# Security and Certificates



# Encryption

## Compliance and Policy Control for File Transfer and Screen Capture

If you send file transfers and screen captures using the Managed file transfer option on Cisco Unified Communications Manager IM and Presence 10.5(2) or later, you can send the files to a compliance server for audit and policy enforcement.

For more information about compliance, see the *Instant Messaging Compliance for IM and Presence Service on Cisco Unified Communications Manager* guide.

For more information about configuring file transfer and screen capture, see the *Cisco Unified Communications Manager IM and Presence Deployment and Installation Guide*.

## Instant Message Encryption

Cisco Jabber uses Transport Layer Security (TLS) to secure Extensible Messaging and Presence Protocol (XMPP) traffic over the network between the client and server. Cisco Jabber encrypts point to point instant messages.

### On-Premises Encryption

The following table summarizes the details for instant message encryption in on-premises deployments.

| Connection | Protocol | Negotiation Certificate | Expected Encryption Algorithm |
|---|---|---|---|
| Client to server | XMPP over TLS v2 | X.509 public key infrastructure certificate | AES 256 bit |

### Server and Client Negotiation

The following servers negotiate TLS encryption with Cisco Jabber using X.509 public key infrastructure (PKI) certificates with the following:

- Cisco Unified Presence
- Cisco Unified Communications Manager

After the server and client negotiate TLS encryption, both the client and server generate and exchange session keys to encrypt instant messaging traffic.

The following table lists the PKI certificate key lengths for Cisco Unified Presence and Cisco Unified Communications Manager IM and Presence Service.

| Version | Key Length |
|---|---|
| Cisco Unified Communications Manager IM and Presence Service versions 9.0.1 and higher | 2048 bit |
| Cisco Unified Presence version 8.6.4 | 2048 bit |
| Cisco Unified Presence versions lower than 8.6.4 | 1024 bit |

### XMPP Encryption

Cisco Unified Presence and Cisco Unified Communications Manager IM and Presence Service both use 256-bit length session keys that are encrypted with the AES algorithm to secure instant message traffic between Cisco Jabber and the presence server.

If you require additional security for traffic between server nodes, you can configure XMPP security settings on Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service. See the following documents for more information about security settings:

- Cisco Unified Presence—*Configuring Security on Cisco Unified Presence*
- Cisco Unified Communications Manager IM and Presence Service—*Security configuration on IM and Presence*

### Instant Message Logging

You can log and archive instant messages for compliance with regulatory guidelines. To log instant messages, you either configure an external database or integrate with a third-party compliance server. Cisco Unified Presence and Cisco Unified Communications Manager IM and Presence Service do not encrypt instant messages that you log in external databases or in third party compliance servers. You must configure your external database or third party compliance server as appropriate to protect the instant messages that you log.

See the following documents for more information about compliance:

- Cisco Unified Presence— *Instant Messaging Compliance Guide*
- Cisco Unified Communications Manager IM and Presence Service—*Instant Messaging Compliance for IM and Presence Service*

For more information about encryption levels and cryptographic algorithms, including symmetric key algorithms such as AES or public key algorithms such as RSA, see *Next Generation Encryption*.

For more information about X.509 public key infrastructure certificates, see the *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* document.

## Cloud-Based Encryption

The following table summarizes the details for instant message encryption in cloud-based deployments:

| Connection | Protocol | Negotiation Certificate | Expected Encryption Algorithm |
|---|---|---|---|
| Client to server | XMPP within TLS | X.509 public key infrastructure certificate | AES 128 bit |
| Client to client | XMPP within TLS | X.509 public key infrastructure certificate | AES 256 bit |

### Server and Client Negotiation

The following servers negotiate TLS encryption with Cisco Jabber using X.509 public key infrastructure (PKI) certificates with the Cisco WebEx Messenger service.

After the server and client negotiate TLS encryption, both the client and server generate and exchange session keys to encrypt instant messaging traffic.

### XMPP Encryption

The Cisco WebEx Messenger service uses 128-bit session keys that are encrypted with the AES algorithm to secure instant message traffic between Cisco Jabber and the Cisco WebEx Messenger service.

You can optionally enable 256-bit client-to-client AES encryption to secure the traffic between clients.

### Instant Message Logging

The Cisco WebEx Messenger service can log instant messages, but it does not archive those instant messages in an encrypted format. However, the Cisco WebEx Messenger service uses stringent data center security, including SAE-16 and ISO-27001 audits, to protect the instant messages that it logs.

