceability on all servers in the cluster that run these services.

Cisco CTL Client Configuration Checklist

Table 3-1 provides a list of configuration tasks that you perform to install and configure the Cisco CTL client for the first time.

Table 3-1 Cisco CTL Client Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	On each Cisco Unified CallManager in the cluster, activate the Cisco CTL Provider service in Cisco Unified CallManager Serviceability. **Tip** If you activated this service prior to a Cisco Unified CallManager upgrade, you do not need to activate the service again. The service automatically activates after the upgrade.	Activating the Cisco CTL Provider Service, page 3-3
Step 2	On the first node, activate the Cisco Certificate Authority Proxy service in Cisco Unified CallManager Serviceability. **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.	Activating the Certificate Authority Proxy Function Service, page 6-5
Step 3	If you do not want to use the default settings, configure ports for the TLS connection. **Tip** If you configured these settings prior to a Cisco Unified CallManager upgrade, the settings migrate automatically.	Configuring Ports for the TLS Connection, page 3-4
Step 4	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.	Configuring the Cisco CTL Client, page 3-7
Step 5	Install the Cisco CTL client.	• System Requirements, page 1-4 • Installation, page 1-11 • Installing the Cisco CTL Client, page 3-6
Step 6	Configure the Cisco CTL client.	Configuring the Cisco CTL Client, page 3-7

Activating the Cisco CTL Provider Service

After you configure the Cisco CTL client, this service changes the cluster 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 Cisco Unified CallManager and Cisco TFTP servers.

If you activate the service and then upgrade Cisco Unified CallManager, Cisco Unified CallManager 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 CallManager Serviceability, choose **Tools > Service Activation**.

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

Step 3 Click the **Cisco CTL Provider** service radio button.

Step 4 Click **Save**.

Step 5 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 the "Configuring Ports for the TLS Connection" section on page 3-4.

Step 6 Verify that the service runs on all servers in the cluster. In Cisco Unified CallManager Serviceability, choose **Tools > Control Center - Feature Services** to verify the state of the service.

Additional Information

See the "Related Topics" section on page 3-16.

Activating the Cisco CAPF Service

For information on activating this service, see the "Activating the Certificate Authority Proxy Function Service" section on page 6-5.

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.

Configuring Ports for the TLS Connection

You may have to configure a different port number if the 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 clusterwide security mode, saving the CTL file to TFTP servers, and retrieving a list of Cisco Unified CallManager and TFTP servers in the cluster.

The Ethernet Phone Port monitors registration requests from the SCCP phone. In nonsecure mode, the phone connects through port 2000. In mixed mode, the Cisco Unified CallManager port for TLS connection equals the value for the Cisco Unified CallManager port number added to (+) 443; therefore, the default TLS connection for Cisco Unified CallManager 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 Cisco Unified CallManager to listen for SIP messages from SIP phones. The default value equals 5061. If you change this port, you must restart the Cisco CallManager service in Cisco Unified CallManager Serviceability and reset the SIP phones.

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

The CTL ports must be opened to the data VLAN from where the CTL client runs. The ports used by the CTL client are also used by phones that are running TLS for signaling back to Cisco Unified CallManager. These ports need to be opened to all VLANs where phones are configured for authenticated or encrypted status.

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:

- To change the Port Number parameter for the Cisco CTL Provider service, perform Step 2 through Step 6.
- To change the Ethernet Phone Port or SIP Phone Secure Port settings, perform Step 7 through Step 11.

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

Step 3 In the Server drop-down list box, 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 CallManager** in Cisco Unified CallManager Administration.

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

Step 9 After the Cisco Unified CallManager 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 CallManager Serviceability.

Step 11 Click **Save**.

Additional Information

See the "Related Topics" section on page 3-16.

Installing the Cisco CTL Client

You must use the client and update the CTL file when the following events occur:

- The first time you set the security mode of the cluster
- The first time you create the CTL file
- After the Cisco Unified CallManager installation
- After you restore a Cisco Unified CallManager server or Cisco Unified CallManager data
- After you change the IP address or hostname of the Cisco Unified CallManager server
- After you add or remove a security token, TFTP server, or Cisco Unified CallManager server

Tip If the Smart Card service is not set to started and automatic on the server or workstation where you plan to install the client, the installation fails.

To install the Cisco CTL client, perform the following procedure:

Procedure

Step 1 From the Windows workstation or server where you plan to install the client, browse to Cisco Unified CallManager Administration, as described in the *Cisco Unified CallManager Administration Guide*.

Step 2 In Cisco Unified CallManager Administration, choose **Application > Plugins.**

The Find and List Plugins window displays.

Step 3 From the Plugin Type equals drop-down list box, choose **Installation** and click **Find**.

Step 4 Locate the Cisco CTL Client.

Step 5 To download the file, click **Download** on the right side of the window, directly opposite the Cisco CTL Client plug-in name.

Step 6 Click **Save**, and save the file to a location that you will remember.

Step 7 To begin the installation, double-click **Cisco CTL Client** (icon or executable depending on where you saved the file).

Note You can also click **Open** from the Download Complete box.

Step 8 The version of the Cisco CTL client displays; click **Continue**.

Step 9 The installation wizard displays. Click **Next**.

Step 10 Accept the license agreement and click **Next**.

Step 11 Choose a folder where you want to install the client. If you want to do so, click Browse to change the default location; after you choose the location, click **Next**.

Step 12 To begin the installation, click **Next**.

Step 13 After the installation completes, click **Finish**.

Additional Information

See the "Related Topics" section on page 3-16.

Upgrading the Cisco CTL Client and Migrating the Cisco CTL File

If you want to make changes to the CTL file after the Cisco Unified CallManager 5.0(4) upgrade, you must delete the Cisco CTL client that you installed prior to the upgrade, install the latest Cisco CTL client, as described in the "Installing the Cisco CTL Client" section on page 3-6, and regenerate the CTL file.

If you did not remove or add any servers before the Cisco Unified CallManager upgrade, you do not need to reconfigure the Cisco CTL client after the upgrade. The Cisco Unified CallManager upgrade automatically migrates the data in the CTL file.

Configuring the Cisco CTL Client

Tip Configure the Cisco CTL client during a scheduled maintenance window because you must restart the Cisco Unified CallManager and Cisco TFTP services in Cisco Unified CallManager Serviceability on all servers in the cluster that run these services.

The Cisco CTL client performs the following tasks:

- Sets the Cisco Unified CallManager cluster security mode.

Tip You cannot set the Cisco Unified CallManager clusterwide parameter to mixed mode through the Enterprise Parameters window of Cisco Unified CallManager Administration. You must configure the CTL client to set the clusterwide mode. For more information, see the "Cisco CTL Client Configuration Settings" section on page 3-11.

- Creates the Certificate Trust List (CTL), which is a file that contains certificate entries for security tokens, Cisco Unified CallManager, and CAPF servers.

  The CTL file indicates the servers that support TLS for the phone connection. The client automatically detects the Cisco Unified CallManager and the Cisco CAPF server and adds certificate entries for these servers.

  The security tokens that you insert during the configuration sign the CTL file.

Before You Begin

Before you configure the Cisco CTL client, verify that you activated the Cisco CTL Provider service and the Cisco Certificate Authority Proxy Function service in Cisco Unified CallManager Serviceability. Obtain at least two security tokens; the Cisco certificate authority issues these security tokens. The security tokens must come from Cisco. You will insert the tokens one at a time into the USB port on the server/workstation. If you do not have a USB port on the server, you may use a USB PCI card.

Obtain the following passwords, hostnames/IP addresses, and port numbers:

- Administrative username and password for Cisco Unified CallManager
- Security token administrative password

See Table 3-2 for a description of the preceding information.

Tip Before you install the Cisco CTL client, verify that you have network connectivity to each server in the cluster. To ensure that you have network connectivity to all servers in the cluster, issue a ping command, as described in the *Cisco Unified Communications Operating System Administration Guide*.

If you installed multiple Cisco CTL clients, Cisco Unified CallManager only accepts CTL configuration information on one client at a time, but you can perform configuration tasks on up to five Cisco CTL clients simultaneously. While you perform configuration tasks on one client, Cisco Unified CallManager automatically stores the information that you entered on the other clients.

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

- Writes the CTL file to all Cisco Unified CallManager servers in the cluster.
- Writes CAPF capf.cer to all Cisco Unified CallManager subsequent nodes (not first node) in the cluster.
- Writes CAPF certificate file in PEM format to all Cisco Unified CallManager subsequent nodes (not first node) in the cluster.
- 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.

To configure the client, perform the following procedure:

Procedure

Step 1 Obtain at least two security tokens that you purchased.

Step 2 Perform one of the following tasks:

- Double-click the **Cisco CTL Client** icon that exists on the desktop of the workstation/server where you installed it.
- Choose **Start > Programs > Cisco CTL Client**.

Step 3 Enter the configuration settings for the Cisco Unified CallManager server, as described in Table 3-2; click **Next**.

Step 4 Click **Set Cisco Unified CallManager Cluster to Mixed Mode**, as described in Table 3-2; click **Next**.

Step 5 Perform the following tasks, depending on what you want to accomplish:

- To add a security token, see Step 6 through Step 12.
- To complete the Cisco CTL client configuration, see Step 17 through Step 21.

Caution You need a minimum of two security tokens the first time that you configure the client. Do not insert the tokens until the application prompts you to do so. If you have two USB ports on the workstation or server, do not insert two security tokens at the same time.

Step 6 When the application prompts you to do so, insert one security token in an available USB port on the workstation or server where you are currently configuring the Cisco CTL client; click **OK**.

Step 7 The security token information displays for the token that you inserted; click **Add**.

Step 8 The detected certificate entries display in the pane.

Step 9 To add other security token(s) to the certificate trust list, click **Add Tokens**.

Step 10 If you have not already done so, remove the token that you inserted into the server or workstation. When the application prompts you to do so, insert the next token and click **OK**.

Step 11 The security token information for the second token displays; click **Add**.

Step 12 For all security tokens, repeat Step 9 through Step 11.

Step 13 The certificate entries display in the pane.

Step 14 Enter the configuration settings, as described in Table 3-2.

Step 15 Click **Next**.

Step 16 Enter the configuration settings, as described in Table 3-2; click **Next**.

Step 17 When you have added all security tokens and servers, click **Finish**.

Step 18 Enter the username password for the security token, as described in Table 3-2; click **OK**.

Step 19 After the client creates the CTL file, a window displays the server, file location, and status of the CTL file on each server. Click **Finish**.

Step 20 Reset all devices in the cluster. See the "Resetting the Devices, Restarting Services, or Rebooting the Server/Cluster" section on page 1-10.

Step 21 In Cisco Unified CallManager Serviceability, restart the Cisco Unified CallManager and Cisco TFTP services that run on each server in the cluster.

Step 22 After you create the CTL file, you may remove the security token from the USB port. Store all security tokens in a safe place that you will remember.

Additional Information

See the "Related Topics" section on page 3-16.

Updating the CTL File

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

- If you add a new Cisco Unified CallManager server to the cluster
- If you change the name or IP address of the Cisco Unified CallManager server in the cluster
- If you enabled the Cisco Certificate Authority Function service in Cisco Unified CallManager Serviceability
- If you need to add or delete additional security tokens

- If you restore the Cisco Unified CallManager server or Cisco Unified CallManager data

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

To update the information that exists in CTL file, perform the following procedure:

Procedure

Step 1 Obtain one security token that you inserted to configure the latest CTL file.

Step 2 Double-click the **Cisco CTL Client** icon that exists on the desktop of the workstation/server where you installed it.

Step 3 Enter the configuration settings for the Cisco Unified CallManager server, as described in Table 3-2; click **Next**.

Tip You make updates in this window for the Cisco Unified CallManager server.

Step 4 To update the CTL file, click **Update CTL File**, as described in Table 3-2; click **Next**.

Caution For all CTL file updates, you must insert one security token that already exists in the CTL file into the USB port. The client validates the signature of the CTL file through this token. You cannot add new tokens until the CTL client validates the signature. If you have two USB ports on the workstation or server, do not insert both security tokens at the same time.

Step 5 If you have not already inserted one security token in an available USB port on the workstation or server where you are currently updating the CTL file, insert one of the security tokens; click **OK**.

Step 6 The security token information displays for the token that you inserted; click **Next**.

The detected certificate entries display in the pane.

Tip You cannot update the Cisco Unified CallManager or Cisco TFTP entries from this pane. To update the Cisco Unified CallManager entry, click **Cancel** and perform Step 2 through Step 6 again.

Step 7 To update existing Cisco CTL entries or to add or delete security tokens, consider the following information:

- To add new security tokens, see "Configuring the Cisco CTL Client" section on page 3-7.
- To delete a security token, see the "Deleting a CTL File Entry" section on page 3-11.

Additional Information

See the "Related Topics" section on page 3-16.

Deleting a CTL File Entry

At any time, you can delete some CTL entries that display in the CTL Entries window of the Cisco CTL client. After you open the client and follow the prompts to display the CTL Entries window, click **Delete Selected** to delete the entry.

You cannot delete servers that run Cisco Unified CallManager, Cisco TFTP, or Cisco CAPF from the CTL file.

Two security token entries must exist in the CTL file at all times. You cannot delete all security tokens from the file.

Additional Information

See the "Related Topics" section on page 3-16.

Updating the Clusterwide Security Mode

You must use the Cisco CTL client to configure the clusterwide security mode. You cannot change the clusterwide security mode from the Enterprise Parameters window in Cisco Unified CallManager Administration.

To change the clusterwide security mode after the initial configuration of the Cisco CTL client, you must update the CTL file, as described in the "Updating the CTL File" section on page 3-9 and Table 3-2. If you change the clusterwide security mode from mixed to nonsecure mode, the CTL file still exists on the servers in the cluster, but the CTL file does not contain any certificates. Because no certificates exist in the CTL file, the phone requests an unsigned configuration file and registers as nonsecure with Cisco Unified CallManager.

Cisco CTL Client Configuration Settings

The cluster can exist in one of two modes, as described in Table 3-2. Only mixed mode supports authentication. When you configure the Cisco CTL client for authentication, you must choose Set Cisco Unified CallManager Cluster to Mixed Mode.

Use Table 3-2 to configure the Cisco CTL client for the first time, to update the CTL file, or to change the mode from mixed to nonsecure.

- For configuration tips, see the "Configuration Tips for Cisco CTL Client Configuration" section on page 3-2.
- For related information and procedures, see the "Related Topics" section on page 3-16.

Table 3-2 Configuration Settings for CTL Client

Setting	Description
CallManager Server	
Hostname or IP Address	Enter the hostname or IP address for the first node.
Port	Enter the port number, which equals the CTL port for the Cisco CTL Provider service that runs on the specified Cisco Unified CallManager server. The default port number equals 2444.

