Security

- Security, on page 1

Security

Set Internet Explorer Security Options

To download certificates from the server, ensure your Internet Explorer security settings are configured as follows:

Step 1 Start Internet Explorer.

Step 2 Navigate to **Tools** > **Internet Options**.

Step 3 Click the **Advanced** tab.

Step 4 Scroll down to the Security section on the Advanced tab.

Step 5 If necessary, clear the **Do not save encrypted pages to disk** check box.

Step 6 Click **OK**.

Manage Certificates and Certificate Trust Lists

The following topics describe the functions that you can perform from the Certificate Management menu:

Note To access the Security menu items, you must log in to Cisco Unified Communications Operating System Administration again with your administrator password.

Display Certificates

To display existing certificates, follow this procedure:

Step 1 Navigate to **Security** > **Certificate Management**.

The Certificate List window displays.

Step 2 You can use the Find controls to filter the certificate list.

Step 3 To view details of a certificate or trust store, click its file name of the certificate under Common Name..

The Certificate Details window displays information about the certificate. The SHA-512 checksum value is also displayed for the certificate to check the file integrity.

Step 4 To return to the Certificate List window, click Close on Certificate Details window.

Download a Certificate

To download a certificate from the Cisco Unified Communications Operating System to your PC, follow this procedure:

Step 1 Navigate to **Security** > **Certificate Management**.

The Certificate List window displays.

Step 2 You can use the Find controls to filter the certificate list.

Step 3 Click the file name of the certificate under Common Name.

The Certificate Details window displays.

Step 4 Click **Download** .PEM File or Download .DER File.

Step 5 In the File Download dialog box, click **Save**.

Delete and Regenerate a Certificate

These sections describe deleting and regenerating a certificate.

Deleting a Certificate

To delete a trusted certificate, follow this procedure:

Caution Deleting a certificate can affect your system operations. Any existing CSR for the certificate that you select from the Certificate list gets deleted from the system, and you must generate a new CSR. For more information, see the Generating a Certificate Signing Request.

Step 1 Navigate to **Security** > **Certificate Management**.

The Certificate List window displays.

Step 2 You can use the Find controls to filter the certificate list.

Step 3 Click the file name of the certificate under Common Name.

The Certificate Details window displays.

Step 4 Click **Delete**.

Regenerating a Certificate

To regenerate a certificate, follow this procedure:

Caution Regenerating a certificate can affect your system operations.

Step 1 Navigate to **Security** > **Certificate Management**.

The Certificate List window displays.

Step 2 Click **Generate Self-signed** > **or** > **Generate CSR**.

The Generate Certificate dialog box opens.

Step 3 Select a certificate name from the Certificate Name list. For a description of the certificate names that display, see Table 1: Certificate Names and Descriptions.

Step 4 Click **Generate**.

Note After you regenerate certificates in Cisco Unified Communications Operating System, you must perform a backup so that the latest backup contains the regenerated certificates. For information on performing a backup, refer to the *Install, Upgrade and Maintenance Guide for Cisco Unity Connection*.

Table 1: Certificate Names and Descriptions

Name	Description
tomcat	This self-signed root certificate gets generated during installation for Unity Connection server and the certificate type is RSA key based.
ipsec	This self-signed root certificate gets generated during installation for IPSec connections with MGCP and H.323 gateways.
tomcat-ECDSA	This self-signed root certificate gets generated during installation for Unity Connection server and the certificate type is EC key based. **Note** CallManager is used only in the naming convention of the certificate, however, the certificate generated is specific to Unity Connection Server.

Using Third-Party CA Certificates

Single-server and Multi-server Certificates Overview

As the name suggests, Single-server certificate contains single FQDN which identifies the trust for that FQDN only. The single FQDN or domain is present in Subject Alternative Name (SAN) extensions. If there are multiple servers in a cluster, then the system requires the generation of an equal number of X.509 certificates, one for each server.

The system uses a multi-server certificate to identify the trust for multiple servers or domains or sub-domains. The SAN extensions of a multi-server certificate contain multiple FQDNs or domains.

Note For telephony integration, multi-server SAN certificate is supported only with SIP integration. However, with SCCP integration, only single-server certificate is supported.