The Cisco WebEx Messenger service cannot log instant messages if you enable AES 256 bit client-to-client encryption.

For more information about encryption levels and cryptographic algorithms, including symmetric key algorithms such as AES or public key algorithms such as RSA, see *Next Generation Encryption*.

For more information about X509 public key infrastructure certificates, see the *Internet X.509 Public Key Infrastructure Certificate and CRL Profile* document.

### Client-to-Client Encryption

By default, instant messaging traffic between the client and the Cisco WebEx Messenger service is secure. You can optionally specify policies in the Cisco WebEx Administration Tool to secure instant messaging traffic between clients.

The following policies specify client-to-client encryption of instant messages:

- **Support AES Encoding For IM—**Sending clients encrypt instant messages with the AES 256-bit algorithm. Receiving clients decrypt instant messages.
- **Support No Encoding For IM—**Clients can send and receive instant messages to and from other clients that do not support encryption.

The following table describes the different combinations that you can set with these policies.

| Policy Combination | Client-to-Client Encryption | When the Remote Client Supports AES Encryption | When the Remote Client Does not Support AES Encryption |
|---|---|---|---|
| **Support AES Encoding For IM** = false<br>**Support No Encoding For IM** = true | No | Cisco Jabber sends unencrypted instant messages.<br>Cisco Jabber does not negotiate a key exchange. As a result, other clients do not send Cisco Jabber encrypted instant messages. | Cisco Jabber sends and receives unencrypted instant messages. |
| **Support AES Encoding For IM** = true<br>**Support No Encoding For IM** = true | Yes | Cisco Jabber sends and receives encrypted instant messages.<br>Cisco Jabber displays an icon to indicate instant messages are encrypted. | Cisco Jabber sends encrypted instant messages.<br>Cisco Jabber receives unencrypted instant messages. |
| **Support AES Encoding For IM** = true<br>**Support No Encoding For IM** = false | Yes | Cisco Jabber sends and receives encrypted instant messages.<br>Cisco Jabber displays an icon to indicate instant messages are encrypted. | Cisco Jabber does not send or receive instant messages to the remote client.<br>Cisco Jabber displays an error message when users attempt to send instant messages to the remote client. |

**Note** Cisco Jabber does not support client-to-client encryption with group chats. Cisco Jabber uses client-to-client encryption for point-to-point chats only.

For more information about encryption and Cisco WebEx policies, see *About Encryption Levels* in the Cisco WebEx documentation.

## Encryption Icons

Review the icons that the client displays to indicate encryption levels.

### Lock Icon for Client to Server Encryption

In both on-premises and cloud-based deployments, Cisco Jabber displays the following icon to indicate client to server encryption:

### Padlock Icon for Client to Client Encryption

In cloud-based deployments, Cisco Jabber displays the following icon to indicate client to client encryption:

## Local Chat History

Cisco Jabber for iPhone and iPad does not encrypt archived instant message stored locally on a mobile device when local chat history is enabled. Disable local chat history if you do not want unencrypted instant messages to be stored locally.

Cisco Jabber for Android does not encrypt archived instant message stored locally on a mobile device when local chat history is enabled. Disable local chat history if you do not want unencrypted instant messages to be stored locally.

If you enable local chat history, Cisco Jabber for Windows does not archive instant messages in an encrypted format. In order to restrict access to chat history, the client saves archives to the following directory: `%USERPROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\History\uri.db`.

If you enable local chat history, Cisco Jabber for Mac does not archive instant messages in an encrypted format. In order to restrict access to chat history, Cisco Jabber saves archives to the following directory: `~/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/History/uri.db`.

For on-premises deployment, if you select the **Save chat archives to:** option in the **Chat Preferences** window of Cisco Jabber for Mac, chat history is stored locally in the Mac file system and can be searched using Spotlight.

Chat history is retained after participants close the chat window and until participants sign out. If you do not want to retain chat history after participants close the chat window, set the Disable_IM_History parameter to true. This parameter is available to all clients except IM-only users.

# Voice and Video Encryption

You can optionally set up secure phone capabilities for all devices. Secure phone capabilities provide secure SIP signaling, secure media streams, and encrypted device configuration files.

If you enable secure phone capabilities for users, device connections to Cisco Unified Communications Manager are secure. However, calls with other devices are secure only if both devices have a secure connection.

