

Security

Revised: February 19, 2019

This chapter describes network access security, toll-fraud access protection, certificate management, and encryption for the Cisco Preferred Architecture (PA) for Enterprise Collaboration.

The first part of this chapter provides an architectural overview while the second part covers deployment procedures. The Architecture section discusses various aspects of security. It starts with a high level discussion of the layered security approach, unauthorized access protection, and toll-fraud protection. Then it focuses on certificate management and encryption. The next portion of this chapter is the Deployment section. It covers the procedures on how to generate and manage certificates and how to enable and provision encryption for all the components in this solution.

Note The information in this chapter assumes that the products are running software version 12.5 or later.

What's New in This Chapter

Table 7-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

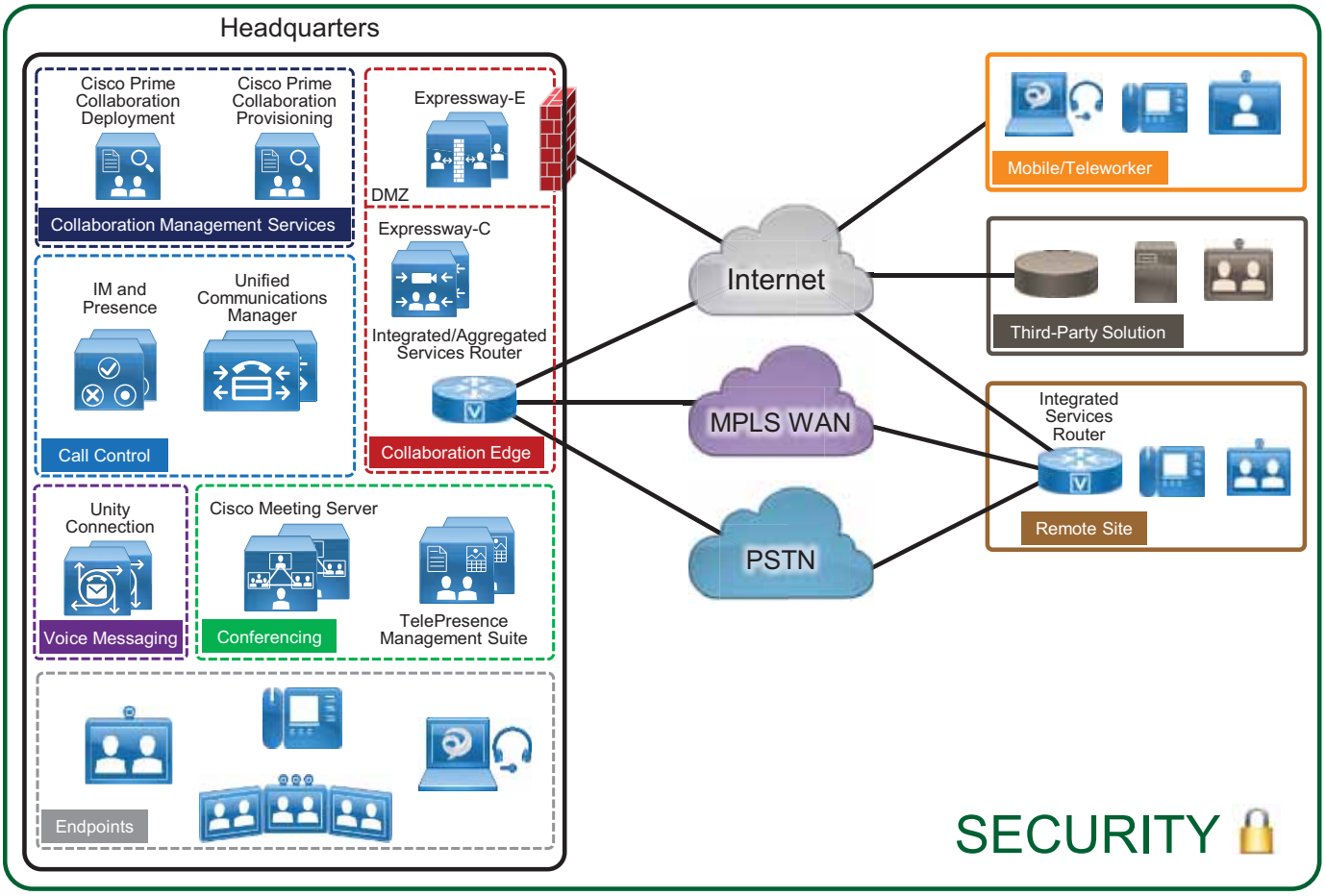
Table 7-1 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in:	Revision Date
Locally Significant Certificate (LSC) installation	Various sections of this chapter	January 23, 2019
SIP OAuth mode and removal of the requirement to install Locally Significant Certificates (LSCs) for Jabber	Various sections of this chapter	January 23, 2019
Cisco Meeting Management	Various sections of this chapter	January 23, 2019
CAPF online CA mode	CAPF Online CA Mode, page 7-39	January 23, 2019
MIC support on CE endpoints	Various sections of this chapter	January 23, 2019
Cisco Prime License Manager is no longer part of this architecture and has been removed from this document	All sections of this chapter	August 30, 2017
Initial Trust Lists (ITL) and tokenless Certificate Trust Lists (CTL)	Various sections of this chapter	August 30, 2017

Core Components

Security applies to all the components in the Cisco Collaboration solution (see Figure 7-1). It is important to implement security across the solution. In fact, it is important to implement security with a layered approach. Do not rely on a single component to provide security, but instead plan for multiple layers of defense.

Figure 7-1 Secure All Components of the Enterprise Collaboration Preferred Architecture



Key Benefits

This deployment provides the following benefits:

- Implementing a layered approach provides multiple layers of defense.
- Protecting access to your network and your systems makes it more difficult to compromise your servers, your Collaboration solution, and the rest of the organization.
- Implementing toll fraud protection mechanisms can prevent unauthorized access to your telephony system, data network, and PSTN lines that would lead to unauthorized financial charges.
- Using encryption and certificates for your various communications can protect against eavesdropping, tampering, and session replay.
- Implementing a good certificate management plan provides a good level of protection while reducing complexity.

Architecture

This section starts with an overview on the security mechanisms for Cisco Collaboration. It then discusses toll-fraud mitigation, and then focuses on certificate management and encryption.

Security in Layers

There are a wide variety of threats that can be addressed by different mechanism. As a general best practice, a layered security approach to secure your collaboration deployment should be used. Physical access to your premises as well as access to your network, servers, endpoints, and systems should be protected and secure. Communications should be encrypted, and a good certificate management system should be deployed. Securing as many components and layers as possible augments the security, and if a layer or component is compromised, your system would still be protected by other security layers and security mechanisms.

Table 7-2 provides examples of collaboration threats and countermeasures. For each threat, multiple countermeasures should be deployed.

Table 7-2 Examples of Collaboration Threats and Countermeasures

Threats	Countermeasures
Denial of Service (DoS)	Physical security; network security; firewall and intrusion prevention system (IPS); QoS
Spam and spam over Internet telephony	Firewall and advanced malware protection (AMP); Cisco Collaboration Edge security; Cisco Unified Communications Manager (Unified CM) dial-plan
Virus	Host-based firewall; IPS; anti-virus software
Toll-fraud	Cisco Unified CM calling search space (CSS) and partitions; toll-fraud prevention and access protection; Cisco Collaboration Edge security
Learning private information	Encryption with certificate management; physical security; network security

Table 7-2 Examples of Collaboration Threats and Countermeasures (continued)

Threats	Countermeasures
Man-in-the-middle attacks	Encryption with certificate management; physical security; network security
Eavesdropping	Encryption with certificate management; physical security; network security
Impersonating others	Encryption with certificate management; physical security; network security
Media tampering	Encryption with certificate management; physical security; network security
Data modification	Encryption with certificate management; physical security; network security
Session replay	Encryption with certificate management; physical security; network security

Physical Security

The first line of defense is physical security. It is important to provide physical security to your premises, network access, and very importantly to your core network infrastructure and servers. When physical security is compromised, simple attacks such as service disruption by shutting down power to your premises and/or servers can be initiated. With physical access, attackers could get access to server devices, reset passwords, and gain access to servers. Physical access also facilitates more sophisticated attacks such as man-in-the-middle attacks, which is why the second security layer, the network security, is critical.

For more information on general security practices, refer to the documentation at the following locations:

https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html

https://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html

Network Security

Network security is the next line of defense. The following section provides examples of some of the network security mechanisms. This section provides only brief coverage of network security and the Deployment section of this guide does not cover it. For more information on network security, refer to network security design guides available at

https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html

Voice and Video VLAN

Separate voice/video and data VLANs are recommended for the following reasons:

- Protection from malicious network attacks

  VLAN access control, 802.1Q, and 802.1p tagging can provide protection for voice devices from malicious internal and external network attacks such as worms, denial of service (DoS) attacks, and attempts by data devices to gain access to priority queues through packet tagging.

- Ease of management and configuration

  Separate VLANs for voice and data devices at the access layer provide ease of management and simplified QoS configuration.

The voice/video VLAN includes the hardware desk phones and video systems. The data VLAN includes end-user desktops and laptops, and software clients such as Jabber. Access lists (ACL), VLAN access lists (VACL), or firewalls can be used to limit traffic between the VLANs.

With wireless access, there are additional considerations. For details, refer to the *Real-Time Traffic over Wireless LAN Solution Reference Network Design Guide* and the *Cisco Collaboration System Solution Reference Network Design (SRND)* guide, both available at https://www.cisco.com/go/ucsrnd.

Layer 2 and Layer 3 Security

Use the standard security features available at Layer 2 and Layer 3.

Port Security

A classic attack on a switched network is a MAC content-addressable memory (CAM) flooding attack. This type of attack floods the switch with so many MAC addresses that the switch does not know which port an end station or device is attached to. When the switch does not know which port a device is attached to, it broadcasts the traffic destined for that device to the entire VLAN. In this way, the attacker is able to see all traffic that is coming to all the users in a VLAN. Either port security or dynamic port security can be used to inhibit a MAC flooding attack. A customer with no requirement to use port security as an authorization mechanism would want to use dynamic port security with the number of MAC addresses appropriate to the function attached to a particular port. For example, a port with only a workstation attached to it would want to limit the number of learned MAC addresses to one. A port with a Cisco Unified IP Phone and a workstation behind it would want to set the number of learned MAC addresses to two (one for the IP phone itself and one for the workstation behind the phone) if a workstation is going to plug into the PC port on the phone. Port security also provides a form of device-level security authorization by checking the MAC address of the endpoint.

DHCP Snooping

Dynamic Host Configuration Protocol (DHCP) snooping prevents a non-approved DHCP or rogue DHCP server from handing out IP addresses on a network by blocking all replies to a DHCP request from untrusted ports. Because most phone deployments use DHCP to provide IP addresses to the phones, you should use the DHCP snooping feature in the switches to secure DHCP messaging. DHCP snooping can also help to protect against DHCP address scope starvation attacks which are used to create a DHCP denial-of-service (DoS) attack. With DHCP snooping enabled, untrusted ports will make a comparison of the source MAC address to the DHCP payload information and fail the request if they do not match. DHCP snooping prevents any single device from capturing all the IP addresses in any given scope, but incorrect configurations of this feature can deny IP addresses to approved users.

Dynamic ARP Inspection

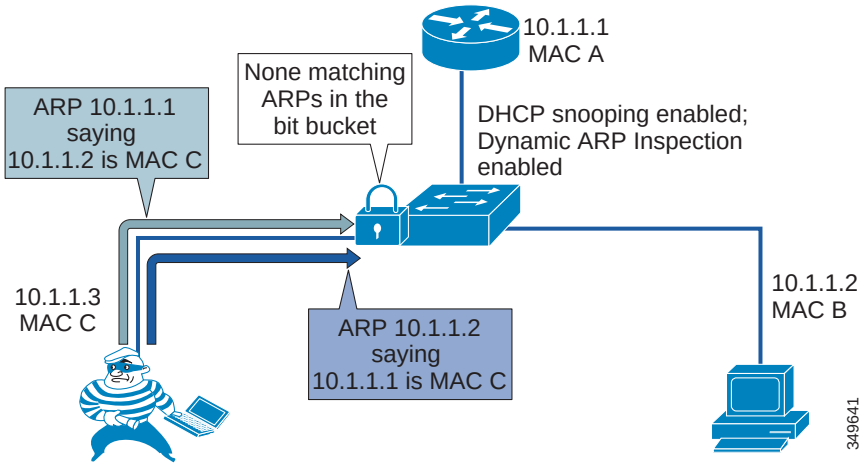
Dynamic Address Resolution Protocol (ARP) Inspection (DAI) is a feature used on the switch to prevent Gratuitous ARP attacks on the devices plugged into the switch and on the router.

Gratuitous ARP (GARP) is an unsolicited ARP reply. In its normal usage, it is sent as a MAC broadcast. All stations on a LAN segment that receive a GARP message will cache this unsolicited ARP reply, which acknowledges the sender as the owner of the IP address contained in the GARP message. Gratuitous ARP has a legitimate use for a station that needs to take over an address for another station on failure. However, Gratuitous ARP can also be exploited by malicious programs that want to illegitimately take on the identity of another station. When a malicious station redirects traffic to itself from two other stations that were talking to each other, the hacker who sent the GARP messages becomes the man in the middle.

Dynamic ARP Inspection (DAI) is used to inspect all ARP requests and replies (gratuitous or non-gratuitous) coming from untrusted (or user-facing) ports to ensure that they belong to the ARP owner. The ARP owner is the port that has a DHCP binding that matches the IP address contained in the ARP reply. ARP packets from a DAI trusted port are not inspected and are bridged to their respective VLANs.

Dynamic ARP Inspection (DAI) requires that a DHCP binding be present to legitimize ARP responses or Gratuitous ARP messages. If a host does not use DHCP to obtain its address, it must either be trusted or an ARP inspection access control list (ACL) must be created to map the host's IP and MAC address. (See Figure 7-2.) Like DHCP snooping, DAI is enabled per VLAN, with all ports defined as untrusted by default. To leverage the binding information from DHCP snooping, DAI requires that DHCP snooping be enabled on the VLAN prior to enabling DAI.

Figure 7-2 Using DHCP Snooping and DAI to Block ARP Attacks



IP Source Guard

IP Source Guard provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports.

Initially, all IP traffic on the protected port is blocked except for DHCP packets. After a client receives an IP address from the DHCP server, or after static IP source binding is configured by the administrator, all traffic with that IP source address is permitted from that client. Traffic from other hosts is denied.

This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address. IP Source Guard is a port-based feature that automatically creates an implicit port access control list (PACL).

802.1X

802.1X is an IEEE standard that permits or denies network connectivity based on the identity of the end user or device. The 802.1X authentication feature can be used to identify and validate the device credentials of a Cisco endpoint before granting it access to the network. 802.1X is a MAC-layer protocol that interacts between an end device and a RADIUS server such as the Cisco Identity Service Engine (ISE). It encapsulates the Extensible Authentication Protocol (EAP) over LAN, or EAPOL, to transport the authentication messages between the end devices and the switch. In the 802.1X authentication process, the Cisco endpoint acts as an 802.1X supplicant, initiates the request to access the network, and provides its certificate (Locally Significant Certificate recommended). The Cisco Catalyst Switch, acting as the authenticator, passes the request to the authentication server and then either allows or restricts the phone from accessing the network.

802.1X can also be used to authenticate the data devices attached to the Cisco Unified IP Phones. An EAPOL pass-through mechanism is used by the Cisco Unified IP Phones, allowing the locally attached PC to pass EAPOL messages to the 802.1X authenticator. The Cisco Catalyst Switch port must be configured in multiple-authentication mode to permit one device on the voice VLAN and multiple authenticated devices on the data VLAN.

Firewalls, IPS, and AMP

Firewalls can be used in conjunction with access control lists (ACLs) to protect the collaboration servers and gateways from devices that are not allowed to communicate with them. You can deploy the Cisco Adaptive Security Appliance (ASA) with FirePOWER services. It combines the ASA firewall functionality and the Next Generation Intrusion Prevention System (NGIPS) as well as Anti-Malware Protection (AMP).

Some UDP and TCP ports used by the Cisco Collaboration systems might have to be opened in firewalls. Refer to the following guides to determine which ports are used:

- For Cisco Unified CM and IM and Presence, refer to the latest version of the *System Configuration Guide for Cisco Unified Communications Manager*, available at https://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html.
- For Cisco Unity Connection, refer to the latest version of the *Security Guide for Cisco Unity Connection*, available at https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html.
- For Cisco Expressway, refer to the latest version of the *Cisco Expressway IP Port Usage for Firewall Traversal Deployment Guide*, available at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.
- For Cisco Jabber, refer to the latest version of the *Planning Guide for Cisco Jabber*, available at https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html.

