Security

This chapter describes Certificate Management and IPSec Management and provides procedures for managing system security.

Set Internet Explorer Security Settings

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 Option**.

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**.

Certificate Management Menu

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

Display Certificates

To display existing certificates, follow this procedure:

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

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

Step 3 To view details of a certificate or trust certificate, click its file name.
The **Certificate Details** window shows information about the certificate.

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

Download Certificate

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

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

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

Step 3 Click the file name of the certificate.
The **Certificate Details** window appears.

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

Step 5 In the dialog box, click **Save File** to download the certificate.

Delete Certificate

To delete a trusted certificate, follow this procedure:

Caution Deleting a certificate can affect your system operations.

Caution Any existing CSR for the certificate that you choose from the Certificate list is deleted from the system. You must generate a new CSR.

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

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

Step 3 Click the filename of the certificate.
The **Certificate Details** window appears.

Step 4 Click **Delete**.

Note You must restart the Unified CCX server. In the case of high availability deployments, restart both the nodes.

Related Topics

Regenerate Certificate, on page 3

Regenerate Certificate

To regenerate a certificate, follow this procedure:

Caution Regenerating a certificate can affect your system operations.

For certificate regeneration, use the supported key lengths 1024 or 2048 from the list.

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 Click **Generate Self-signed**.
The **Generate New Self-signed Certificate** dialog box opens.

Step 3 Choose a certificate name from the **Certificate Purpose** list.
The following table contains descriptions of the certificate names that appear:

Name	Description
tomcat	This self-signed root certificate is generated during installation for the HTTPS server.
ipsec	This self-signed root certificate is generated during installation for IPSec connections with MGCP and H.323 gateways.

Step 4 Click **Generate**.

Step 5 After you regenerate a certificate, you must restart the Unified CCX server. In the case of high availability deployments, restart both the nodes.

What to Do Next

After you regenerate a certificate in Cisco Unified Communications Operating System, you must perform a backup so that the latest backup contains the regenerated certificates.

Upload Certificate to Server

Caution Uploading a new certificate can affect your system operations. After you upload a new certificate, you must restart the Unified CCX server (in the case of high availability deployments, restart both nodes).

Note The system does not distribute trust certificates to other cluster node automatically. If you must have the same certificate on more than one node, you must upload the certificate to each node individually.

Upload Certificate or Certificate Chain

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 Click **Upload Certificate or Certificate Chain**.
The **Upload Certificate or Certificate Chain** dialog box opens.

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

Step 4 Select the file to upload by performing one of the following steps:

- In the **File Upload** text box, enter the path to the file, or
- Click the **Browse** button and navigate to the file; then, click **Open**.
  Cisco Unified CCX supports Privacy Enhanced Mail (PEM) Base64 encoded format of X.509 certificate (only one PEM certificate in a file), Distinguished Encoding Rules (DER) format of X509 Certificate and DER format of PKCS#7 (Public-Key Cryptography Standards) Certificate Chain. The system does not support PEM format of PKCS#7 Certificate Chain.

Step 5 Click the **Upload** button to upload the file to the server.

Note After you upload a certificate, you must restart the Unified CCX server. In the case of high availability deployments, restart both the nodes.

Directory Trust Certificate

Note Uploading a Directory Trust Certificate is not applicable for Unified CCX.

Obtain 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 more documentation:

Procedure

Step 1 Generate a CSR on the server.
See Generate Certificate Signing Request, on page 5.

Step 2 Download the CSR to your PC.
See Download Certificate Signing Request, on page 6.

Step 3 Use the CSR to obtain an application certificate from a CA.
Get information about obtaining application certificates from your CA. See Application Certificates, on page 6 for more notes.

Step 4 Obtain the CA root certificate.
Get information about obtaining a root certificate from your CA. See Application Certificates, on page 6 for more notes.

Step 5 Upload the CA root certificate to the server.
See Upload Certificate or Certificate Chain, on page 4.

Step 6 Upload the application certificate to the server.
See Application Certificates, on page 6.

Step 7 Restart the Unified CCX server. In the case of high availability deployments, restart both the nodes.

Generate Certificate Signing Request

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

For CSR generation, use the supported key lengths 1024 or 2048 from the list.