# Federal Information Processing Standards

**Note** This section applies to Cisco Jabber for Windows only.

The Federal Information Processing Standard (FIPS) 140 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules, including the set of hardware, software, and firmware that implements approved security functions and is contained within the cryptographic boundary.

FIPS requires that all encryption, key exchange, digital signatures, and hash and random number generation functions used within Cisco Jabber for Windows be compliant with the FIPS 140.2 requirements for the security of cryptographic modules.

Cisco Jabber for Windows is compliant with FIPS 140.2. In order to run the client in FIPS mode, you must enable FIPS on your Windows operating system. The client detects that the operating system is in FIPS mode and runs in FIPS mode.

FIPS mode results in the client managing certificates more strictly. Users in FIPS mode may see certificate errors in the client if a certificate for a service expires and users do not reenter their credentials before they expire. Users also see a FIPS icon in their hub window to indicate the client is running in FIPS mode.

# Certificate Validation

### The Certificate Validation Process

Cisco Jabber validates server certificates when authenticating to services. When attempting to establish secure connections, the services present Cisco Jabber with certificates. Cisco Jabber validates the presented certificate against what is in the client device's local certificate store. If the certificate is not in the certificate store, the certificate is deemed untrusted and Cisco Jabber prompts the user to accept or decline the certificate.

If the user accepts the certificate, Cisco Jabber connects to the service and saves the certificate in the certificate store or keychain of the device . If the user declines the certificate, Cisco Jabber does not connect to the service and the certificate is not saved to the certificate store or keychain of the device.

If the certificate is in the local certificate store of the device, Cisco Jabber trusts the certificate. Cisco Jabber connects to the service without prompting the user to accept or decline the certificate.

Cisco Jabber authenticates to two services on the Cisco Unified Communications Manager server. The service names are Cisco Tomcat and Extensible Messaging and Presence Protocol (XMPP). A certificate signing request (CSR) must be generated for each service. Some public certificate authorities do not accept more than one CSR per fully qualified domain name (FQDN). Which means that the CSR for each service may need to be sent to separate public certificate authorities.

Ensure that you specify FQDN in the service profile for each service, instead of the IP address or hostname.

### Signed Certificates

Certificates can be signed by the certificate authority (CA) or self-signed.

- CA-signed certificates—Users are not prompted because you are installing the certificate on the devices yourself. CA-signed certificates can be signed by a Private CA or a Public CA. Many certificates that are signed by a Public CA are stored in the certificate store or keychain of the device.
- Self-signed certificates—Certificates are signed by the services that are presenting the certificates, and users are always prompted to accept or decline the certificate.

**Note** We recommend that you don't use self-signed certificates.

### Certificate Validation Options

Before setting up certificate validation, you must decide how you want the certificates to be validated:

- Whether you are deploying certificates for on-premises or cloud-based deployments.
- What method you are using to sign the certificates.
- If are you deploying CA-signed certificates, whether you are going to use public CA or private CA.
- Which services you need to get certificates for.

# Required Certificates for On-Premises Servers

On-premises servers present the following certificates to establish a secure connection with Cisco Jabber:

| Server | Certificate |
|---|---|
| Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service | HTTP (Tomcat)<br>XMPP |
| Cisco Unified Communications Manager | HTTP (Tomcat) and CallManager certificate (secure SIP call signaling for secure phone) |
| Cisco Unity Connection | HTTP (Tomcat) |
| Cisco WebEx Meetings Server | HTTP (Tomcat) |

| Server | Certificate |
|---|---|
| Cisco VCS Expressway<br>Cisco Expressway-E | Server certificate (used for HTTP, XMPP, and SIP call signaling) |

### Important Notes

- Security Assertion Markup Language (SAML) single sign-on (SSO) and the Identity Provider (IdP) require an X.509 certificate.
- You should apply the most recent Service Update (SU) for Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service before you begin the certificate signing process.
- The required certificates apply to all server versions.
- Each cluster node, subscriber, and publisher, runs a Tomcat service and can present the client with an HTTP certificate.

  You should plan to sign the certificates for each node in the cluster.
- To secure SIP signaling between the client and Cisco Unified Communications Manager, you should use Certification Authority Proxy Function (CAPF) enrollment.

