



# CHAPTER 13

## Managing Certificates

---

Cisco ISE relies on public key infrastructure (PKI) to provide secure communication for the following:

- Client and server authentication for Transport Layer Security (TLS)-related Extensible Authentication Protocol (EAP) protocols
- HTTPS communication between your client browser and the management server

Cisco ISE provides a web interface for managing PKI credentials. There are two types of credentials:

- Local certificates—Used to identify the Cisco ISE server to other entities such as EAP supplicants, external policy servers, or management clients. Local certificates are also known as identity certificates. Along with the local certificate, a private key is stored in Cisco ISE to prove its authenticity.

Cisco ISE identifies when a local certificate is about to expire and logs a warning in the audit logs. The expiration date also appears in the local certificate list page (Administration > System > Certificates > Local Certificates). The audit log message is logged in the *catalina.out* file. You can download this file as part of the support bundle (Operations > Troubleshoot > Download Logs). The *catalina.out* file will be available in this directory: `support\apache_logs`. There are two types of audit log messages that provide information on local certificate expiration warnings:

- Certificate expiring in < 90 days—AuditMessage: 34100: Certificate.ExpirationInDays, Certificate.IssuedBy, Certificate.CertificateName, Certificate.IssuedTo
- Certificate has expired—AuditMessage: 34101: Certificate.ExpirationDate, Certificate.IssuedBy, Certificate.CertificateName, Certificate.IssuedTo
- Certificate authority certificates—Used to verify remote certificates that are presented to Cisco ISE. Certificate authority certificates have a dependency relation that forms a Certificate Trust List (CTL) hierarchy. This hierarchy connects a certificate with its ultimate root certificate authority (CA) and verifies the authenticity of the certificate.

In a distributed deployment, at the time of registering a secondary node to the primary node, the secondary node should present a valid certificate. Usually, the secondary node will present its local HTTPS certificate. To provide authentication for deployment operations that require direct contact with the secondary node, the CTL of the primary node should be populated with the appropriate trust certificates, which can be used to validate the HTTPS certificate of the secondary node. Before you register a secondary node in a deployment, you must populate the CTL of the primary node. If you do not populate the CTL of the primary node, node registration fails. Node registration also fails if certificate validation fails for some reason.

**Note**

After you obtain the backup from your standalone ISE node or primary Administration ISE node, if you change the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore the data. Otherwise, if you try to restore data using the older backup, the communication between the nodes might fail.

This chapter contains the following sections:

- [Local Server Certificates, page 13-2](#)
- [Certificate Signing Requests, page 13-15](#)
- [Certificate Authority Certificates, page 13-16](#)
- [Simple Certificate Enrollment Protocol Profiles, page 13-25](#)
- [OCSP Services, page 13-27](#)

## Local Server Certificates

After installation, Cisco ISE generates, by default, a self-signed local certificate and private key, and stores them on the server. For certificate-based authentications, Cisco ISE authenticates itself to clients using the default self-signed certificate that is created at the time of installation. This self-signed certificate is used for both HTTPS and EAP protocols to authenticate clients. This self-signed certificate is valid for one year and its key length is set to 1024 bits. At the time of generation, this certificate is used for both EAP and HTTPS protocols. You can change this definition after you have imported or generated other local certificates. In a self-signed certificate, the hostname of Cisco ISE is used as the common name (CN) because it is required for HTTPS communication.

**Note**

When you change the HTTPS local certificate on a node, existing browser sessions that are connected to that node do not automatically switch over to the new certificate. You must restart your browser to see the new certificate. This note applies for both Firefox and Internet Explorer 8 browsers.

Currently, Cisco ISE automatically creates self-signed certificates after initial installation. Cisco strongly recommends installing a CA-signed certificate and configuring it for use by HTTPS or EAP or both. You can import a CA certificate and its private key or request a CA for a CA-signed certificate. To request a CA-signed certificate, you must generate a Certificate Signing Request (CSR) from the Cisco ISE user interface, export it, and send it to a CA. The CA will sign the certificate and return it to you. You must then bind the certificate that the CA returned with the private key that is stored with the CSR in Cisco ISE. After you bind this certificate with the private key, you can configure it for HTTPS or EAP or both.

Cisco ISE provides a web interface that allows you to do the following:

- Import a local certificate and its private key from files residing on the system that is running the client browser. The private key can be encrypted or unencrypted. If the private key is encrypted, you must specify the password to decrypt it. After importing it into Cisco ISE, you can designate it as the certificate for Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) mutual authentication, or HTTPS communication between browser clients and the management server, or both. Cisco ISE checks the certificate for basic X509 certificate format, checks if the private key matches the public key in the certificate, and prevents duplicate certificates.