Table 3-2 Configuration Settings for CTL Client (continued)

Setting	Description
Username and Password	Enter the same username and password that has administrative privileges on the first node.
Radio Button	
Set Cisco Unified CallManager Cluster to Mixed Mode	Mixed mode allows authenticated or encrypted Cisco Unified IP Phones and nonauthenticated Cisco Unified IP Phones to register with Cisco Unified CallManager. In this mode, Cisco Unified CallManager ensures that authenticated or encrypted devices use a secure port. **Note** Cisco Unified CallManager disables auto-registration if you configure the cluster for mixed mode.
Set Cisco Unified CallManager Cluster to Non-Secure Mode	All devices register as unauthenticated with Cisco Unified CallManager, and Cisco Unified CallManager supports image authentication only. When you choose this mode, the 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 Cisco Unified CallManager. **Tip** To revert the phone to the default nonsecure mode, you must delete the CTL file from the phone and all Cisco Unified CallManager servers. You can use auto-registration in this mode.
Update CTL File	After you have created the CTL file, you must choose this option to make any changes to the CTL file. Choosing this option ensures that the Cluster Security mode does not change.
Security Token	
User Password	The first time that you configure the Cisco CTL client, enter **Cisco123**, the case-sensitive default password, to retrieve the private key of the certificate and ensure that the CTL file gets signed.

Verifying the Security Mode for the Cisco Unified CallManager Cluster

To verify the security mode for the Cisco Unified CallManager cluster, perform the following procedure:

Procedure

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

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

Tip You cannot configure this value in Cisco Unified CallManager Administration. This value displays after you configure the Cisco CTL client.

Additional Information

See the "Related Topics" section on page 3-16.

Setting the Smart Card Service to Started and 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 plug-in.

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

After you upgrade the operating system, apply service releases, upgrade Cisco Unified CallManager, 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.

Additional Information

See the "Related Topics" section on page 3-16.

Changing the Security Token Password (Etoken)

This administrative password retrieves the private key of the certificate and ensures that the CTL file gets signed. Each security token comes with a default password. You can change the security token password at any time. If the Cisco CTL client prompts you to change the password, you must change the password before you can proceed with the configuration.

To review pertinent information on setting passwords, click the **Show Tips** button. If you cannot set the password for any reason, review the tips that display.

To change the security token password, perform the following procedure:

Procedure

Step 1 Verify that you have installed the Cisco CTL client on a Windows server or workstation.

Step 2 If you have not already done so, insert the security token into the USB port on the Windows server or workstation where you installed the Cisco CTL client.

Step 3 Choose **Start > Programs > etoken > Etoken Properties**; right-click **etoken** and choose **Change etoken password**.

Step 4 In the Current Password field, enter the password that you originally created for the token.

Step 5 Enter a new password.

Step 6 Enter the new password again to confirm it.

Step 7 Click **OK**.

Additional Information

See the "Related Topics" section on page 3-16.

Deleting the CTL File on the Cisco Unified IP Phone

Caution Cisco recommends that you perform this task in a secure lab environment, especially if you do not plan to delete the CTL file from the Cisco Unified CallManager servers in the cluster.

Delete the CTL file on the Cisco Unified IP Phone if the following cases occur:

- You lose all security tokens that signed the CTL file.
- The security tokens that signed the CTL file appear compromised.

- You move a phone out of a secure cluster; for example, to a storage area, to a nonsecure cluster, or to another secure cluster in a different domain.
- You move a phone from an area with an unknown security policy to a secure cluster.
- You change the alternate TFTP server address to a server that does not exist in the CTL file.

To delete the CTL file on the Cisco Unified IP Phone, perform the tasks in Table 3-3.

Table 3-3 Deleting the CTL File on the Cisco Unified IP Phone

Cisco Unified IP Phone Model	Tasks
Cisco Unified IP Phones 7960 and 7940	Under the Security Configuration menu on the phone, press **CTL file**, **unlock** or ****#**, and **erase**.
Cisco Unified IP Phone 7970	Perform one of the following methods: • Unlock the Security Configuration menu, as described in *Cisco Unified IP Phone Administration Guide for* Cisco Unified CallManager. Under the CTL option, press the **Erase** softkey. • Under the Settings menu, press the **Erase** softkey. **Note** Pressing the Erase softkey under the Settings menu deletes other information besides the CTL file. For additional information, refer to the *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager.*

Additional Information

See the "Related Topics" section on page 3-16.

Determining the Cisco CTL Client Version

To determine which version of the Cisco CTL client you are using, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- Double-click the **Cisco CTL Client** icon that exists on the desktop.
- Choose **Start > Programs > Cisco CTL Client**.

Step 2 In the Cisco CTL client window, click the icon in the upper, left corner of the window.

Step 3 Choose **About Cisco CTL Client**. The version of the client displays.

Additional Information

See the "Related Topics" section on page 3-16.

Verifying or Uninstalling the Cisco CTL Client

Uninstalling the Cisco CTL client does not delete the CTL file. Likewise, the clusterwide security mode and the CTL file do not change when you uninstall the client. If you choose to do so, you can uninstall the CTL client, install the client on a different Windows workstation or server, and continue to use the same CTL file.

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

Procedure

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

Step 2 Double-click **Add Remove Programs**.

Step 3 To verify that the client installed, locate **Cisco CTL Client**.

Step 4 To delete the client, click **Remove**.

Additional Information

See the "Related Topics" section on page 3-16.

Where to Find More Information

Related Topics

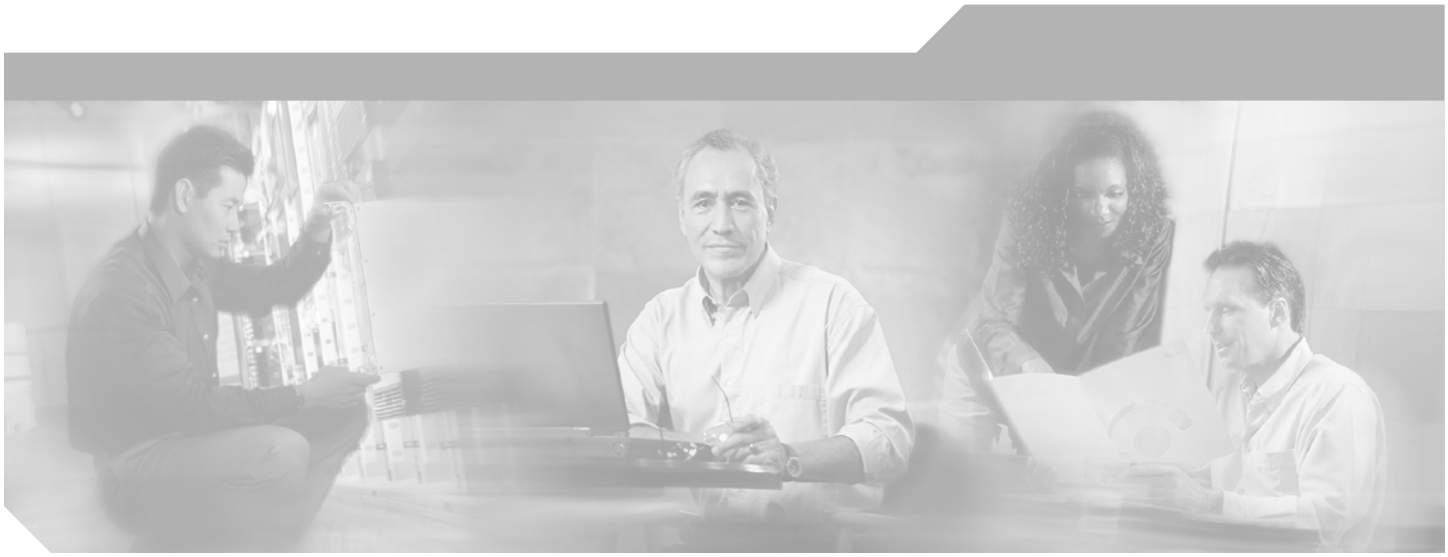
- Using the Certificate Authority Proxy Function, page 6-1

Related Cisco Documentation

Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager

Troubleshooting Guide for Cisco Unified CallManager

Cisco Systems



PART 2

Security for Cisco Unified IP Phones and Cisco Unity Voice Messaging Ports

CHAPTER 4

Phone Security Overview

This chapter contains information on the following topics:

Understanding How Security Works for Phones

When you perform a new installation of Cisco Unified CallManager, the Cisco Unified CallManager cluster boots up in nonsecure mode; when the phones boot up after the Cisco Unified CallManager installation, all devices register as nonsecure with Cisco Unified CallManager.

After you upgrade from Cisco Unified CallManager 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 Cisco Unified CallManager 5.0 installation creates a self-signed certificate on Cisco Unified CallManager and TFTP servers. After you configure the cluster for authentication, Cisco Unified CallManager uses this self-signed certificate to authenticate with supported Cisco Unified IP Phones. After a self-signed certificate exists on the Cisco Unified CallManager and TFTP servers, Cisco Unified CallManager does not reissue the certificates during each Cisco Unified CallManager upgrade. You must create a new CTL file with the new certificate entries.

Tip For information on unsupported or nonsecure scenarios, see the "Interactions and Restrictions" section on page 1-5.

Cisco Unified CallManager 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.

Cisco Unified CallManager retains the authentication and encryption status of the device when a user uses Cisco Extension Mobility. Cisco Unified CallManager 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 Unified 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.

Supported Phone Models

This security document does not list the security features that are supported on your Cisco Unified IP Phone. For a list of security features that are supported on your phone, refer to the phone administration and user documentation that supports Cisco Unified CallManager 5.0(4) or the firmware documentation that supports your firmware load.

Although you may be able to configure the security features in Cisco Unified CallManager Administration, the features may not work until you install a compatible firmware load on the Cisco TFTP server.

Viewing Security Settings on the Phone

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 Unified IP Phone administration and user documentation that supports your phone model and this version of Cisco Unified CallManager.

When Cisco Unified CallManager classifies a call as authenticated or encrypted, an icon displays on the phone to indicate the call state. To determine when Cisco Unified CallManager classifies the call as authenticated or encrypted, refer to the "Interactions and Restrictions" section on page 1-5.

Phone Security Configuration Checklist

Table 4-1 describes the tasks to configure security for supported phones.

Table 4-1 Phone Security Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	If you have not already done so, configure the Cisco CTL client and ensure that the cluster security mode equals Mixed Mode.	Configuring the Cisco CTL Client, page 3-1
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).	Using the Certificate Authority Proxy Function, page 6-1
Step 3	Configure phone security profiles.	Configuring a Phone Security Profile, page 5-1
Step 4	Apply a phone security profile to the phone.	Applying a Phone Security Profile, page 5-9

Table 4-1 Phone Security Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 5	If a SIP phone supports digest authentication, configure the digest credentials in the End User window in Cisco Unified CallManager Administration.	• Configuring Digest Credentials in the End User Configuration Window, page 8-3 • End User Digest Credential Configuration Settings, page 8-3
Step 6	After you configure digest credentials, choose the Digest User from the Phone Configuration window in Cisco Unified CallManager Administration.	Configuring the Digest User in the Phone Configuration Window, page 8-4
Step 7	On Cisco Unified SIP IP Phone 7960 or 7940, enter the digest authentication username and password (digest credentials) that you configured in the End User Configuration window.	The *Cisco Unified CallManager Security Guide* 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 Unified IP Phone administration guide that supports your phone model and this version of Cisco Unified CallManager.
Step 8	Encrypt the phone configuration file, if the phone supports this functionality.	Configuring Encrypted Phone Configuration Files, page 7-1
Step 9	To harden the phone, disable phone settings in Cisco Unified CallManager Administration.	Phone Hardening, page 9-1

Where to Find More Information

Related Topics

- Interactions and Restrictions, page 1-5
- Authentication, Integrity, and Authorization Overview, page 1-14
- Encryption Overview, page 1-18
- Configuration Checklist Overview, page 1-20
- Using the Certificate Authority Proxy Function, page 6-1
- Phone Security Configuration Checklist, page 4-2
- Configuring a Phone Security Profile, page 5-1
- Configuring Encrypted Phone Configuration Files, page 7-1
- Phone Hardening, page 9-1

Related Cisco Documentation

- *Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager*
- *Cisco Unified CallManager Troubleshooting Guide*

Configuring a Phone Security Profile

This chapter contains information on the following topics:

Phone Security Profile Overview

Cisco Unified CallManager 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 Cisco Unified CallManager 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.

Configuration Tips for Phone Security Profiles

Consider the following information when you configure phone security profiles in Cisco Unified CallManager Administration:

- When you configure phones, you must select a security profile in the Phone Configuration window. If the device does not support security, apply the nonsecure profile.

- You cannot delete or change predefined, nonsecure 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 reconfigured settings apply to all phones that are assigned that profile.
- You can rename security files that are assigned to devices. The phones that are assigned the old profile name and settings assume the new profile name and settings.
- The CAPF settings in the Phone Security Profile, authentication and key size, also display in the Phone Configuration window. You must configure CAPF settings for certificate operations that involve manufacture-installed certificates (MICs) or locally significant certificates (LSCs). You can update these fields directly in the Phone Configuration window.
  - If you update the CAPF settings in the security profile, the settings get updated in the Phone Configuration window.
  - If you update the CAPF settings in the Phone Configuration window and a matching profile is found, Cisco Unified CallManager applies the matching profile to the phone.
  - If you update the CAPF settings in the Phone Configuration window, and no matching profile is found, Cisco Unified CallManager creates a new profile and applies the new profile to the phone.
- If you configured the device security mode prior to a Cisco Unified CallManager 5.0 or later upgrade, Cisco Unified CallManager creates a profile that is based on the model and protocol and applies the profile to the device.

Finding a Phone Security Profile

To find a phone security profile, perform the following procedure:

Procedure

Step 1 In Cisco Unified CallManager Administration, choose **System > Security Profile > Phone Security Profile**.

All security profiles that are available on the system display.

Step 2 From the drop-down list boxes, choose your search criteria for the security profiles that you want to list and click **Find**.

Note To find all security profiles that are registered in the database, click **Find** without specifying any search criteria.

The window refreshes and displays the security profiles that match your search criteria.

Step 3 Click the **Name** link for the security profile that you want to view.

Tip To search for the Name or Description within the search results, check the **Search Within Results** check box, enter your search criteria as described in this procedure, and click **Find**.

Additional Information

See the "Related Topics" section on page 5-11.

Configuring a Phone Security Profile

To add, update, or copy a security profile, perform the following procedure:

Procedure

Step 1 In Cisco Unified CallManager Administration, choose **System > Security Profile > Phone Security Profile**.

Step 2 Perform one of the following tasks:

- To add a new profile, click the **Add New** button and continue with Step 3.
- To copy an existing security profile, locate the appropriate profile as described in "Finding a Phone Security Profile" section on page 5-2, click the **Copy** button next to the security profile that you want to copy, and continue with Step 3.
- To update an existing profile, locate the appropriate security profile as described in "Finding a Phone Security Profile" section on page 5-2 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 5-1 for SCCP phones or Table 5-2 for SIP phones.