The following table describes the basic differences between single-server and multi-server certificates.

Table 2: Configuration Comparison of Certificates

Single-server certificate	Multi-server certificate
It contains a single FQDN or domain in either the CN field and/or SAN extensions.	It contains multiple FQDNs or domains present in SAN extensions.
The system uses a single certificate for each server in a cluster.	A single certificate identifies multiple servers.
The administrator regenerates the certificate and private key on each individual server in situations such as certificate expiry, private key compromise, etc.	Since this certificate covers only one public and private key pair common to all servers, it requires secure transfer of same private key to all the servers in a cluster along with the certificate. If the private key is compromised on any server, the certificate and private key needs to be regenerated for all the servers.
Generation of single server certificate can become an overhead for the administrator in a large cluster because the administrator needs to perform steps such as generate Certificate Signing Request (CSR), send CSR to CA for signing, upload signed certificate etc for each of the servers in the cluster.	There is less overhead for the administrator in managing multi-server certificates since he or she performs the steps only once on a given server, and the system distributes the associated private key and signed certificates to all the servers in the cluster.

Cisco Unified Communications Operating System supports certificates that a third-party Certificate Authority (CA) issues with PKCS # 10 Certificate Signing Request (CSR).

The following table provides an overview of this process, with references to additional documentation:

	Task	For More Information
Step 1	Login to Cisco Unified Communications Operating System Administration window.	Cisco Unified Communications Operating System Administration allows the system administrator to select the distribution type, when generating a CSR for the individual certificate purposes that supports the multi-server option. The system automatically populates the CSR with the required SAN entries and displays the default SAN entries on the screen. On generating a multi-server CSR, the system automatically distributes that CSR to all the required servers in the cluster. Similarly, on upload of a multi-server CA signed certificate, the system automatically distributes that certificate to all the required servers in the cluster
Step 2	Generate a CSR on the server.	See the Generating a Certificate Signing Request.
Step 3	Download the CSR to your PC.	See the Downloading a Certificate Signing Request.
Step 4	Use the CSR to obtain an application certificate from a CA.	Get information about obtaining application certificates from your CA. See Third-Party CA Certificates for additional notes.
Step 5	Obtain the CA root certificate.	Get information about obtaining a root certificate from your CA. See Third-Party CA Certificates for additional notes.
Step 6	Upload the CA root certificate to the server.	See the Upload Trust Certificate.
Step 7	Upload the application certificate to the server.	See the Upload Application Certificate.

	Task	For More Information
Step 8	Restart the services that are affected by the new certificate.	For all certificate types, restart the corresponding service: • If you update Tomcat certificate, you must restart the Cisco tomcat service, Connection IMAP Server, Cisco Dirsync service, Connection Jetty service, SMTP service and Connection Conversation Manager service. • If you update tomcat-ECDSA certificate, you must also restart the Connection Conversation Manager service. See the Cisco Unified Communications Manager Serviceability Administration Guide for information about restarting services.

Generating a Certificate Signing Request

To regenerate a certificate signing request, follow this procedure:

Step 1 Select **Security** > **Certificate Management**.

The Certificate List window displays.

Step 2 Use the find control to filter the certificate list.

Step 3 Click **Generate CSR**, the Generate Certificate Signing Request dialog box opens.

Step 4 From the Certificate Purpose drop-down list box, select the required certificate purpose.

Step 5 From the Distribution drop-down list box, select the required distribution list item.

Note The Multi-server (SAN) option is available only when you select tomcat or tomcat-ECDSA from the Certificate Purpose drop-down list box. Click **Generate CSR**.

By default, the system populates the CN field with the server FQDN (or hostname). You can modify the value, if required. For self-signed certificate, the CN is not configurable.

Step 6 For Multi-server (SAN), additional domains can be added in Subject Alternate Names field.

Step 7 From the Key Length drop-down list box, select value as per the certificate purpose.

- If tomcat or ipsec is the certificate purpose, select 1024, 2048, 3072, or 4096.
- If tomcat-ECDSA is the certificate purpose, select 256, 384 or 521.

Step 8 From the Hash Algorithm drop-down list box, select as per the certificate purpose.