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 Click **Generate CSR**.
The **Generate Certificate Signing Certificate** dialog box opens.

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

Note For the current release of the Cisco Unified Operating System, the Directory option no longer appears in the list of Certificate Names.

Step 4 Click **Generate**.

Download Certificate Signing Request

To download a Certificate Signing Request, follow this procedure:

Procedure

Step 1 Navigate to **Security** > **Certificate Management**.
The **Certificate List** window appears.

Step 2 Click **Download CSR**.
The **Download Certificate Signing Request** dialog box opens.

Step 3 Select the certificate name from the **Certificate Name** list.

Step 4 Click **Download CSR**.

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

Application 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. Collect information about obtaining these certificates from your CA. The process varies among CAs.

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 PEM encoding formats.

For all certificate types, obtain and upload a CA root certificate and an application certificate on each node. Or upload Certificate Chain that has both the application certificate and the chain of the corresponding certificate issuer.

The CSRs for Tomcat and IPSec use the following extensions:

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

1. Upload the CA root certificate of the CA that signed an application certificate. If a subordinate CA signs an application certificate, you must upload the CA root certificate of the subordinate CA, not the root CA.
2. You upload CA root certificates and application certificates by using the same Upload Certificate dialog box. When you upload a CA root certificate, choose the certificate name with the format *certificate type*-**trust**.
3. When you upload an application certificate, choose the certificate name that only includes the certificate type. For example, choose **tomcat-trust** when you upload a Tomcat CA root certificate; choose **tomcat** when you upload a Tomcat application certificate. Restart the Unified CCX Engine.

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 Navigate to **Security** > **Certificate Monitor**.
The **Certificate Monitor** window appears.

Step 2 Enter the required configuration information.
See the table below for a description of the Certificate Monitor Expiration fields.

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

Table 1: 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 Email 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.

IPSec Management

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

- Set Up New IPSec Policy, on page 8
- Manage IPSec Policies, on page 10

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

Set Up New IPSec Policy

Any changes that you make to an IPSec policy during a system upgrade are lost, so do not modify or create IPSec policies during an upgrade.

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

Procedure

Step 1 Navigate to **Security** > **IPSEC Configuration**.
The **IPSEC Policy List** window appears.

Step 2 Click **Add New**.
The **IPSEC Policy Configuration** window appears.

Step 3 Enter the appropriate information on the **IPSEC Policy Configuration** window. See the table below for descriptions of the fields on this window.

Step 4 Click **Save** to set up the new IPSec policy.

Table 2: 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.
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 Unified CCX, you may need to change the name of your pre-shared IPSec keys, so they are compatible with current versions of Unified CCX.
Peer Type	Specifies whether the peer is the same type or different.
Certificate Name	If you choose Different for the Peer Type, enter the new certificate name.
Destination Address	Specifies the IP address or FQDN of the destination.
Destination Port	Specifies the port number at the destination.

Field	Description
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 protocol: • TCP • UDP • Any
Encryption Algorithm	From the drop-down list, choose 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
ESP Algorithm	From the drop-down list, choose 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, choose 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, choose the phase Two DH value. Choices include: 2, 1, and 5.

Field	Description
Enable Policy	Check the check box to enable the policy.

Manage IPSec Policies

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

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

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

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

Procedure

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 by using your Administrator password.

The **IPSEC Policy List** window appears.

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

a) Click the policy name.
The **IPSEC Policy Configuration** window appears.

b) To enable or disable the policy, click 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.

To use **Bulk Certificate Management** to export certificates, use the following procedure:

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

   The Bulk Certificate Management window displays.
2. Enter the appropriate information on the **Bulk Certificate Management** window.
3. To save the values you entered, click **Save**.
4. To export certificates, click **Export**.

   The **Bulk Certificate Export** popup window displays.
5. From the drop-down menu, choose **Tomcat** as the type of certificate to export.
6. Click **Export**.

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

You can also use the **Bulk Certificate Management** window to import certificates that you have exported from other clusters. However, before the **Import** button displays, you must complete the following activities:

- Export the certificates from at least two clusters to the SFTP server.
- Consolidate the exported certificates.