Step 4 Click **Save**.

Additional Steps

After you create the security profile, apply it to the phone, as described in the "Applying a Phone Security Profile" section on page 5-9.

If you configured digest authentication in the phone security profile for a SIP phone, you must configure the digest credentials in the End User Configuration window. You then must associate the user with the phone by using the Digest User setting in the Phone Configuration window.

Additional Information

See the "Related Topics" section on page 5-11.

Phone Security Profile Configuration Settings

Table 5-1 describes the settings for the SCCP phone security profiles.

Table 5-2 describes the settings for the SIP Phone Security Profile.

Only settings that the selected phone type and protocol support display.

- For configuration tips, see the "Configuration Tips for Phone Security Profiles" section on page 5-1.
- For related information and procedures, see the "Related Topics" section on page 5-11.

Table 5-1 SCCP Phone Security Profile

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.
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 phone. A TCP connection opens to Cisco Unified CallManager. • **Authenticated**—Cisco Unified CallManager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens. • **Encrypted**—Cisco Unified CallManager 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.
TFTP Encrypted Config	When this check box is checked, Cisco Unified CallManager encrypts phone downloads from the TFTP server. Refer to Configuration File Encryption, page 1-20, and Configuring Encrypted Phone Configuration Files, page 7-1, for more information.

Table 5-1 SCCP Phone Security Profile (continued)

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/upgrades, deletes, or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • **By Null String**— Installs/upgrades, deletes, or troubleshoots a locally significant certificate without 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/upgrades, deletes, or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication occurs via the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via 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 even though a MIC and 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 via the other certificate, you must update the authentication mode. • **By Existing Certificate (Precedence to MIC)**—Installs/upgrades, deletes, or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via 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 (see Configuration Tips for Phone Security Profiles, page 5-1, for more details). Refer to the *Cisco Unified CallManager Administration Guide* for information about configuring these settings on the Phone Configuration window.

Table 5-1 SCCP Phone Security Profile (continued)

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. Other options include 512 and 2048. 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 (see Configuration Tips for Phone Security Profiles, page 5-1, in this section for more details). Refer to the *Cisco Unified CallManager Administration Guide* for configuring these settings on the Phone Configuration window.

Table 5-2 SIP Phone Security Profile

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, Cisco Unified CallManager 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.
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 phone. A TCP connection opens to Cisco Unified CallManager. • **Authenticated**—Cisco Unified CallManager provides integrity and authentication for the phone. A TLS connection that uses NULL/SHA opens. • **Encrypted**—Cisco Unified CallManager 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 SIP hops.

Table 5-2 SIP Phone Security Profile (continued)

Setting	Description
Transport Type	When Device Security Mode is **Non Secure**, choose one of the following options from the drop-down list box (not all options may display): • **TCP**—Choose the Transmission Control Protocol to ensure that packets get received in the same order 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 that 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, Cisco Unified CallManager challenges all SIP requests from the phone. Digest authentication does not provide device authentication, integrity, or confidentiality. Choose a security mode of authenticated or encrypted to use these features. **Note** For more information on digest authentication, see the Digest Authentication, page 1-16, and Configuring Digest Authentication for the SIP Phone, page 8-1.
TFTP Encrypted Config	When this check box is checked, Cisco Unified CallManager encrypts 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. Refer to Configuration File Encryption, page 1-20, and Configuring Encrypted Phone Configuration Files, page 7-1, for more information.
Exclude Digest Credentials in Configuration File	When this check box is checked, Cisco Unified CallManager omits digest credentials in phone downloads from the TFTP server. This option exists for Cisco Unified IP SIP Phone models 7905, 7912, 7940, and 7960 only. Refer to Configuration File Encryption, page 1-20, and Configuring Encrypted Phone Configuration Files, page 7-1, for more information.

Table 5-2 SIP Phone Security Profile (continued)

Setting	Description
Authentication Mode	This field allows you to choose the authentication method that the phone uses during the CAPF certificate operation. This option exists for Cisco phones only. From the drop-down list box, choose one of the following options: • **By Authentication String**—Installs/upgrades or troubleshoots a locally significant certificate only when the user enters the CAPF authentication string on the phone. • **By Null String**— Installs/upgrades or troubleshoots a locally significant certificate without 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/upgrades or troubleshoots a locally significant certificate if a manufacture-installed certificate (MIC) or locally significant certificate (LSC) exists in the phone. If a LSC exists in the phone, authentication occurs via the LSC, regardless whether a MIC exists in the phone. If a LSC does not exist in the phone, but a MIC does exist, authentication occurs via 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 even though a MIC and 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 via the other certificate, you must update the authentication mode. • **By Existing Certificate (Precedence to MIC)**—Installs/upgrades or troubleshoots a locally significant certificate if a LSC or MIC exists in the phone. If a MIC exists in the phone, authentication occurs via the MIC, regardless whether a LSC exists in the phone. If a LSC exists in the phone, but a MIC does not exist, authentication occurs via 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 (see Configuration Tips for Phone Security Profiles, page 5-1, in this section for more details). Refer to the *Cisco Unified CallManager Administration Guide* for information about configuring these settings on the Phone Configuration window.

Table 5-2 SIP Phone Security Profile (continued)

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. Other options include 512 and 2048. 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 (see Configuration Tips for Phone Security Profiles, page 5-1, in this section for more details). Refer to the *Cisco Unified CallManager Administration Guide* for information about configuring these settings on the Phone Configuration window.
SIP Phone Port	This setting applies to SIP phones that are using UDP transport. Enter the port number for Cisco Unified SIP IP Phones that are using UDP to listen for SIP messages from Cisco Unified CallManager. The default setting equals 5060. Phones that are using TCP or TLS ignore this setting.

Applying a Phone Security Profile

You apply a phone security profile to the phone in the Phone Configuration window.

Before You Begin

Before you apply a security profile that uses certificates for authentication of the phone, ensure that phone contains a locally significant certificate (LSC) or manufacture-installed certificate (MIC). If the phone does not contain a certificate, perform the following steps:

1. In the Phone Configuration window, apply a nonsecure profile.
2. In the Phone Configuration window, install a certificate by configuring the CAPF settings. For more information on performing this task, see the "Using the Certificate Authority Proxy Function" section on page 6-1.
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 Find the phone, as described in the *Cisco Unified CallManager Administration Guide*.

Step 2 After the Phone Configuration window displays, locate the **Device Security Profile**.

Step 3 From the **Device Security Profile** drop-down list box, choose the security profile that applies to the device. Only the phone security profiles that are configured for the phone type and protocol display.

Step 4 Click **Save**.

Step 5 To reset the phone, click **Reset**.

Additional Steps

If you configured digest authentication for SIP phones, you must configure the digest credentials in the End User Configuration window. Then, you must configure the Digest User setting in the Phone Configuration window. For more information about configuring digest users and digest credentials, refer to "Configuring Digest Authentication for the SIP Phone" section on page 8-1.

Additional Information

See the "Related Topics" section on page 5-11.

Deleting a Phone Security Profile

This section describes how to delete a phone security profile from the Cisco Unified CallManager database.

Before You Begin

Before you can delete a security profile from Cisco Unified CallManager 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** 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 CallManager System Guide.*

Procedure

Step 1 Find the security profile by using the procedure in the "Finding a Phone Security Profile" section on page 5-2.

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 the **Delete Selected** icon or the **Delete Selected** button.

Step 3 To delete a single security profile, perform one of the following tasks:

- In the Find and List window, check the check box next to the appropriate security profile; then, click the **Delete Selected** icon or the **Delete Selected** button.
- In the Find and List window, click the Name link for the security profile. After the specific Security Profile Configuration window displays, click the **Delete** icon or the **Delete** button.

Step 4 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Additional Information

See the "Related Topics" section on page 5-11.

Finding Phones that Use Phone Security Profiles

To find a phone that uses the Phone Security Profile, perform the following procedure:

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

Step 2 From the **Find Phone where** drop-down list box, choose **Security Profile**.

Step 3 If you want to do so, specify additional search criteria for the security profile by choosing an option in the drop-down list box next to the Find Phone drop-down list box; then, enter the specific search criteria.

Step 4 After you specify your search criteria, click **Find**. The search results display.

Additional Information

See the "Related Topics" section on page 5-11.

Where to Find More Information

Related Topics

- Digest Authentication, page 1-16
- Configuration File Encryption, page 1-20
- Phone Security Profile Overview, page 5-1
- Configuration Tips for Phone Security Profiles, page 5-1
- Finding a Phone Security Profile, page 5-2
- Configuring a Phone Security Profile, page 5-3
- Phone Security Profile Configuration Settings, page 5-3
- Applying a Phone Security Profile, page 5-9
- Deleting a Phone Security Profile, page 5-10
- Finding Phones that Use Phone Security Profiles, page 5-11
- Configuring Encrypted Phone Configuration Files, page 7-1
- Configuring Digest Authentication for the SIP Phone, page 8-1
- Phone Hardening, page 9-1

Related Cisco Documentation

Cisco Unified CallManager Administration Guide

Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager

CHAPTER 6

Using the Certificate Authority Proxy Function

This chapter provides information on the following topics:

Certificate Authority Proxy Function Overview

Certificate Authority Proxy Function (CAPF), which automatically installs with Cisco Unified CallManager, 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 Unified IP Phone models.
- Upgrades existing locally significant certificates on the phones.
- Retrieves phone certificates for viewing and troubleshooting.
- Authenticates via the manufacture-installed certificate.

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 all servers in the cluster, uses the .0 extension. To verify that the CAPF certificate exists, display the CAPF certificate at the Cisco Unified Communications platform GUI.

Cisco Unified IP Phone and CAPF Interaction

When the phone interacts with CAPF, the phone authenticates itself to CAPF 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 is never exposed externally. CAPF signs the phone certificate and then sends the certificate back to the phone in a signed message.

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.

If you choose a 2048-bit key for the certificate, establishing a connection between the phone, Cisco Unified CallManager, and secure SRST-enabled gateway during phone boot-up and failover may take more than 60 seconds. Unless you want the highest possible security level, do not configure the 2048-bit key.

Consider the following information about how CAPF interacts with the Cisco Unified IP Phone 7960 and 7940 when the phone is reset by a user or by Cisco Unified CallManager.

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 CallManager 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 Support 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 CallManager 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 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.
- Cisco Unified CallManager does not support SCEP or third-party CA-signed LSC certificates, such as Microsoft CA or Keon CA, in this release. Support for third-party certificates is scheduled for a future release. Customers who currently use third-party CA should re-issue a long expiration period (at least 6 months) for their certificates before migration to 5.0 to ensure that certificates will not expire until support for third-party certificates is available.

- 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.
- All servers in the Cisco Unified CallManager 5.0(4) cluster must use the same administrator username and password, so CAPF can authenticate to all servers in the cluster.
- 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.

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

Configuring CAPF in Cisco Unified CallManager Serviceability

You perform the following tasks in Cisco Unified CallManager Serviceability:

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

Refer to the *Cisco Unified CallManager Serviceability* guides for more information.

CAPF Configuration Checklist

Table 6-1 provides a list of tasks that you perform to install, upgrade, or troubleshoot locally significant certificates.

Table 6-1 CAPF Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Determine whether a locally significant certificate exists in the phone. Determine whether you need to copy CAP 1.0(1) data to the Cisco Unified CallManager 4.0 publisher database server. **Tip** If you used the CAPF utility with Cisco Unified CallManager 4.0 and verified that the CAPF data exists in the Cisco Unified CallManager 5.0 database, you can delete the CAPF utility that you used with Cisco Unified CallManager 4.0.	• Phone documentation that supports your phone model and this version of Cisco Unified CallManager • *Data Migration Assistant 2.0 User Guide*

Table 6-1 CAPF Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
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.	Activating the Certificate Authority Proxy Function Service, page 6-5
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.	Configuring the Cisco CTL Client, page 3-7
Step 4	If necessary, update CAPF service parameters.	• Updating CAPF Service Parameters, page 6-6 • Using CAPF to Install, Upgrade, Troubleshoot, or Delete Certificates From the Phone, page 6-6
Step 5	To install, upgrade, or troubleshoot locally significant certificates in the phone, use Cisco Unified CallManager Administration.	• Using CAPF to Install, Upgrade, Troubleshoot, or Delete Certificates From the Phone, page 6-6 • CAPF Settings in the Phone Configuration Window, page 6-7 • Finding Phones Based on LSC Status or Authentication String, page 6-8
Step 6	If it is required for certificate operations, enter the authentication string on the phone.	Entering the Authentication String on the Phone, page 6-9

Activating the Certificate Authority Proxy Function Service

Cisco Unified CallManager 5.0 does not automatically activate the Certificate Authority Proxy Function service in Cisco Unified CallManager Serviceability.

Activate this service only 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, as described in the "Updating the CTL File" section on page 3-9.

To activate the service, perform the following procedure:

Procedure

Step 1 In Cisco Unified CallManager 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**.

Additional Information

See the "Related Topics" section on page 6-10.

Updating 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, the key size, and so on.

For the CAPF service parameters to show Active status in Cisco Unified CallManager Administration, you must activate the Certificate Authority Proxy Function service, as described in "Activating the Certificate Authority Proxy Function Service" section on page 6-5.

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

Procedure

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

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

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.

Additional Information

See the "Related Topics" section on page 6-10.

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

Use Table 6-2 as a reference when you use CAPF.

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

Procedure

Step 1 Find the phone, as described in the *Cisco Unified CallManager 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 6-2.

Step 4 Click **Save**.

Step 5 Click **Reset**.

Additional Information

See the "Related Topics" section on page 6-10.

CAPF Settings in the Phone Configuration Window

Table 6-2 describes the CAPF settings in the Phone Configuration window in CiscoUnified CallManager Administration.

- For configuration tips, see the "CAPF System Interactions and Requirements" section on page 6-3.
- For related information and procedures, see the "Related Topics" section on page 6-10.

Table 6-2 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 CallManager creates two trace files, one for each certificate type. By choosing the Troubleshoot option, you can verify that an LSC or MIC exists in the phone. **Tip** 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.
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.

Table 6-2 CAPF Configuration Settings (continued)

Setting	Description
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.

Finding Phones Based on LSC Status or Authentication String

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

Procedure

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

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

- **LSC Status**—Choosing this option returns a list of phones that use CAPF to install, upgrade, delete, or troubleshoot locally significant certificates.
- **Authentication String**—Choosing this option returns a list of phones with an authentication string that is specified in the Authentication String field.

Step 3 If you want to do so, specify additional search criteria for the LSC status or authentication string by choosing an option in the drop-down list box next to the Find Phone Where drop-down list box; then, enter the specific search criteria.

Step 4 After you specify your search criteria, click **Find**.

Tip To search for additional information within the search results, check the **Search Within Results** check box, enter your search criteria, and click **Find**.

