

# CHAPTER **6**

# **Security**

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

- Set Internet Explorer Security Options
- Manage Certificates and Certificate Trust Lists
- IPSEC Management

# **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 <b>Tools &gt; Internet Options</b> .
Step 3	Click the <b>Advanced</b> tab.
Step 4	Scroll down to the Security section on the Advanced tab.
Step 5	If necessary, clear the <b>Do not save encrypted pages to disk</b> check box.
Step 6	Click <b>OK</b> .

# **Manage Certificates and Certificate Trust Lists**

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

- Display Certificates
- Download a Certificate or CTL
- Delete and Regenerate a Certificate
- Upload a Certificate or Certificate Trust List

• Using Third-Party CA Certificates



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

# **Display Certificates**

To display existing certificates, follow this procedure:

	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.	
	The Certificate Configuration window displays information about the certificate.	
Step 4	To return to the Certificate List window, select <b>Back To Find/List</b> in the Related Links list; then, click <b>Go</b> .	

# **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

Certificate List window displays. can use the Find controls to filter the certificate list.
can use the Find controls to filter the certificate list.
k the file name of the certificate or CTL.
Certificate Configuration window displays.
k Download.
he File Download dialog box, click Save.
:] :]

# **Delete and Regenerate a Certificate**

These sections describe deleting and regenerating a certificate:

• Deleting a Certificate

• Regenerating a Certificate

### **Deleting a Certificate**

To delete a trusted certificate, follow this procedure:

$\triangle$	
Caution	

Deleting a certificate can affect your system operations. Any existing CSR for the certificate that you
choose 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" procedure on page 6-7.

#### 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 or CTL.	
	The Certificate Configuration window displays.	
Step 4	Click <b>Delete</b> .	

# **Regenerating a Certificate**

To regenerate a certificate, follow this procedure:

	Regenerating a certificate can affect your system operations.
	Procedure
	Navigate to Security > Certificate Management.
	The Certificate List window displays.
	Click Generate New.
,	The Generate Certificate dialog box opens.
	Choose a certificate name from the Certificate Name list. For a description of the certificate names that display, see Table 6-1.
	Click Generate New.

1

Name	Description
tomcat	This self-signed root certificate gets generated during installation for the HTTPS server.
ipsec	This self-signed root certificate gets generated during installation for IPSec connections with MGCP and H.323 gateways.
CallManager	This self-signed root certificate automatically installs when you install Cisco Unified Communications Manager. This certificate provides server identification, including the server name and the Global Unique Identifier (GUID).
CAPF	The system copies this root certificate to your server or to all servers in the cluster after you complete the Cisco CTL client configuration.

Table 6-1	Certificate Names and Descriptions
-----------	------------------------------------

# **Upload a Certificate or Certificate Trust List**



Uploading a new certificate or certificate trust list (CTL) file can affect your system operations. After you upload a new certificate or certificate trust list, you must restart the CiscoCallManager service by navigating to **Cisco Unified Serviceability > Tools > Service Activation**. For more information, see the *Cisco Unified Serviceability Administration Guide*.

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.

These sections describe how to upload a CA root certificate, application certificate, or CTL file to the server:

- Upload a Certificate
- Upload a Certificate Trust List
- Upload a Directory Trust Certificate

### **Upload a Certificate**

#### Procedure

Step 1	Navigate to Security > Certificate Management.
	The Certificate List window displays.
Step 2	Click Upload Certificate.
	The Upload Certificate dialog box opens.

- **Step 3** Select the certificate name from the **Certificate Name** list.
- **Step 4** 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 Certificate** text box. If you are uploading a CA root certificate, leave this text box empty.
- **Step 5** Select the file to upload by doing one of the following steps:
  - In the Upload File text box, enter the path to the file.
  - Click the **Browse** button and navigate to the file; then, click **Open**.
- **Step 6** To upload the file to the server, click the **Upload File** button.