- If tomcat or ipsec is the certificate purpose, select SHA1 or SHA256.
- If tomcat-ECDSA is the certificate purpose, select SHA384 SHA512.

Step 9 Click Generate to generate a new CSR.

Note The new CSR that is generated for a specific certificate type overwrites any existing CSR for that type. The CSR is automatically distributed to all the required servers in the cluster.

Downloading a Certificate Signing Request

To download a Certificate Signing Request, follow this procedure:

Step 1 Select **Security** > **Certificate Management**.

The Certificate List window displays.

Step 2 From the list, click the Common Name of the entry with type 'CSR Only' and a Distribution value matching the Common Name.

Note For multi-server SAN certificate, click the Common Name of the entry with type 'CSR Only' and a Distribution value of 'Multi-Server (SAN)'.

The CSR Details window appears.

Step 3 Click **Download CSR**.

Step 4 After the CSR download completes, click Close.

You need to restart the tomcat service after configuring the Multi-server SAN certificate on both Publisher and Subscriber in a cluster. See the procedure below:

Step 1 Sign in to the Unity Connection server with an SSH application.

Step 2 Run the following CLI command to restart the Tomcat service:

utils service restart Cisco Tomcat

Third-Party CA Certificates

To use an application certificate that a third-party CA issues, you must obtain both the signed application certificate and the CA root certificate from the CA or PKCS#7 Certificate Chain (DER format), which contains both the application certificate and CA certificates. Retrieve information about obtaining these certificates from your CA. The process varies among CAs.

Cisco Unified Operating System Administration generates CSRs in PEM encoding format. The system accepts certificates in DER and PEM encoding formats and PKCS#7 Certificate chain in PEM format. For all certificate types, you must obtain and upload a CA root certificate and an application certificate on each node.

Cisco Unified Operating System Administration CSRs include extensions that you must include in your request for an application certificate from the CA. If your CA does not support the ExtensionRequest mechanism, you must enable the X.509 extensions, shown as follows:

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment
```

Note You can generate a certificate signing request (CSR) for your certificates and have them signed by a third party CA with a SHA256 signature. You can then uploads this signed certificate back to Cisco Unified Operating System Administration, allowing for Tomcat and other certificates to be support SHA256.

Upload Trust Certificate

To upload a trust certificate, follow this procedure:

Step 1 Navigate to **Security** > **Certificate Management**.

The Certificate List window displays.

Step 2 Click **Upload Certificate/Certificate Chain**.

The Upload Certificate Trust List dialog box opens.

Step 3 Select the certificate name from the **Certificate Purpose** drop-down list.

Step 4 Enter the name of the CA root certificate in the **Description** text box.

Step 5 Select the file to upload, click the **Browse** button and navigate to the file; then, click **Open**.

Step 6 To upload the file to the server, click the **Upload** button.

Note In case of trust certificate, the system automatically distributes the certificate to other nodes of the cluster.

Upload Application Certificate

Cisco Unified Communications Operating System supports certificates that a third-party CA issues with PKCS#10 Certificate Signing Request (CSR).

Step 1 Generate a CSR on the server.

Step 2 Download the CSR to your PC.

Step 3 Use the CSR to obtain an application certificate from a CA or PKCS#7 format certificate chain, which may contain application certificate along with CA certificate.

Step 4 Obtain the CA certificate or certificate chain.

To upload tomcat application certificate, select **tomcat** from Certificate Purpose list.

To upload ipsec application certificate, select **ipsec** from Certificate Purpose list.

To upload tomcat-ECDSA application certificate, select **tomcat-ECDSA** from Certificate Purpose list.

Step 5 Select the certificate from the **Certificate Purpose** drop-down list.

Step 6 Select the file to upload, click the **Browse** button and navigate to the file; then, click **Open**.

Step 7 To upload the file to the server, click the **Upload** button.

Note The system does not distribute application certificates to other cluster nodes automatically. If you need to have the same certificate on more than one node, you must upload the certificate to each node individually. However, in case of SAN certificate, the system distributes the certificates to other cluster nodes automatically.

Monitor Certificate Expiration Dates

The system can automatically send you an e-mail when a certificate is close to its expiration date. To view and configure the Certificate Expiration Monitor, follow this procedure:

Step 1 To view the current Certificate Expiration Monitor configuration, navigate to **Security** > **Certificate Monitor**.

The Certificate Monitor window displays.

Step 2 Enter the required configuration information. See Table 3: certificatesexpiration monitor fields (table)Certificate Monitor Field Descriptions for a description of the Certificate Monitor Expiration fields.

Step 3 To save your changes, click **Save**.

Table 3: Certificate Monitor Field Descriptions

Field	Description
Notification Start Time	Enter the number of days before the certificate expires that you want to be notified.
Notification Frequency	Enter the frequency for notification, either in hours or days.
Enable E-mail Notification	Select the check box to enable e-mail notification.
Email IDs	Enter the e-mail address to which you want notifications sent. **Note** For the system to send notifications, you must configure an SMTP host.

Certificate Revocation

You can use the Online Certificate Status Protocol (OCSP) to obtain the revocation status of the certificate.

To configure OCSP, follow this procedure:

Step 1 Navigate to **Security** > **Certificate Management**.

The Certificate List window displays.

Step 2 Check the Enable OCSP check box in the Online Certificate Status Protocol Configuration area.

Step 3 Choose Use OCSP URI from Certificate if the certificate is configured with OCSP URI and that to be used to contact OCSP Responder.

Step 4 Choose Use configured OCSP URI if external or configured URI is used to contact OCSP Responder. Enter the URI of the OCSP Responder, where certificate revocation status is verified, in the OCSP Configured URI field.

Step 5 Check the check box for Enable Revocation Check to perform the revocation check.

Note The certificate revocation service is active for LDAP and IPSec connections, when revocation and expiry check enterprise parameter is set to enabled.

Step 6 Enter the Check Every value to check the periodicity of the certificate revocation status.

- Click Hours or Days to check the revocation status hourly or daily.

Step 7 Click Save.

Warning You must upload the OCSP Responder certificate to tomcat-trust before enabling OCSP.

Note The Certificate revocation status check is performed only during upload of a Certificate or Certificate chain and the appropriate alarm will be raised if a certificate is revoked.

The Cisco Certificate Expiry Monitor service must be restarted to ensure certificate revocation. Navigate to Cisco Unified Serviceability > Tool > Control Center - Network Services and restart the Cisco Certificate Expiry Monitor service.

Generating IPSEC Certificate

To generate or regenerate the ipsec certificate on standalone or cluster, follow this procedure:

Step 1 Navigate to **Security** > **Certificate Management**.