Additional Information

See the "Related Topics" section on page 6-10.

Generating a 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 CallManager Administration, choose **Device > Phone**.

The Find/List window displays.

Step 2 In the Find Phone Where drop-down list box, choose one of the following options:

- Device Name
- Device Description
- LSC Status
- Authentication String
- Security Profile

Tip If you want to do so, specify additional search criteria by choosing an option in the drop-down list box next to the Find Phone Where drop-down list box; then, enter the specific search criteria.

The search results display.

Tip To search for additional information within the search results, check the **Search Within Results** check box, enter your search criteria, and click **Find**.

Step 3 In the Related Links drop-down list box, choose **CAPF Report in File**; then, click **Go**.

Step 4 Save the file to a location that you will remember.

Step 5 Use Microsoft Excel to open the .csv file.

Additional Information

See the "Related Topics" section on page 6-10.

Entering the Authentication String on the Phone

If you chose the By Authentication String mode and generated an authentication string in Cisco Unified CallManager, you must enter the authentication string on the phone before the locally significant certificate installation occurs.

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. For information on how to enter the authentication string on the phone, refer to the phone documentation that supports your phone model and this version of Cisco Unified CallManager.

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, as described in "Activating the Certificate Authority Proxy Function Service" section on page 6-5.

- The first node is functional and running. Ensure that the server runs for each certificate installation.
- A signed image exists on the phone; refer to the Cisco Unified IP Phone administration documentation that supports your phone model.

Additional Information

See the "Related Topics" section on page 6-10.

Where to Find More Information

Related Topics

- Certificate Authority Proxy Function Overview, page 6-2
- Cisco Unified IP Phone and CAPF Interaction, page 6-2
- CAPF System Interactions and Requirements, page 6-3
- Configuring CAPF in Cisco Unified CallManager Serviceability, page 6-4
- CAPF Configuration Checklist, page 6-4
- Activating the Certificate Authority Proxy Function Service, page 6-5
- Updating CAPF Service Parameters, page 6-6
- Using CAPF to Install, Upgrade, Troubleshoot, or Delete Certificates From the Phone, page 6-6
- CAPF Settings in the Phone Configuration Window, page 6-7
- Finding Phones Based on LSC Status or Authentication String, page 6-8
- Generating a CAPF Report, page 6-8
- Entering the Authentication String on the Phone, page 6-9

Related Cisco Documentation

Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager

Cisco Unified CallManager Serviceability

Configuring Encrypted Phone Configuration Files

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.

This chapter contains information on the following topics:

Understanding Encryption of the Phone Configuration File

To secure digest credentials and secured passwords in phone downloads from Cisco Unified CallManager, you must enable the TFTP Encrypted Config option in the Phone Security Profile Configuration window and perform additional tasks in Cisco Unified CallManager Administration.

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

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

If the phone supports encrypted phone configuration files and if you 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 SIP phone when the TFTP encrypted configuration setting is False, digest credentials may get sent in the clear. See "Disabling Encryption for the Phone Configuration Files" section on page 7-9 for more information.**

Some phone models do not support encrypted phone configuration files, as described in "Supported Phone Models" section on page 7-4. The phone model and protocol determines the method that the system uses to encrypt the configuration file. Supported methods rely on Cisco Unified CallManager 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.

Cisco Unified CallManager supports the following methods:

- Manual Key Distribution
- Symmetric Key Encryption with Phone Public Key

The information in the "Manual Key Distribution" and "Symmetric Key Encryption with Phone Public Key" sections assumes that you configured the cluster for Mixed Mode and that you enabled the TFTP Encrypted Config parameter in Cisco Unified CallManager Administration.

Manual Key Distribution

Tip For a list of phone models that support this method, see "Supported Phone Models" section on page 7-4.

With manual key distribution, a 128- or 256-bit symmetric key, which is stored in the Cisco Unified CallManager database, encrypts the phone configuration file after the phone resets. To determine the key size for your phone model, see "Supported Phone Models" section on page 7-4.

To encrypt the configuration file, the administrator can either manually enter the key into Cisco Unified CallManager Administration or prompt Cisco Unified CallManager Administration 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 "Supported Phone Models" section on page 7-4.

When the phone contains the symmetric key, the phone always requests the encrypted configuration file. Cisco Unified CallManager downloads the encrypted configuration file to the phone, which the TFTP server signs. Not all phone types validate the signer of the configuration file; see "Supported Phone Models" section on page 7-4 for more information.

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 that the phone requests an unencrypted configuration file the next time that it is reset.

Symmetric Key Encryption with Phone Public Key

Tip For a list of phone models that support this method, see "Supported Phone Models" section on page 7-4.

For more information about The Certificate Authority Proxy Function (CAPF), see "Certificate Authority Proxy Function Overview" section on page 6-2. The Certificate Authority Proxy Function (CAPF) authenticates Cisco Unified IP Phones to Cisco Unified Call Manager and issues phone certificates (LSCs)

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). 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 Cisco Unified CallManager 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 Unified IP Phone models 7911, 7941, 7961, 7970, and 7971 request an encrypted file (.enc.sgn file), Cisco Unified CallManager 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 Cisco Unified CallManager database. If the error condition is resolved, the phone requests an encrypted configuration file the next time that it resets.

Supported Phone Models

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

Phone Model and Protocol	Encryption Method
Cisco Unified SIP IP Phone 7905 or 7912	Supports manual key distribution— Encryption algorithm: RC4 Key size: 256 bits File signing support: No
Cisco Unified SIP IP Phone 7940 or 7960	Supports manual key distribution— Encryption algorithm: Advanced Encryption Standard (AES) 128 Key size: 128 bits File signing support: These SIP phones receive signed, encrypted configuration files but ignore the signing information
Cisco Unified SIP IP Phone 7970 or 7971; Cisco Unified SIP IP Phone 7941 or 7961; Cisco Unified SIP IP Phone 7911; Cisco Unified SIP IP Phone 7906 Cisco Unified SCCP IP Phone 7970 or 7971; Cisco Unified SCCP IP Phone 7941 or 7961; Cisco Unified SCCP IP Phone 7911; Cisco Unified SCCP IP Phone 7906	Supports symmetric key encryption with phone public key (PKI encryption)— Encryption algorithm: AES 128 Key size: 128 bits File signing support: Yes

Configuration Tips for Encrypted Configuration Files

Cisco recommends 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 Cisco Unified CallManager Administration and in the phone. If the symmetric key is missing from either the phone or Cisco Unified CallManager 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 Cisco Unified CallManager 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 SCCP Phone models 7905, 7912, 7940, and 7960 because these phones do not receive confidential data in the configuration file download.
- Only SIP phone security profiles display the Enable Digest Authentication flag and the TFTP Exclude Digest Credentials in Configuration File flag.
- The default setting for TFTP Encrypted Config specifies false (not checked). If you apply the default, non-secure profile to the phone, digest credentials and secured passwords get sent in the clear.

- For Cisco Unified Phone models that use public key encryption, Cisco Unified CallManager does not require you to set the Device Security Mode to authenticated or encrypted to enable encrypted configuration files. Cisco Unified CallManager uses the CAPF process for downloading its public key during registration.
- You may choose to download unencrypted configuration files to phones if you know your environment is secure or to avoid manually configuring symmetric keys for phones that are not PKI-enabled; however, Cisco does not recommend using this method.
- For Cisco Unified IP SIP Phone models 7905, 7912, 7940, and 7960, Cisco Unified CallManager 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 is useful for initializing digest credentials because it does not require you to first configure a symmetric key and enter it on the phone, uses the TFTP Exclude Digest Credential in Configuration File setting.

  With this method, you send the digest credentials to the phone in an unencrypted configuration file. After the credentials are in the phone, Cisco recommends that you keep the TFTP file encryption setting disabled and enable the TFTP Exclude Digest Credential in Configuration File flag on the corresponding 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.
- Be aware that the TFTP Exclude Digest Credentials flag is valid for all Cisco Unified IP SIP Phone models. If the TFTP Exclude Digest Credentials flag is set for these phone models, Cisco Unified CallManager excludes the digest credentials, regardless whether the TFTP Encrypted Config flag is set. **Be sure that the digest credentials are loaded on the phone at least once, or the phone may fail to register**.

Encryption Configuration File Configuration Checklist

Use Table 7-1 to guide you through the configuration process for encrypted configuration files in Cisco Unified CallManager Administration.

Table 7-1 Encryption Configuration File Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Verify that the Cluster Security Mode is configured for Mixed Mode.	Configuring the Cisco CTL Client, page 3-1
Step 2	In Cisco Unified CallManager Administration, check the TFTP Encrypted Config check box in the Phone Security Profile. Be sure to apply the profile to the phone.	• Configuration Tips for Encrypted Configuration Files, page 7-4 • Enabling Phone Configuration File Encryption, page 7-6 • Applying a Phone Security Profile, page 5-9

Table 7-1 Encryption Configuration File Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 3	Determine which phones support manual key distribution and which phones support symmetric key encryption with phone public key (PKI encryption).	Supported Phone Models, page 7-4
Step 4	If your phone supports manual key distribution, perform the manual key distribution tasks in Cisco Unified CallManager Administration.	• Configuration Tips for Encrypted Configuration Files, page 7-4 • Configuring Manual Key Distribution, page 7-6 • Manual Key Distribution Configuration Settings, page 7-7
Step 5	If your phone supports manual key distribution, enter the symmetric key on the phone; reset the phone.	Entering the Symmetric Key on the Phone, page 7-8
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.	• Verifying That an LSC or MIC Certificate Is Installed, page 7-8 • Using the Certificate Authority Proxy Function, page 6-1

Enabling 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.

To access the TFTP encryption flag, find the appropriate device security profile for the phone, as described in "Finding a Phone Security Profile" section on page 5-2. Check the TFTP Encrypted Config check box to enable configuration file encryption.

Additional Information

See the "Related Topics" section on page 7-10

Configuring Manual Key Distribution

To determine whether your phone supports manual key distribution, see "Supported Phone Models" section on page 7-4.

The following procedure assumes that

- The phone exists in the Cisco Unified CallManager database,
- A compatible firmware load exists on the TFTP server,
- You enabled the TFTP Encrypted Config parameter in Cisco Unified CallManager Administration.

Procedure

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

Step 2 After the Phone Configuration window displays, configure the manual key distribution settings that are described in Table 7-2. Once configured, the key should not be changed.

Step 3 Click **Save**.

Step 4 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.

Additional Information

See the "Related Topics" section on page 7-10.

Manual Key Distribution Configuration Settings

Table 7-2 describes the manual distribution configuration settings in the Phone Configuration window.

- For configuration tips, see "Configuration Tips for Encrypted Configuration Files" section on page 7-4.
- For related information and procedures, see the "Related Topics" section on page 7-10.

Table 7-2 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 CallManager rejects the value. Cisco Unified CallManager supports the following key sizes: • Cisco Unified IP Phone models 7905 and 7912 (SIP Protocol only)—256 bits • Cisco Unified IP Phone models 7940 and 7960 (SIP Protocol only)—128 bits After the key is configured, you should not change it.
Generate String	If you want Cisco Unified CallManager 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.

Entering the Symmetric Key on the Phone

For information on how to enter the symmetric key on the phone after you configure manual key distribution in Cisco Unified CallManager Administration, refer to the Cisco Unified IP Phone administration guide that supports your phone model and protocol.

Verifying That an LSC or MIC Certificate Is Installed

This procedure applies to Cisco Unified IP Phones that use PKI encryption.To determine whether your phone supports the method, symmetric key encryption with phone public key (PKI encryption), see the "Supported Phone Models" section on page 7-4.

The following procedure assumes that the phone exists in the Cisco Unified CallManager database and that you enabled the TFTP Encrypted Config parameter in Cisco Unified CallManager Administration.

Procedure

Step 1 Verify that a manufacture-installed certificate (MIC) or a locally significant certificate (LSC) exists in the phone.

Tip By choosing the Troubleshooting option in the CAPF settings section of the Phone Configuration window, 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.

Step 2 If a certificate does not exist, install an LSC by using the CAPF functionality in the Phone Configuration window. For information on how to install a LSC, see the "Using the Certificate Authority Proxy Function" section on page 6-1.

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

Additional Information

See the "Related Topics" section on page 7-10.

Verifying That the Phone Configuration File Is Encrypted

When the phone configuration file is encrypted, it uses the following format:

- Cisco Unified IP Phone models 7905 and 7912 (SIP protocol only)—LD <MAC>.x
- Cisco Unified IP Phone models 7940 and 7960 (SIP protocol only)—SIP<MAC>.cnf.enc.sgn
- Cisco Unified IP Phone models 7911, 7941, 7961, 7970, and 7971 (SIP protocol only)—SIP<MAC>.cnf.xml.enc.sgn
- Cisco Unified IP Phone models 7911, 7941, 7961, 7970, and 7971 (SCCP protocol only)—SEP<MAC>.cnf.xml.enc.sgn

Disabling Encryption for the Phone Configuration Files

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

Warning **If digest authentication is True for the SIP phone 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 Cisco Unified CallManager database.

If Cisco Unified IP Phone models 7911, 7941, 7961, 7970, and 7971 request an encrypted file (.enc.sgn file) when the encrypted configuration setting gets updated to false, the phone requests a unencrypted, signed file (.sgn file).

If Cisco Unified IP SIP Phone models 7940/7960/7905/7912 request an encrypted file when the encryption configuration setting gets updated to false, administrators must remove the symmetric key from the phone GUI so that the phone requests an unencrypted configuration file the next time that it is reset.

Tip For Cisco Unified IP SIP Phone models 7940 and 7960, enter a 32-byte 0 as the key value for the symmetric key at the phone GUI to disable encryption. For Cisco Unified IP SIP Phone models 7905 and 7912, 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.

Excluding 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 TFTP Exclude Digest Credentials in Configuration File check box for the security profile that is applied to the phone.

You may need to uncheck this check box to update the configuration file for changes to digest credentials. See "Configuration Tips for Encrypted Configuration Files" section on page 7-4 for more information.

Additional Information

See the "Related Topics" section on page 7-10.

Where to Find More Information

Related Topics

- Understanding Encryption of the Phone Configuration File, page 7-1
- Supported Phone Models, page 7-4
- Configuration Tips for Encrypted Configuration Files, page 7-4
- Encryption Configuration File Configuration Checklist, page 7-5
- Enabling Phone Configuration File Encryption, page 7-6
- Configuring Manual Key Distribution, page 7-6
- Manual Key Distribution Configuration Settings, page 7-7
- Entering the Symmetric Key on the Phone, page 7-8
- Verifying That an LSC or MIC Certificate Is Installed, page 7-8
- Verifying That the Phone Configuration File Is Encrypted, page 7-8
- Disabling Encryption for the Phone Configuration Files, page 7-9
- Excluding Digest Credentials from Phone Configuration File Download, page 7-9
- Using the Certificate Authority Proxy Function, page 6-1
- Configuration Tips for Phone Security Profiles, page 5-1

Related Cisco documentation

- *Cisco Unified CallManager Bulk Administration Guide*
- Cisco Unified IP Phone administration guide for the phone model and protocol

CHAPTER 8

Configuring Digest Authentication for the SIP Phone

When you configure digest authentication for SIP phones, Cisco Unified CallManager challenges the identity of the phone every time that the phone sends a SIP request to Cisco Unified CallManager. For additional information on how digest authentication works for SIP phones, see the "Digest Authentication" section on page 1-16.

