Security

This chapter describes Certificate Management and IPSec Management and provides procedures for performing the following tasks:

- Manage Certificates and Certificate Trust Lists
- Display Certificates
- Download a Certificate or CTL
- Delete and Regenerate a Certificate
- Upload a Certificate or Certificate Trust List
- Download a Certificate Signing Request
- Monitor Certificate Expiration Dates
- IPSEC Management
- Display or Change an Existing IPSec Policy
- Set Up a New IPSec Policy

Set Internet Explorer Security Options

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

Procedure

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 Certificate Management menu options allow you to perform the following functions:

- Display certificates
- Upload certificates and Certificate Trust Lists (CTL)
- Download certificates and CTLs
- Delete certificates
- Regenerate certificates
- Download and generate Certificate Signing Requests (CSR)
- Monitor certificate expiration dates

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

Display Certificates

To display existing certificates, follow this procedure:

Procedure

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

The Select Certificates or Trust Store window displays.

Step 2 Check the check box for the type of certificate that you want to display: Own Certificates or Trust Certificates.

The Display Certificates or Trust Units window displays.

Step 3 Check the check box for the certificate type that you want to display.

The Display Certificates or Trust Store window displays.

Step 4 Check the check box for the certificate of trust store that you want to display.

The Details of a Certificate window displays.

Step 5 After you have viewed the certificate details, choose another menu option to close the Details of Certificate window.

Download a Certificate or CTL

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

Procedure

Step 1 Navigate to **Security>Cerificate Management>Download Cert/CTL**.

The Select Certificate/CTL/CSR Download windows displays.

Step 2 Check the check box for the appropriate download type: Own Cert, Trust Cert, or CTL file. Click **Next**.

The Download Certificates or Trust Units window displays.

Step 3 Check the check box for the existing certificate type that you want to download and click **Next**.

The Display Certificate/CTL/CSR Download window displays.

Step 4 Check the check box for existing certificates that you want to download and click **Next**.

The Certificate/CTL/CSR Download window displays.

Step 5 Click the **Continue** link.

A directory listing that shows the certificates that you chose displays.

Step 6 To save the certificate or CTL to your PC, right-click the name of the certificate or CTL and choose **Save As**.

Step 7 Enter the location where you want to save the certificate or CTL.

Step 8 Click **Save**.

Delete and Regenerate a Certificate

Deleting a Certificate

To delete a trusted certificate, follow this procedure:

Caution Deleting a certificate can affect your system operations.

Procedure

Step 1 Navigate to **Security>Certificate Management>Delete/Regenerate Cert**.

Step 2 Check the **Delete Trust Cert** check box and click **Next**.

The Display Certificates or Trust Units For Delete/Regenerate window displays.

Step 3 Check the check box for the existing certificate type that you want to delete and click **Next**.

The Delete Certificates or Trust Store window displays.

Step 4 Check the Existing Certificate Name check box for the certificate that you want to delete and click **Delete.**

Regenerating a Certificate

To regenerate a certificate, follow this procedure:

Caution Regenerating a certificate can affect your system operations.

Procedure

Step 1 Navigate to **Security>Certificate Management>Delete/Regenerate Cert**.

The Select Certificates or Trust Store for Deletion window displays.

Step 2 Check the **Regenerate Self-Signed Cert** check box and click **Next**.

Step 3 Check the appropriate **Existing Certificates Types** check box for the certificate that you want to regenerate, and click **Next**.

Step 4 Check the appropriate **Existing Certificate** check box and click **Regenerate**.

Upload a Certificate or Certificate Trust List

Caution Uploading a new certificate or certificate trust list (CTL) file can affect your system operations.

Note The system does not distribute trust 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.

To upload a CA root certificate, application certificate, or CTL file to the server, follow these steps:

Procedure

Step 1 Navigate to **Security>Certificate Management>Upload Certificate/CTL**.

The Select Certificate/CTL Upload window displays.

Step 2 Choose one of the radio buttons; then, click **Next**:

- Upload Own Cert—To upload an application certificate that is issued by a third party CA.
- Upload Trust Cert—To upload a CA root certificate or a trusted application certificate.
- Upload CTL File—To upload a CTL file.

The Certificate type for the upload including CTL window displays.