QoS

Quality of Service (QoS) can be used to ensure collaboration traffic receives appropriate priority over other traffic in the network, and it can safeguard against network flood attacks (a type of Denial of Service attack). While QoS is not a security feature in and of itself, when properly implemented it does ensure that packets with the appropriate QoS levels are given priority. This can prove effective against

some packet flood attacks that attempt to bombard the network with packets to overwhelm interface buffers. With QoS those buffers are protected when the unmarked packets are dropped and the properly marked packets are allowed.

Refer to the Bandwidth Management chapter for more information on Collaboration QoS policies.

Preventing Unauthorized Access

Most of the Cisco Collaboration products have a hardened platform. For example, the platforms used by Cisco Unified CM, IM and Presence Service, and Unity Connection are locked down; the root account is disabled; third-party software installation is not allowed; a host-based intrusion protection (SELinux) and host-based firewall (iptables) are installed and enabled by default; a complex password policy is applied to administrative accounts; and secure management interfaces (HTTPS, SSH, SFTP) are enforced. Further – with the ability to assign users to access control groups and therefore to specific roles – administrators, end users, and application users can be given only the permissions they need. All installation packages are signed and include both the OS and application. System audit logging is available, which is critical for determining what might have happened when issues arise.

Servers deployed at the edge should be well secured because they are more exposed to the Internet. On the Cisco IOS gateway or Cisco Unified Border Element, there are many security features available, such as access control lists (ACLs), IP trust list, call threshold, call spike protection, bandwidth-based call admission control (CAC), media policing, NBAR policing, and voice policies. On Cisco Expressway, Call Processing Language (CPL) rules, host-based firewall (with dynamic system rules, non-configurable application rules, and user-configurable rules), and automated intrusion protection can be configured to protect the system.

Even though securing endpoints might not seem as critical as securing servers, endpoints should also be secured. Firstly, it is typically easier to access endpoints because they can be accessed by end users and are not locked down in a data center. Secondly, compromising endpoints can also be damaging. Critical information about the endpoint and the system it is registered to can be discovered on the phone screen and on the phone's web interface. Logs can be downloaded. Some endpoints such as Cisco TelePresence endpoints provide the endpoint administrator user many advanced capabilities, including call control of the endpoint and even capturing packets. On those endpoints, do not leave the default empty password but instead configure strong passwords. In general, when the settings Web Access, Web Admin, Console Access, Telnet Access, and SSH Access are available on an endpoint, we recommend disabling them. Those features should be enabled only when needed; for example, when troubleshooting an endpoint. An access control list should be configured to limit access to these interfaces to a management station or stations accessible by the administrator. If you decide to enable Web Access on an endpoint, allow only HTTPS (and not HTTP).

The Settings Access parameter on the Unified CM administration phone pages allows users to access the device settings when they press the Settings button. We recommend disabling this parameter or setting it to Restricted when available (this disables the access to administrative tasks). If you are performing an operation where endpoints could possibly loose the trust relationship with Unified CM (for example, when migrating endpoints from one Unified CM cluster to another Unified CM cluster and not distributing one ITLRecovery certificate and private key across all Unified CM clusters), you may temporarily enable Setting Access. You could also enable it temporarily for Unified CM upgrades as a precaution, even though Unified CM certificates should not be modified during upgrades. In case endpoints lose the trust with Unified CM, temporarily enabling Setting Access would allow the users to recover trust by going to the menu on their phone and resetting the security settings, which deletes the Initial Trust List (ITL) or Certificate Trust List (CTL). Alternatively, if trust is lost, it could also be recovered by using the ITL recovery key (refer to the CTL and ITL section for more information).

If not already enforced by default, ensure that complex password and PIN policies (for example, number of allowed failed logins, failed login account lockout duration, minimum credential length) are configured for administrators and users across all Cisco Collaboration products.

Toll Fraud Mitigation

Cisco Unified CM

On Cisco Unified CM, several mechanisms can be used to prevent toll fraud. Partitions and calling search spaces (CSS) provide segmentation and access control to the directory numbers, route patterns, directory URIs, and SIP route patterns that can be called or the device or line that is placing the call. As a best practice, apply the most restrictive class of service possible based on partitions and calling search spaces. For example, for SIP trunks connecting to PSTN gateways and Expressways, create an inbound calling search space that does not allow access to any of the PSTN gateway partitions. To prevent all offnet-to-offnet transfers, classify the SIP trunks to PSTN gateways as **Offnet** with the **Call Classification** enterprise parameter and set the **Block OffNet to OffNet Transfer** CallManager service parameter to **True**. Other mechanisms can also be used, such as time-of-day routing, forced authentication code (FAC), and using the **Drop Ad hoc Conferences** CallManager service parameter (set to **When No OnNet Parties Remain in the Conference**). If auto-registration is enabled, create a device pool with a restricted calling search space. We also recommend proactively monitoring system call detail records (CDRs).

Cisco Unity Connection

Unauthorized users could use the transfer feature in Cisco Unity Connection to place unauthorized calls. There are two main ways to prevent toll fraud with Unity Connection:

- On Unity Connection — Restriction tables control the phone numbers that can be used for transferring calls, for message notification, and for other Unity Connection functions. Each class of service has several restriction tables associated with it, and you can add more as needed. Refer to the Voice Messaging chapter for more details and for an example.
- On Unified CM — For the calling search space and rerouting calling search space, include only the required partitions. Refer to Table 2-21, Class of Service for Voicemail.

For more details, refer to the latest version of the *Security Guide for Cisco Unity Connection*, available at

https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html

Also refer to *Troubleshoot Toll Fraud via Unity Connection*, available at

https://www.cisco.com/c/en/us/support/docs/unified-communications/unity-connection/119337-technote-cuc-00.html

Cisco Expressway

With Expressway business-to-business deployments, use Call Processing Language (CPL) rules to allow or reject calls from the Default Zone. For example, if you want to reject any business-to-business calls with 9 as a prefix (to avoid unauthorized calls to the PSTN), you can create a CPL rule with the settings in Table 7-3.

Table 7-3 CPL Settings for Business-to-Business Calls

Source Type	Zone
Originating zone	DefaultZone
Destination pattern	9.*
Action	Reject

Cisco IOS Gateway and Cisco Unified Border Element

The telephony denial-of-service (TDoS) attack mitigation feature prevents Cisco IOS Gateways and Cisco Unified Border Element from responding to Session Initiation Protocol (SIP) requests arriving from untrusted IP addresses, which helps prevent toll fraud and leads to an improvement in performance. The SIP stack authenticates the source IP address of an incoming SIP request and blocks the response if the source IP address does not match any IP address in the trusted IP address list. The IP addresses configured in the dial-peer session target or in the voice class server-group are automatically part of the trusted IP address list. Additional trusted IP addresses can be added with the command **ip address trusted list**.

This TDoS feature is configured with the command:

```
voice service voip
  ip address trusted authenticate
```

If Cisco Unified Border Element is not deployed as a registrar server, disable the registrar service to avoid consuming unnecessary resources.

Certificate Management

Certificates are critical in a Cisco Collaboration deployment. They allow individuals, computers, and other services on the network to be authenticated and are required when establishing secure connections. Implementing good certificate management provides a good level of protection while reducing complexity.

This sections starts with a brief overview of the public key infrastructure (PKI). Then general guidance is provided. Finally, architecture details for the various Cisco Collaboration products are provided.

Brief PKI Overview

The public key infrastructure (PKI) provides a mechanism to secure communications and validate identities of communicating parties. Communications are made secure through encryption, and identities are validated through the use of public/private key pairs and digital identity certificates.

Public/Private Key Pair

A public and private key pair comprises two uniquely related cryptographic keys mathematically related. Whatever is encrypted with a public key may be decrypted only by its corresponding private key (which must be kept secret), and vice versa.

Certificates

A digital certificate is an electronic credential that is used to certify the identity of individuals, computers, and other services on a network. It is a wrapper around the public key. It provides information about the owner of the public key. It is used, for example, in a TLS handshake to authenticate the other party or used to digitally sign a file. Certificates deployed with Cisco Collaboration products are based on the X.509 standards. The certificates include the following information, among others:

- Public Key
- Common Name (CN)
- Organization Name (O)
- Issuer Name
- Validity period (Not before, not after)
- Extensions (optional) — For example, Subject Alternate Name (SAN)

A certificate can be self-signed or signed by a certificate authority (CA).

Certificate Validation During TLS Handshake

When a client initiates a TLS connection to a server, the server sends its certificate during the TLS handshake so that the client can authenticate the server. This happens, for example, when an administrator or end-user connects to the Unified CM pages or when the Jabber client starts and connects to the Unified CM UDS server, IM and Presence server, and Unity Connection server.

In some cases, the server also authenticates the client and requests the client to send its certificate. This is mutual authentication (mutual TLS, or MTLS) and it is used, for example, between Unified CM and Cisco endpoints in encrypted mode (configured with media and signaling encryption), with SIP trunks connecting two Unified CM clusters, or with SIP trunks connecting Unified CM to Unity Connection, a Cisco IOS Gateway, or Expressway (if TLS verify is configured on Expressway).

When a certificate is received, the verification consists of checking the following items:

- Identity — The subject or identity for which the certificate is issued must match the identity that the initiator of the session intended to reach. The hostname (FQDN) is checked against the common name (CN) or Subject Alternate Name (SAN) extension.
- Validity period — The current time and date must be within the certificate's validity range.
- Revocation status of the certificate
- Trust — The certificate must be trusted. A certificate is considered trusted if the signing (issuing) party is trusted. Trust with signing parties typically is established by importing the certificate of the signing party into a store of trusted certificates (trust store). Refer to the section on CA-Signed Certificates Instead of Self-Signed Certificates for more details.

General Guidance on Certificates

Some servers such as Cisco Unified CM and IM and Presence Service can have different certificates for the various system services. Some servers such as Cisco Expressway have only one certificate for the service they provide. Table 7-4 lists the server certificates for this Preferred Architecture. As discussed in the next section, ECDSA certificates are not covered in this document.

Table 7-4 Server Certificates in the Cisco Collaboration Preferred Architecture

Service	Certificate	Description
Cisco Unified CM	tomcat	Used for secure web connections. Also used for services such as LDAP, ILS and LBM.
Cisco Unified CM	CallManager	Used for secure signaling by CallManager service and for TFTP configuration files signature.
Cisco Unified CM	CAPF	Required by endpoints when connecting to the Certificate Authority Proxy Function (CAPF) service.
Cisco Unified CM	TVS	Required when connecting to the Trust Verification Service (TVS).
Cisco Unified CM	ITLRecovery	Used for the ITL and tokenless CTL files signature.
Cisco Unified CM	ipsec	For IPsec connections. IPsec can be enabled, but it is not covered in this document. IPsec certificates are also used with Disaster Recovery System.
Cisco Unified CM	authz	Used for OAuth.
IM and Presence Service	tomcat	For SIP clients (Unified CM), Web services, SOAP, LDAP.
IM and Presence Service	cup	For SIP Proxy, Presence Engine, SIP federation.
IM and Presence Service	cup-xmpp	For secure XMPP (IM)
IM and Presence Service	cup-xmpp-s2s	For secure XMPP federation
IM and Presence Service	ipsec	For IPsec
Cisco Unity Connection	tomcat	Unity Connection web services certificate. Used for media and signaling encryption to the voice mail ports.
Cisco Unity Connection	ipsec	For IPsec
Cisco Expressway-C	Server	For all secure connections from/to Expressway-C.
Cisco Expressway-E	Server	For all secure connections from/to Expressway-E.
Cisco Meeting Server	Database client	For Cisco Meeting Servers with the Call Bridge service without a database, to connect securely to Cisco Meeting Server nodes with a database
Cisco Meeting Server	Shared certificate used for Web Admin, Call Bridge, XMPP, Web Bridge, and database server	For simplicity, except for the database client, we use the same certificate for all Cisco Meeting Server nodes and services.
Cisco Meeting Management	Server	For web connections and call bridge connections
Survivable Remote Site Telephony (SRST), Cisco IOS Gateway, Cisco Unified Border Element	Cisco IOS certificate	With SRST, the SRST certificate is included in the configuration file of each endpoint.

Table 7-4 Server Certificates in the Cisco Collaboration Preferred Architecture (continued)

Service	Certificate	Description
Cisco Prime Collaboration Deployment	tomcat	For Web services
Cisco Prime Collaboration Provisioning	Provisioning	For Provisioning Web Access

There are also other ECDSA certificates, but as discussed in the section on RSA and ECDSA, they are not used for the deployment guidance in this chapter, so they are not listed in Table 7-4.

In general, the Cisco Collaboration servers are installed by default with a self-signed certificate. The exception is Cisco Meeting Server, which has no certificate installed by default.

Cisco Unified CM self-signed certificates are valid for 5 years, except the ITLRecovery certificate, which is valid for 20 years. The validity for this certificate is longer because it acts as a system-wide trust anchor.

RSA and ECDSA

Certificates for the Cisco Collaboration products are typically based on RSA (Rivest, Shamir, and Adelman) for public/private keys and digital signatures. Some products also support Elliptical Curve Digital Signature Algorithm (ECDSA) certificates, but for simplicity the general recommendation is to use RSA-based certificates, and that is what is covered in this document.

For endpoints, we recommend using RSA-based Locally Significant Certificates (LSCs). For Unified CM SIP TLS, ECDSA and RSA are always enabled, but by default RSA is preferred over ECDSA, so RSA certificates are negotiated. This is the recommended configuration. For HTTPS, with Unified CM, IM and Presence Service, and Unity Connection, ECDSA is not enabled by default. It may be enabled by changing the HTTPS Ciphers enterprise parameter, but the recommendation is to use the default settings (ECDSA disabled).

Note Encryption cipher suites based on ECDHE do not require certificates based on ECDSA; they can be negotiated with certificates based on RSA.

CA-Signed Certificates Instead of Self-Signed Certificates

By default, when installing servers for the Cisco products discussed here, self-signed certificates are installed (except with Cisco Meeting Server, where no certificate is installed by default). To establish trust with a service based on a self-signed certificate, the server self-signed certificates must be imported into the trusted certificates store (or trust store) of all entities requiring secure connections to the service (clients). If not, with servers initiating the connections (for example, with Unified CM SIP trunks), the connection will fail. With Jabber and web browsers, users are prompted with warning messages and can accept the certificates, which then are in general added to the trusted certificate store. This should be avoided because being prompted multiple times to accept a number of certificates during startup of the client is not a good user experience. Even more important is the fact that most users will not actually verify whether the presented certificate is correct by checking the certificate's fingerprint, and instead will just accept any certificate. This breaks the security concept of certificate-based authentication for secure session establishment.

Importing self-signed certificates can be handled if the set of communicating parties is small, but it becomes less practical for large numbers of communication peers. This is the main reason why we recommend replacing most default self-signed certificates with certificates that are signed by a CA. It

simplifies certificate management. With CA-signed certificates, it is not necessary to import each server certificate in the client trust store; but instead, importing the root CA certificate to the client trust store is sufficient. On the server side, in general, the root CA certificate must also be imported to the server trust store; and if using intermediate CA(s), all the certificates in the certificate chain must also be imported to the server trust store. Using CA-signed certificates also allows for issuing new service certificates without having to update all client or server trusted certificate stores, as long as the signing CA's root certificate has already been added to the trusted certificate stores of all clients. CA-signed certificate is also a requirement when using multi-server certificates.

As an example of the benefit of using a CA-signed certificate: If self-signed certificates are used with Jabber clients, the Unified CM Tomcat certificate (for UDS and for downloading TFTP configuration file), the IM and Presence tomcat and cup-xmpp certificates (for login and secure chat), and the Unity Connection Tomcat certificate (for visual voice mail) would have to be imported into the trust store of each client running Jabber. With CA-signed certificate, only the signing CA's root certificate needs to be imported.

In general, using a CA-signed certificate for the Tomcat certificates is the most beneficial because they are widely used and are user-facing certificates. Using CA-signed certificates for the CallManager certificates is also beneficial because it allows the use of multi-server certificates (see the section on Multi-Server Certificates for more details) and avoids importing the CallManager certificates for all of the entities that connect to Unified CM subscribers via a SIP trunk.

However, it is not necessary to sign all of the certificates with an enterprise CA. Some certificates are used only for internal operations and are provided to the entity that needs them without any user intervention. For example, the Trust Verification Service (TVS) certificate is included in the Initial Trust List (ITL) file, and that ITL file is automatically downloaded by the endpoints when they boot, restart, or reset. Similarly, the ITLRecovery certificate is included in the Certificate Trust List (CTL) and Initial Trust List (ITL). Thus there are no benefits to signing those certificates with an external CA. There are also no real benefits to signing the CAPF certificate by an external CA. It does not provide support for Certificate Authority Proxy Function (CAPF) certificate or endpoint Locally Significant Certificate (LSC) revocation. Also, when configuring phone VPN or 802.1x, importing the root CA certificate into the ASA trust store is not sufficient. The CAPF certificate would still have to be imported because the endpoints do not send the certificate chain (and therefore do not send the CAPF certificate) during a TLS handshake.