# Certificate Signing Request Formats and Requirements

A public certificate authority (CA) typically requires a certificate signing request (CSR) to conform to specific formats. For example, a public CA might only accept CSRs that have the following requirements:

- Are Base64-encoded.
- Do not contain certain characters, such as `@&!`, in the **Organization**, **OU**, or other fields.
- Use specific bit lengths in the server's public key.

If you submit CSRs from multiple nodes, public CAs might require that the information is consistent in all CSRs.

To prevent issues with your CSRs, you should review the format requirements from the public CA to which you plan to submit the CSRs. You should then ensure that the information you enter when configuring your server conforms to the format that the public CA requires.

**One Certificate Per FQDN—**Some public CAs sign only one certificate per fully qualified domain name (FQDN).

For example, to sign the HTTP and XMPP certificates for a single Cisco Unified Communications Manager IM and Presence Service node, you might need to submit each CSR to different public CAs.

# Revocation Servers

To validate certificates, the certificate must contain an HTTP URL in the **CDP** or **AIA** fields for a reachable server that can provide revocation information. If a certificate authority (CA) revokes a certificate, the client does not allow users to connect to that server.

Users are not notified of the following outcomes:

- The certificates do not contain revocation information.
- The revocation server cannot be reached.

To ensure that your certificates are validated when you get a certificate issued by a CA, you must meet one of the following requirements:

- Ensure that the **CRL Distribution Point** (CDP) field contains an HTTP URL to a certificate revocation list (CRL) on a revocation server.
- Ensure that the **Authority Information Access** (AIA) field contains an HTTP URL for an Online Certificate Status Protocol (OCSP) server.

# Server Identity in Certificates

As part of the signing process, the CA specifies the server identity in the certificate. When the client validates that certificate, it checks that:

- A trusted authority has issued the certificate.
- The identity of the server that presents the certificate matches the identity of the server specified in the certificate.

**Note** Public CAs generally require a fully qualified domain name (FQDN) as the server identity, not an IP address.

### Identifier Fields

The client checks the following identifier fields in server certificates for an identity match:

- XMPP certificates
  - `SubjectAltName\OtherName\xmppAddr`
  - `SubjectAltName\OtherName\srvName`
  - `SubjectAltName\dnsNames`
  - `Subject CN`
- HTTP certificates
  - `SubjectAltName\dnsNames`
  - `Subject CN`

**Tip** The `Subject CN` field can contain a wildcard (`*`) as the leftmost character, for example, `*.cisco.com`.

### Prevent Identity Mismatch

If users attempt to connect to a server with an IP address, and the server certificate identifies the server with an FQDN, the client cannot identify the server as trusted and prompts the user.

If your server certificates identify the servers with FQDNs, you should plan to specify each server name as FQDN throughout your environment.

## Certificates for Multiserver SANs

If you use a multiserver SAN, you only need to upload a certificate to the service once per cluster per tomcat certificate and once per cluster per XMPP certificate. If you do not use a multiserver SAN, then you must upload the certificate to the service for every Cisco Unified Communications Manager node.

# Certificate Requirements for Cloud-Based Servers

Cisco WebEx Messenger and Cisco WebEx Meeting Center present the following certificates to the client:

- Central Authentication Service (CAS)
- WLAN Authentication and Privacy Infrastructure (WAPI)

**Important** Cisco WebEx certificates are signed by a public certificate authority (CA). Cisco Jabber validates these certificates to establish secure connections with cloud-based services.

As of Cisco Jabber for Windows 9.7.2 and Cisco Jabber for Mac 9.6.1, Cisco Jabber validates the XMPP certificate received from Cisco WebEx Messenger. If your operating system does not contain the following certificates for Cisco WebEx Messenger, you must provide them:

- VeriSign Class 3 Public Primary Certification Authority—G5 (stored in the Trusted Root Certificate Authority)
- VeriSign Class 3 Secure Server CA—G3 (stored in the Intermediate Certificate Authority)

The same set of certificates are applicable for Cisco Jabber for Android, iPhone and iPad.

The certificate that is stored in the Intermediate Certificate Authority validates the Cisco WebEx Messenger server identity.

For Cisco Jabber for Windows 9.7.2 or later, you can find more information and installation instructions for the root certificate at http://www.identrust.co.uk/certificates/trustid/install-nes36.html.

For Cisco Jabber for Mac 9.6.1 or later and iOS, you can find more information for the root certificate on the Apple support website at https://support.apple.com.