Step 3 In the Certificate type for the upload including CTL window, do the following steps:

a. Select the type of certificate or CTL from the **Existing certificate types** list.

b. If you are uploading an application certificate that was issued by a third party CA, enter the name of the CA root certificate in the **Root Cert Name (without any extensions)** text box. If you are uploading a CA root certificate or CTL, leave this text box empty.

c. Click **Next**.

The Upload Certificate/CTL window displays.

Step 4 In the Upload Certificate/CTL window, do the following steps:

a. Select the file to upload by doing one of the following steps:

- In the **File Name for Upload** text box, enter the path to the file.
- Click the **Browse** button and navigate to the file; then, click **Open**.

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

Download a Certificate Signing Request

To download a Certificate Signing Request, follow this procedure:

Procedure

Step 1 Navigate to **Security>Certificate Management>Download/Generate CSR**.

The Select Certificate type for CSR window displays.

Step 2 Check the **Existing Certificate Types** check box for the CSR that you want to download.

Step 3 Check the **Download CSR if any** check box.

The Certificate/CTL/CSR Download window displays.

Step 4 Click **Continue**.

A directory listing shows the certificates that you chose.

Step 5 To save the CSR to your PC, right-click the name of the certificate or CTL and choose **Save As**.

Step 6 Enter the location where you want to save the certificate or CTL.

Step 7 Click **Save**.

Using Third Party CA Certificates

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	Generate a CSR on the server.	See the "Generating a Certificate Signing Request" section on page 6-6.
Step 2	Download the CSR to your PC.	See the "Download a Certificate Signing Request" section on page 6-5.
Step 3	Use the CSR to obtain an application certificate from a CA.	Get information about obtaining application certificates from your CA. See "Obtaining Third-Party CA Certificates" section on page 6-7 for additional notes.
Step 4	Obtain the CA root certificate.	Get information about obtaining a root certificate from your CA. See "Obtaining Third-Party CA Certificates" section on page 6-7 for additional notes.
Step 5	Upload the CA root certificate to the server.	See the "Upload a Certificate or Certificate Trust List" section on page 6-4.
Step 6	Upload the application certificate to the server.	See the "Upload a Certificate or Certificate Trust List" section on page 6-4.
Step 7	If you updated the certificate for CAPF or Cisco Unified CallManager, generate a new CTL file.	See the *Cisco Unified CallManager Security Guide*.
Step 8	Restart the services that are affected by the new certificate.	For all certificate types, restart the corresponding service (for example, restart the Tomcat service if you updated the Tomcat certificate). In addition, if you updated the certificate for CAPF or Cisco Unified CallManager, restart the TFTP service. See the *Cisco Unified CallManager Serviceability Administration Guide* for information about restarting services.

Generating a Certificate Signing Request

To generate a Certificate Signing Request (CSR), follow these steps:

Procedure

Step 1 Navigate to **Security>Certificate Management>Download/Generate CSR**.

The Select Certificate type for CSR window displays.

Step 2 Choose the type of certificate to generate in the **Existing Certificate Types** area.

Step 3 Choose the **Generate a new CSR** radio button.

Step 4 Click **Next**.

The Cert/IPSEC Operation (CSR/Config/Assoc Create) Done window displays and states that the CSR was successfully generated.

Obtaining Third-Party CA Certificates

To use an application certificate that a third party CA issues, you must obtain from the CA both the signed application certificate and the CA root certificate. Get information about obtaining these certificates from your CA. The process varies among CAs.

CAPF and Cisco Unified CallManager 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 that are listed on the final page of the CSR generation process.

Cisco Unified Communications Operating System generates certificates in DER and PEM encoding formats and generates CSRs in PEM encoding format. It accepts certificates in DER and DER encoding formats.

Cisco verified third-party certificates that were obtained from Microsoft, Keon, and Verisign CAs. Certificates from other CAs might work but have not been verified.

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:

Procedure

Step 1 To view the current Certificate Expiration Monitor configuration, navigate to **Security>Certificate Management>Cert Expiry Monitor>Display Config**.

The Show Cert Expiry Monitoring Config window, which shows a summary of the current configuration information, displays.

Step 2 To configure the Certificate Expiration Monitor, navigate to **Security>Certificate Management>Cert Expiry Monitor>Change Config**.

The Change Cert Expiry Monitoring Config window displays.

Step 3 Enter the required configuration information. See Table 6-1 for a description of the Certificate Expiration Monitor fields.