Table 7-5 list the certificates that Cisco recommends to be signed by a CA.

Table 7-5 Certificates to be Signed by a CA

Product	Certificate	Notes
Cisco Unified CM and IM and Presence Service	tomcat	Used for various applications, including administrators and users accessing the web interface and Jabber accessing UDS and logging in.
Cisco Unified CM	CallManager	Used for various applications, including SIP trunks.
Cisco Unified CM	ipsec	Only if IPsec is used
IM and Presence Service	xmpp	
IM and Presence Service	xmpp-s2s	
Cisco Unity Connection	tomcat	Used for various applications, including administrators and users accessing the web interface and Jabber accessing visual voice mail.
Cisco Expressway-C	Server	
Cisco Expressway-E	Server	Use a public CA.

Table 7-5 Certificates to be Signed by a CA (continued)

Product	Certificate	Notes
Survivable Remote Site Telephony (SRST) and Cisco IOS Gateway	SRST and Cisco IOS Gateway	
Cisco Unified Border Element	Cisco IOS	In general, use an enterprise CA. If the SIP service provider supports encryption, use a public CA.
Cisco Meeting Server	Server	Shared certificate for all Cisco Meeting Server services
Cisco Meeting Server	Database client	
Cisco Meeting Management	Server	
Cisco TelePresence Management Suite (TMS)	Server	
Cisco Prime Collaboration Deployment	tomcat	
Cisco Prime Collaboration Provisioning	Provisioning	

Multi-Server Certificates

To further simplify certificate management, a multi-server certificate can be used. Instead of having a certificate for each node, a single CA-signed certificate can be used across all the nodes in a cluster. A single corresponding private key is also used across all the nodes and is automatically propagated across the nodes. We recommend using multi-server certificates wherever available, as described in Table 7-6.

Table 7-6 Multi-Server Certificate Support

Product	Certificate	Notes
Unified CM and IM and Presence Service	tomcat	Single Tomcat certificate across all the Unified CM and IM and Presence nodes in a cluster. Generate the Certificate Signing Request (CSR) and upload the CA-issued certificate on the Unified CM publisher node.
Unified CM	CallManager	
IM and Presence Service	xmpp	
IM and Presence Service	xmpp-s2s	
Unity Connection	tomcat	

With Cisco Meeting Server, you can also issue a single certificate and single private key shared across all the nodes in the Cisco Meeting Server cluster (in addition to a separate certificate for the database client). However, the private key is not propagated automatically; it has to be imported manually to each Cisco Meeting Server node.

Note Wildcard certificates are not supported for the Cisco Collaboration products discussed in this chapter, except for Cisco Meeting Server. For Cisco Meeting Server, we recommend issuing a standard (non-wildcard) certificate and using that certificate for all Cisco Meeting Server services and nodes. (A second certificate for the database client would have to be generated.)

Public versus Private CA

Besides the requirement to use a public CA for the Expressway-E certificates, you could use either a public or enterprise CA (private or internal CA) to sign the various certificates of the Cisco Collaboration products in this document. The benefits of using a public CA include the fact that some clients and servers by default already trust major public CAs, and it is not required to establish trust between those devices and the public CA (import CA certificate in the client trust store). With a public CA, your IT organization also does not have to install and maintain internal CA servers. But the major drawbacks are the cost to issue certificates and restrictions that some public CAs might have.

What we recommend and describe in this document is the use of an enterprise CA for the certificates that we recommend to be CA-signed, except for the Expressway-E certificates which must be signed by a public CA and except for the Cisco Unified Border Element certificate if the SIP service provider supports encryption.

Cisco Unified CM and IM and Presence

This section describes certificate management for Cisco Unified CM and IM and Presence.

Unified CM Mixed Mode

As discussed later in the section on Unified CM Mixed Mode for Media and Signaling Encryption, Unified CM mixed mode enables media and signaling encryption on the phones and TelePresence endpoints. The tokenless approach to enable mixed mode is recommended and covered in this document.

CTL and ITL

The Certificate Trust List (CTL) and Initial Trust List (ITL) are files that include Unified CM certificates. Those files are downloaded by Cisco endpoints. These trust lists allow the endpoints to get the minimum set of Unified CM certificates to build the trust to Unified CM services. The ITL files are always present in a Unified CM cluster, whether the Unified CM cluster is in non-secure mode or mixed mode. The CTL file is present and relevant only when Unified CM is in mixed mode.

The CTL and ITL files are signed by using the System Administrator Security Token (SAST, see Table 7-7) and contain a list of records. Each record contains a certificate, a certificate role or function, and pre-extracted certificate fields for easy look-up by the endpoint. Table 7-7 lists the certificate roles.

Table 7-7 Certificate Roles in CTL and ITL Files

Certificate Role	Certificates	Description
TFTP	CallManager	To authenticate Unified CM TFTP server. For example, used to verify TFTP configuration file signatures. Records with this certificate role are included in the ITL file when Unified CM is not in mixed mode.
CCM+TFTP	CallManager	To authenticate CallManager Service with encrypted signaling; and to authenticate the Unified CM TFTP server when verifying TFTP configuration file signatures. Records with this certificate role are included in the ITL and CTL files when Unified CM is in mixed mode.
System Administrator Security Token (SAST)	With tokenless CTL: ITLRecovery and CallManager certificate on publisher With ITL: ITLRecovery and CallManager certificates on TFTP servers	To authenticate the SAST, which is the entity that signs the CTL, ITL, or TFTP configuration files. This type of record is included in the ITL and CTL files. The ITL and tokenless CTL files are signed by using the ITL recovery key. The TFTP configuration files are signed by using the TFTP servers' CallManager private keys.
Certificate Authority Proxy Function (CAPF)	CAPF	To authenticate CAPF service during secure communications with CAPF. A record with this certificate role is included in the ITL and CTL files if the CAPF service is activated on the Unified CM publisher.
Trust Verification Service (TVS)	TVS	To authenticate TVS service when connecting to TVS. Present in the ITL file only.

The ITL is signed by using the ITLRecovery private key. Each Unified CM node running the TFTP service has its own ITL file that it provides to the endpoints.

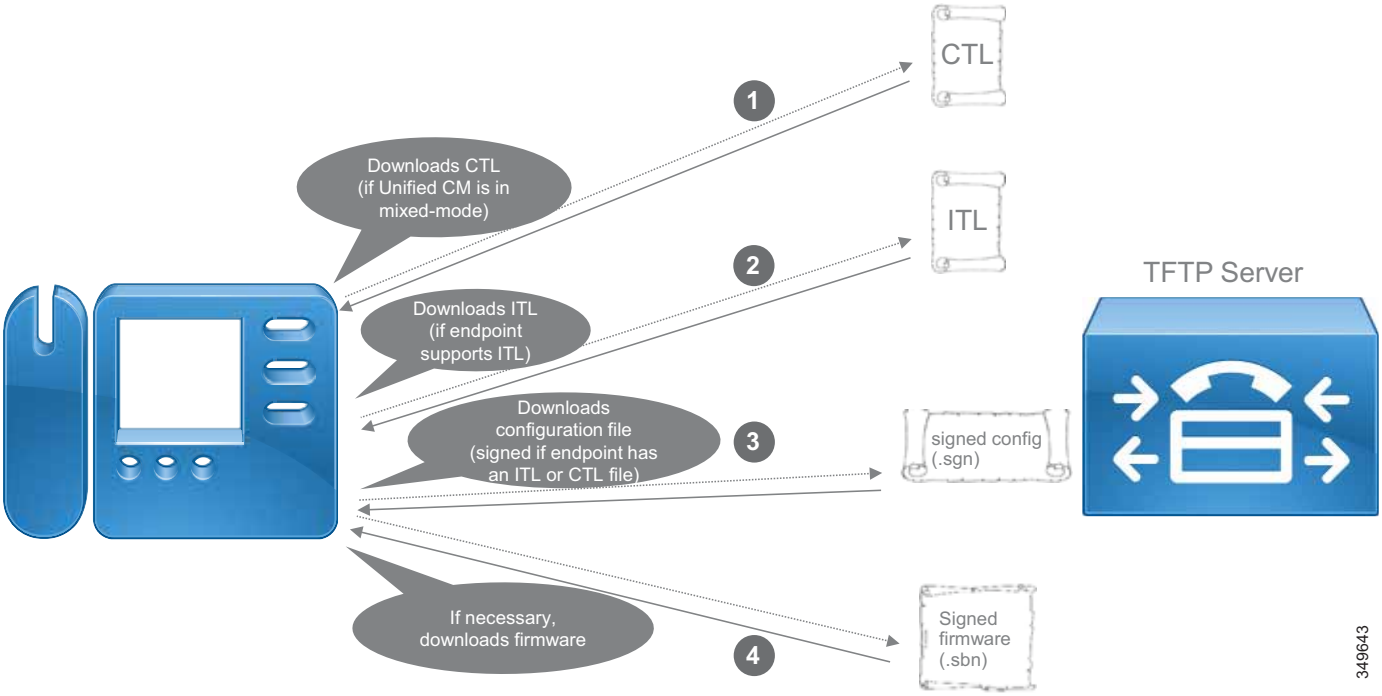
The CTL file is signed by using the private key of a System Administrator Security Token (SAST). With tokenless CTL, the SAST is the ITLRecovery private key. There is only one CTL file shared across the entire Unified CM cluster.

When endpoints boot or reset, before downloading their configuration file, they download the Certificate Trust List (CTL) from their TFTP server if Unified CM is in mixed mode. Then they download their TFTP server's Initial Trust List (ITL), if ITL is supported by the endpoint. Jabber does not support ITL, but the rest of the endpoints in this Preferred Architecture do support it. If the endpoint is newly deployed and it is the first time the endpoint connects to Unified CM, it does not have an existing CTL or ITL file and therefore does not have a list of certificates it can use to validate the CTL or ITL signature. In that case, the endpoint simply accepts the CTL/ITL file in a one-time leap of faith and stores the certificates that are part of those files. Once the endpoint has a trusted list of certificates, it can use them to validate the signatures of subsequent CTL and ITL files.

If an endpoint supports ITL or if Unified CM is in mixed mode (in which case a CTL file is downloaded by the endpoints), the endpoint possesses the ITLRecovery certificate from the ITL/CTL file(s) and therefore requests a configuration file that is signed by using the CallManager private key on the Unified CM TFTP server. If not (for example, as is the case with Jabber and when Unified CM is not in mixed mode), it requests a non-signed configuration file. After downloading its configuration file, the

endpoint then verifies that it has the correct firmware. If not, it downloads the relevant firmware and validates the signature of the firmware to ensure it was not tampered with. Figure 7-3 summarizes the files downloaded by the endpoints when they start up.

Figure 7-3 Files Downloaded by Endpoints During Startup



Endpoint Certificates

Endpoint certificates are used mainly for endpoints in secure mode; that is, when performing media and signaling encryption on the endpoints. They may also be used for encrypted TFTP configuration files, 802.1x authentication, phone VPN, or when accessing the endpoint's web server via HTTPS.

There are two types of certificates on Cisco endpoints:

- Manufacturing Installed Certificate (MIC)
- Locally Significant Certificate (LSC)

MICs are pre-installed on the endpoints during the manufacturing process and are signed by Cisco Manufacturing CA. They are valid for 10 years and there is no certificate revocation support. An MIC could be used for media and signaling encryption, but as explained later, we recommend generating an LSC instead. The Cisco IP Phone 7800 Series and 8800 Series (including the Cisco Unified IP Conference Phone 8831), CE-based TelePresence endpoints (Cisco MX, SX, Webex DX, and Webex Room Series), and the Cisco TelePresence IX5000 Series endpoints all have MICs. Jabber does not have a MIC.

LSCs are certificates that you install in your own deployment. They can be signed by the Certificate Authority Proxy Function (CAPF) service running on the Unified CM publisher node or they can be signed by an external CA. All Cisco endpoints in this Preferred Architecture support LSCs. LSCs are valid for up to 5 years, and the validity of the LSC can be tracked easily from the Unified CM Administration page or by receiving email notification as the expiration date approaches. With all

endpoints listed in this guide, LSCs are based on SHA2 and can be based on a key length of 2048 bits or even up to 4096 bits with Jabber and the Cisco IP Phone 7800 Series and 8800 Series endpoints. Once a LSC is installed, the MIC is not used any longer.

The goal of an MIC is to prove that the phone is a genuine Cisco phone and has been signed by Cisco Manufacturing CA. One of the benefits of using an MIC is to prevent a non-legitimate client spoofing a legitimate MAC address that is configured on your Unified CM cluster. However, the MIC does not prove the endpoint is part of your own Unified CM cluster. So do not use authentication based on the MIC for 802.1x or VPN; otherwise, any Cisco endpoint, even the ones that are not part of your organization, would be able to authenticate. The general recommendation is to use the MIC during the first CAPF enrollment to generate the first LSC on the endpoint. Once the endpoint has an LSC, then the recommendation is always to use the LSC rather than the MIC for authentication when renewing the LSCs. For endpoints that do not have or expose an MIC (for example, Jabber), CAPF enrollment authentication can be based on an authentication string or null string. Authentication based on an authentication string is more secure but requires the user to enter a string manually on the endpoint. If this is not practical, authentication based on a null string can be chosen, but this effectively bypasses any endpoint authentication during the first CAPF enrollment. Once Jabber has an LSC, as with the rest of the endpoints, authentication based on the LSC is recommended for any LSC renewals.

There are three ways to issue LSCs on the phones:

- The first method is to have the CAPF service in Cisco Unified CM sign the LSCs. This is the easiest method.
- The second method is to use an online external CA (Microsoft CA) that issues LSCs to phones through the CAPF service when initiating the CAPF enrollment. The main benefit of this method is that the LSCs are signed by your own CA.
- The third method is similar to the second method. The LSCs are issued by an external CA, but in an off-line manner where the endpoint Certificate Signing Request (CSR) files have to be exported manually from Unified CM, signed by the external CA, and then imported back into Unified CM. This method is not covered in this Preferred Architecture because of those manual steps.



Note With endpoints using a wireless connection and with Jabber endpoints, the LSC issued by CAPF is used only with Unified CM and cannot be extended to 802.1X or EAP.

Considerations with Jabber

Jabber does not need to have a certificate installed in order to perform encrypted media and signaling. As discussed in the section on Cisco Expressway, when Jabber connects via mobile and remote access (MRA), as with any other endpoints, endpoint certificates do not need to be installed. When Jabber is inside the enterprise network, an LSC installation is not required in this Preferred Architecture because OAuth and the SIP OAuth mode are enabled in that case.

Survivable Remote Site Telephony (SRST)

Secure SRST is supported. When the Unified CM servers become unreachable, endpoints register to the local SRST router, and endpoints configured in encrypted mode in Unified CM still have their media and signaling encrypted when registering to the SRST router.

At a high level, this is how secure SRST is provisioned:

1. First, generate a certificate for the SRST router. As with most certificates, using a CA-signed certificate simplifies certificate management.
2. When Unified CM is configured with the **Is SRST Secure** setting enabled (check-box selected), Unified CM requests the SRST certificate from the credential server running on the SRST router and inserts the SRST certificate in the configuration file of the endpoints that are configured with SRST.
3. Manually import into the SRST router the trust certificates corresponding to the entity that signed the endpoint LSCs. If you used CAPF to issue the LSCs, this is the CAPF certificate. If you use an external CA to issue the LSCs, this the CA certificate (or trust chain certificates).
4. When the WAN goes down and/or the Unified CM servers become unreachable, the endpoints communicate securely with SRST. The endpoints authenticate SRST with the SRST certificate in their TFTP configuration file, and SRST authenticates the endpoints with the certificate corresponding to the entity that issued the LSCs (CAPF or external CA certificate) that you imported in the previous step.

Cisco Unity Connection

This document covers Cisco Unity Connection media and signaling encryption using Next Generation Encryption (NGE). With this configuration, Unity Connection Tomcat certificates are used instead of the Unity Connection Root and SIP certificates. A SIP trunk is configured between Unified CM and Unity Connection. This SIP trunk is secure, and Unified CM and Unity Connection are mutually authenticated. Unified CM is authenticated with its CallManager certificate while Unity Connection is authenticated with its Tomcat certificate. As mentioned earlier, the recommendation is to sign those certificates with an enterprise CA so that no certificate exchange between Unified CM and Unity Connection is required. The root CA certificate just needs to be imported to the Unified CM CallManager trust store and to the Unity Connection Tomcat trust store. Note that Unity Connection also automatically downloads the Unified CM CallManager certificates from the Unified CM TFTP servers to its Tomcat trust store.