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

This chapter contains information on the following topics:

SIP Phone Digest Authentication Configuration Checklist

Table 8-1 describes the tasks to configure digest authentication for SIP phones.

Table 8-1 SIP Phone Digest Authentication Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Configure the SIP phone security profiles; make sure that you check the **Enable Digest Authentication** check box.	Configuring a Phone Security Profile, page 5-1
Step 2	Apply a SIP phone security profile to the phone.	Configuring a Phone Security Profile, page 5-1
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.	Configuring Digest Authentication Service Parameters, page 8-2

Table 8-1 SIP Phone Digest Authentication Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 4	Configure the digest credentials in the End User Configuration window.	• Configuring Digest Credentials in the End User Configuration Window, page 8-3 • End User Digest Credential Configuration Settings, page 8-3
Step 5	Choose the Digest User in the Phone Configuration window. Choosing a digest user for a Cisco Unified SIP IP Phone models 7970, 7971, 7961G/41G, 7961GE/41GE, and 7911 ensures that the digest credentials get included in the phone configuration file.	Configuring the Digest User in the Phone Configuration Window, page 8-4
Step 6	On the Cisco Unified SIP IP Phone models 7940 or 7960, enter the digest credentials that you configured in the End User Configuration window.	The *Cisco Unified CallManager Security Guide* does not provide information on how to enter the digest authentication credentials on the phone. For information on how to perform this task, refer to the Cisco Unified IP Phone administration guide that supports your phone model and this version of Cisco Unified CallManager.

Configuring Digest Authentication Service Parameters

The SIP Realm Station service parameter, which supports the Cisco CallManager service, specifies the string that is used in the realm field when Cisco Unified CallManager challenges a SIP phone in response to a 401 Unauthorized message. 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 Cisco Unified CallManager Administration, choose **System > Service Parameters**.

Step 2 From the Server drop-down list box, choose a node where you activated the Cisco Unified 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 CAPF service parameters, click the question mark or the parameter name link.

Step 5 Click **Save**.

Additional Information

See the "Related Topics" section on page 8-4.

Configuring Digest Credentials in the End User Configuration Window

The following procedure assumes that the end user exists in the Cisco Unified CallManager 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 CallManager Administration Guide*.

Step 2 After the specific End User Configuration window displays, enter the appropriate settings, as described in Table 8-2.

Step 3 Click **Save**.

Step 4 Repeat the procedure to configure digest credentials for additional end users.

Additional Steps

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

After you choose the digest user, enter the digest authentication credentials that you get from the End User Configuration window on the Cisco Unified SIP IP Phone 7960 or 7940.

Additional Information

See the "Related Topics" section on page 8-4.

End User Digest Credential Configuration Settings

Table 8-2 describes the settings for the digest credential settings in the End User Configuration window in Cisco Unified CallManager Administration. For related procedures, see the "Configuring the Digest User in the Phone Configuration Window" section on page 8-4.

Table 8-2 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.

Configuring the Digest User in the Phone Configuration Window

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

Procedure

Step 1 Find the phone, as described in the *Cisco Unified CallManager 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, Cisco Unified CallManager challenges all SIP requests from the phone; Cisco Unified CallManager 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, then Cisco Unified CallManager 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.

Additional Information

See the "Related Topics" section on page 8-4.

Where to Find More Information

Related Topics

- Digest Authentication, page 1-16
- Configuring a Phone Security Profile, page 5-1
- SIP Phone Digest Authentication Configuration Checklist, page 8-1
- Configuring Digest Authentication Service Parameters, page 8-2
- Configuring Digest Credentials in the End User Configuration Window, page 8-3
- End User Digest Credential Configuration Settings, page 8-3
- Configuring the Digest User in the Phone Configuration Window, page 8-4

Related Cisco Documentation

Cisco Unified IP Phone administration guide that supports your phone model and this version of Cisco Unified CallManager

CHAPTER 9

Phone Hardening

To tighten security on the phone, you can perform tasks in the Phone Configuration window in Cisco Unified CallManager Administration. This chapter contains information on the following topics:

Disabling the Gratuitous ARP Setting

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 of Cisco Unified CallManager Administration.

Note Disabling this functionality does not prevent the phone from identifying its default router.

Disabling Web Access Setting

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.

Disabling the PC Voice VLAN Access Setting

By default, Cisco Unified 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 of Cisco Unified CallManager Administration, packets that are received from the PC port that use voice VLAN functionality will drop. Various Cisco Unified IP Phone models use this functionality differently.

- Cisco Unified IP Phone 7940 and 7960 drop any packets that are tagged with the voice VLAN, in or out of the PC port.
- Cisco Unified IP Phone 7970 drops any packet that contains an 802.1Q tag on any VLAN, in or out of the PC port.
- Cisco Unified IP Phone 7912 cannot perform this functionality.

Disabling the Setting Access Setting

By default, pressing the Settings button on a Cisco Unified IP Phone provides access to a variety of information, including phone configuration information. Disabling the Setting Access setting in the Phone Configuration window of Cisco Unified CallManager Administration prohibits access to all options that normally display when you press the Settings 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 Cisco Unified CallManager 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 Cisco Unified CallManager Administration.

Disabling the PC Port Setting

By default, Cisco Unified CallManager enables the PC port on all Cisco Unified 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 of Cisco Unified CallManager Administration. Disabling the PC port proves useful for lobby or conference room phones.

Configuring Phone Hardening

Caution The following procedure disables functionality for the phone.

To disable functionality for the phone, perform the following procedure:

Procedure

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

Step 2 Specify the criteria to find the phone and click **Find** or click **Find** to display a list of all phones.

Step 3 To open the Phone Configuration window for the device, click the device name.

Step 4 Locate the following product-specific parameters:

- PC Port
- Settings Access
- Gratuitous ARP
- PC Voice VLAN Access
- Web Access Setting

Tip To review information on these settings, click the question mark that displays next to the parameters in the Phone Configuration window.

Step 5 From the drop-down list box for each parameter that you want to disable, choose **Disabled**. To disable the speakerphone or speakerphone and headset, check the corresponding check boxes.

Step 6 Click **Save**.

Step 7 Click **Reset**.

Additional Information

See the "Related Topics" section on page 9-3.

Where to Find More Information

Related Topics

- Disabling the Gratuitous ARP Setting, page 9-1
- Disabling Web Access Setting, page 9-1
- Disabling the PC Voice VLAN Access Setting, page 9-2
- Disabling the Setting Access Setting, page 9-2
- Disabling the PC Port Setting, page 9-2
- Configuring Phone Hardening, page 9-3

Related Cisco Documentation

Cisco Unified IP Phone Administration Guide for Cisco Unified CallManager

CHAPTER 10

Configuring Voice Messaging Ports for Security

This chapter contains information on the following topics:

Voice Messaging Security Overview

To configure security for Cisco Unified CallManager voice messaging ports and Cisco Unity SCCP devices, you choose a secure device security mode for the port. If you choose an authenticated voice mail 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 encrypted voice mail port, the system first authenticates the devices and then sends encrypted voice streams between the devices.

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

Note In this document, the use of the term, server, refers to a server in the Cisco Unified CallManager cluster. The use of the phrase, voice-mail server, refers to a Cisco Unity server.

Configuration Tips for Voice Messaging Security

Consider the following information before you configure security:

- You must run Cisco Unity 4.0(5) or later with this version of Cisco Unified CallManager.
- You must perform security tasks for Cisco Unity by using the Cisco Unity Telephony Integration Manager; for information on how to perform these tasks, refer to the *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*.

- In addition to the procedures that are described in this chapter, you must use the certificate management feature in Cisco Unified Communications Operating System Administration to save the Cisco Unity certificate to the trusted store. For more information on this task, refer to the *Cisco Unified Communications Operating System Administration Guide.*

  After you copy the certificate, you must restart the Cisco CallManager service on each server in cluster.
- If Cisco Unity certificates expire or change for any reason, use the certificate management feature in the Cisco Unified Communications Operating System Administration 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 Cisco Unified CallManager.
- 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 must match the voice messaging port device security mode that is configured in Cisco Unified CallManager Administration. In Cisco Unified CallManager 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 for Cisco Unified CallManager and Cisco Unity, the Cisco Unity ports fail to register with Cisco Unified CallManager, and Cisco Unity cannot accept calls on those ports.

- Changing the security profile for the port requires a reset of Cisco Unified CallManager devices and a restart of the Cisco Unity software. If you apply a security profile in Cisco Unified CallManager Administration that uses a different device security mode than the previous profile, you must change the setting in Cisco Unity.
- You cannot change the Device Security Mode for existing voice-mail servers through the Voice Mail Port Wizard. If you add ports to an existing voice-mail server, the device security mode that is currently configured for the profile automatically applies to the new ports.

Secure Voice Messaging Port Configuration Checklist

Use Table 10-1 as a reference when you configure security for voice-messaging ports.

Table 10-1 Configuration Checklist for Securing Voice Messaging Ports

Configuration Steps		Related Procedures and Topics
Step 1	Verify that you installed and configured the Cisco CTL Client for Mixed Mode.	Configuring the Cisco CTL Client, page 3-1
Step 2	Verify that you configured the phones for authentication or encryption.	Phone Security Overview, page 4-1 Configuring a Phone Security Profile, page 5-1

Table 10-1 Configuration Checklist for Securing Voice Messaging Ports (continued)

Configuration Steps		Related Procedures and Topics
Step 3	Use the certificate management feature in the Cisco Unified Communications Operating System Administration to copy the Cisco Unity certificate to the trusted store on each server in the cluster; then, restart the Cisco CallManager service on each server.	• Configuration Tips for Voice Messaging Security, page 10-1 • *Cisco Unified Communications Operating System Administration Guide* • *Cisco Unified CallManager Serviceability Administration Guide*
Step 4	In Cisco Unified CallManager Administration, configure the device security mode for the voice messaging ports.	• Applying a Security Profile to a Single Voice Messaging Port, page 10-3 • Applying the Security Profile in the Voice Mail Port Wizard, page 10-4
Step 5	Perform security-related configuration tasks for Cisco Unity voice messaging ports; for example, configure Cisco Unity to point to the Cisco TFTP server.	*Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*
Step 6	Reset the devices in Cisco Unified CallManager Administration and restart the Cisco Unity software.	• *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x* • Applying a Security Profile to a Single Voice Messaging Port, page 10-3

Applying a Security Profile to a 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 apply a security profile, review the following sections:

- Voice Messaging Security Overview, page 10-1
- Configuration Tips for Voice Messaging Security, page 10-1
- Secure Voice Messaging Port Configuration Checklist, page 10-2

Procedure

Step 1 Find the voice messaging port, as described in the *Cisco Unified CallManager 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**.

Additional Information

See the "Related Topics" section on page 10-4.

Applying the Security Profile in the Voice Mail Port Wizard

To change the security setting for an existing voice-mail server, see the "Applying a Security Profile to a Single Voice Messaging Port" section on page 10-3.

Before you apply a security profile, review the following sections:

- Voice Messaging Security Overview, page 10-1
- Configuration Tips for Voice Messaging Security, page 10-1
- Secure Voice Messaging Port Configuration Checklist, page 10-2

To apply the Device Security Mode setting in the Voice Mail Port Wizard for a new voice-mail server, perform the following procedure:

Procedure

Step 1 In Cisco Unified CallManager Administration, choose **Voice Mail > 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 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 CallManager Administration Guide*. Click **Next**.

Step 6 Continue the configuration process, as described in the *Cisco Unified CallManager Administration Guide*. When the Summary window displays, click **Finish**.

Additional Information

See the "Related Topics" section on page 10-4.

Where to Find More Information

Related Topics

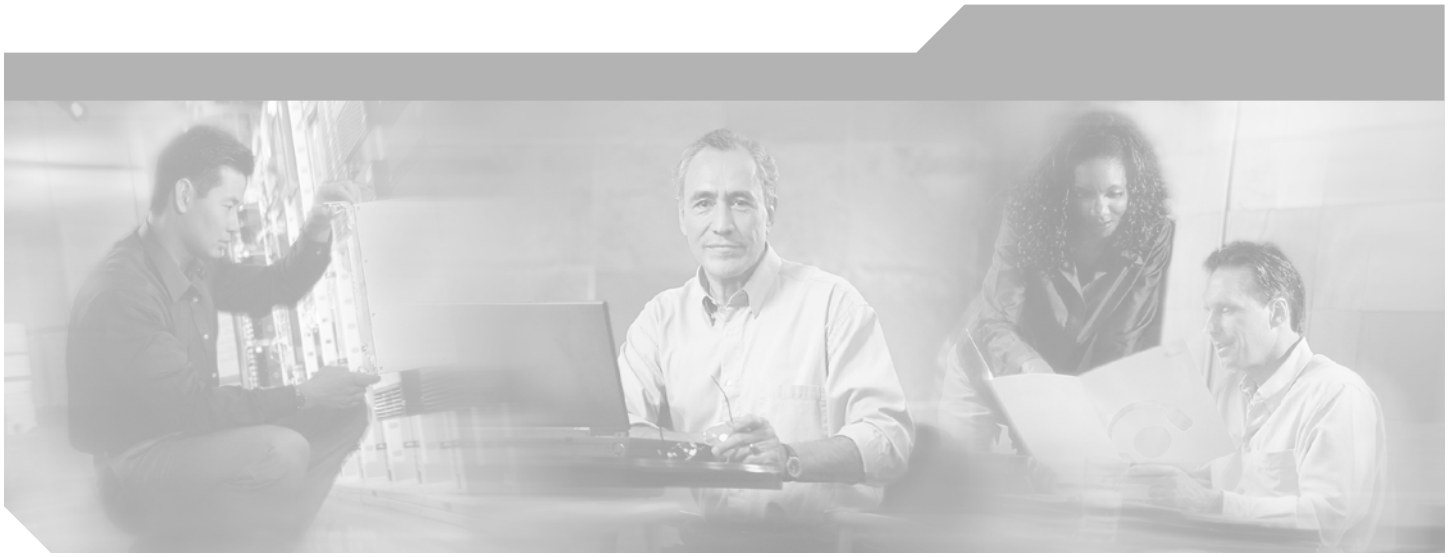
- System Requirements, page 1-4
- Interactions and Restrictions, page 1-5
- Certificate Types, page 1-12
- Configuration Checklist Overview, page 1-20
- Voice Messaging Security Overview, page 10-1
- Configuration Tips for Voice Messaging Security, page 10-1
- Applying a Security Profile to a Single Voice Messaging Port, page 10-3

- Applying the Security Profile in the Voice Mail Port Wizard, page 10-4

Related Cisco Documentation

- *Cisco Unified CallManager 5.0 Integration Guide for Cisco Unity 4.x*
- *Cisco Unified Communications Operating System Administration Guide*

Cisco Systems



PART 3

Security for Cisco CTI, JTAPI, and TAPI Applications

CHAPTER 11

Configuring Authentication and Encryption 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 Cisco Unified CallManager Administration to configure authentication and encryption for the CTI/TAPI/JTAPI application.