The Certificate List window displays.

Step 2 Click **Generate Self-signed** > or > **Generate CSR**.

The Generate Certificate dialog box opens.

Step 3 Select ipsec from the **Certificate Purpose** drop-down list.

Step 4 Click **Generate**.

After generating the certificate, ipsec and ipsec trust will be updated with the certificate for standalone or publisher server.

Step 5 In case of subscriber server, follow Step 1 to Step 4 for generating ipsec certificate. After generating, download the ipsec certificate from subscriber server.

Step 6 Navigate to **Security** > **Certificate Management** on subscriber server.

Step 7 Click **Upload Certificate/Certificate Chain**.

The Upload Certificate Trust List dialog box opens.

Step 8 Select the ipsec-trust from the **Certificate Purpose** drop-down list.

Step 9 Browse the certificate and click **Upload**.

Step 10 After uploading the ipsec certificate to subscriber server, restart the below services first on publisher server and then subscriber server.

- Cisco DRF Master
- Cisco DRF Local

IPSEC Management

The following topics describe the functions that you can perform with the IPSec menu:

Note IPSec does not automatically get set up between nodes in the cluster during installation.

Set Up a New IPSec Policy

To set up a new IPSec policy and association, follow this procedure:

Note Do not modify or create IPSec policies during an upgrade because any changes that you make to an IPSec policy during a system upgrade gets lost.

Caution IPSec affects the performance of your system, especially with encryption.

Step 1 Navigate to **Security** > **IPSEC Configuration**.

The IPSEC Policy List window displays.

Step 2 Click **Add New**.

The IPSEC Policy Configuration window displays.

Step 3 Enter the appropriate information on the IPSEC Policy Configuration window. For a description of the fields on this window, see Table 4: IPSecpolicy fields (table)IPSEC Policy and Association Field Descriptions.

Step 4 To set up the new IPSec policy, click **Save**.

Table 4: IPSEC Policy and Association Field Descriptions

Field	Description
Policy Group Name	Specifies the name of the IPSec policy group. The name can contain only letters, digits, and hyphens.
Policy Name	Specifies the name of the IPSec policy. The name can contain only letters, digits, and hyphens.

Field	Description
Authentication Method	Specifies the authentication method.
Preshared Key	Specifies the preshared key if you selected Pre-shared Key in the Authentication Name field. **Note** Pre-shared IPSec keys can contain alphanumeric characters and hyphens only, not white spaces or any other characters. If you are migrating from a Windows-based version of Cisco Unified Communications Manager, you may need to change the name of your pre-shared IPSec keys, so they are compatible with current versions of Cisco Unified Communications Manager.
Peer Type	Specifies whether the peer is the same type or different.
Destination Address	Specifies the IP address or FQDN of the destination.
Destination Port	Specifies the port number at the destination.
Source Address	Specifies the IP address or FQDN of the source.
Source Port	Specifies the port number at the source.
Mode	Specifies Transport mode.
Remote Port	Specifies the port number to use at the destination.
Protocol	Specifies the specific protocol, or Any: • TCP • UDP • Any
Encryption Algorithm	From the drop-down list, select the encryption algorithm. Choices include • DES • 3DES
Hash Algorithm	Specifies the hash algorithm • SHA1—Hash algorithm that is used in phase 1 IKE negotiation • MD5—Hash algorithm that is used in phase 1 IKE negotiation

Field	Description
ESP Algorithm	From the drop-down list select the ESP algorithm. Choices include • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
Phase One Life Time	Specifies the lifetime for phase One, IKE negotiation, in seconds.
Phase One DH	From the drop-down list, select the phase One DH value. Choices include: 2, 1, and 5.
Phase Two Life Time	Specifies the lifetime for phase Two, IKE negotiation, in seconds.
Phase Two DH	From the drop-down list, select the phase Two DH value. Choices include: 2, 1, and 5.
Enable Policy	Check the check box to enable the policy.

Managing Existing IPSec Policies

To display, enable or disable, or delete an existing IPSec policy, follow this procedure:

Note Do not modify or create IPSec policies during an upgrade because any changes made to an IPSec policy during a system upgrade, gets lost.

Caution IPSec affects the performance of your system, especially with encryption.

Caution Any changes that you make to the existing IPSec policies can impact your normal system operations.

Step 1 Navigate to **Security** > **IPSEC Configuration**.

Note To access the Security menu items, you must log in to Cisco Unified Communications Operating System Administration again with your Administrator password.

The IPSEC Policy List window displays.

Step 2 To display, enable, or disable a policy, follow these steps:

a) Click the policy name.

The IPSEC Policy Configuration window displays.

b) To enable or disable the policy, use the **Enable Policy** check box.

c) Click **Save**.

Step 3 To delete one or more policies, follow these steps:

a) Check the check box next to the policies that you want to delete.

You can click **Select All** to select all policies or **Clear All** to clear all the check boxes.

b) Click **Delete Selected**.

Bulk Certificate Management