**Note**

You can also choose the import option when you have exported the certificate and private key from another Cisco ISE server. You must specify a password to encrypt the private key while exporting it from another Cisco ISE server. You can import certificates only in Privacy-Enhanced Mail (PEM) and Distinguished Encoding Rules (DER) formats.

- View a list of local certificates that are stored in Cisco ISE and their expiration dates.
- Edit a local certificate. You can change the friendly name and description and the protocol associations (HTTPS or EAP or both). You can request a renewal of self-signed certificates and thereby extend the expiration date.
- Delete a local certificate.
- Generate a self-signed certificate.
- Generate a CSR.
- Export a CSR to a file that resides on the system that is running the client browser to forward the CSR to a CA that will sign the certificate.
- Delete a CSR.
- Bind a CA certificate to its private key.
- Replace a local certificate with a duplicate certificate.

**Note**

To plan your Inline Posture deployment and to know more about the Extended Key Usage (EKU) requirements for Inline Posture see the [“Guidelines for Configuring Certificates for Inline Posture” section on page 10-12](#).

This section contains the following topics:

- [Viewing Local Certificates, page 13-3](#)
- [Adding a Local Certificate, page 13-4](#)
- [Editing a Local Certificate, page 13-11](#)
- [Deleting a Local Certificate, page 13-13](#)
- [Exporting a Local Certificate, page 13-13](#)

## Viewing Local Certificates

The Local Certificate page lists all local certificates added to Cisco ISE.

**Prerequisite:**

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

**To view the local certificate list, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Certificates**.

**Step 2** From the Certificate Operations navigation pane on the left, click **Local Certificates**.

The Local Certificate page appears and provides the following information for the local certificates as shown in [Figure 13-1](#):

- Friendly Name—Name of the certificate.
- Protocol—Protocols for which to use this certificate.
- Issued To—Certificate subject or the CN to which the certificate is issued.  
The common name is usually the fully qualified domain name of the ISE node.
- Issued By—Server that issued this certificate.
- Valid From—Date on which the certificate was created.
- Expiration Date—Expiration date of the certificate.
- Expiration Status—Provides information about the status of the certificate expiration. There are five icons and categories of informational message that appear in this column:
  1. Active (green icon)
  2. Expiring in less than 90 days (blue icon)
  3. Expiring in less than 60 days (yellow icon)
  4. Expiring in less than 30 days (orange icon)
  5. Expired (red icon)

**Figure 13-1** Local Certificate List Page

Friendly Name	Protocol	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
Positron.cisco.cor	HTTPS,EAP	Positron.cisco.cor	Positron.cisco.cor	Wed, 28 Sep 2012	Thu, 27 Sep 2012	Active (Green icon)

## Adding a Local Certificate



### Note

If your Cisco ISE deployment has multiple nodes in a distributed setup, you must add a local certificate to each node in your deployment individually because the private keys are not stored in the local database and are not copied from the relevant nodes.

You can add a local certificate to Cisco ISE in one of the following ways:

- [Importing a Server Certificate, page 13-5](#)
- [Generating a Self-Signed Certificate, page 13-7](#)
- [Generating a Certificate Signing Request, page 13-8](#) and [Binding a CA-Signed Certificate, page 13-10](#)

## Importing a Server Certificate

Before you import a local certificate, ensure that you have the local certificate and the private key file on the system that is running the client browser.



### Note

When you change the HTTPS local certificate on a node, existing browser sessions connected to that node do not automatically switch over to the new certificate. You must restart your browser to see the new certificate. This note applies for both Firefox and Internet Explorer 8 browsers.

### Prerequisites:

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.
- If the local certificate that you import contains the basic constraints extension with the CA flag set to true, ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set.

To import a server certificate, complete the following steps:

**Step 1** Choose **Administration > System > Certificates**.

**Step 2** From the Certificate Operations navigation pane on the left, click **Local Certificates**.



### Note

To import a local certificate to a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

**Step 3** Choose **Add > Import Local Server Certificate**.

The Import Local Server Certificate page appears as shown in [Figure 13-2](#).

**Figure 13-2 Import Local Server Certificate Page**

**Step 4** Click **Browse** to choose the certificate file and the private key from the system that is running your client browser.

If the private key is encrypted, enter the **Password** to decrypt it.