Step 4 To save your changes, click **Submit**.

Table 6-1 Certificate Expiration Monitor Field Descriptions

Field	Description
Notification/Alert Start Time	Enter the number of days before the certificate expires that you want to be notified.
Initial Frequency of Notification	Enter the frequency for notification, either in hours or days.

Table 6-1 Certificate Expiration Monitor Field Descriptions (continued)

Field	Description
Click on the right to Enable/Disable	To turn on e-mail notification, click **Enable**.
Email IDs entered for Notification	Enter the e-mail address to which you want notifications sent. **Note** For the system to send notifications, you must configure an SMTP host.

IPSEC Management

The IPSec menu options allow you to perform the following functions:

- Display or change an existing IPSec policy
- Set up a new IPSec policy

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

Display or Change an Existing IPSec Policy

To display or change an existing IPSec policy, follow this procedure:

Note Because any changes that you make to an IPSec policy during a system upgrade will get lost, do not modify or create IPSec policies during an upgrade.

Caution IPSec, especially with encryption, will affect the performance of you system.

Procedure

Step 1 Navigate to **Security>IPSEC Management>Display/Change IPSEC**.

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

The Display IPSEC Policy window displays.

Step 2 Check the appropriate Existing Policy check box, and click **Next**.

Step 3 Perform one of the following actions:

- To view an IPSec policy, click the **Display Detail** link.
- To delete an IPSec policy, click **Delete**.
- To activate an IPSec policy, click **Enable**.
- To deactivate an IPSec policy, click **Disable**.

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

Step 4 If you click the Display Detail link, the Association Details window displays. For an explanation of the fields in this window, see Table 6-2.

Set Up a New IPSec Policy

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

Note Because any changes you make to an IPSec policy during a system upgrade will get lost, do not modify or create IPSec policies during an upgrade.

Caution IPSec, especially with encryption, will affect the performance of you system.

Procedure

Step 1 Navigate to **Security > IPSEC Management > Setup New IPSEC**.

The Setup Select window displays.

Step 2 Check the **Certificate** or **Pre-Shared Key** check box.

- If you check Certificate, check **Same Type** or **Different Type** node.
- If you check Pre-Shared Key, enter the key name.

Step 3 Click **Next**.

The Setup IPSEC Policy and Association window displays.

Step 4 Enter the appropriate information on the Setup IPSEC Policy and Association window. For a description of the fields on this window, see Table 6-2.

Step 5 To set up the new IPSec policy, click **Submit**.

Table 6-2 IPSEC Policy and Association Field Descriptions

Field	Description
Policy Name	Specifies the name of the IPSec policy.
Dest. Address Type	Specifies the Destination Address Type: • IP—Dotted IP address of the destination • FQDN—Fully qualified domain name of the destination
Source Address Type	Specifies the Source Address Type: • IP—Dotted IP address of the source • FQDN—Fully qualified domain name of the source

Table 6-2 IPSEC Policy and Association Field Descriptions (continued)

Field	Description
Tunnel/Transport	Specifies tunnel or transport.
Protocol	Specifies the specific protocol, or Any: • TCP • UDP • Any
Dest. Port	Specifies the port number to use at the destination.
Phase 1 Life Time in Seconds	Specifies the lifetime for phase 1, IKE negotiation, in seconds.
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
Phase 2 Life Time in Seconds	Specifies the lifetime for phase 2, IKE negotiation, in seconds.
AH Algorithm	Because this field is not functional, use the ESP Algorithm field instead to select an authentication algorithm.
Assoc. Name	Specifies the association name that is given to each IPSec association.
Dest. Address	Specifies the IP address or FQDN of the destination.
Source Address	Specifies the IP address or FQDN of the source.
Remote Port	Specifies the port number at the destination.
Source Port	Specifies the port number at the source.
Encryption Algorithm	From the drop-down list, choose the encryption algorithm. Choices include: • DES • 3DES
Phase 1 DH Value	From the drop-down list, choose the phase 1 DH value. Choices include: 2, 1, 5, 14, 16, 17, and 18.
ESP Algorithm	From the drop-down list, choose the ESP algorithm. Choices include: • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
Phase 2 DH Value	From the drop-down list, choose the phase 2 DH value. Choices include: 2, 1, 5, 14, 16, 17, and 18.