### **Upload a Certificate Trust List**

#### Procedure

Step 1	Navigate to Security > Certificate Management.
	The Certificate List window displays.
Step 2	Click Upload Certificate.
	The Upload Certificate Trust List dialog box opens.
Step 3	Select the certificate name from the Certificate Name list.
Step 4	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 <b>Root Certificate</b> text box. If you are uploading a CA root certificate, leave this text box empty.
Step 5	Select the file to upload by doing one of the following steps:
	• In the <b>Upload File</b> text box, enter the path to the file.
	• Click the <b>Browse</b> button and navigate to the file; then, click <b>Open</b> .
Step 6	To upload the file to the server, click the <b>Upload File</b> button.

# **Upload a Directory Trust Certificate**

#### Procedure

Navigate to <b>Security &gt; Certificate Management</b> .
The Certificate List window displays.
Click Upload Certificate.
The Upload Certificate Trust List dialog box opens.
Select directory-trust from the Certificate Name list.
Enter the file to upload in the Upload File field.
To upload the file, click the Upload File button.
Log into Cisco Unified Serviceability.

- **Step 7** Navigate to **Tools > Control Center Feature Services**.
- **Step 8** Restart the service **Cisco Dirsync**.
- **Step 9** Log in to the Cisco Unified Communications Operating System CLI as an administrator.
- Step 10 To restart the Tomcat service, enter the command utils service restart Cisco Tomcat.
- Step 11 After the services have been restarted, you can add the directory agreement for SSL.

# **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 6-7.
Step 2	Download the CSR to your PC.	See the "Download a Certificate Signing Request" section on page 6-7.
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" section on page 6-4.
Step 6	Upload the application certificate to the server.	See the "Upload a Certificate" section on page 6-4.
Step 7	If you updated the certificate for CAPF or Cisco Unified Communications Manager, generate a new CTL file.	See the Cisco Unified Communications Manager 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 Communications Manager, restart the TFTP service.
		<b>Note</b> If you updated the Tomcat certificate, you also must restart the Connection IMAP Server service in Cisco Unity Connection Serviceability.
		See the Cisco Unified Communications Manager Serviceability Administration Guide for information about restarting services.

### **Generating a Certificate Signing Request**

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

Proced	lure
Navig	ate to Security > Certificate Management.
The C	ertificate List window displays.
Click	Generate CSR.
The G	enerate Certificate Signing Request dialog box opens.
Select	the certificate name from the Certificate Name list.
Note	For the current release of the Cisco Unified Operating System, the Directory option no longer displays in the list of Certificate Names. However, you can still upload a Directory Trust certificate from a previous release, which is required for the DirSync service to work in Secure mode.
	Navig The C Click The G Select Note

### **Download a Certificate Signing Request**

To download a Certificate Signing Request, follow this procedure:

Step 1	Navigate to Security > Certificate Management.
	The Certificate List window displays.
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 <b>Save</b> .

### **Obtaining 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. Get information about obtaining these certificates from your CA. The process varies among CAs.

CAPF and Cisco Unified Communications Manager 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 PEM encoding formats.

# **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 Monitor.

The Certificate Monitor window displays.

- **Step 2** Enter the required configuration information. See Table 6-2 for a description of the Certificate Monitor Expiration fields.
- **Step 3** To save your changes, click **Save**.

#### Table 6-2 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.
	<b>Note</b> 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 a New IPSec Policy
- Managing Existing IPSec Policies



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:

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.
IPSec, especially with encryption, will affect the performance of your system.
Procedure
Procedure Navigate to Security > IPSEC Configuration.
Procedure Navigate to Security > IPSEC Configuration. The IPSEC Policy List window displays.
Procedure Navigate to Security > IPSEC Configuration. The IPSEC Policy List window displays. Click Add New.
Procedure Navigate to Security > IPSEC Configuration. The IPSEC Policy List window displays. Click Add New. The IPSEC Policy Configuration window displays.

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

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 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.

#### Table 6-3 IPSEC Policy and Association Field Descriptions

I

Field	Description
Source Port	Specifies the port number at the source.
Mode	Specifies Tunnel or 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, 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, 5, 14, 16, 17, and 18.
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, 5, 14, 16, 17, and 18.
Enable Policy	Check the check box to enable the policy.

