C H A P T E R 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, page 1-2
- System Requirements, page 1-4
- Features List, page 1-4
- Security Icons, page 1-5
- Interactions and Restrictions, page 1-5
- Best Practices, page 1-10
- Installation, page 1-11
- TLS and IPSec, page 1-12
- Certificate Types, page 1-12
- Authentication, Integrity, and Authorization Overview, page 1-14
- Encryption Overview, page 1-18
- Configuration Checklist Overview, page 1-20
- Where to Find More Information, page 1-24

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 Cisco Unified 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.

Cisco Unified CallManager supports integration with third-party certificate authorities (CAs) by using a PKCS#10 certificate signing request (CSR) mechanism, which is accessible at the Cisco Unified Communications Operating System Certificate Manager GUI. Customers who currently use third-party CAs should use the CSR mechanism to issue certificates for both CallManager and CAPF. Cisco has verified the PKCS#10 CSR mechanism with these CAs: Keon and Microsoft. Cisco has not verified certificate issuance with other external CAs that support PKCS#10 CSRs. SCEP interface support is not available in this release of Cisco Unified CallManager.

Be sure to run the CTL client after you upload a third-party, CA-signed certificate to the platform to update the CTL file. After running the CTL Client, restart the appropriate service(s) — CCM & TFTP when updating CCM certificate, CAPF when updating CAPF certificate, and so on. 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

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.	Activating the Cisco CTL Provider Service, page 3-3
	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.	

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