Cisco Expressway

New installations of Cisco Expressway software ship with a temporary trusted CA and a server certificate issued by that temporary CA. We recommend replacing the server certificate with a CA-signed certificate and installing root CA certificates or certificate chains for the authorities that you trust.

Expressway-C certificates can be signed by either an enterprise CA or a public CA, and as mentioned earlier, this document assumes an enterprise CA is used. As for Expressway-E, the requirement is to sign the server certificate with a public CA. There are two reasons for this requirement:

- Hardware endpoints capable of mobile and remote access (MRA) have a list of over 100 public root CA certificates that they trust and that are included in the endpoint firmware. There is no mechanism for adding additional root CA certificates, and thus the Expressway-E certificate must be signed by one of those public CAs. The list of supported public CAs is available on https://www.cisco.com in

the endpoint documentation; for example, https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html.

- Cisco Expressway-E is an Internet-facing component that communicates with endpoints, other organizations, and even the Cisco Collaboration Cloud. For this reason the public key infrastructure (PKI) underlying public CA trust is required to provide maximum security and trust with minimal effort.

CAPF enrollment is not supported while endpoints are connected to the enterprise over mobile and remote access (MRA). That means LSCs cannot be installed when endpoints are connecting over MRA. But it does not prevent an endpoint from utilizing end-to-end encryption (encryption for all call legs), even if it does not have an MIC. Indeed, MICs and LSCs are not needed nor used when connecting over MRA.

Note If an endpoint is configured in encrypted mode (with a phone security profile configured with the **Device Security Mode** set to **Encrypted**) and does not have an MIC or LSC, it is still able to connect successfully over MRA. However, if or when the endpoint connects directly to the enterprise (on-premises), it must have a certificate, otherwise it will not register. This does not apply to Jabber because it uses the OAuth token.

Since CAPF enrollment is not supported with MRA, there are also considerations with TFTP configuration file encryption for MRA endpoints. Refer to the section on TFTP Configuration File Encryption for more details.

The Collaboration Edge chapter also has some security considerations for Cisco Expressway. Refer that chapter for more details.

Cisco Meeting Server

By default, Cisco Meeting Server does not have any certificates. Cisco Meeting Server supports multiple options for the certificates, but the recommendation in this document is to issue a CA-signed certificate for the database client and another CA-signed certificate for the rest of the services, and then copy those certificates and corresponding private keys across the nodes in the Cisco Meeting Server cluster.

Cisco Meeting Management

Cisco Meeting Management uses a certificate to identify itself to browsers and to call bridges. During setup, Meeting Management generates a self-signed certificate. It should be replaced by a CA-signed certificate.

Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Deployment uses the same platform as Unified CM, but it does not have a graphical user interface for certificate management. For HTTPS, ECDSA is disabled, so it is necessary to sign only the Tomcat certificate with a CA. Use the platform's command line interface (CLI) to generate a Certificate Signing Request (CSR) and upload a CA-signed Tomcat certificate.

Cisco Prime Collaboration Deployment uses SOAP services, based on HTTPS, to connect to the Cisco Collaboration products to export and/or import data during Cisco Prime Collaboration Deployment tasks.

Cisco Prime Collaboration Provisioning

By default, Cisco Prime Collaboration Provisioning has a signed certificate. We recommend replacing it with a certificate signed by the enterprise CA. Certificate chains are not supported with Cisco Prime Collaboration Provisioning. To perform provisioning, Cisco Prime Collaboration Provisioning connects to the various Cisco Collaboration servers via an encrypted connection.

Encryption

With more services extending beyond the internal network, and with internal networks potentially subject to internal attacks, encryption and authentication are becoming increasingly critical.

Encryption protects against attacks such as eavesdropping, tampering, and session replay. If an unauthorized user is able to capture the traffic, he/she would not be able to decrypt the contents of the communication or modify it without knowing the encryption keys. Encryption also provides authentication through digital certificates when the encrypted communication is set up.

In general, we recommend enabling encryption on the various server connections, as discussed in the TLS Overview section. For Jabber we recommend enabling encrypted media and signaling, which is simple to provision and manage since Jabber can use the OAuth token to perform encrypted media and signaling and does not need an LSC. For phones and TelePresence endpoints, we recommend enabling encrypted media and signaling if possible, but it would require more configuration because mixed-mode would have to be enabled and LSCs would have to be installed (the recommendation is to use LSCs instead of MICs).

The authentication can be one-way authentication; for example, between an administrator or end user using a web browser to access web services, where the client (browser) authenticates the web server but where the server does not authenticate the client (browser). Alternatively, the authentication can be two-way with Mutual TLS (MTLS), where the server also authenticates the client. MTLS is used, for example, with the signaling between endpoints and the Unified CM server they are registered to or with Unified CM SIP trunks.

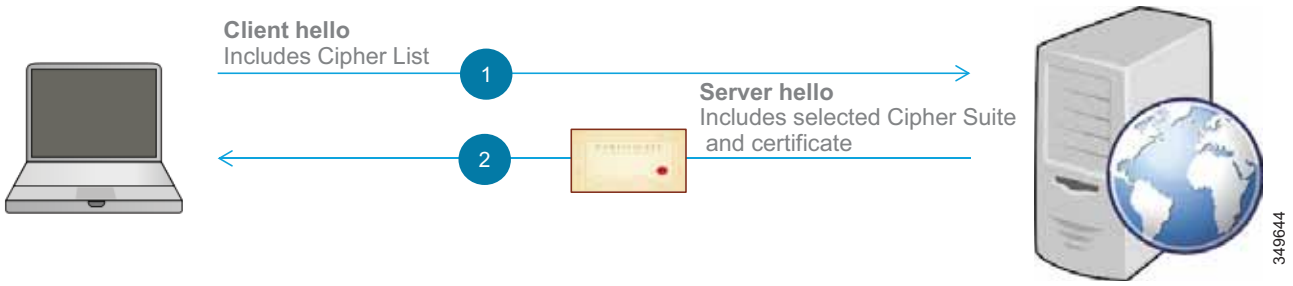
TLS Overview

Transport Layer Security (TLS) is a method for encrypting TCP traffic and is commonly used for web services traffic as well as SIP signaling. The following steps present an overview on how a TLS session is established:

1. A TLS connection is initiated by a TLS client, which connects to a TLS server. The client establishes a TCP connection with the server, sending first a Client Hello that contains a random number and its capabilities. These capabilities include the list of cipher suites the client supports.
2. The TLS server selects one of the cipher suites, typically taking into account the cipher suite preference of the client, and replies with a Server Hello. This message also includes another random number and the server certificate so that the client can authenticate it.

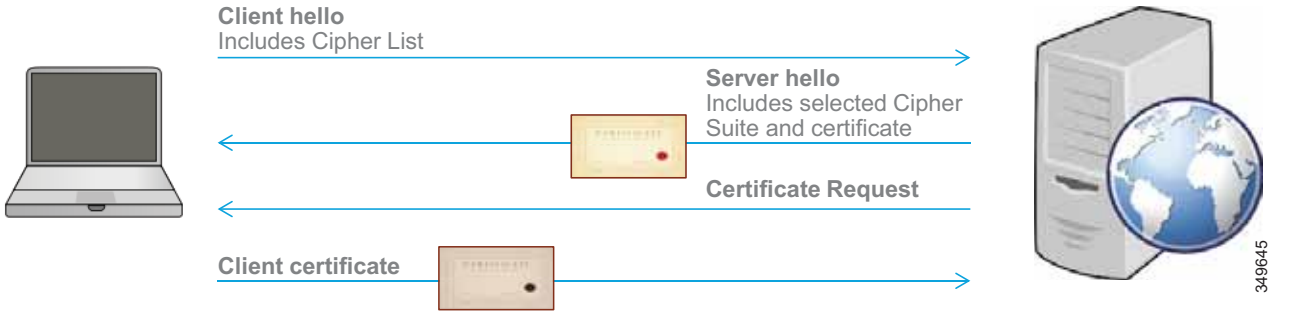
Figure 7-4 illustrates these two steps for establishing a TLS session. For simplicity, it does not include all the messages and possible variations in the TLS handshake. The server certificate could be sent in the Server Hello message or could be sent separately.

Figure 7-4 TLS Handshake



The authentication can be one-way authentication; for example, when an administrator or end user uses a web browser to access web services, where the client (browser) authenticates the web server but where the server does not authenticate the client (browser). Alternatively, the authentication can be two-way with Mutual TLS (MTLS), where the server also authenticates the client. MTLS is used, for example, with the signaling between endpoints and the Unified CM server they are registered to or with Unified CM SIP trunks. With Mutual TLS (MTLS), the server also authenticates the client. The server sends a CertificateRequest to the client, which in turn sends its client certificate. Figure 7-5 illustrates this flow at a high level.

Figure 7-5 MTLS Handshake



With RSA, the client encrypts the pre-master secret with the server's public key and sends it to the server. With Diffie-Hellman (DH) key agreement algorithms, the pre-master secret is not sent over the network; instead, the client and server exchange data (computed from random numbers and signed by the private key for authentication purposes) so that the client and the server can derive the pre-master secret on their own. DH combined with changing random numbers (Diffie-Hellman Ephemeral) allows for Perfect Forward Secrecy (PFS).

Then, the master secret is derived and session keys are computed from the master secret. From this point, the client and server stop using the public-private key pair (asymmetric encryption) and start using the shared session keys for encryption (symmetric encryption).

In general, Cisco Collaboration products support TLS version 1.2. However, some products might not support it yet and some older products will not support it at all. In order to maximize interoperability, we recommend using the default configuration and not explicitly disabling TLS 1.0 or TLS 1.1 unless you have specific requirements for doing so. With the default configuration, when both client and server

interfaces support TLS 1.2 as is typically the case, TLS 1.2 is negotiated. For more information on TLS 1.2 support with Cisco Collaboration products and the ability to disable lower versions of TLS, refer to the latest version of the *TLS Compatibility Matrix for Cisco Collaboration Products*, available at

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html

Cisco Unified CM with IM and Presence and Endpoints

There are three main types of connections to encrypt:

- HTTPS and administrative or user interfaces

  Most of those interfaces use encryption by default. For example, the Unified CM administrative web interface and the Unified CM end-user portal use HTTPS. If passwords or other sensitive information is sent in a connection, encrypt that connection; for example, for Unified CM integrated with LDAP, use LDAP over SSL. Or on the endpoints, for example, configure HTTPS for web services such as Extension Mobility.

- Signaling

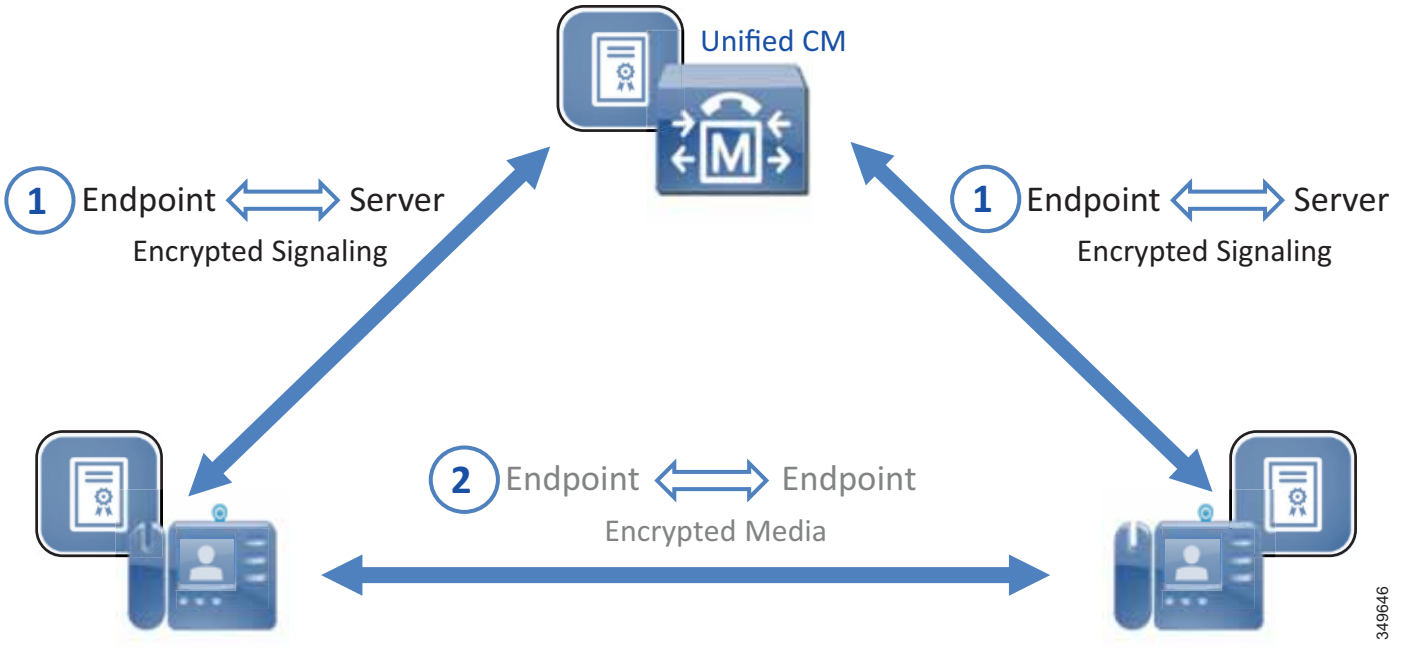
  TLS is mainly used to encrypt call control signaling; for example, with SIP signaling between endpoints and Unified CM servers or in SIP trunks. TLS is also used for other TCP communications such as XMPP.

- Media

  The media traffic can be encrypted using Secure RTP (SRTP). The signaling must also be encrypted because the media encryption keys are exchanged between the endpoints through the signaling to Unified CM (using SDES).

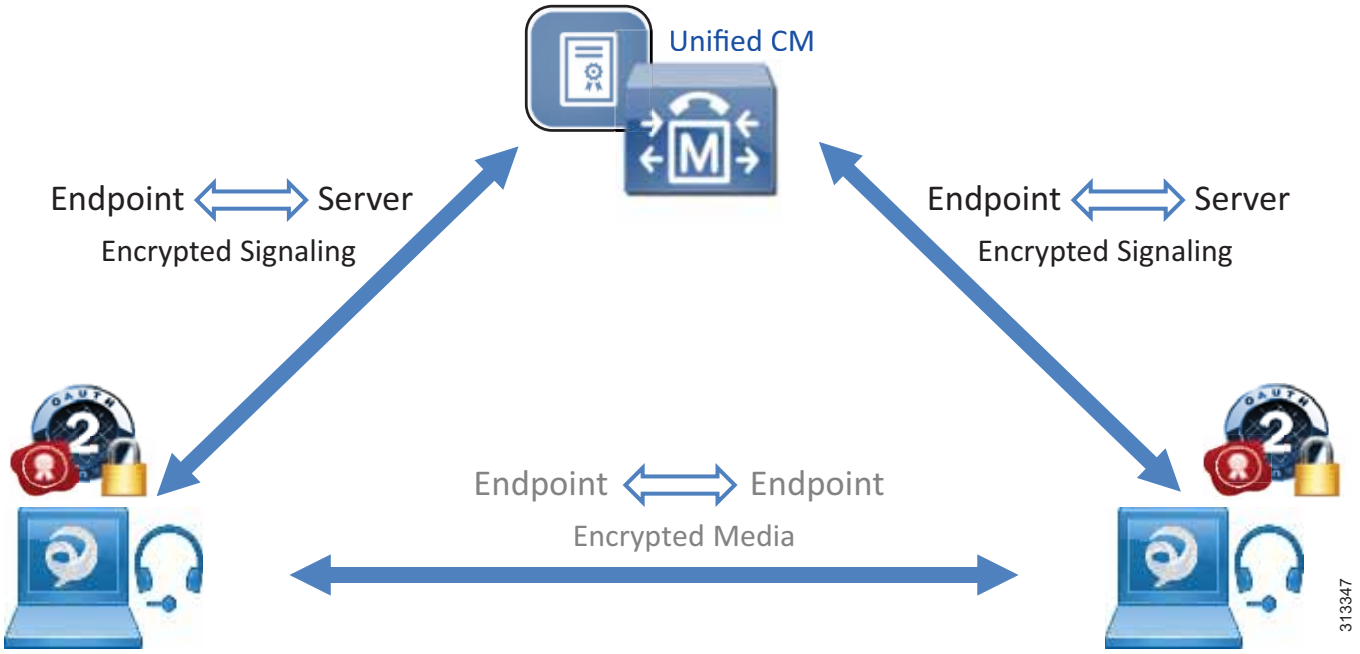
Figure 7-6 shows a high-level view of the encrypted signaling and media on the endpoints. TLS is first set up for the SIP signaling between the endpoints and Unified CM (endpoint registration), as shown by step 1 in the figure. When an endpoint is placing a call, media encryption keys are generated and are sent through the SIP TLS channel, and the media is encrypted with SRTP, as shown by step 2 in the figure. As shown in Figure 7-6, with phones and TelePresence endpoints, the TLS handshake authentication for signaling is based on certificates on Unified CM and on the endpoints.