 Table 6-3
 IPSEC Policy and Association Field Descriptions (continued)

# **Managing Existing IPSec Policies**

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

Беса	ise any changes that you make to an IPSec policy during a system upgrade will get lost, do not	
modif	y or create IPSec policies during an upgrade.	
IPSec	, especially with encryption, will affect the performance of your system.	
Any (	hanges that you make to the existing IPSec policies can impact your normal system operations	
	nanges that you make to the existing it see ponetes can impact your normal system operations.	
Proce	dure	
Navigate to <b>Security &gt; IPSEC Configuration</b> .		
<u>Note</u>	To access the Security menu items, you must log in to Cisco Unified Communications Operation System Administration again by using your Administrator password.	
Note	To access the Security menu items, you must log in to Cisco Unified Communications Operation System Administration again by using your Administrator password. PSEC Policy List window displays.	
Note Note The II	To access the Security menu items, you must log in to Cisco Unified Communications Operatin System Administration again by using your Administrator password. PSEC Policy List window displays. splay, enable, or disable a policy, follow these steps:	
Note	To access the Security menu items, you must log in to Cisco Unified Communications Operatin System Administration again by using your Administrator password. PSEC Policy List window displays. uplay, enable, or disable a policy, follow these steps: lick the policy name.	
Note The I To dis a. C	To access the Security menu items, you must log in to Cisco Unified Communications Operatin System Administration again by using your Administrator password. PSEC Policy List window displays. splay, enable, or disable a policy, follow these steps: lick the policy name. he IPSEC Policy Configuration window displays.	
Note Note The I To dis a. C T b. T	To access the Security menu items, you must log in to Cisco Unified Communications Operatin System Administration again by using your Administrator password. PSEC Policy List window displays. eplay, enable, or disable a policy, follow these steps: lick the policy name. he IPSEC Policy Configuration window displays. o enable or disable the policy, use the <b>Enable Policy</b> check box.	
Note Note The I To dis a. C T b. T c. C	To access the Security menu items, you must log in to Cisco Unified Communications Operatin System Administration again by using your Administrator password. PSEC Policy List window displays. uplay, enable, or disable a policy, follow these steps: lick the policy name. he IPSEC Policy Configuration window displays. o enable or disable the policy, use the <b>Enable Policy</b> check box. lick <b>Save</b> .	
<b>Note</b> The II To dis <b>a.</b> C <b>T</b> <b>b.</b> T <b>c.</b> C To de	To access the Security menu items, you must log in to Cisco Unified Communications Operatin System Administration again by using your Administrator password. PSEC Policy List window displays. splay, enable, or disable a policy, follow these steps: lick the policy name. he IPSEC Policy Configuration window displays. o enable or disable the policy, use the <b>Enable Policy</b> check box. lick <b>Save</b> . lete one or more policies, follow these steps:	
Note The I To dis a. C T b. T c. C To de a. C	To access the Security menu items, you must log in to Cisco Unified Communications Operatin System Administration again by using your Administrator password. PSEC Policy List window displays. eplay, enable, or disable a policy, follow these steps: lick the policy name. he IPSEC Policy Configuration window displays. o enable or disable the policy, use the <b>Enable Policy</b> check box. lick <b>Save</b> . lete one or more policies, follow these steps: heck the check box next to the policies that you want to delete.	
Note The II To dis a. C T b. T c. C To de a. C Y	To access the Security menu items, you must log in to Cisco Unified Communications Operatin System Administration again by using your Administrator password. PSEC Policy List window displays. eplay, enable, or disable a policy, follow these steps: lick the policy name. he IPSEC Policy Configuration window displays. o enable or disable the policy, use the <b>Enable Policy</b> check box. lick <b>Save</b> . lete one or more policies, follow these steps: heck the check box next to the policies that you want to delete. ou can click <b>Select All</b> to select all policies or <b>Clear All</b> to clear all the check boxes.	

Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 7.x