Main page: Cisco Unified Presence, Release 7.x

Contents

Previous Topic

- Cisco Unified Operating System Administration for Cisco Unified Presence
- Security Certificates
- How to Manage Certificates and Certificate Trust Lists
- How to Use Third-Party CA Certificates

Security Certificates

The operating system security options enable you to manage security certificates in these two ways:

- Certificate Management-Manages certificates, Certificate Trust Lists (CTL), and Certificate Signing Requests (CSR). You can display, upload, download, delete, and regenerate certificates.
- Certificate Monitor-Allows you to monitor the expiration dates of the certificates on the server.

How to Manage Certificates and Certificate Trust Lists

- Viewing Certificates
- Downloading a Certificate or a Certificate Trust List
- Deleting a Certificate
- Regenerating a Certificate
- Uploading a Certificate or a Certificate Trust List
- Uploading a Directory Trust Certificate

Viewing Certificates

Before You Begin

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

Procedure

1. Log in to Cisco Unified Operating System Administration.

2. Select **Security > Certificate Management**.

3. Perform one of the following actions:

If you want to:	Action

Filter the certificate list	Enter your search criteria, and use the Find controls as follows: 1. To filter or search records, perform one of the following actions: ◊ From the first list box, select a search parameter. ◊ From the second list box, select a search pattern. ◊ Specify the appropriate search text, if applicable. 2. Click **Find**.
View details of a certificate or trust store	Click the .PEM or .DER file name of the certificate.
Return to the Certificate List window	1. Select **Back To Find/List** in the Related Links list. 2. Click **Go**.

Related Topics

- Getting More Information

Downloading a Certificate or a Certificate Trust List

Before You Begin

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

Procedure

1. Log in to Cisco Unified Operating System Administration.

2. Select **Security > Certificate Management**.

3. If required, use the Find controls to filter the certificate list as follows:

    1. To filter or search records, perform one of the following actions:

        ◊ From the first list box, select a search parameter.
        ◊ From the second list box, select a search pattern.
        ◊ Specify the appropriate search text, if applicable.
    2. Click **Find**.

4. Click the file name of the certificate or CTL.

5. Click **Download**.

6. Click **Save**.

Related Topics

- Getting More Information

Deleting a Certificate

A trusted certificate is the only type of certificate that you can delete. You can not delete a self-signed certificate that is generated by the system.

Caution! Deleting a certificate can affect your system operations. If there is an existing CSR for the certificate you select from the Certificate list, it is deleted from the system and you must generate a new CSR. For more information, see the Generating a Certificate Signing Request.

Before You Begin

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

Procedure

1. Log in to Cisco Unified Operating System Administration.
2. Select **Security > Certificate Management**.
3. If required, use the Find controls to filter the certificate list as follows:
    1. To filter or search records, perform one of the following actions:
        - ◊ From the first list box, select a search parameter.
        - ◊ From the second list box, select a search pattern.
        - ◊ Specify the appropriate search text, if applicable.
    2. Click **Find**.
4. Click the file name of the certificate or CTL.
5. Click **Delete**.

Related Topics

- Getting More Information

Regenerating a Certificate

A certificate of type "cert" is the only type of certificate that you can regenerate.

Caution! Regenerating a certificate can affect your system operations.

Before You Begin

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

Procedure

1. Log in to Cisco Unified Operating System Administration.
2. Select **Security > Certificate Management**.
3. Click **Generate New**.
4. Select a certificate name from the Certificate Name list.

Table: Certificate Names and Descriptions

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.
sipproxy	This self-signed root certificate is generated during: ◊ Installation for third-party applications ◊ Integration with Microsoft LCS or OCS servers ◊ ASA federation ◊ Communication with Cisco Unified Communications Manager ◊ Intercluster TLS communications
Presence Engine	This self-signed root certificate is generated during installation and is currently not used.

5. Click **Generate New**.

Troubleshooting Tips

Restart the Tomcat web server after you upload or regenerate a Tomcat certificate, in a Cisco Unified Presence cluster.

Related Topics

- Getting More Information

Uploading a Certificate or a Certificate Trust List

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

Before You Begin

- 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 access the Security menu items, you must log out and log back in to Cisco Unified Operating System Administration using your Administrator password.