Figure 7-6 Signaling and Media Encryption with the Phones and TelePresence Endpoints



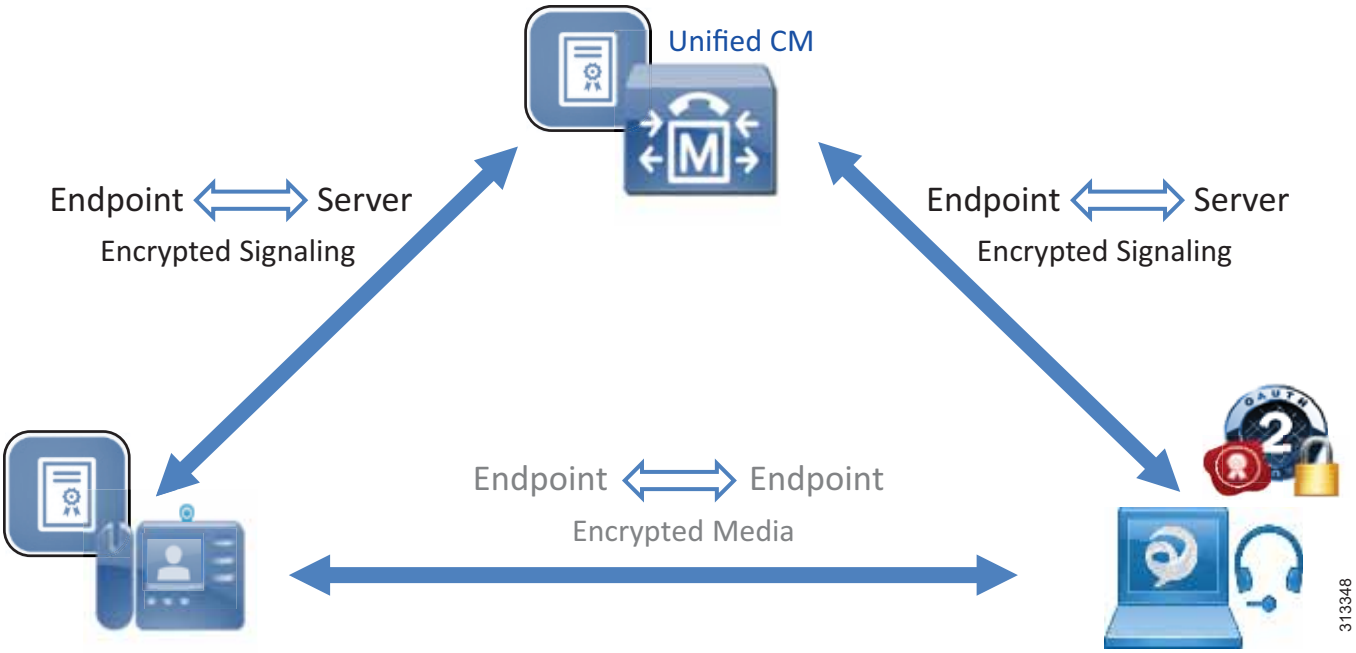
In order to perform media and signaling encryption, Jabber clients in this Preferred Architecture use the OAuth token for the TLS authentication, as shown in Figure 7-7.

Figure 7-7 Signaling and Media Encryption with Jabber



Phones and TelePresence endpoints that use their LSC to encrypt media and signaling can place and receive encrypted calls to Jabber clients that use the OAuth token, as depicted in Figure 7-8.

Figure 7-8 Signaling and Media Encryption with Phones or TelePresence Endpoints and Jabber



Note To encrypt the communications between the nodes within a Unified CM cluster with IM and Presence (for example, Intra-Cluster Communication Signaling (ICCS)), IPsec must be deployed. However, because configuring and operating IPsec adds considerable complexity and affects the scalability of the system, and because Unified CM and IM and Presence nodes are typically located in protected and trusted data centers, deploying IPsec typically is not necessary for most deployments and is not covered in this document.

Cipher Suite Support

A cipher suite is a combination of cryptographic algorithms used to establish a TLS session. The list of supported cipher suites to encrypt communication links depends on the Cisco Collaboration products. The standard cipher suites are supported across the Cisco Collaboration solution. Some products such as Cisco Unified CM, IM and Presence, Unity Connection, and most endpoints listed in this document (for example, Cisco Jabber, Cisco IP Phone 7800 Series and 8800 Series, and Cisco Webex DX Series) support newer and stronger cipher suites that we refer to as Next Generation Encryption (NGE). These stronger cipher suites are based on newer algorithms and/or have longer cryptographic keys, and they are more difficult to compromise. In general, the strongest cipher suite that is supported by both client and server is negotiated. If a client supports only weaker cipher suites, then a weaker cipher might be negotiated. If you want to avoid negotiating down to cipher suites that are too weak, it is in general possible to restrict the cipher suites that can be negotiated. For example, on Unified CM there is a setting to limit TLS cipher suite negotiation to the strongest cipher suite (only AES 256 with SHA 384), another setting to allow strong and medium-strength cipher suites (adds AES 128 with SHA 256), and a setting to allow all supported cipher suites. For more granularity, it is possible to configure the list of cipher suites that can be allowed. For the digital signature algorithm used to set up a TLS connection, RSA is supported across the Cisco Collaboration solution. The other digital signature algorithm that can be used is Elliptic Curve Digital Signature Algorithm (ECDSA), which provides the same level of security as

RSA but with smaller keys. However, it is not supported across all Unified CM services, across all Cisco Collaboration products, or on the endpoints, and it requires the server and sometimes the client to have an ECDSA-based certificate. Refer to the Certificate Management section for more details on RSA and ECDSA.

Note Encryption cipher suites based on ECDHE do not require certificates based on ECDSA; they can be negotiated with certificates based on RSA.

The following list discusses cipher suites for the various type of connections and provides our recommendation:

- HTTPS connection

  For Unified CM with IM and Presence, there is one Enterprise Parameter setting for the HTTPS cipher suites. This parameter determines whether RSA-only cipher suites are allowed or all cipher suites (RSA and ECDSA) are allowed. We recommend using the default value, which is to allow RSA-only cipher suites (refer to the RSA and ECDSA section for more details).

  The typical cipher suites that are negotiated are TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 or TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. For those cipher suites, ECDHE (Elliptical Curve Diffie Hellman Ephemeral) and RSA represent the ciphers used for the digital signature algorithm and key agreement. AES (Advanced Encryption Standard), GCM (Gallois Counter Mode) and SHA (Secure Hash Algorithm) represent the ciphers used for the actual encryption and authentication of the encrypted packets.

- SIP TLS (signaling)

  With Unified CM, by default, cipher suites based on RSA are preferred over the ones based on ECDSA. This is the recommended configuration because ECDSA is not supported by all endpoints and is not supported across all Cisco Collaboration servers.

  By default, all supported cipher suites are enabled. As described earlier, stronger cipher suites will be negotiated first, and typically TLS_ECDHE_RSA with AES256_GCM_SHA384 is negotiated. However, there could be some cases where both parties do not support this cipher suite and a lower strength cipher would need to be negotiated. To maximize cipher suite compatibility across the various components in the solution, we recommend using the default setting (allow all cipher suites, with RSA preferred).

- SRTP (media)

  With Unified CM, by default all ciphers are enabled. As described earlier, stronger cipher suites will be attempted first, and typically the strongest one, AEAD AES-256 GCM (Authenticated Encryption with Associated Data, Advanced Encryption Standard, 256 key size, Galois Counter Mode), is negotiated. However, Cisco IOS Gateways, some endpoints, and some servers might not support this cipher suite. For this reason, we recommend using the default setting and allowing fallback to weaker cipher suites. To verify which cipher suites are supported for any Cisco endpoint, go to Cisco Unified Reporting page of Unified CM (**System Reports** > **Unified CM Phone Feature List**).

Unified CM Mixed Mode for Media and Signaling Encryption

When Unified CM is first installed, it is in what we call "non-secure mode" even though most security features are actually available in this mode. For example, signed TFTP configuration file, encrypted TFTP configuration file, signed phone firmware, HTTPS access to web services, CAPF enrollment to install a Local Significant Certificate (LSC), SIP trunk encryption, Phone VPN, and 802.1x, are all

possible by default with Unified CM in non-secure mode. Media and signaling encryption on Jabber is also possible when SIP OAuth mode is enabled (refer to the section on SIP OAuth with Jabber for more details). The one security feature that is missing with non-secure mode is media and signaling encryption for phones and TelePresence endpoints. To enable it, the Export-Controlled functionality has to be allowed in Smart Licensing, Unified CM has to be configured in mixed mode, and the Restricted version of Unified CM software is required. (Media and signaling encryption is not available with the Unrestricted version of Unified CM.)

An important consideration with mixed mode and encryption is certificate management on the phones and TelePresence endpoints. Because the recommendation is to use LSCs instead of MICs on the endpoints, CAPF enrollment (LSC installation) on the phones and TelePresence endpoints would have to be performed on the phones and TelePresence endpoints where media and signaling encryption is enabled. The administrator has to monitor the validity of the LSCs and replace the certificates before they expire. The endpoints also need to have the current server certificates. For example, if they don't have the current CallManager certificate and are configured with media and signaling encryption, they will not register with Unified CM. (Refer to the CTL and ITL section for more details.)

There are two ways to enable mixed mode:

- Hardware USB eTokens

  This is the traditional way to enabled mixed mode. It requires a minimum of two Hardware USB eTokens (KEY-CCM-ADMIN-K9= or new KEY-CCM-ADMIN2-K9=). One eToken is used to sign the Certificate Trust List (CTL) file. The other eToken(s) provide redundancy in case the first eToken is lost or is not available anymore. To enable mixed mode, the CTL Client software must be installed onto a Microsoft Windows desktop. When this CTL client software is running, the USB eTokens will have to be inserted on the desktop. After mixed mode is configured, a CTL file is created for the Unified CM cluster, and the USB eTokens are removed and taken off-line.

- Tokenless (software eTokens)

  With this method, USB tokens and a Microsoft Windows desktop are not required. Mixed mode is enabled simply through a CLI command, **utils ctl set-cluster mixed-mode**. The CTL file is not signed by a hardware USB eToken, but is signed by the ITLRecovery private key.

The tokenless method is recommended and it is the method that is covered in this document. With the tokenless method, enabling mixed mode and updating the CTL file is simpler. There is no need to acquire the USB eTokens, install the CTL client on a Microsoft Windows desktop, and run the CTL Client when enabling mixed mode or when updating the CTL file. Only one CLI command needs to be issued. The CTL signature is signed using a longer private key (ITLRecovery private key). Also, beginning with Cisco Unified CM 12.0, the ITL and tokenless CTL files are signed by the ITLRecovery private key, so renewing the CallManager certificate will not lead to a loss of trust between the endpoints and Unified CM if there are issues with the Trust Verification Service (TVS).

SIP OAuth with Jabber

To enable media and signaling encryption on Jabber, mixed-mode could be enabled and an LSC could be installed on Jabber. The drawback of this approach is that installing an LSC and maintaining it can require additional administrative overhead with Jabber. For example, if the Jabber endpoint is reset, a new LSC would have to be installed. Instead of installing an LSC on Jabber, we recommend enabling the OAuth token for SIP. In this mode, Jabber can perform media and signaling encryption without an LSC and without the need to enable mixed-mode on Unified CM.

To enable the OAuth token to be used with SIP, the Export-Controlled functionality has to be allowed in Smart Licensing, and the Restricted version of Unified CM software is required. (Media and signaling encryption is not available with the Unrestricted version of Unified CM.)

Note If you wish to enable encrypted media and signaling for endpoints other than Jabber, you still must enable mixed-mode on Unified CM.

TFTP Configuration File Encryption

Without TFTP configuration file encryption, TFTP configuration files are available in plain text from any of the Unified CM TFTP servers. The type of information available in a TFTP configuration file includes, for example, phone firmware information and information on the Unified CM cluster. More importantly, if usernames and passwords are provisioned in the Unified CM administration phone page, they are also saved in plain text in the TFTP configuration files. Therefore, the general recommendation is to enable TFTP configuration file encryption for phones and TelePresence endpoints that are on-premises (not connecting through mobile and remote access (MRA)). This is especially important if usernames, passwords, or sensitive information are configured in the Unified CM administration phone page.

With MRA phones and MRA TelePresence endpoints, if TFTP configuration file encryption is configured, the MRA endpoint must first be deployed on-premises and must register directly to Unified CM before being deployed in the Internet and connecting through MRA, even if it has an MIC. Moreover, LSCs cannot be installed or renewed on endpoints that are connecting via MRA. Therefore, when the LSC expires, the endpoint would have to be brought back into the corporate network. For this reason, it is simpler not to enable TFTP configuration file encryption for endpoints (especially Jabber) connecting through MRA. However, ensure that sensitive information (passwords, for example) is not configured for those endpoints.

Jabber clients are enabled for SIP OAuth mode in this Preferred Architecture and do not need an LSC for encrypted media and signaling, but they would need one for TFTP configuration file encryption. Because managing LSCs on Jabber clients requires additional administrative overhead (for example, resetting Jabber deletes the LSC and a new LSC would have to be installed) and because LSCs are not required for encrypted media and signaling, in general we recommend not installing LSCs on Jabber clients and therefore not deploying TFTP configuration file encryption on Jabber clients whether they are on-premises or connecting via MRA. However, ensure that no sensitive information is configured for the Jabber clients.

Secure SRST

Survivable Remote Site Telephony (SRST) routers based on the Cisco 4000 Series Integrated Services Routers can also be configured with secure SRST. When endpoints cannot establish communications with the Unified CM call processing servers, they fail-over to SRST, and media and signaling are still encrypted with secure SRST. The endpoints and the SRST routers are able to establish a secure and authenticated session because the endpoints have the SRST certificate in their TFTP configuration file and the SRST routers have the certificate of the CA that signed the LSC in their trust store (CAPF certificate or external CA certificate, manually imported by the administrator).

Cisco Meeting Server

Internal communications between Cisco Meeting Server nodes use encryption (TLS). For external communications between Cisco Meeting Server and other servers or devices, encryption could be forced or optional, depending on the type of communications. For example, the RESTful API communication between Unified CM and Cisco Meeting Server is always encrypted. But the SIP signaling and media between Cisco Meeting Server and Unified CM or endpoints can be configured with or without encryption (encryption is recommended). In a conference, if all participating endpoints are encrypted

(encrypted media and signaling), a lock icon is displayed on all endpoints that support the conference lock. If one of the participating endpoints is not secure, an unlocked icon is displayed on all endpoints that support the conference lock.

Cisco Unity Connection

This document covers Cisco Unity Connection media and signaling encryption using Next Generation Encryption (NGE). With encryption, the signaling to/from Unity Connection and the media between the endpoints and the Unity Connection voicemail ports are encrypted. By default, the TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 cipher suite is negotiated for the signaling between Unified CM and Unity Connection.

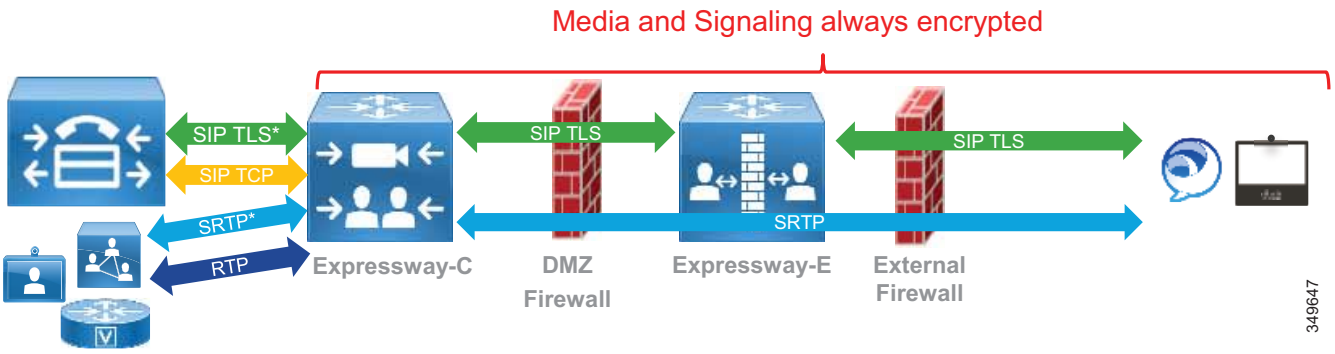
Cisco Expressway

This section discusses mobile and remote access (MRA) and business-to-business communications with Cisco Expressway.