This document does not describe how to install the Cisco JTAPI or TSP plug-ins that are available in Cisco Unified CallManager 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.

This chapter provides information on the following topics:

Understanding Authentication for CTI, JTAPI, and TAPI Applications

Cisco Unified CallManager 5.0 allows you to secure the signaling connections and media streams between CTIManager and CTI/JTAPI/TAPI applications.

Tip 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. 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 Cisco Unified CallManager self-signed certificate that installs automatically on the Cisco Unified CallManager server during the 5.0 installation; after you install the Cisco CTL client and generate the CTL file, this certificate gets 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 and the JTAPI/TSP client downloads it from the TFTP server, the JTAPI/TSP client uses the security tokens in the CTL file to authenticate the digital signature of the new file; contents of the file include the Cisco Unified CallManager self-signed 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, as described in the "Configuring the Cisco CTL Client" section on page 3-1. 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) in Cisco Unified CallManager 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. For example, if Cisco Unified CallManager Assistant runs two instances of the service on two different nodes in the cluster, each instance must have its own certificate. One certificate does not cover all instances. To ensure that the certificate installs on the node where Cisco CallManager Assistant service is running, you configure a unique Instance ID for each Application User or End User CAPF Profile in Cisco Unified CallManager Administration, as described in Table 11-2.

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.

In addition to the tasks that are described in the preceding paragraphs, you must add the application users or the end users to the Standard CTI Secure Connection user group in Cisco Unified CallManager 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.

Understanding 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.

Cisco Unified CallManager Assistant, Cisco QRT, and Cisco WebDialer do not support encryption. CTI clients that connect to the CTIManager service may support encryption if the client sends voice packets.

If you want to secure the media streams between the application and CTIManager, you must add the application users or the end users to the Standard CTI Allow Reception of SRTP Key Material user group in Cisco Unified CallManager Administration. After the application user and end user(s) get added to this group and 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. Although the 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. Be aware that the applications should not record or store the SRTP key materials.

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 Before the application and end user can use SRTP, verify that the user exists in the Standard CTI Enabled and Standard CTI Secure Connection user groups, which serve as a baseline configuration for TLS. TLS is required for SRTP connections. 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.

Although Cisco Unified CallManager 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 Overview for CTI, JTAPI, and TAPI Applications

Certificate Authority Proxy Function (CAPF), which automatically installs with Cisco Unified CallManager, 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 Cisco Unified CallManager supports:

- Application User CAPF Profile—This profile allows you to issue locally significant certificates to secure application users. After you issue the certificate and perform other security-related tasks, 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. For example, 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. If you activate multiple web services or applications on the same server, for example, you must configure two Application User CAPF Profiles, one for each service on the server.
- End User CAPF Profile—This profile allows you to issue locally significant certificates to CTI clients. After you issue the certificate and perform other security-related tasks, 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, as configured in the Cisco CTL client, equals 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.

Configuration Checklist for Securing CTI, JTAPI, and TAPI

Table 11-1 provides a list of tasks that you perform to secure the CTI/JTAPI/TAPI application.

Table 11-1 CTI/JTAPI/TAPI Security Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Verify that the CTI application and any JTAPI/TSP plug-ins are installed and running. **Tip** The application user should be assigned to the Standard CTI Enabled group.	• Computer Telephony Integration, *Cisco Unified CallManager System Guide, Release 5.0* • *Cisco JTAPI Installation Guide for Cisco Unified CallManager 5.0* • *Cisco TAPI Installation Guide for Cisco Unified CallManager 5.0* • *Cisco Unified CallManager Administration Guide*

Table 11-1 CTI/JTAPI/TAPI Security Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 2	Verify that the following CallManager security features are installed (if not installed, install and configure these features): • Verify that you installed the CTL client for 5.0 and the CTL file has run so that 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. **Tip** The CTI/JTAPI/TAPI application cannot access the CTL file if the cluster security mode does not equal Mixed Mode.	• Configuring the Cisco CTL Client, page 3-1 • Updating CAPF Service Parameters, page 11-9 • *Cisco Unified CallManager Administration Guide*
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 and end user, but not both.	Adding Application and End Users to the Security-Related Users Groups, page 11-7
Step 4	If you want to use SRTP to secure the media streams between CTIManager and the application, add the application user or end user to the Standard CTI Allow Reception of SRTP Key Material user group. Before the application or end user can use SRTP, verify that the user exists in theStandard CTI Enabled and Standard CTI Secure Connection user group, which serves as a baseline configuration for TLS and SRTP connections. After you add the user to these groups, you can add the user to the Standard CTI Allow Reception of SRTP Key Material user group. The application or end user cannot receive SRTP session keys if it does not exist in these three groups. Cisco Unified CallManager Assistant, Cisco QRT, and Cisco WebDialer do not support encryption. CTI clients that connect to the CTIManager service may support encryption if the client sends voice packets.	Adding Application and End Users to the Security-Related Users Groups, page 11-7 Role Configuration, *Cisco Unified CallManager Administration Guide*

Table 11-1 CTI/JTAPI/TAPI Security Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 5	Configure the Application User CAPF Profile or End User CAPF Profile in Cisco Unified CallManager Administration.	• CAPF Overview for CTI, JTAPI, and TAPI Applications, page 11-4 • Configuring the Application User or End User CAPF Profile, page 11-10 • CAPF Settings in the Application User and End User CAPF Profile Windows, page 11-11
Step 6	Enable the corresponding security-related parameters in the CTI/JTAPI/TAPI application.	Configuring JTAPI/TAPI Security-Related Service Parameters, page 11-14

Adding Application and End Users to the 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 Cisco Unified CallManager Administration by default. You cannot delete these groups.

If you want the application user or end users to use a TLS connection when communicating with CTIManager, you must add the application user or end users to the Standard CTI Secure Connection user group. A CTI application can be assigned to either an application user or and 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. TLS is required for SRTP connections. 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 Cisco Unified CallManager Assistant, Cisco QRT, and Cisco WebDialer do not support encryption, you do not need to add the application users, Unified CMQRTSecureSysUser, 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 CallManager Administration Guide*. For information about security-related settings in the Role Configuration window, refer to the *Cisco Unified CallManager Administration Guide*

Procedure

Step 1 In Cisco Unified CallManager 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:

- Verify that the application or end users exist in the Standard CTI Enabled group.
- To add an application user or end users to the Standard CTI Secure Connection user group, click the **Standard CTI Secure Connection** link.
- 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 through Step 7.

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 Step 9 through Step 11.

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 ends users that you want to add to the group; then, click **Add Selected**.

The users display in the User Group window.

Additional Information

See the "Related Topics" section on page 11-15.

Activating the Certificate Authority Proxy Function Service

Cisco Unified CallManager 5.0 does not automatically activate the Certificate Authority Proxy Function service in Cisco Unified CallManager Serviceability. For information on activating the Certificate Authority Proxy Function service, refer to the *Cisco Unified CallManager Serviceability Administration Guide*.

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, as described in the "Updating the CTL File" section on page 3-9.

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 all servers in the cluster, uses the .0 extension. To verify that the CAPF certificate exists, display the CAPF certificate at the Cisco Unified Communications platform GUI.

Updating CAPF Service Parameters

IThe 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, the key size, and so on

Tip Cisco Unified CallManager does not support SCEP or third-party CA-signed LSC certificates, such as Microsoft CA or Keon CA, in this release. Support for third-party certificates is scheduled for a future release. Customers who currently use third-party CA should re-issue a long expiration period (at least 6 months) for their certificates before migration to 5.0 to ensure that certificates will not expire until support for third-party certificates is available.

For the CAPF service parameters to display as Active in Cisco Unified CallManager Administration, you must activate the Certificate Authority Proxy Function service in Cisco Unified CallManager 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 Cisco Unified CallManager Administration, choose **System > Service Parameters**.

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

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 CallManager Serviceability.

Additional Information

See the "Related Topics" section on page 11-15.

Finding an Application User or End User CAPF Profile

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

Procedure

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

- **User Management > Application User CAPF Profile**
- **User Management > End User CAPF Profile**

The Find and List window displays.

Step 2 From the drop-down list boxes, choose your search criteria for the profiles that you want to list and click **Find**.

Note To find all Application User CAPF Profiles or End User CAPF Profiles that are registered in the database, click **Find** without specifying any search criteria.

The window refreshes and displays the profiles that match your search criteria.

Step 3 For the profile that you want to view, click the **Instance ID** link, the **Application User** link (for Application User CAPF Profile only), or the **End User ID** link (for End User CAPF Profile only).

Tip To search for the Instance ID, Application User (for Application User CAPF Profile only), or End User ID (for End User CAPF Profile only) within the search results, check the **Search Within Results** check box, enter your search criteria as described in this procedure, and click **Find**.

Additional Information

See the "Related Topics" section on page 11-15.

Configuring the Application User or End User CAPF Profile

Use Table 11-2 as a reference when you install/upgrade/troubleshoot locally significant certificates for JTAPI/TAPI/CTI applications.

Tip Although the following procedure supports both Application User and End User CAPF Profiles, you cannot configure both types at the same time. Cisco recommends that you configure the Application User CAPF Profile before you configure the End User CAPF Profile.

Procedure

Step 1 In Cisco Unified CallManager Administration, choose one of the following options:

- **User Management > Application User CAPF Profile**.
- **User Management > End User CAPF Profile**.

Step 2 After the Find/List Application User or End User CAPF Profile Configuration window displays, perform one of the following tasks:

- To find an existing Application User or End User CAPF Profile, specify your search criteria and click **Find**.

  Clicking Find without specifying search criteria displays all Application User CAPF Profiles or End User CAPF Profiles in the system.
- To add a new Application User or End User CAPF Profile, click **Add New**.

Step 3 After the CAPF Profile profile configuration window displays, enter the configuration settings, as described in Table 11-2.

Step 4 Click **Save**.

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

Additional Steps

If you configured the Unified CMQRTSecureSysUser, IPMASecureSysUser, or WDSecureSysUser in the Application User CAPF Profile Configuration window, you must configure service parameters, as described in the "Configuring JTAPI/TAPI Security-Related Service Parameters" section on page 11-14.

Additional Information

See the "Related Topics" section on page 11-15.

CAPF Settings in the Application User and End User CAPF Profile Windows

Table 11-2 describes the CAPF settings in the Application User and End User CAPF Profile windows in Cisco Unified CallManager Administration.

- For configuration tips, see the "CAPF System Interactions and Requirements for CTI, JTAPI, and TAPI Applications" section on page 11-5.
- For related information and procedures, see the "Related Topics" section on page 11-15.

Table 11-2 Application and End User CAPF Profile Configuration Settings

Setting	Description
Application User	For this setting, users that exist in the Application User window display. From the drop-down list box, choose the application user where you want to perform the CAPF operation. This setting does not display in the End User CAPF Profile window.
End User	For this setting, users that exist in the End User window display. From the drop-down list box, choose the end user where you want to perform the CAPF operation. This setting does not display in the Application User CAPF Profile window.
Instance ID	Multiple connections (instances) for the application can run in the cluster. To use TLS for every connection between the application and CTIManager, each instance that runs on the application PC (for end users) or server (for application users) must have a unique certificate. For example, if two instances of a service or application runon two servers in the cluster, each instance must have its own certificate. CAPF uses the Application User/End User and Instance ID configuration to determine where to perform the certificate operation. For the application user or end user that you are configuring, enter a unique string by using the following characters: a-z, A-Z, dash (-), underscore (_), or period (.). This field relates to the CAPF Profile Instance ID for Secure Connection to CTIManager service parameter that supports web services and applications. For information on how to access this parameter, see the "Configuring JTAPI/TAPI Security-Related Service Parameters" section on page 11-14.
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 acts as the method by which the application authenticates with CAPF during the specified certificate operation. By default, Cisco Unified CallManager Administration displays By Authentication String, which 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.

Table 11-2 Application and End User CAPF Profile Configuration Settings (continued)

Setting	Description
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.
Key Size (bits)	From the drop-down list box, choose the key size for the certificate. The default setting equals 1024. Other options include 512 and 2048. 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. If you choose a 2048-bit key for the certificate, establishing a connection between the application and Cisco Unified CallManager may take more than 60 seconds. Unless you want to use the highest possible security level, do not configure the 2048-bit key.
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 in conjunction with the CAPF Operation Expires in (days) enterprise parameter, which specifies the default number of days in which the certificate operation must be completed. If you want to do so, you can update this parameter.
Operation Status	This field displays the progress of the certificate operation; for example, <operation type> pending, failed, or successful, where operating type equals the specified Certificate Operation. You cannot change the information that displays in this field.

Deleting an 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 Cisco Unified CallManager database.

Before You Begin

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

Procedure

Step 1 Find the Application User CAPF Profile or End User CAPF Profile by using the procedure in the "Finding an Application User or End User CAPF Profile" section on page 11-10.

Step 2 To delete multiple profiles, check the check boxes next to the appropriate check box in the Find and List window; then, click the **Delete Selected** icon or the **Delete Selected** button.

Step 3 To delete a single profile, perform one of the following tasks:

- In the Find and List window, check the check box next to the appropriate profile; then, click the **Delete Selected** icon or the **Delete Selected** button.
- In the Find and List window, click the Name link for the profile. After the specific Application User or End User CAPF Profile Configuration window displays, click the **Delete Selected** icon or the **Delete Selected** button.

Step 4 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Additional Information

See the "Related Topics" section on page 11-15.

Configuring 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 the web service or application:

- 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 Cisco Unified CallManager Administration, choose **System > Service Parameters**.

Step 2 From the Server drop-down list box, choose the server where the web service or application is activated.

Step 3 From the Service drop-down list box, choose the web service or application:

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.

Viewing the Certificate Operation Status for the 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.