Procedure

1. Log in to Cisco Unified Operating System Administration.

2. Select **Security > Certificate Management**.

3. Click **Upload Certificate**.

4. Select the name of the certificate or CTL from the **Certificate Name** list.

5. Perform one of the following actions:

    1. 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.
    2. If you are uploading a CA root certificate, leave **Root Certificate** text box empty.

6. Select the file to upload by completing one or of the following actions:

    - Enter the path to the file in the **Upload File** text box.
    - Click **Browse** and navigate to the file.
    - Click **Open**.

7. Click **Upload File** to upload the file to the server.

Troubleshooting Tips

Restart the Tomcat web server after you upload or regenerate a Tomcat certificate, in a Cisco Unified Presence cluster.

Related Topics

- Getting More Information

Uploading a Directory Trust Certificate

Procedure

1. Log in to Cisco Unified Operating System Administration.
2. Select **Security > Certificate Management**.
3. Click **Upload Certificate**.
4. Select **directory-trust** from the **Certificate Name** list.
5. Enter the file to upload in the **Upload File** field.
6. Click **Upload File**.
7. Log into Cisco Unified Serviceability.
8. Select **Tools > Control Center - Feature Services**.
9. Restart the service **Cisco Dirsync**.
10. Log in to the Cisco Unified Operating System CLI as an administrator.
11. Enter the command **`utils service restart Cisco Tomcat`** to restart the Tomcat service.
12. After the services have been restarted, you can add the directory agreement for SSL.

Related Topics

- Getting More Information

How to Use Third-Party CA Certificates

- Third-Party Certificates
- Managing the Third-Party Certificate Process
- Generating a Certificate Signing Request
- Downloading a Certificate Signing Request
- Monitoring Certificate Expiration Dates

Third-Party Certificates

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

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 Presence Certificate Signing Requests (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 in the final window of the CSR generation process.

Cisco Unified 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.

Managing the Third-Party Certificate Process

This procedure provides an overview of the third-party certificate process, with references to each step in sequence:

Step #	Task	For More Information
1	Generate a CSR on the server.	See Generating a Certificate Signing Request.
2	Download the CSR to your PC.	See Downloading a Certificate Signing Request.
3	Use the CSR to obtain an application certificate from a CA.	Get information about obtaining application certificates from your CA.
4	Obtain the CA root certificate.	Get information about obtaining a root certificate from your CA.
5	Upload the CA root certificate to the server.	See Uploading a Certificate or a Certificate Trust List.
6	Upload the application certificate to the server.	See Uploading a Certificate or a Certificate Trust List.
7	If you updated the certificate for CAPF or Cisco Unified Presence, generate a new CTL file.	See Uploading a Certificate or a Certificate Trust List.
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).

Related Topics

- Getting More Information

Generating a Certificate Signing Request

Before You Begin

- To access the Security menu items, you must log in again to Cisco Unified Operating System Administration using your Administrator password.
- For the current release of the Cisco Unified Operating System, the Directory option is no longer available 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.

Procedure

1. Log in to Cisco Unified Operating System Administration.
2. Select **Security > Certificate Management**.
3. Click **Generate CSR**.
4. Select the certificate name from the **Certificate Name** list.
5. Click **Generate CSR**.

Related Topics

- Getting More Information

Downloading a Certificate Signing Request

Before You Begin

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

Procedure

1. Log in to Cisco Unified Operating System Administration.
2. Select **Security > Certificate Management**.
3. Click **Download CSR**.
4. Select the certificate name from the **Certificate Name** list.
5. Click **Download CSR**.
6. Click **Save**.

Related Topics

- Getting More Information

Monitoring Certificate Expiration Dates

The system can automatically send you an email when a certificate is close to its expiration date.

Procedure

1. Log in to Cisco Unified Operating System Administration.
2. Select **Security > Certificate Monitor** to view the current Certificate Expiration Monitor configuration.
3. Enter the required configuration information.

Table: 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	Check the check box to enable email notification.
E-mail IDs	Enter the email address to which you want notifications sent. **Note:** For the system to send notifications, you must configure an SMTP host.

4. Click **Save**.

Related Topics

- Getting More Information