Mobile and Remote Access (MRA)

The media and signaling between an MRA endpoint and Expressway-C are always encrypted. If an MRA endpoint calls an endpoint inside the corporate network, then the call leg inside the corporate network (that is, the signaling between Expressway-C and Unified CM, and the media between Expressway-C and the internal endpoint) may be encrypted depending on the configuration. If the MRA endpoint is configured with a phone security profile in non-encrypted mode, then this internal call leg is not encrypted. If Unified CM is in mixed mode and if the MRA endpoint is configured with a phone security profile in encrypted mode, then the SIP signaling between Expressway-C and Unified CM is encrypted. In addition to that, if the internal endpoint is also configured in encrypted mode, then the media between Expressway-C and the internal endpoint is encrypted (SRTP), and therefore the media and signaling are encrypted end-to-end (or more precisely, all the call legs are encrypted). See Figure 7-9.

Figure 7-9 Media and Signaling Encryption for MRA Endpoints



The certificates used for SIP TLS authentication with MRA differs somewhat from on-premises calls. When an endpoint connects to the enterprise through MRA, the endpoint verifies the Expressway-E server certificate but the server does not check the endpoint certificate. This TLS connection does not use mutual authentication. The MIC or LSC on the MRA client, whether it is present or not, is not verified. The user on the MRA client is then authenticated via the username and password against the Cisco Unified CM user database or integrated LDAP server (or IdP if Jabber is deployed with Single Sign-On). For the call leg between Expressway-C and Unified CM, if the MRA endpoint is configured

with the encrypted mode, Expressway-C establishes a SIP TLS connection with Unified CM and sends its own certificate on behalf of the MRA endpoint. When Unified CM receives this certificate, it verifies that the phone security profile's name configured for that MRA endpoint is part of the SAN extension of the Expressway-C certificate.

Business-to-Business Communications

With business-to-business communications, the connection between Expressway and the other party does not have to be encrypted. This depends on the **Transport** parameter in the Expressway zone configuration. If **Transport** is set to **TLS**, certificate verification is not required. The administrator can disable certificate verification by setting the **TLS verify** parameter in the Expressway zone configuration to **Off**.

Cisco IOS Gateway and Cisco Unified Border Element

Cisco IOS Gateways and Cisco Unified Border Element support TLS and SRTP. For SRTP, the cipher suite AES_CM_128_HMAC_SHA1_32 is negotiated by default. The cipher suite AES_CM_128_HMAC_SHA1_80 can also be configured. In order to support the NGE cipher suites, SRTP pass-through must be configured. The main downside with SRTP pass-through is that media interworking between RTP and SRTP (handling RTP in one call leg and SRTP in the other call leg) is not supported.

By default, if the Cisco IOS Gateway or Cisco Unified Border Element initiates a call and request SRTP but the called endpoint does not support SRTP, the call is dropped. To maximize interoperability, configure **srtp fallback** and **srtp negotiate**. When they are configured, the By default, if the Cisco IOS Gateway or Cisco Unified Border Element does not drop the call but instead falls back from SRTP to RTP.

For more information on the SRTP commands, refer to the *Cisco IOS Voice Command Reference*, available at https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/vcr4/vcr4-cr-book/vcr-s11.html.

Multi-Cluster Considerations

In a multi-cluster deployment, if clusters are located in the same data center, encryption between the clusters is not critical. However, if the clusters are located in different data centers and are connected over service provider links, we recommend enabling encryption on the following intercluster links:

- SIP trunks

  Encrypt the SIP trunks between the clusters. With the CallManager certificates signed by a CA and the CA certificate (or root CA certificate) already in the CallManager-trust store, no additional operations related to certificates are required for intercluster SIP trunk encryption.

- Intercluster Lookup Service (ILS) connections

  Encrypt Intercluster Lookup Service (ILS) connections. To enable ILS encryption, we recommend using TLS certificates (Tomcat certificates) for authentication and a shared password across the clusters for authorization. With the Tomcat certificates signed by a CA and the CA certificate (or root CA certificate) already in the Tomcat trust store, no additional operations related to certificates are required to enable ILS encryption.

- Location Bandwidth Manager (LBM) links

  If call admission control (CAC) is configured, intercluster LBM links should also be encrypted. LBM encryption is also based on Tomcat certificates, and with the Tomcat certificate signed by a CA and the CA certificate already in the Tomcat trust store, there are no additional operations related to certificates required to enable LBM encryption.

High Availability Considerations for Collaboration Security

There is high availability for the Unified CM Trust Verification Service (TVS). The TVS runs as a network service on all Unified CM nodes. Endpoints use the same TVS nodes as the Unified CM call processing nodes they are configured with in the Cisco Unified CM group. Their primary TVS server is their primary call processing subscriber, and their backup TVS server is their backup call processing subscriber.

The Unified CM publisher has a critical role with security components. The publisher runs the CAPF service to which the phones connect. Therefore, if the publisher is down, CAPF operations are not possible. For example, Locally Significant Certificate (LSC) installation is not possible. Generating a multi-server certificate and enabling/disabling mixed mode are also operations that are performed on the publisher and require it to be running.

Collaboration Security Capacity Planning

Enabling encryption can slightly increase the CPU and memory utilization on the servers. However, except for Cisco Unified Border Element, the simplified sizing deployments described in the Sizing chapter are not affected by enabling encryption.

Deployment

This section provides information on the deployment of certificate management and encryption. It starts with certificate management since that needs to be done first. Once all the certificates are in place, you can enable and configure encryption.

This section provides deployment information for the following components of the Enterprise Collaboration Preferred Architecture:

- Cisco Unified CM with IM and Presence and Endpoints
- Cisco Unity Connection
- Collaboration Edge (Cisco Expressway, Cisco IOS Gateways, and Cisco Unified Border Element)
- Conferencing
- Collaboration Management Services

Cisco Unified CM with IM and Presence and Endpoints

For Cisco Unified CM with IM and Presence and for endpoints, at a high level, perform the following configurations:

- Cipher Suites Configuration
- Server Certificate Generation and Management
- Certificate Monitoring
- LDAP over SSL Configuration
- SIP Trunk Encryption

For media and signaling encryption on the endpoints, also perform the following configurations:

- Mixed mode configuration
- CAPF enrollment and configuration of media and signaling encryption on the endpoints
- Secure SRST configuration

Cipher Suites Configuration

There are three main types of secure connections, and there is a cipher enterprise parameter for each of them:

- HTTPS

  As discussed in the Cipher Suite Support section, we recommend using the default value for the **HTTPS Ciphers** enterprise parameter, **RSA Ciphers only**. If you want to enable ECDSA ciphers, change the setting to **All Supported EC and RSA Ciphers**.

- TLS (signaling)

  As discussed in the Cipher Suite Support section, we recommend using the default value for the **TLS Ciphers** enterprise parameter, **All Ciphers RSA Preferred**. However, if you have specific requirements and, for example, need to disable the negotiation of weaker cipher suites or wish to negotiate ECDSA over RSA cipher suites, the **TLS Ciphers** enterprise parameter can be modified.

- SRTP (media)

  As discussed in the Cipher Suite Support section, we recommend using the default value for the **SRTP Ciphers** enterprise parameter, **All Supported Ciphers**. However, if you have specific requirements and, for example, need to disable the negotiation of weaker cipher suites, the **SRTP Ciphers** enterprise parameter can be modified and can be set to **Strongest - AEAD AES-256 GCM cipher only** or to **Medium - AEAD AES-256 GCM, AEAD AES-128 GCM ciphers only**, but note that some endpoints and servers do not support these cipher suites. See the Cipher Suite Support section for more details.

Server Certificate Generation and Management

As mentioned in the section on CA-Signed Certificates Instead of Self-Signed Certificates, we recommend using CA-signed certificates for most certificates. For a list of certificates to be signed by a CA, refer to Table 7-5. For the certificates that do not need to be CA-signed, they do not need to be modified or regenerated.

At a high level, the procedure to issue CA-signed certificates is as follows:

1. Upload the root CA certificate or certificate chain into the corresponding server trust store.
2. Generate the certificate signing requests (CSR) for the desired certificate.
3. Download the CSRs.
4. Submit the CSRs to the signing CA.
5. Upload the new CA-signed certificate using the appropriate type.

With Unified CM, IM and Presence Service, and Unity Connection, these operations are performed from the OS Administration web interface of your system.

For more detailed steps, refer to the latest version of the *Security Guide for Cisco Unified Communications Manager*, available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

1. Upload the root CA certificate

The first step is to import the root CA certificate (or certificate chain if using public CAs). With Unified CM and IM and Presence Service, this operation needs be done only on the publisher, and the certificate will then automatically be distributed to the trust stores of the other nodes in the cluster.

Go to the OS Administration page and select **Security** > **Certificate Management** > **Upload Certificate/Certificate chain**, and then upload the root CA certificate (or certificate chain) into the trust store of the service for which you are issuing a CA-signed certificate. Note that the RSA and ECDSA certificates share the same trust store. Table 7-8 lists the trust stores where the CA certificate needs to be imported.

Table 7-8 Trust Stores Where the CA Certificate is Imported for Unified CM with IM and Presence Service

Product	Node Where the CA Certificate Should be Uploaded
Unified CM	tomcat-trust
Unified CM	callManager-trust
IM and Presence Service	tomcat-trust
IM and Presence Service	cup-xmpp-trust

2. Generate the certificate signing requests (CSR)

To generate a certificate signing request (CSR), go to the OS Administration page and select **Security** > **Certificate Management** > **Generate CSR**.

Some certificates support the multi-server feature; see Table 7-6 for the list. For those certificates, generate the CSR on the publisher and select **Multi-Server (SAN)** in the **Distribution** field of the CSR page. See Table 7-9 for where to generate the CSR for multi-server certificates. For the other certificates, issue a CSR on each node and use the default value for the **Distribution** field.

Table 7-9 CSRs for Multi-Server Certificates

Product	Certificate	Where to Generate the CSR
Unified CM and IM and Presence Service	tomcat	Unified CM publisher
Unified CM	callManager	Unified CM publisher
IM and Presence Service	xmpp	IM and Presence Service publisher
IM and Presence Service	xmpp-s2s	IM and Presence Service publisher

In general, you do not have to change the default value for the **Common Name** field. This field is by default set to the FQDN of the node where you are generating the CSR. With a multi-server certificate, a "-ms" is appended after the hostname portion of the FQDN.

In general, we recommend using a **Key Length** of 2048 bits or larger and a **Hash Algorithm** set to **SHA256**. Therefore, you can use the default value for those fields.

3. Download the CSRs

4. Submit the CSRs to the signing CA

The CA generates corresponding certificates.

Key usage and extended key usage extensions restrict the purposes for which a key may be used. Ensure that the X.509 key usage and X.509 extended key usage in the issued certificate match the request in the CSR. A common problem is that the enterprise CA issuing and signing the certificate is not configured with the appropriate certificate template and does not issue a certificate with the appropriate key usage extension. For example, the Unified CM Tomcat certificate must include the TLS Web Client Authentication extended key usage (EKU). Failure to use a template that includes the TLS Web Client EKU will result in TLS connection setup failures for inter-server communications – for example, Intercluster Lookup Service (ILS) and User Data Store (UDS) – due to the incorrect key usage. Table 7-10 shows an example of the Key Usage Requirements. As a general rule, generate a CSR, note the Key Usage and Extended Key Usage specified in the CSR, ensure the enterprise CA has a certificate template that contains the correct Key Usage and Extended Key and, if not, create a new certificate template. After submitting the CSR to the CA and getting back the certificate, ensure that the Key Usage and Extended Key Usage are still there.

Table 7-10 Key Usage and Extended Key Usage Requirements

Product	Certificate	X509v3 Key Usage	X509v3 Extended Key Usage
Unified CM and IM and Presence Service	tomcat	Digital Signature, Key Encipherment, Data Encipherment	TLS Web Server Authentication, TLS Web Client Authentication
Unified CM	CallManager	Digital Signature, Key Encipherment, Data Encipherment	TLS Web Server Authentication, TLS Web Client Authentication
Unified CM	CAPF	Digital Signature, Certificate Sign	TLS Web Server Authentication
IM and Presence Service	cup-xmpp	Digital Signature, Key Encipherment, Data Encipherment	TLS Web Server Authentication, TLS Web Client Authentication
IM and Presence Service	cup-xmpp-s2s	Digital Signature, Key Encipherment, Data Encipherment	TLS Web Server Authentication, TLS Web Client Authentication

5. Upload the new CA-signed certificate using the appropriate type

Upload the certificate and select the corresponding value for the **Certificate Purpose** field. For example, if uploading the Tomcat certificate, select **tomcat** for the **Certificate Purpose** field.

For multi-server certificates, perform the upload operation on the publisher node and not on the subscriber nodes.

Once certificates are uploaded, services must be restarted. The GUI indicates which service to restart. For example, with the CallManager certificate, the Cisco Tftp, Cisco CallManager, and Cisco CTIManager services must be restarted.

Certificate Monitoring

Monitor Certificate Validity

Enable certificate validity monitoring on Unified CM for server certificates and LSCs.

Go to **Cisco Unified CM OS Administration** > **Security** > **Certificate Monitor**, and enter the number of days before expiration to begin notification as well as the frequency of the notifications. Enable email notification. Select **Enable LSC monitoring** so that both server certificates and LSCs are monitored.

Certificate Validity Check for Long-Lived Sessions

Unified CM can periodically check the revocation and expiry status of the certificates for long-lived connections. This is done for CTI connections with JTAPI/TAPI applications and LDAP connections (and IPsec, which is not covered in this document).

To enable certificate validity check (expiry and revocation status check) for long-lived connections, enable the Unified CM Enterprise Parameter **Certificate Validity Check**.

For certificate revocation status validation, also configure Online Certificate Status Protocol (OCSP) in **Cisco Unified CM OS Administration** > **Security** > **Revocation**.

LDAP over SSL Configuration

Configure LDAP over SSL for the connections to Microsoft Active Directory.

On Unified CM, perform the following steps:

- If the LDAP certificate is self-signed, import it into the Unified CM tomcat-trust store.

  If the LDAP certificate is signed by a CA, import the root CA certificate into the Unified CM tomcat-trust store. If you configured Online Certificate Status Protocol (OCSP) to monitor the revocation status of the LDAP certificate, also import the LDAP certificate itself.

- In **Cisco Unified CM Administration** > **System** > **LDAP** > **LDAP directory** and in **Cisco Unified CM Administration** > **System** > **LDAP** > **Authentication**, change the **LDAP port** to a secure port and the enable the **Use TLS** option (check the box). Typically, the LDAP secure port is 3268 if synchronizing against a global catalog (GC) or 636 if synchronizing against the Windows Microsoft Active Directory domain controller (DC). For more information about DC and GC behavior and port numbers, refer to the Microsoft documentation at https://technet.microsoft.com/en-us/library/cc978012.aspx.

SIP Trunk Encryption

This section explains how to configure encryption for Unified CM SIP trunks.

For each type of SIP trunk, create a secure SIP Trunk security profile in the Unified CM Administration interface (under **System** > **Security**) for all the existing SIP trunk security profiles. Use the same parameter as the existing SIP trunk security profile (see the Call Control chapter), except for the parameters listed in Table 7-11.

Table 7-11 SIP Trunk Security Profile Parameters for Secure SIP Trunks

Parameter	Value
Device Security Mode	Encrypted
Incoming Transport Type	TLS
Outgoing Transport Type	TLS
X.509 Subject Name	The common name (CN) of the remote party. For example: • Unity Connection: us-cuc-ms.ent-pa.com (multi-server certificate) • Cisco Meeting Server: cms.ent-pa.com (Cisco Meeting Server xmpp domain name) • Expressway-C (business-to-business): CN of the Expressway-C cluster • Cisco IOS Gateway and Cisco Unified Border Element: List of CNs used by Cisco IOS Gateway and Cisco Unified Border Element • Other Unified CM cluster: emea-cm-pub-ms.ent-pa.com (CallManager multi-server certificate)
Incoming Port	Typically, enter 5061. For SIP trunks to Expressway, since mobile and remote access (MRA) and business-to-business are enabled on the same Expressway cluster in this Preferred Architecture, use a different port for business-to-business (for example, port 5561).

In the configuration for each SIP trunk, use the settings described in Table 7-12.

Table 7-12 SIP Trunk Configuration for Secure SIP Trunks

Parameter	Value
SRTP Allowed When this option is enabled, Encrypted TLS must configured in the network to provide end-to-end security. Failure to do so will expose keys and other information.	Selected (check the box)
SIP Information > Destination - > Destination port	5061
SIP Trunk security profile	Select the SIP trunk security profile you created in the previous step
Outgoing Transport Type	TLS

Note Do not encrypt the Presence SIP trunk between Unified CM nodes and IM and Presence nodes because not all messages are encrypted.