Where to Find More Information

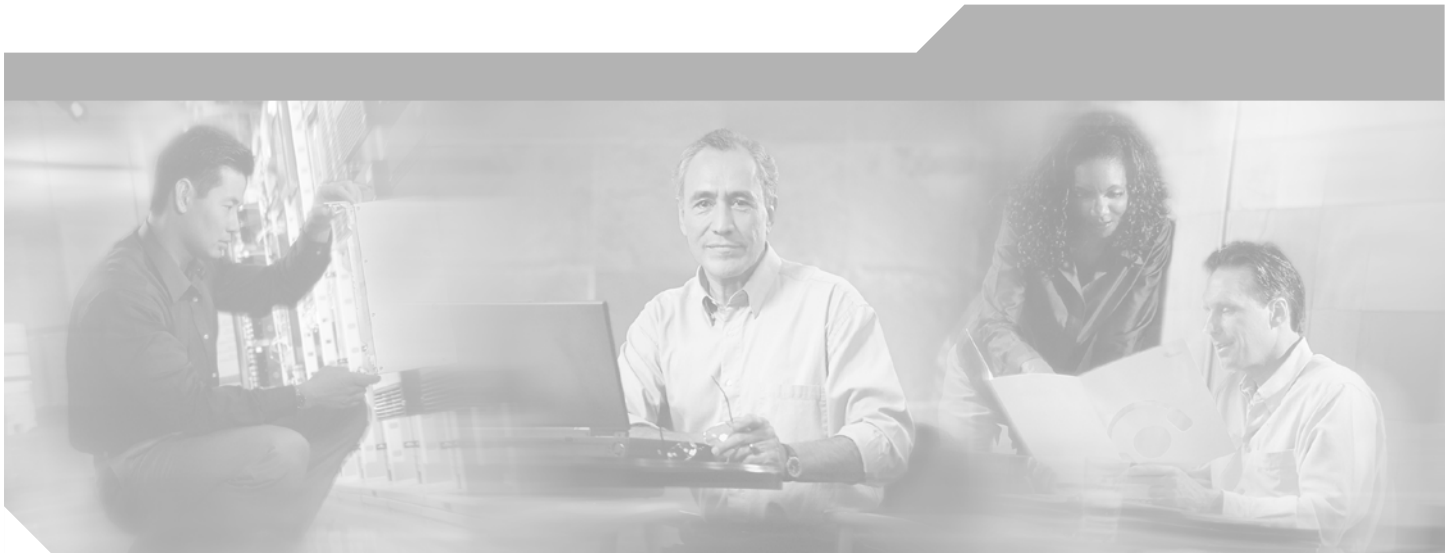
Related Topics

- Configuring the Cisco CTL Client, page 3-1
- Understanding Authentication for CTI, JTAPI, and TAPI Applications, page 11-2
- Understanding Encryption for CTI, JTAPI, and TAPI Applications, page 11-3
- CAPF Overview for CTI, JTAPI, and TAPI Applications, page 11-4
- CAPF System Interactions and Requirements for CTI, JTAPI, and TAPI Applications, page 11-5
- Configuration Checklist for Securing CTI, JTAPI, and TAPI, page 11-5
- Adding Application and End Users to the Security-Related Users Groups, page 11-7
- Activating the Certificate Authority Proxy Function Service, page 11-8
- Updating CAPF Service Parameters, page 11-9
- Finding an Application User or End User CAPF Profile, page 11-10
- Configuring the Application User or End User CAPF Profile, page 11-10
- CAPF Settings in the Application User and End User CAPF Profile Windows, page 11-11
- Deleting an Application User CAPF or End User CAPF Profile, page 11-13
- Configuring JTAPI/TAPI Security-Related Service Parameters, page 11-14
- Viewing the Certificate Operation Status for the Application or End User, page 11-15

Related Cisco Documentation

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

Cisco Systems



Part 4

Security for SRST References, Trunks, and Gateways

CHAPTER 12

Configuring a Secure Survivable Remote Site Telephony (SRST) Reference

This chapter contains information on the following topics:

Overview for Securing the SRST

A SRST-enabled gateway provides limited call-processing tasks if the Cisco Unified CallManager cannot complete the call. Secure SRST-enabled gateways contain a self-signed certificate. After you perform SRST configuration tasks in Cisco Unified CallManager Administration, Cisco Unified CallManager uses a TLS connection to authenticate with the Certificate Provider service in the SRST-enabled gateway. Cisco Unified CallManager then retrieves the certificate from the SRST-enabled gateway and adds the certificate to the Cisco Unified CallManager database.

After you reset the dependent devices in Cisco Unified CallManager 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.

Configuration Tips for Securing the SRST

Ensure that the following criteria are met, so the TLS handshake occurs between the secure phone and the SRST-enabled gateway:

- The SRST reference contains a self-signed certificate.
- You configured the cluster for mixed mode through the Cisco CTL client.
- You configured the phone for authentication or encryption.
- You configured the SRST reference in Cisco Unified CallManager Administration.
- You reset the SRST-enabled gateway and the dependent phones after the SRST configuration.

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

For MIC authentication with Cisco Unified IP Phone models 7911G, 7941G and 7941G-GE, 7961G and 7941G-GE, 7970G, and 7971G-GE, download the following certificates to the SRST-enabled gateway: CiscoCA.pem, CiscoManufacturingCA.pem, and CiscoRootCA2048.pem. These three certificates comprise the root certificates that allow the secure SRST to verify the phone MIC during the TLS handshake.

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 Cisco Unified CallManager 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 the Cisco Unified CallManager servers in the cluster.
- When the cluster security mode equals nonsecure, the system ignores the security-related configuration in Cisco Unified CallManager Administration; for example, the device security mode, the IS SRST Secure? check box, and so on. The configuration does not get deleted in Cisco Unified CallManager Administration, 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 Cisco Unified CallManager release, the configuration automatically migrates during the Cisco Unified CallManager upgrade.
- If phones in encrypted or authenticated mode fail over to SRST, and, during the connection with SRST, the Cisco Unified CallManager cluster switches from mixed mode to nonsecure mode, these phones will not fall back to Cisco Unified CallManager automatically. Administrators must power down the SRST router to force these phones to reregister to Cisco Unified CallManager. After phones fall back to Cisco Unified CallManager, administrators can power up SRST and failover and fallback will be automatic again.

Secure SRST Configuration Checklist

Use Table 12-1 to guide you through the SRST configuration process for security.

Table 12-1 Configuration Checklist for Securing the SRST

Configuration Steps		Related Procedures and Topics
Step 1	Verify that you performed all necessary tasks on the SRST-enabled gateway, so the device supports Cisco Unified CallManager and security.	*Cisco IOS SRST Version 3.3 System Administrator Guide* that supports this version of Cisco Unified CallManager, which you can obtain at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/voice/srst/srst33/srst33ad/index.htm
Step 2	Verify that you performed all necessary tasks to install and configure the Cisco CTL client.	Configuring the Cisco CTL Client, page 3-1
Step 3	Verify that a certificate exists in the phone.	Refer to the Cisco Unified IP Phone documentation for your phone model.
Step 4	Verify that you configured the phones for authentication or encryption.	Applying a Phone Security Profile, page 5-9
Step 5	In Cisco Unified CallManager Administration, configure the SRST reference for security, which includes enabling the SRST reference in the Device Pool Configuration window.	Configuring Secure SRST References, page 12-3
Step 6	Reset the SRST-enabled gateway and phones.	Configuring Secure SRST References, page 12-3

Configuring Secure SRST References

Consider the following information before you add, update, or delete the SRST reference in Cisco Unified CallManager 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 12-2.
- Updating a Secure SRST Reference—Performing SRST updates in Cisco Unified CallManager 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, Cisco Unified CallManager replaces the SRST-enabled gateway certificate in the trust folder on each server in the cluster.
- Deleting a Secure SRST Reference—Deleting a secure SRST reference removes the SRST-enabled gateway certificate from the Cisco Unified CallManager database and the cnf.xml file in the phone.

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

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

Procedure

Step 1 In Cisco Unified CallManager Administration, choose **System > SRST**.

Step 2 Perform one of the following tasks:

- To add a new SRST reference, click the **Add New** button and continue with Step 3.
- To copy an existing SRST reference, locate the appropriate SRST reference as described in the *Cisco Unified CallManager Administration Guide*, click the **Copy** button next to the reference that you want to copy and continue with Step 3.
- To update an existing SRST reference, locate the appropriate SRST reference as described in the *Cisco Unified CallManager Administration Guide* and continue with Step 3.

Step 3 Enter the security-related settings as described in Table 12-2.

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

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**.

Additional Steps

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

Additional Information

See the "Related Topics" section on page 12-6.

Security Configuration Settings for SRST References

Table 12-2 describes the available settings for secure SRST references in Cisco Unified CallManager Administration.

- For configuration tips, see the"Configuration Tips for Securing the SRST" section on page 12-2.
- For related information and procedures, see the "Related Topics" section on page 12-6.

Table 12-2 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 Cisco Unified CallManager 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. Cisco Unified CallManager 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 Cisco Unified CallManager 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.

Deleting Security from the SRST Reference

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

If the SRST Certificate Is Deleted from the Gateway

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

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

Where to Find More Information

Related Topics

- Overview for Securing the SRST, page 12-1
- Configuration Tips for Securing the SRST, page 12-2
- Secure SRST Configuration Checklist, page 12-3
- Configuring Secure SRST References, page 12-3
- Security Configuration Settings for SRST References, page 12-4
- Deleting Security from the SRST Reference, page 12-5
- If the SRST Certificate Is Deleted from the Gateway, page 12-5

Related Cisco Documentation

- *Cisco IOS SRST Version 3.3 System Administrator Guide*
- *Cisco Unified CallManager Administration Guide*

CHAPTER 13

Configuring Encryption for Gateways and Trunks

This chapter contains information on the following topics:

Overview for Cisco IOS MGCP Gateway Encryption

Cisco Unified CallManager 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, Cisco Unified CallManager generates a master encryption key and salt for secure calls and sends them to the gateway for the SRTP stream only. Cisco Unified CallManager 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 Cisco Unified CallManager 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 SCCP phone, a shield icon displays on the phone because Cisco Unified CallManager classifies the call as authenticated. Cisco Unified CallManager 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.

Overview for 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 Cisco Unified CallManager if you configure an IPSec association in the Cisco Unified Communications Platform Administration. For information on creating an IPSec association between Cisco Unified CallManager 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 Cisco Unified CallManager through the signaling path, which you secure through IPSec. Although Cisco Unified CallManager 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 Cisco Unified CallManager 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, Cisco Unified CallManager uses RTP to communicate with the device. If you check the check box, Cisco Unified CallManager 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 Cisco Unified CallManager Administration, Cisco strongly recommends that you configure IPSec, so security-related information does not get sent in the clear. Cisco Unified CallManager 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, Cisco Unified CallManager classifies the call as secure. If the MTP Required check box is checked, Cisco Unified CallManager disables audio pass-through for the call and classifies the call as nonsecure. If no MTP is involved in the call, Cisco Unified CallManager may classify the call as encrypted, depending on the SRTP capabilities of the devices.

For SRTP-configured devices, Cisco Unified CallManager 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, Cisco Unified CallManager 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.

Cisco Unified CallManager classifies outbound faststart calls over a trunk or gateway as nonsecure. If you check the SRTP Allowed check box in Cisco Unified CallManager Administration, Cisco Unified CallManager disables the Enable Outbound FastStart check box.

Overview for SIP Trunk Encryption

Secure SIP trunks can support secure calls over TLS; be aware, though, that the trunk supports signaling encryption but does not support media encryption (SRTP). Because the trunk does not support media encryption, the shield icon may display on the phones during the call; that is, if all devices in the call support authentication or signaling encryption.

To configure signaling encryption for the trunk, choose the following options when you configure the SIP trunk security profile:

- In the Incoming Transport Type drop-down list box, choose TLS.
- In the Outgoing Transport Type drop-down list box, choose TLS.
- In the Device Security Mode drop-down list box, choose Encrypted.

After you configure the SIP trunk security profile, apply it to the trunk. If you have not already done so, configure IPSec.

Tip SIP trunks rely on IPSec configuration to ensure that security-related information does not get sent in the clear. Cisco Unified CallManager does not verify that you configured IPSec correctly. If you do not configure IPSec correctly, security-related information may get exposed.

Secure Gateway and Trunk Configuration Checklist

Use Table 13-1 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. You can obtain this document at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_11/gtsecure.htm

Table 13-1 Configuration Checklist for Securing the MGCP Gateway

Configuration Steps		Related Procedures and Topics
Step 1	Verify that you installed and configured the Cisco CTL Client; verify that the cluster security mode equals mixed mode.	Configuring the Cisco CTL Client, page 3-1
Step 2	Verify that you configured the phones for encryption.	Phone Security Overview, page 4-1
Step 3	Configure IPSec. **Tip** You may configure IPSec in the network infrastructure, or you may configure IPSec between Cisco Unified CallManager and the gateway or trunk. If you implement one method to set up IPSec, you do not need to implement the other method.	• Considerations for Configuring IPSec in the Network Infrastructure, page 13-5 • Considerations for Configuring IPSec Between Cisco Unified CallManager and the Gateway or Trunk, page 13-5
Step 4	For H.323 IOS gateways and intercluster trunks, check the SRTP Allowed check box in Cisco Unified CallManager Administration.	The SRTP Allowed check box displays in the Trunk Configuration or Gateway Configuration window in Cisco Unified CallManager Administration. For information on how to display these windows, refer to the trunk and gateway chapters in the *Cisco Unified CallManager Administration Guide*.
Step 5	For SIP trunks, configure the SIP trunk security profile and apply it to the trunk; that is, if you have not already done so.	• Overview for SIP Trunk Encryption, page 13-3 • Configuring the SIP Trunk Security Profile, page 14-2
Step 6	Perform security-related configuration tasks on the gateway.	• *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*

Considerations for Configuring IPSec in the Network Infrastructure

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 Cisco Unified CallManager and the device, review the following information before you configure IPSec:

- Cisco recommends that you provision IPSec in the infrastructure rather than in the Cisco Unified CallManager 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*, which you can obtain at the following URL:

  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns241/c649/ccmigration_09186a00801ea79c.pdf
- Review the *Cisco IOS Security Configuration Guide, Release 12.2* (or later), which you can obtain at the following URL:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080087df1.html
- 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 "Secure Gateway and Trunk Configuration Checklist" section on page 13-4.

Caution Failing to configure the IPSEC connections and verify that the connections are active may compromise privacy of the media streams.

Considerations for Configuring IPSec Between Cisco Unified CallManager and the Gateway or Trunk

For information on configuring IPSec between Cisco Unified CallManager and the gateways or trunks that are described in this chapter, refer to the *Cisco Unified Communications Operating System Administration Guide*.

Configuring the SRTP Allowed Check Box

The SRTP Allowed check box displays in the following configuration windows in Cisco Unified CallManager 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

To configure the SRTP Allowed check box for H.323 gateways and gatekeeper or non-gatekeeper controlled H.323/H.245/H.225 trunks, perform the following procedure:

Procedure

Step 1 Find the gateway or trunk, as described in the *Cisco Unified CallManager Administration Guide*.

Step 2 After you open the configuration window for the gateway/trunk, check the SRTP Allowed check box.

Step 3 Click **Save**.

Step 4 To reset the device, click **Reset**.