To support the Extension Mobility Cross Cluster (EMCC) feature, the system allows you to execute a bulk import and export operation to and from a common SFTP server that has been configured by the cluster administrator. For more information about using Bulk Certificate Management, see the *Cisco Unified Communications Manager Security Guide.*

For Bulk Certificate Management, use the following procedure:

Step 1 Navigate to **Security** > **Bulk Certificate Management**. The Bulk Certificate Management window displays.

Step 2 Enter the appropriate information on the Bulk Certificate Management window. For a description of the fields on this window, see Table 5: Bulk Certificate Management Field Description.

Step 3 To save the values you entered, click **Save**

Step 4 To export certificates, click **Export**. The Bulk Certificate Export popup window displays.

Step 5 From the drop-down menu, choose the type of certificate you want to export:

- Tomcat
- TFTP
- All

Step 6 Click **Export**.

The system exports and stores the certificates you chose on the central SFTP server.

Table 5: Bulk Certificate Management Field Description

Field	Description
IP Address	Enter the IP address of the common server where you want to export the certificates

Field	Description
Port	Enter the port number. Default: 22
User ID	Enter the User ID you want to use to log into the server.
Password	Enter the appropriate password.
Directory	Enter a directory on the server where you want to save the certificates. Example: /users/cisco.

Session Management

Platform Administrator is allowed to terminate the active web sessions of a user or administrator for the following web interfaces of Cisco Unity Connection:

- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability
- Cisco Personal Communications Assistant
- Cisco Unity Connection Web Inbox
- Cisco Unity Connection SRSV

To terminate the active web sessions of a user or administrator, use the following procedure:

Step 1 Navigate to **Security** > **Session Management**. The Session Management window displays.

Step 2 On the Session Management window, enter the alias of the active logged-in user in **User ID** field.

Step 3 Select **Terminate Session** to terminate the active web sessions of the user.

Note In case of a cluster, you must terminate the web sessions for each node of the cluster.

Note Session termination is not applicable for platform users. To terminate the active web sessions, platform user must logout the sessions or wait until the sessions are timed out.

Cipher Management

Cisco Unity Connection supports **Cipher Management** that allows administrator to control set of ciphers that are used for every TLS and SSH connection. You can configure the recommended ciphers for various secure interfaces of Cisco Unity Connection.

TLS Interfaces

You can configure ciphers for the TLS interfaces mentioned in below.

Interfaces	Description
All TLS	You can configure the ciphers for all supported TLS interfaces of Cisco Unity Connection. Example: SIP, SCCP, HTTPS, Jetty, SMTP, LDAP and IMAP inerfaces.
HTTPS TLS	You can configure the ciphers for all Cisco Tomcat interfaces of Cisco Unity Connection.
SIP TLS	You can configure the ciphers for SIP interfaces of Cisco Unity Connection. Example: Telephony User Interface to support secure SIP call in Unity Connection. **Note** Cipher configuration for SIP interface is not supported for unrestricted version of Cisco Unity Connection.

SSH Interfaces

You can configure ciphers and algorithm for the SSH interfaces mentioned below.

Interfaces	Description
SSH Ciphers	You can configure the cipher for SSH interfaces of Cisco Unity Connection.
SSH Key Exchange	You can configure the SSH Key Exchange algorithm for SSH interfaces of Cisco Unity Connection.
SSH MAC	You can configure the SSH MAC algorithm for SSH interfaces of Cisco Unity Connection.

For information on recommended ciphers, see the "Cipher Management" section in the *Security Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Configuring Cipher String

To configure the cipher string for TLS and SSH interfaces, do the following procedure:

Step 1 Navigate to **Security** > **Cipher Management**. The Cipher Management page appears.

Step 2 On the Cipher Management page, enter the cipher string in **Cipher String** field for **All TLS**, **HTTPS TLS** and **SIP TLS** interfaces.

Note The cipher string configured either for **HTTPS TLS** or **SIP TLS** interface overrides the cipher string configured in ALL TLS field.

Note The ciphers configured on the **Cipher Management** page will override the cipher configuration of **Edit General Configuration** page. Hence it is recommended to use **Cipher Management** page for configuring the ciphers for TLS and HTTPS interfaces.

Step 3 Enter the cipher string in **Cipher String** field for SSH Ciphers.

Step 4 Enter the algorithm string in **Algorithm String** field to configure the key algorithm for SSH Key Exchange.

Step 5 Enter the algorithm string in **Algorithm String** field to configure the MAC algorithm for SSH MAC.

Step 6 Select **Save**.

After saving the page, you must do the following:

- Reboot both nodes in the cluster for successful configuration of ciphers on **All TLS**, **SSH Ciphers**, **SSH Key Exchange** and **SSH MAC** interfaces.
- Restart the Cisco Tomcat service for successful configuration of ciphers on **HTTPS TLS** interface.
- Restart the Connection Conversation Manager service for successful configuration of ciphers on **SIP TLS** interface.