Media and Signaling Encryption on the Endpoints

To configure media and signaling encryption on the endpoints, perform the following high-level steps:

- Enable the OAuth token for SIP (for Jabber).
- Enable mixed mode.
- Create phone security profiles with encrypted mode to enable media and signaling encryption.
- Associate the phone security profiles to the endpoints and install a Locally Significant Certificate (LSC) on the phones and TelePresence endpoints, except for the endpoints connecting only through MRA.

The following sections provide more details on these steps.

Enable the OAuth Token for SIP

With the OAuth token enabled for SIP, Jabber can perform media and signaling encryption, without the need to install an LSC or enable mixed mode.

To enable the SIP OAuth mode, enter the following CLI command:

```
utils sipOAuth-mode enable
```

Restart the CallManager services on all Unified CM nodes running this service. If you plan to enable mixed mode, you can wait to restart the CallManager service until after you enable mixed mode.

Phone Security Profile for Jabber

After enabling the SIP OAuth mode for the Unified CM cluster, create a phone security profile for Jabber endpoints.

Enable Mixed Mode

Before enabling mixed mode, activate the CAPF service on the Unified CM publisher first. If you activate the CAPF service after enabling mixed mode, the Certificate Trust List (CTL) file will need to be updated.

This document covers enabling mixed mode with the command line interface (CLI) (tokenless). To enable mixed mode, perform the following steps:

- SSH into the Unified CM publisher.
- Enter the **utils ctl set-cluster mixed-mode** CLI command.
- Restart the TFTP, CallManager, and CTIManager services on all Unified CM nodes running those services.

For more details, refer to the latest version of the *Security Guide for Cisco Unified Communications Manager*, available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

CAPF Online CA Mode

If you chose the CAPF online CA mode where the LSC endpoint certificates are signed by an external CA, perform the following the steps:

1. Import the CA certificate (or trust chain) to the Unified CM CAPF-trust.
2. Import the CA server IIS certificate or its CA certificate (or trust chain) to the Unified CM tomcat-trust, if not already done.
3. If some phones or TelePresence endpoints are configured in encrypted mode, import the CA certificate (or trust chain) to the Unified CM CallManager-trust, if not already done.
4. Configure the CAPF service parameters on the Unified CM publisher. Use the following settings:

Field	Setting
Certificate Issuer to Endpoint	Online CA
Online CA Hostname	Common Name (CN) in the certificate used by Microsoft IIS service. Typically, this is an FQDN.
Online CA Port	Typically 443
Online CA Template	Name of the certificate template defined in the Microsoft CA
Online CA Type	**Microsoft CA**
Online CA Username	Username of a user that has the right permissions to issue a certificate using the certificate template specified above
Online CA Password	Password of a user that has the right permissions to issue a certificate using the certificate template specified above

5. Activate the Cisco Certificate Enrollment Service on the Unified CM publisher, if not already done.
6. Restart the CAPF service.

Phone Security Profiles and LSC Installation

At this point in the configuration process, the server certificates are generated and Unified CM is in mixed mode.

The next step is to create a phone security profile with Device Security Mode set to **Encrypted** to enable media and signaling encryption on the endpoints. The following considerations apply to the phone security profiles:

- When creating phone security profiles, use the Phone Security Profile Type **Universal Device Template**. This type of phone security profile is not specific to a particular phone model, so it can be applied to any phone model. This simplifies the configuration and the certificate management. With a phone security profile that is specific to a phone model, when a new type of phone is added, a new phone security profile has to be created and the Expressway-C certificate needs to be regenerated with the new phone security device profile name added as a SAN if MRA endpoints are using this phone security profile. With a universal phone security profile, there is no need to create a new phone security profile or to regenerate a new Expressway-C certificate each time you add a new device type.
- A phone security profile can be associated to both MRA and non-MRA endpoints. But ensure that the phone security profile name is in FQDN format if it is associated to MRA endpoints.
- Since our recommendation is to use media and signaling encryption, set the Device Security Mode setting to **Encrypted**.
- To enable TFTP configuration file encryption, select the **TFTP Encrypted Config** option (check the box). As discussed in the Architecture section, the recommendation is to enable TFTP encrypted configuration for on-premises endpoints and to disable it for endpoints connecting over MRA (and ensure that no sensitive information is entered in the phone page). **TFTP Encrypted Config** also requires the endpoint to have a certificate installed (MIC or LSC).
- Select the **Enable OAuth Authentication** checkbox for the phone security profiles that will be used by Jabber endpoints (see Table 7-14).
- The phone security profile also specifies the authentication mode used when an endpoint connects to CAPF. In general, we recommend using the authentication mode **By Existing Certificate (precedence to LSC)**. With this setting, if an endpoint has only an MIC, the existing MIC is used for authentication to CAPF. If the endpoint has an LSC (with or without an MIC), then the LSC is used instead. So this works well for endpoints that have either an MIC or an LSC.

  If an endpoint does not have an MIC or LSC, this authentication mode cannot be used until an LSC is installed. Instead, authentication based on an authentication string or null string must be used for the initial LSC installation. Authentication based on an authentication string is more secure but requires the administrator to enter the authentication string on the device configuration page and requires the user to enter the string manually on the endpoint. If this is not practical, authentication based on a null string can be chosen, but this effectively bypasses any endpoint authentication during this first CAPF enrollment. Once the LSC is installed, then a phone security profile with the authentication mode **By Existing Certificate (precedence to LSC)** should be assigned.
- For the Key Order setting in the phone security profile, select **RSA Only**; and for the RSA Key Size setting select **2048** or larger.

With these considerations, you would create 3 phone security profiles. Table 7-13 shows how they differ. Use the values discussed above for the rest of the settings.

Table 7-13 Phone Security Profiles to Configure

Phone Security Profile Name Examples	Authentication Mode (for CAPF Enrollment)	TFTP Encrypted Configuration File	OAuth Authentication
UDT-Encrypted-LSC-TFTPenc.ent-pa.com	By Existing Certificate (precedence to LSC)	Enabled	Disabled
UDT-Encrypted-LSC.ent-pa.com	By Existing Certificate (precedence to LSC)	Disabled	Disabled
UDT-Encrypted-NullString.ent-pa.com	By Null String or By Authentication String	Disabled	Disabled
UDT-Jabber-SIPOAuth	By Null String or By Authentication String	Disabled	Enabled

Once the phone security profiles are configured, go to **Cisco Unified CM Administration** > **Device** > **Phone**, associate them to the endpoints and proceed to the LSC installation, depending on the type of endpoints. Table 7-14 shows which action to perform depending on the type of endpoint.

Table 7-14 Association of Phone Security Profiles and LSC Installation

Type of Endpoints	Procedure (Phone Security Profile Association and LSC Installation)
Cisco IP Phones and Cisco TelePresence Endpoints (MIC support)	• Associate **UDT-Encrypted-LSC-TFTPenc.ent-pa.com** (for TFTP configuration file encryption) or **UDT-Encrypted-LSC.ent-pa.com** (for no TFTP configuration file encryption) to the endpoint. • Install LSC.
Jabber clients (on-premises or MRA)	• Associate **UDT-Jabber-SIPOAuth**
MRA hardware endpoints	• Associate **UDT-Encrypted-NullString.ent-pa.com**

To associate a phone security profile to a phone, go to the phone configuration page and select the desired security profile in the **Device security profile** setting.

To configure LSC installation, select **Install/Upgrade** for the **Certificate Operation** field on the phone configuration page. In the Certification Authority Proxy Function (CAPF) Information section in the phone configuration page, the CAPF information from the phone security profile should be populated automatically. You need to update only the **Operation Completes By** field to a future date, if it is not already set.

Then, after associating the phone security profile and optionally configuring LSC installation, save the configuration. Apply the configuration or reset the endpoint. At this point, the phone security profile should be applied. If the LSC installation was configured, the endpoint gets an LSC. (With an authentication string, in some cases, the user has to press the **Update** button for the LSC installation to proceed.) The endpoint should also be configured with media and signaling encryption.

Tip The Cisco Unified Communications Manager Bulk Administration Tool (BAT) or Cisco Prime Collaboration Provisioning can be used to assign the phone security profile and/or to perform the CAPF enrollment.

Typically you do not need to install an LSC on Jabber endpoints. Jabber does not need an LSC in order to perform encrypted media and signaling when SIP OAuth mode is enabled. Jabber would still need an LSC in order to support TFTP configuration file encryption. But because managing LSC certificates on Jabber requires additional administrative overhead, we usually do not recommend deploying TFTP configuration file encryption with Jabber endpoints, and therefore installing LSC certificates on Jabber is not needed.

Enable Secure Survivable Remote Site Telephony (SRST)

With Survivable Remote Site Telephony (SRST), use the following procedure:

- Use the enterprise CA to sign the certificate of the SRST router. For details on certificate management on a Cisco IOS router, refer to the section on Cisco IOS Gateway and Cisco Unified Border Element.
- Import, into the SRST router, the trust certificate corresponding to the entity that signed the endpoint LSCs, so that SRST is able to authenticate the LSCs. If you used CAPF to issue the LSCs, this is the CAPF certificate. If you use an external CA to issue the LSCs, this is the CA certificate (or trust chain certificates).
- Enable secure SRST by enabling (checking the box) **Is SRST Secure?** in the SRST reference configuration in **Cisco Unified CM Administration** > **System** > **SRST**.

For more details, refer to the latest version of the *Security Guide for Cisco Unified Communications Manager*, available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Cisco Unity Connection

This section covers Cisco Unity Connection media and signaling encryption using Next Generation Encryption (NGE), which uses the Unity Connection Tomcat certificate instead of the Unity Connection Root and SIP certificates.

At a high-level the steps for enabling NGE for media and signaling on Unity Connection are as follows:

- On Unity Connection, manage certificates.
- On Unity Connection, configure encryption for the telephony integration.
- On the Unified CM, enable encryption on the SIP trunk to Unity Connection.

First, manage the certificates on Unity Connection. On Unity Connection, perform the following steps:

- On the Unity Connection publisher node, upload the root CA certificate (or certificate chain) into the Unity Connection tomcat-trust store. Similarly, upload the root CA certificate into the CallManager-trust store (required with CA-signed CallManager certificates). Those certificates are automatically propagated to the trust stores on the Unity Connection subscriber node.
- On the Unity Connection publisher node, issue a CSR to get a multi-server Tomcat certificate and get it signed by the enterprise CA. As an example, the common name is us-cuc-ms.ent-pa.com. The X509v3 key usage extensions are Digital Signature, Key Encipherment, and Data Encipherment. The X509v3 extended key usage extensions are TLS Web Server Authentication and TLS Web Client Authentication. Since this is a multi-server certificate, the certificate is automatically

installed on the Unity Connection subscriber when you install it on the Unity Connection publisher. After installing this new Tomcat certificate, restart the Tomcat service on both Unity Connection nodes.

For details on uploading the CA certificate or issuing a CA-signed Tomcat certificate, refer to the Cisco Unified CM and IM and Presence section. The procedure is the same for Unity Connection.

Since we are assuming the same CA is used with Cisco Unified CM and Unity Connection, there is no need to import the CA certificate into the Unified CM tomcat-trust store; it should already be there.

Next, configure encryption on Unity Connection:

- In **Cisco Unity Connection Administration** > **Telephony Integrations** > **Security** > **SIP Security Profile**, create a new SIP security profile with the following settings:

Field	Setting
Port	5061
Do TLS	Select this check box

  This SIP security profile is automatically assigned the display name **5061/TLS**.

- Under **Telephony Integrations** > **Port Group**, select the port group **PhoneSystem-1** and modify the port group with the following settings:

Field	Setting
SIP Security Profile	Select the SIP Security Profile you created in the previous step (**5061/TLS**)
Enable Next Generation Encryption	Select this check box
Secure RTP	Select this check box

- On the **Port Group** page, go to **Edit** > **Servers**. In the SIP Servers configuration, ensure that 5061 is configured for the TLS port. In the TFTP Servers configuration, ensure that the Unified CM TFTP servers are configured. This is how Unity Connection automatically downloads the CallManager certificates in its CallManager-trust store when the Port Group has been reset.

Next, enable encryption on the Unified CM SIP trunk to Unity Connection:

- A SIP trunk security profile with encryption and the appropriate X.509 Subject Name should already have been created (see Table 7-11). Select this SIP trunk security profile for the SIP trunk to Unity Connection.

At this point, on Unified CM the encrypted SIP trunk should be in full service. When a phone connects to a voicemail port, the media and signaling should also be encrypted. LDAP over SSL should also be configured. Go to **Cisco Unity Connection Administration** > **System Settings** > **LDAP**; and in the **LDAP Directory Configuration** and **LDAP Authentication** pages, select **Use TLS** and configure the port 636, similarly to the LDAP over SSL configuration on Unified CM.

Collaboration Edge

This section provides high-level information for deploying certificate management and encryption on Cisco Expressway, Cisco IOS Gateways, and Cisco Unified Border Element.

Cisco Expressway

This section discusses certificate management first, then it explains the settings to use for encryption.

Cisco Expressway Certificate Management

As mentioned in the Architecture section, new installations of Cisco Expressway software ship with a temporary trusted CA and a server certificate issued by that temporary CA. Replace the temporary CA certificates with the CA certificates that you trust, and generate CA-signed certificates for Expressway. As discussed in the Architecture section, use the enterprise CA to sign the Expressway-C certificates and a public CA to sign the Expressway-E certificates. The list of the supported public CAs for Expressway-E is available in the endpoint documentation on cisco.com; for example, see the *Certificate Authority Trust List* available at https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-technical-reference-list.html.

To implement certificate management for Cisco Expressway, use the steps outlined in the following sections.

Upload the CA Root Certificate.

Go to the **Trusted CA certificate** page (**Maintenance** > **Security certificates** > **Trusted CA certificate**). On this page, replace the existing certificates with a new root CA certificate or certificate chain. Subsequent CA certificates are appended to the existing list of CA certificates. Upload the CA certificate listed in Table 7-15. This operation has to be done on each Expressway node of both Expressway-C and Expressway-E clusters.

Table 7-15 Cisco Expressway Trust Store

Expressway-C Trust Store	Expressway-E Trust Store
• Root CA certificate from the public CA that signed the Expressway-E certificate • Root CA certificate (or certificate chain) from the enterprise CA that signs the Unified CM CallManager and Expressway-C certificates	• Root CA certificate (or certificate chain) from the public CA that signed the Expressway-E certificate • Root CA certificate from the enterprise CA that signs the Unified CM CallManager and Expressway-C certificates • With business-to-business or cloud communications, root CA certificates of other businesses

Generate a Certificate Signing Request (CSR) for each Expressway node.

1. Go to **Maintenance** > **Security** > **Server certificate**.
2. Generate a CSR.

   Subject Alternate Name (SAN) extensions for IM and Presence chat node aliases should be added automatically. Additional SAN extensions might have to be added, depending on whether your Expressway node is an Expressway-C or an Expressway-E node and depending on the features that are deployed. For more details, refer to Table 7-16.

Table 7-16 Subject Alternate Names (SAN) to be Added to the CSR

Add the items below as Subject Alternate Name (SAN)	When Generating a CSR for the Following Purposes:		
	Mobile and Remote Access	**XMPP Federation**	**Business-to-business calls**
Expressway-C cluster name	On Expressway-C only	On Expressway-C only	On Expressway-C only
Unified CM registrations domains[1]	Required on Expressway-E only	–	–
XMPP federation domains	–	Required on Expressway-E only	–
IM and Presence chat node aliases (federated group chat)	–	Required on both Expressway-C and Expressway-E	–
Unified CM phone security profile names (FQDN format)[2]	Required on Expressway-C only	–	–

1. The Unified CM registration domains used in the Expressway configuration and Expressway-E certificate are the domains that MRA clients will use to look up the _collab-edge DNS SRV record in the process of service discovery. The Unified CM registration domains enable MRA registrations on Unified CM, and in our case these domains will match the domain used on Unified CM for SIP URIs. However, these domains are primarily for service discovery, and the SIP domains used on Unified CM do not have to match.
2. There is no need to add the phone security profile name that is used for Jabber in the SAN in the Expressway-C certificate, because SIP OAuth is used (see Table 7-14).

For more information, refer to the latest version of the *Cisco Expressway Certificate Creation and Use Deployment Guide*, available at https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html.

As mentioned earlier, for simplicity reasons we recommend Universal Device Template (UDT) so that you do not have to enter a long list phone security profile names in the Expressway-C SANs. With our example in this chapter, in the CSR **Unified CM phone security profile names** field you would enter UDT-Encrypted-LSC-TFTPenc.ent-pa.com, UDT-Encrypted-RSA-LSC.ent-pa.com, and UDT-Encrypted-AuthString.ent-pa.com (or UDT-Encrypted-NullString.ent-pa.com).