Step 5 Verify that you configured IPSec correctly.

Additional Information

See the "Related Topics" section on page 13-6.

Where to Find More Information

Related Topics

- Authentication, Integrity, and Authorization Overview, page 1-14
- Encryption Overview, page 1-18
- Overview for Cisco IOS MGCP Gateway Encryption, page 13-1
- Overview for H.323 Gateway and H.323/H.225/H.245 Trunk Encryption, page 13-2
- Overview for SIP Trunk Encryption, page 13-3
- Secure Gateway and Trunk Configuration Checklist, page 13-4
- Considerations for Configuring IPSec in the Network Infrastructure, page 13-5
- Considerations for Configuring IPSec Between Cisco Unified CallManager and the Gateway or Trunk, page 13-5

Related Cisco Documentation

- *Cisco Unified Communications Operating System Administration Guide*
- *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*

- *Cisco IOS Security Configuration Guide, Release 12.2* (or later)
- *Voice and Video Enabled IPSec Virtual Private Networks Solution Reference Network Design Guide*

Configuring the SIP Trunk Security Profile

This chapter contains information on the following topics:

SIP Trunk Security Profile Overview

Cisco Unified CallManager 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 Cisco Unified CallManager 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.

Configuration Tips for SIP Trunk Security Profile

Consider the following information when you configure SIP trunk security profiles in Cisco Unified CallManager 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 Cisco Unified CallManager 5.0 or later upgrade, Cisco Unified CallManager creates a profile for the SIP trunk and applies the profile to the device.

Finding a SIP Trunk Security Profile

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

Procedure

Step 1 In Cisco Unified CallManager Administration, choose **System > Security Profile > SIP Trunk Security Profile.**

The Find and List window displays.

Step 2 From the drop-down list boxes, choose your search criteria for the security profiles that you want to list and click **Find**.

Note To find all SIP trunk security profiles that are registered in the database, click **Find** without specifying any search criteria.

The window refreshes and displays the security profiles that match your search criteria.

Step 3 Click the **Name** link for the security profile that you want to view.

Tip To search for the Name or Description within the search results, check the **Search Within Results** check box, enter your search criteria as described in this procedure, and click **Find**.

Additional Information

See the "Related Topics" section on page 14-8.

Configuring the SIP Trunk Security Profile

To add, update, or copy a SIP trunk security profile, perform the following procedure:

Procedure

Step 1 In Cisco Unified CallManager Administration, choose **System > Security Profile > SIP Trunk Security Profile**.

Step 2 Perform one of the following tasks:

- To add a new profile, click the **Add New** button and continue with Step 3.
- To copy an existing security profile, locate the appropriate profile as described in "Finding a SIP Trunk Security Profile" section on page 14-2, click the **Copy** button next to the security profile that you want to copy, and continue with Step 3.
- To update an existing profile, locate the appropriate security profile as described in "Finding a SIP Trunk Security Profile" section on page 14-2 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 14-1.

Step 4 Click **Save**.

Additional Steps

After you create the security profile, apply it to the trunk, as described in the "Applying a SIP Trunk Security Profile" section on page 14-7.

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.

Additional Information

See the "Related Topics" section on page 14-8.

SIP Trunk Security Profile Configuration Settings

Table 14-1 describes the settings for the SIP Trunk Security Profile.

- For configuration tips, refer to the "Configuration Tips for SIP Trunk Security Profile" section on page 14-1.
- For related information and procedures, see the "Related Topics" section on page 14-8.

Table 14-1 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.
Description	Enter a description for the security profile.

Table 14-1 SIP Trunk Security Profile Configuration Settings (continued)

Setting	Description
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 Cisco Unified CallManager. • **Authenticated**—Cisco Unified CallManager provides integrity and authentication for the trunk. A TLS connection that uses NULL/SHA opens. • **Encrypted**—Cisco Unified CallManager provides integrity, authentication, and signaling encryption for the trunk. A TLS connection that uses AES128/SHA opens for signaling. **Note** SIP trunks support signaling encryption (not SRTP).
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 Cisco Unified CallManager 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.
Enable Digest Authentication	Check this check box to enable digest authentication. If you check this check box, Cisco Unified CallManager 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. For more information on digest authentication, see the Digest Authentication, page 1-16, and Configuring Digest Authentication for the SIP Trunk, page 15-1. **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, Cisco Unified CallManager 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.

Table 14-1 SIP Trunk Security Profile Configuration Settings (continued)

Setting	Description
X.509 Subject Name	This field applies if you configured TLS for the incoming and outgoing transport type. For device authentication, enter the subject name of the X.509 certificate for the SIP trunk device. If you have a Cisco Unified CallManager cluster or if you use SRV lookup for the TLS peer, a single trunk may resolve to multiple hosts, which results in multiple X.509 subject names for the trunk. If multiple X.509 subject names exist, 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 X.509 Subject Names my_cm1, my_cm2. SIP TLS trunk2 on port 5071 has X.509 Subject Names my_cm2, my_cm3. SIP TLS trunk3 on port 5061 can have X.509 Subject Name my_ccm4 but cannot have X.509 Subject Name my_cm1.
Incoming Port	Choose the incoming port. Enter a value that is a unique port number from 1024-65535. 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.

Table 14-1 SIP Trunk Security Profile Configuration Settings (continued)

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. Cisco Unified CallManager 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, meaning Cisco Unified CallManager 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. For information on configuring digest authentication for the trunk, see the Configuring Digest Authentication for the SIP Trunk, page 15-1. For more information about authorization, refer to Authorization, page 1-17, and Interactions, page 1-6. For more information about configuring application level authorization at the Application User Configuration window, see the *Cisco Unified CallManager Administration Guide*.
Accept Presence Subscription	If you want Cisco Unified CallManager 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 Cisco Unified CallManager 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.

Table 14-1 SIP Trunk Security Profile Configuration Settings (continued)

Setting	Description
Accept Unsolicited Notification	If you want Cisco Unified CallManager 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 Header Replacement	If you want Cisco Unified CallManager 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.

Applying a 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 CallManager 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 **Reset**.

Additional Steps

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. See "Configuring a SIP Realm" section on page 15-4.

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.

Additional Information

See the "Related Topics" section on page 14-8.

Deleting a SIP Trunk Security Profile

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

Before You Begin

Before you can delete a security profile from Cisco Unified CallManager 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 CallManager System Guide*.

Procedure

Step 1 Find the security profile by using the procedure in the "Finding a SIP Trunk Security Profile" section on page 14-2.

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 the **Delete Selected** icon or the **Delete Selected** button.

Step 3 To delete a single security profile, perform one of the following tasks:

- In the Find and List window, check the check box next to the appropriate security profile; then, click the **Delete Selected** icon or the **Delete Selected** button.
- In the Find and List window, click the **Name** link for the security profile. After the specific Security Profile Configuration window displays, click the **Delete Selected** icon or the **Delete Selected** button.

Step 4 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Additional Information

See the "Related Topics" section on page 14-8.

Where to Find More Information

Related Topics

- SIP Trunk Security Profile Overview, page 14-1
- Configuration Tips for SIP Trunk Security Profile, page 14-1
- Finding a SIP Trunk Security Profile, page 14-2
- Configuring the SIP Trunk Security Profile, page 14-2
- SIP Trunk Security Profile Configuration Settings, page 14-3
- Applying a SIP Trunk Security Profile, page 14-7

- Deleting a SIP Trunk Security Profile, page 14-8
- Authorization, page 1-17
- Interactions, page 1-6
- Digest Authentication, page 1-16

Related Cisco Documentation

Cisco Unified CallManager Administration Guide

Cisco Unified CallManager System Guide

CHAPTER 15

Configuring Digest Authentication for the SIP Trunk

When you configure digest authentication for SIP trunks, Cisco Unified CallManager challenges the identity of the SIP user agent that connects to the trunk every time that the trunk sends a SIP request to Cisco Unified CallManager. The SIP user agent, in turn, can challenge the identity of Cisco Unified CallManager. For additional information on how digest authentication works for SIP trunks, see the "Digest Authentication" section on page 1-16.

This chapter contains information on the following topics:

SIP Trunk Digest Authentication Configuration Checklist

Table 15-1 describes the tasks to configure digest authentication for SIP trunks.

Table 15-1 SIP Trunk Security Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Configure the SIP trunk security profiles; make sure that you check the **Enable Digest Authentication** check box.	• Configuring the SIP Trunk Security Profile, page 14-2 • Digest Authentication, page 1-16
Step 2	Apply a SIP trunk security profile to the trunk.	Applying a SIP Trunk Security Profile, page 14-7

Table 15-1 SIP Trunk Security Configuration Checklist (continued)

Configuration Steps		Related Procedures and Topics
Step 3	Configure the enterprise parameter, Cluster ID, if not configured. This parameter supports Cisco Unified CallManager as a UAS; that is, Cisco Unified CallManager challenges the identity of the SIP user agent.	Configuring Digest Authentication Enterprise Parameters, page 15-2
Step 4	If Cisco Unified CallManager acts as a user agent server (UAS) for the trunk, configure the digest credentials for the application user in the Application User Configuration window.	• Configuring the Digest Credentials in the Application User Configuration Window, page 15-2 • Application User Digest Credential Configuration Settings, page 15-3
Step 5	If Cisco Unified CallManager acts as user agent client (UAC), configure SIP realm. Cisco Unified CallManager acts as a user agent client when the trunk challenges the identity of Cisco Unified CallManager.	• Digest Authentication, page 1-16 • Configuring a SIP Realm, page 15-4 • SIP Realm Configuration Settings, page 15-5

Configuring Digest Authentication Enterprise Parameters

To configure the enterprise parameter, Cluster ID, for digest authentication, choose **System > Enterprise Parameters** in Cisco Unified CallManager Administration. Locate the **Cluster ID** parameter and update the value, as described in the help that supports the parameter. This parameter supports Cisco Unified CallManager as a UAS; that is, Cisco Unified CallManager challenges the identity of the SIP user agent.

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.

Configuring the Digest Credentials in the Application User Configuration Window

If Cisco Unified CallManager acts as a user agent server, that is, Cisco Unified CallManager challenges the identity of the SIP user agent, you must configure the digest credentials for the application user in the Application User Configuration window in Cisco Unified CallManager Administration. Cisco Unified CallManager uses these credentials to verify the identity of SIP UACs.

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 CallManager Administration Guide*.

Step 2 Click on the application user link.

Step 3 After the specific Application User Configuration window displays, enter the appropriate settings, as described in Table 15-3.

Step 4 Click **Save**.

Additional Information

See the "Related Topics" section on page 15-6.

Application User Digest Credential Configuration Settings

Table 15-3 describes the settings for the digest credential settings in the Application User Configuration window in Cisco Unified CallManager Administration. For related information and procedures, see the "Related Topics" section on page 15-6.

Table 15-2 Digest Authentication 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.

Finding a SIP Realm

To find a SIP Realm, perform the following procedure:

Procedure

Step 1 In Cisco Unified CallManager Administration, choose **User Management > SIP Realm**.

The Find and List window displays.

Step 2 From the drop-down list boxes, choose your search criteria for the SIP realm that you want to list and click **Find**.

Note To find all SIP realms that are registered in the database, click **Find** without specifying any search criteria.

The window refreshes and displays the SIP realms that match your search criteria.

Step 3 Click the **Realm** link for the SIP realm that you want to view.

Tip To search for the Realm or User within the search results, check the **Search Within Results** check box, enter your search criteria as described in this procedure, and click **Find**.

Additional Steps

If you have not already done so, configure the Cluster ID enterprise parameter, as described in the "Configuring Digest Authentication Enterprise Parameters" section on page 15-2.

Additional Information

See the "Related Topics" section on page 15-6.

Configuring a SIP Realm

If Cisco Unified CallManager acts as user agent client (UAC), you must configure SIP Realm for each SIP trunk user agent. Cisco Unified CallManager acts as a user agent client when the trunk peer challenges the identity of Cisco Unified CallManager.

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

Procedure

Step 1 In Cisco Unified CallManager Administration, choose **User Management > SIP Realm**.

Step 2 Perform one of the following tasks:

- To add a new SIP Realm, click the **Add New** button and continue with Step 3.
- To update an existing SIP Realm, locate the appropriate security profile as described in "Finding a SIP Realm" section on page 15-3 and continue with Step 3.

Step 3 Enter the appropriate settings as described in Table 15-3.

Step 4 Click **Save**.

Step 5 Perform the procedure for all realms that you must add or update.

Additional Steps

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

Additional Information

See the "Related Topics" section on page 15-6.

SIP Realm Configuration Settings

If Cisco Unified CallManager acts as user agent client (UAC), you must configure SIP Realm. Cisco Unified CallManager acts as a user agent client when the trunk peer challenges the identity of Cisco Unified CallManager. The realm provides the trunk-side credentials.

Table 15-3 describes the settings for the SIP Realm. For related information and procedures, see the "Related Topics" section on page 15-6.

Table 15-3 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. Characters can be alphanumeric, period, dash, underscore, and space.
User	Enter the user name that you want to associate with Cisco Unified CallManager; for example, enter the server name. The SIP trunk uses this user name when the identity of Cisco Unified CallManager gets challenged.
Password	Enter the password that you want to associate with Cisco Unified CallManager; the SIP trunk uses this password when the identity of Cisco Unified CallManager gets challenged.
Password Confirmation	To confirm that you entered the password correctly, enter the password in this field.

Deleting a SIP Realm

This section describes how to delete a SIP Realm from the Cisco Unified CallManager database.

Procedure

Step 1 Find the SIP Realm by using the procedure in the "Finding a SIP Realm" section on page 15-3.

Step 2 To delete multiple SIP Realms, check the check boxes next to the appropriate check box in the Find and List window; then, click the **Delete Selected** icon or the **Delete Selected** button.

Step 3 To delete a single SIP Realm, perform one of the following tasks:

- In the Find and List window, check the check box next to the appropriate SIP Realm; then, click the **Delete Selected** icon or the **Delete Selected** button.
- In the Find and List window, click the **Realm** link. After the specific SIP Realm Configuration window displays, click the **Delete Selected** icon or the **Delete Selected** button.

Step 4 When prompted to confirm the delete operation, click **OK** to delete or **Cancel** to cancel the delete operation.

Additional Information

See the "Related Topics" section on page 15-6

Where to Find More Information

Related Topics

- Digest Authentication, page 1-16
- SIP Trunk Digest Authentication Configuration Checklist, page 15-1
- Configuring Digest Authentication Enterprise Parameters, page 15-2
- Configuring the Digest Credentials in the Application User Configuration Window, page 15-2
- Application User Digest Credential Configuration Settings, page 15-3
- Finding a SIP Realm, page 15-3
- Configuring a SIP Realm, page 15-4
- SIP Realm Configuration Settings, page 15-5
- Deleting a SIP Realm, page 15-5

A

B

C

D

E

F

H

I

T

V