**Step 5** If you would like to specify a **Friendly Name** for the certificate, enter it in the field below the private key password. If you do not specify a name, Cisco ISE automatically creates a name in the format `<common name>#<issuer>#<nnnnn>` where `<nnnnn>` is a unique five-digit number.

**Step 6** If you want Cisco ISE to validate certificate extensions, enable the **Enable Validation of Certificate Extensions** option.



**Note** If you enable the **Enable Validation of Certificate Extensions** option, and the certificate that you are importing contains a basic constraints extension with the Certificate Authority (CA) flag set to true, ensure that the key usage extension is present, and that the “keyEncipherment” bit or the “keyAgreement” bit, or both, are also set.

**Step 7** In the Protocol group box:

- Check the **EAP** check box to use this certificate for EAP protocols to identify the ISE node.
- Check the **Management Interface** check box to use this certificate to authenticate the web server (GUI).



**Note** If you check the Management Interface check box, ensure that the CN value in the Certificate Subject is the fully qualified domain name (FQDN) of the node. Otherwise, the import process will fail.

**Step 8** In the Override Policy area, check the **Replace Certificate** check box to replace an existing certificate with a duplicate certificate. A certificate is considered a duplicate if it has the same subject or issuer and the same serial number as an existing certificate. This option updates the content of the certificate, but retains the existing protocol selections for the certificate.



**Note** If Cisco ISE is set to operate in FIPS mode, the certificate must be 2048 bits in size and use either SHA-1 or SHA-256 encryption.

**Step 9** Click **Submit** to import the local certificate.

If you import a local certificate to your primary ISE node, and if the management interface option is enabled on the node in your deployment, Cisco ISE automatically restarts the application server on the node. Otherwise, you must restart the secondary nodes that are connected to your primary ISE node.

To restart the secondary nodes, from the command-line interface (CLI), enter the following commands:

- application stop ise**
- application start ise**

Refer to the [Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x](#) for more information on these commands.

## Generating a Self-Signed Certificate

### Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To generate a self-signed certificate, complete the following steps:

- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **Local Certificates**.



**Note** To generate a self-signed certificate from a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

- Step 3** Choose **Add > Generate Self Signed Certificate**.

The Generate Self Signed Certificate page appears, as shown in [Figure 13-3](#).

**Figure 13-3** Generating a Self-Signed Certificate Page

- Step 4** Enter the following information:
- **Certificate Subject**—A distinguished name (DN) identifying the entity that is associated with the certificate. The DN must include a common name (CN) value.
  - **Required Key Length**—Valid values are 512, 1024, 2048, 4096. (If you are deploying Cisco ISE as a FIPS-compliant policy management engine, you must specify a 2048 bit or larger key length).
  - **Digest to Sign With**—You can choose to encrypt and decrypt certificates using either SHA-1 or SHA-256.
  - **Certificate Expiration**. You can specify a time period in days, weeks, months, or years.

- If you would like to specify a **Friendly Name** for the certificate, enter it in the field below the private key password. If you do not specify a name, Cisco ISE automatically creates a name in the format `<common name>#<issuer>#<nnnnn>` where `<nnnnn>` is a unique five-digit number.

**Step 5** In the Protocol group box:

- Check the **EAP** check box to use this certificate for EAP protocols to identify the ISE node.
- Check the **Management Interface** check box to use this certificate to authenticate the web server (GUI). You must also reboot the Cisco ISE if you are turning on this function for the first time.



**Note**

If you check the Management Interface check box, ensure that the CN value in the Certificate Subject is the FQDN of the node. Otherwise, the self-signed certificate will not be generated.

**Step 6** In the Override Policy area, check the **Replace Certificate** check box to replace an existing certificate with a duplicate certificate. A certificate is considered a duplicate if it has the same subject or issuer and the same serial number as an existing certificate. This option updates the content of the certificate, but retains the existing protocol selections for the certificate.

**Step 7** Click **Submit** to import the local certificate.

If you import a local certificate to your primary ISE node, and if the management interface option is enabled on the node in your deployment, Cisco ISE automatically restarts the application server on the node. Otherwise, you must restart the secondary nodes that are connected to your primary ISE node.

To restart the secondary nodes, from the command-line interface (CLI), enter the following commands:

- a. **application stop ise**
- b. **application start ise**

Refer to the [Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x](#) for more information on these commands.



**Note**

If you are using a self-signed certificate and you must change the hostname of your Cisco ISE node, Cisco ISE will continue to use the self-signed certificate with the old hostname after the hostname change. You must log into the administrative user interface of the Cisco ISE node, delete the existing self-signed certificate that has the old hostname, and generate a new self-signed certificate.