3. Download the CSR and submit it to the CA so that a CA-signed certificate can be issued. Use the Base 64 format. Verify that the X509v3 Key Usage and X509v3 Extended Key Usage in the CSR are present in the certificate issued by the CA, as shown in Table 7-17.

Table 7-17 Cisco Expressway Key Usage and Extended Key Usage

Certificate	X509v3 Key Usage	X509v3 Extended Key Usage
Expressway-C and Expressway-E	Digital Signature, Key Encipherment	TLS Web Server Authentication, TLS Web Client Authentication

4. Upload the new certificate

Cisco Expressway Encryption Configuration

MRA and XMPP Federation

TLS is used for the Unified Communications zone on Expressway-C. Ensure that **TLS verify** is set to **On** for all Unified Communications services: Unified CM servers, IM and Presence Service nodes, and Unity Connection. You configure this when performing Unified Communications service node discovery (**Configuration** > **Unified Communications**). This ensures that Expressway-C nodes verify the certificates of the Unified Communications nodes.

The Unified Communications traversal zone between Expressway-C and Expressway-E is implicitly configured with TLS certification verification enabled and with media encryption. On the Expressway-C MRA traversal zone, set the **Authentication policy** to **Do not check credentials**. On the Expressway-E MRA traversal zone, set the **Authentication policy** to **Do not check credentials** and enter a **TLS verify subject name** that matches the cluster name of the Expressway-C certificate (added as a SAN in the Expressway-C certificate).

The media and signaling traffic between an MRA endpoint and Expressway-E are always encrypted. In order to encrypt the call leg inside the corporate network (that is, the signaling between Expressway-C and Unified CM, and the media between Expressway-C and the internal endpoint), configure the MRA endpoint and the endpoints inside the network with a phone security profile in encrypted mode. When you do so, the media and signaling are encrypted end-to-end (all the call legs are encrypted).

With XMPP federation, we recommend setting the **Security mode** to **TLS Required**. However, there are cases where it should be set to **TLS optional**. For example, **TLS Required** is not supported with Cisco WebEx Messenger; so if you have XMPP federation with an enterprise using Cisco WebEx Messenger, you should use **TLS Optional**. In this scenario, you should also set **Require Client-side security certificates** to **Off**.

Business-to-Business Communications

As mentioned in the Architecture section, configure Call Processing Language (CPL) rules.

Also, for the Unified CM neighbor zone on Expressway-C, use the recommended settings in Table 7-18.

Table 7-18 Expressway-C Business-to-Business Unified CM Neighbor Zone Configuration

Field	Setting
Port	If MRA and business-to-business are enabled on the same Expressway cluster, use a port other than 5061 (for example, port 5561).
Transport	TLS
TLS Verify	On
Media Encryption	Best Effort

For the traversal zone on Expressway-C, use the recommended settings in Table 7-19.

Table 7-19 Expressway-C Business-to-Business Traversal Zone Configuration

Field	Setting
Port	The port has to be different than 5060, 5061, and ports used with other traversal zones. For example, use a port in the range 7*xxx*.
Transport	TLS
TLS Verify	On
Media Encryption	Auto

For the traversal zone on Expressway-E, use the recommended settings in Table 7-20.

Table 7-20 Expressway-E Business-to-Business Traversal Zone Configuration

Field	Setting
Port	Same port as the one on Expressway-C for the traversal zone
Transport	TLS
TLS Verify	On
TLS Verify subject name	SAN of the Expressway-C cluster name
Media Encryption	Best effort

For the default zone (incoming calls), on Expressway-E, use the recommended settings in Table 7-21.

Table 7-21 Expressway-E Default Zone Configuration

Field	Setting
Enable Mutual TLS on Default Zone	Off
Authentication Policy	Do not check credentials
Media Encryption	Best effort

For the DNS zone (outgoing calls) on Expressway E, use the recommended settings in Table 7-22.

Table 7-22 Expressway-E DNZ Zone Configuration

Field	Setting
TLS Verify	Off
Media Encryption	Best effort

On Unified CM at this point, the SIP trunk security profile should already have been created. Refer to Table 7-11 for details.

Cisco IOS Gateways and Cisco Unified Border Element

This section discusses certificate management first, then it discusses encryption configuration.

Certificate Management

With Cisco IOS Gateways and Cisco Unified Border Element (CUBE), we also recommend using CA-signed certificates.

There are various ways to upload the certificates. The following procedure is based on the manual certificate enrollment using the terminal. Certificates are in PEM (base 64) format.

1. Create an RSA keypair.

   For example: **crypto key generate rsa general-keys label CUBE modulus 2048**

2. Create a PKI trustpoint for Cisco Unified Border Element (CUBE).

   For example, with a manual enrollment using the terminal:

```
crypto pki trustpoint CUBE-Certificate
 enrollment terminal pem
 subject-name CN=US-CUBE1.ent-pa.com
 revocation-check none
 rsakeypair CUBE
 hash sha256
```

3. Authenticate the trustpoint with the CA and accept the CA certificate.

   Basically, this uploads the CA certificate for that trustpoint.

   For example: **crypto pki authenticate CUBE-Certificate**

   And then paste the CA certificate in PEM format.

4. Enroll the trustpoint with the CA server. Basically, this creates the Certificate Signing Request (CSR).

   For example: **crypto pki enroll CUBE-Certificate**

   In this step, you do not have to include the router serial number or the IP address in the subject name.

5. Sign this CSR with the CA.

   Use a CA template that is for Client and Server Web Authentication (TLS Web Client Authentication and TLS Web Server Authentication in the X509v3 Extended Key Usage).

6. Import the certificate that was just generated into the Cisco gateway.

   For example, if you are manually importing the certificate in PEM format using the terminal: **crypto pki import CUBE-Certificate certificate**

   If the Unified CM certificate was not signed by a CA, then the Unified CM CallManager certificate of all the Unified CM call processing subscriber nodes would need to be imported in the Cisco IOS Gateways and Cisco Unified Border Element (CUBE) using a new trustpoint.

Once the certificate management is done, proceed with the encryption configuration.

Encryption Configuration

Follow these steps:

1. Associate the trustpoint with the Cisco IOS voice process.

   For example:

```
sip-ua
 crypto signaling remote-addr [UnifiedCMIPaddress1] [mask] trustpoint CUBE-Certificate
 crypto signaling remote-addr [UnifiedCMIPaddress2] [mask] trustpoint CUBE-Certificate
```

2. Enable TLS transport for the dial-peers.

   For example:

```
dial-peer voice 300 voip
 session protocol sipv2
 session transport tcp tls
```

3. Enable secure signaling.

   For example, to enable secure signaling to/from specific devices, configure the following:

```
sip-ua
 crypto signaling remote-addr [UnifiedCMIPaddress1] [mask] trustpoint CUBE-Certificate
 crypto signaling remote-addr [UnifiedCMIPaddress2] [mask] trustpoint CUBE-Certificate
```

4. Enable SRTP.

   Cisco IOS Gateways and Cisco Unified Border Element (CUBE) support AES_CM_128_HMAC_SHA1_80 and AES_CM_128_HMAC_SHA1_32 (default). To enable AES_CM_128_HMAC_SHA1_80, configure:

```
voice service voip
  sip
    srtp-auth sha1-80
```

   With SRTP pass-thru, stronger ciphers can be used between the source and destination devices, and Cisco Unified Border Element would just forward the packet without processing it. To configure **srtp passthru**, configure:

```
voice service voip
 srtp pass-thru
```

Conferencing

This section describes how to deploy Cisco Meeting Server and Cisco TelePresence Management Suite (TMS) for conferencing services.

Cisco Meeting Server

Cisco Meeting Server does not provide a web interface to manage certificates. Certificate management is done via the mainboard management processor (MMP) commands.

Use the following high-level steps to generate and install the Cisco Meeting Server certificates:

- Generate a single CSR (and private key) for all services. In this CSR, specify the XMPP domain in the CN field and in the SAN extension. Also specify the FQDN of all the Cisco Meeting Server nodes in the SAN extension. Download the private key via SFTP. Sign the CSR by your enterprise CA. Ensure that the Extended Key Usage **Server Authentication** and **Client Authentication** are present. In this guide we refer to this certificate as the *shared certificate*.
- If you are deploying Cisco Meeting Server running the Call Bridge service with no local database, generate a CSR (and private key) for the database client with **CN=postgres**. Download the private key via SFTP. Sign the CSR by your enterprise CA. Ensure that the Extended Key Usage **Client Authentication** is present.
- Upload via SFTP the new shared CA-signed certificate (and associated private key) and CA certificate to all Cisco Meeting Server nodes. Also upload the new database client CA-signed certificate (and associated private key) to the Cisco Meeting Server nodes running the Call Bridge service with no local database.
- Install the certificates.
  - Web Admin: On each node running this service, disable the service, install the shared certificate and associated private key, and then enable the service.
  - Call Bridge: On each node running this service, install the shared certificate and associated private key, and restart the service.
  - XMPP: On each node running this service, disable the service, install the shared certificate and associated private key, and then enable the service
  - Web Bridge: On each node running this service, install the shared certificate and associated private key and the CA certificate, and restart the service.
  - Database server: On each node with a local database, ensure that database clustering is not activated, then install the shared certificate and associated private key. Once this is done, clustering configuration between the nodes can be enabled.
  - Database client: On each node running the Call Bridge service with no local database, ensure that database clustering is not activated, then install the database client certificate and associated private key. Once this is done, clustering configuration between the nodes can be enabled.

The following sections provide examples of the above steps. In those examples, the shared Cisco Meeting Server certificate signed by the enterprise CA is CAsignedCluster.cer, the corresponding private key is CAsignedCluster.key, and the root CA certificate is rootCAcert.cer.

Generate CSRs.

For the database client certificate:

```
pki csr dbclusterclient CN:postgres
```

For the shared certificate:

```
pki csr CAsignedCluster CN:cms.ent-pa.com OU:"TME" O:"Cisco" L:"San Jose"
ST:CaliforniaC:USsubjectAltName:us-acano1.ent-pa.com,us-acano2.ent-pa.com,us-cmsdb.ent
-pa.com,us-cmscb.ent-pa.com, cms.ent-pa.com
```

Install certificates for the various services and Cisco Meeting Server nodes.

On each node running the Web Admin service:

```
webadmin disable
webadmin certs CAsignedCluster.key CAsignedCluster.cer
webadmin enable
```

On each node running the Call Bridge service:

```
callbridge certs CAsignedCluster.key CAsignedCluster.cer
callbridge restart
```

On each node running the XMPP service:

```
xmpp disable
xmpp certs none
xmpp certs CAsignedCluster.key CAsignedCluster.cer
xmpp enable
```

On each node running the Web Bridge service:

```
webbridge disable
webbridge certs CAsignedCluster.key CAsignedCluster.cer
webbridge trust rootCAcert.cer
webbridge enable
```

On each node with a local database:

```
database cluster certs CAsignedCluster.key CAsignedCluster.cer dbclusterclient.key
dbclusterclient.cer rootCAcert.cer
```

On each node running the Call Bridge service but with no local database:

```
database cluster certs dbclusterclient.key dbclusterclient.cer rootCAcert.cer
```

For more information, refer to the latest version of the *Cisco Meeting Server, Certificate Guidelines for Scalable and Resilient Server Deployments*, available at https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html.

On Unified CM, ensure that a SIP trunk security profile is configured with encryption, TLS, and the Cisco Meeting Server XMPP domain name in the X.509 Subject Name, as described in the section on SIP Trunk Encryption. Associate this SIP trunk security profile with all the SIP trunks to CMS nodes running the Call Bridge service.

Cisco Meeting Management

Cisco Meeting Management is installed by default with a self-signed certificate.

Generate a CA-signed certificate with the **CDRreceiveraddress** as well as any addresses your users will use for the browser interface.

The private key and certificate are created outside of Cisco Meeting Management by performing the following steps:

1. Generate a private key using the following command:

   ```
   openssl genrsa -out us-cmm-privatekey.pem 2048
   ```

2. Generate a certificate signing request (CSR) using the private key from step 1:

   ```
   openssl req -new -key us-cmm-privatekey.pem -out us-cmm-certcsr.pem
   ```

3. Enter the data requested, including Country, State or province, Organization name, and so forth.
4. Send the Cisco Meeting Management certificate signing request file, **us-cmm-certcsr.pem**, to be signed by your enterprise certificate authority (CA). You should receive the signed certificate, **us-cmm.cer**, back from the CA.
5. Upload the private key and certificate.
6. Restart Cisco Meeting Management.

Cisco TelePresence Management Suite

The private key and certificate are created outside of Cisco TelePresence Management Suite (TMS). You can do this with OpenSSL, for example, by following these high-level steps:

1. Generate a private key using the following command:

   ```
   openssl genrsa -out us-tms1-privatekey.pem 2048
   ```

2. Generate a certificate signing request (CSR) using the private key above:

   ```
   openssl req -new -key us-tms1-privatekey.pem -out us-tms1-certcsr.pem
   ```

3. Enter the data requested, including Country, State or province, Organization name, and so forth.
4. Send the TMS certificate signing request file, us-tms1-certcsr.pem, to be signed by your enterprise certificate authority (CA). You should receive the signed certificate, us-tms1.cer, back from the CA.
5. Combine the signed certificate with the private key:

   ```
   openssl pkcs12 -export -inkey us-tms1-privatekey.pem -in us-tms1.cer -out
   us-tms1-cert-key.p12 -name us-tms1-cert-key
   ```

6. On TMS, import the root CA certificate into the Certification Authority Trust store. Also import the new TMS certificate and associated private key to the Personal trust store.
7. With Microsoft Management Console (MMC) and the certificate Snap-in, select the certificate you just imported, right-click, and select **All Tasks** > **Manage Private Keys**. Provide read and full control permissions to the users that are used by TMS (in most cases they will be the SERVICE and NETWORK SERVICE users).
8. Go to the TMS tool and in **Security Settings** > **TLS Certificates**, select the new certificate.
9. Go to IIS and configure binding to the new certificate.
10. Restart the IIS and TMS services.

For more information, refer to the latest version of the *Cisco TelePresence Management Suite Administrator Guide*, available at https://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html.

Also refer to the *TMS Certificates with TMS Tools for TLS Communication Configuration Example*, available at https://www.cisco.com/c/en/us/support/docs/conferencing/telepresence-management-suite-tms/118723-configure-tms-00.html.

Collaboration Management Services

Cisco Prime Collaboration Deployment

Cisco Prime Collaboration Deployment does not have a graphical user interface (GUI) for the platform administration. To issue a CA-signed certificate, go to the command line interface (CLI) and issue a CSR. Use the CLI commands **set csr gen tomcat** to generate a CSR, **show csr own tomcat /tomcat.csr** to display the CSR in PEM format, **set cert import trust tomcat** to import CA and/or subordinate CA certificates, and **set cert import own tomcat tomcat-trust/**<*tomcat-certificate-name*> to import the Tomcat certificate.

Restart the Tomcat service with the command **utils service restart Cisco Tomcat**.

Cisco Prime Collaboration Provisioning

Certificate operations are available from **Administration** > **Updates** > **SSL Certificates**. Click on **Generate CSR** to generate a CSR.

The following parameters are used: Key Type RSA, Key length is 2048, and Hash Algorithm is SHA-256. Sign the CSR by your enterprise root CA.

Click on **Upload** to upload the CA-signed PCP certificate and the LDAP certificate.

Then restart Apache via the GUI or the CLI.

For more details, refer to the latest version of the *Cisco Prime Collaboration Provisioning Guide - Standard and Advanced*, available at https://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-user-guide-list.html.

Multi-Cluster Considerations

In a multi-cluster deployment, if clusters are not part of the same data center, enable encryption for the intercluster links.

For the SIP trunks, since our recommendation is to use CA-signed certificates for CallManager, and assuming the same CA is used for the different clusters, there is no need to exchange CallManager or CA certificates between the clusters.

To enable ILS encryption, we recommend using TLS certificates for authentication and using a password for authorization. In the Unified CM ILS configuration page, select the **Use TLS Certificates** option (check the box), select the **Use Password** option (check the box), and enter a password that will be shared between the Unified CM clusters. With the Tomcat certificate signed by the enterprise CA, and with the enterprise root CA certificate (or certificate chain) already in the Tomcat trust store, there are no additional operations required to enable ILS encryption for the certificates.

To enable LBM encryption, simply set the Unified CM Enterprise Parameter **LBM Security Mode** to **Secure**. Again, with the Tomcat certificate signed by the enterprise CA, and with the enterprise root CA certificate already in the Tomcat trust store, there are no additional operations required to enable LBM encryption for the certificates.