## Generating a Certificate Signing Request

**Prerequisite:**

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

**To generate a certificate signing request (CSR), complete the following steps:**

**Step 1** Choose **Administration > System > Certificates**.

**Step 2** From the Certificate Operations navigation pane on the left, click **Local Certificates**.



**Note** To generate a CSR from a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

**Step 3** Choose **Add > Generate Certificate Signing Request**.

The Generate Certificate Signing Request page appears as shown in [Figure 13-4](#).

**Figure 13-4** Generating a Certificate Signing Request

Local Certificates > Generate Certificate Signing Request

Generate Certificate Signing Request

**Certificate**

\* Certificate Subject

\* Key Length

\* Digest to Sign With

**Step 4** Enter the certificate subject and the required key length. The certificate subject is a distinguished name (DN) identifying the entity that is associated with the certificate. The DN must include a common name value. Elements of the distinguished name are:

- C = Country
- S = Test State or Province
- L = Test Locality (City)
- O = Organization Name
- OU = Organizational Unit Name
- CN = Common Name
- E = E-mail Address

An example of Certificate Subject in a CSR should look like “CN=Host-ISE.cisco.com, OU=Cisco O=security, C=US, S=NC, L=RTP, e=test@test.com.”



**Note** When populating the Certificate Subject field, do not encapsulate the string in quotes.



**Note** If you intend to use the certificate generated from this CSR for HTTPS communication (Management Interface), ensure that the CN value in the Certificate Subject is the FQDN of the node. Otherwise, you will not be able to select Management Interface when binding the generated certificate.

**Step 5** Choose to encrypt and decrypt certificates using either SHA-1 or SHA-256.



**Note** If Cisco ISE is set to operate in FIPS mode, the certificate must be 2048 bits in size and use either SHA-1 or SHA-256 encryption.

**Step 6** Click **Submit** to generate a CSR.

A CSR and its private key are generated and stored in Cisco ISE. You can view this CSR in the Certificate Signing Requests page. You can export the CSR and send it to a CA to obtain a signature.

## Binding a CA-Signed Certificate

After your CSR is signed by a CA and returned to you, use this process to bind the CA-signed certificate with its private key. You can also use the bind function to import a CA-signed certificate and its respective private key that you have exported from another Cisco ISE box in your deployment.

### Prerequisites:

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.
- If the certificate that you bind contains the basic constraints extension with the CA flag set to true, ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set.

To bind a CA-signed certificate, complete the following steps:

**Step 1** Choose **Administration > System > Certificates**.

**Step 2** From the Certificate Operations navigation pane on the left, click **Local Certificates**.



**Note** To bind a CA-signed certificate to a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

**Step 3** Choose **Add > Bind CA Certificate**.

The Bind CA Signed Certificate page appears as shown in [Figure 13-5](#).

**Figure 13-5 Binding a CA-Signed Certificate**

- Step 4** Click **Browse** to choose the CA-signed certificate.
- Step 5** If you would like to specify a **Friendly Name** for the certificate, enter it in the field below the private key password. If you do not specify a name, Cisco ISE automatically creates a name in the format *<common name>#<issuer>#<nnnnn>* where *<nnnnn>* is a unique five-digit number.
- Step 6** If you want Cisco ISE to validate certificate extensions, enable the **Enable Validation of Certificate Extensions** option.



**Note** If you enable the **Enable Validation of Certificate Extensions** option, and the certificate that you are importing contains a basic constraints extension with the Certificate Authority (CA) flag set to true, ensure that the key usage extension is present, and that the “keyEncipherment” bit or the “keyAgreement” bit, or both, are also set.

- Step 7** In the Protocol group box:
- Check the **EAP** check box to use this certificate for EAP protocols to identify the ISE node.
  - Check the **Management Interface** check box to use this certificate to authenticate the web server (GUI).



**Note** If you check the Management Interface check box, ensure that the CN value in the Certificate Subject is the FQDN of the node. Otherwise, the bind operation will fail.

- Step 8** In the Override Policy area, check the **Replace Certificate** check box to replace an existing certificate with a duplicate certificate. A certificate is considered a duplicate if it has the same subject or issuer and the same serial number as an existing certificate. This option updates the content of the certificate, but retains the existing protocol selections for the certificate.
- Step 9** Click **Submit** to bind the CA-signed certificate.

## Editing a Local Certificate

### Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

**To edit a local certificate, complete the following steps:**

- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **Local Certificates**.

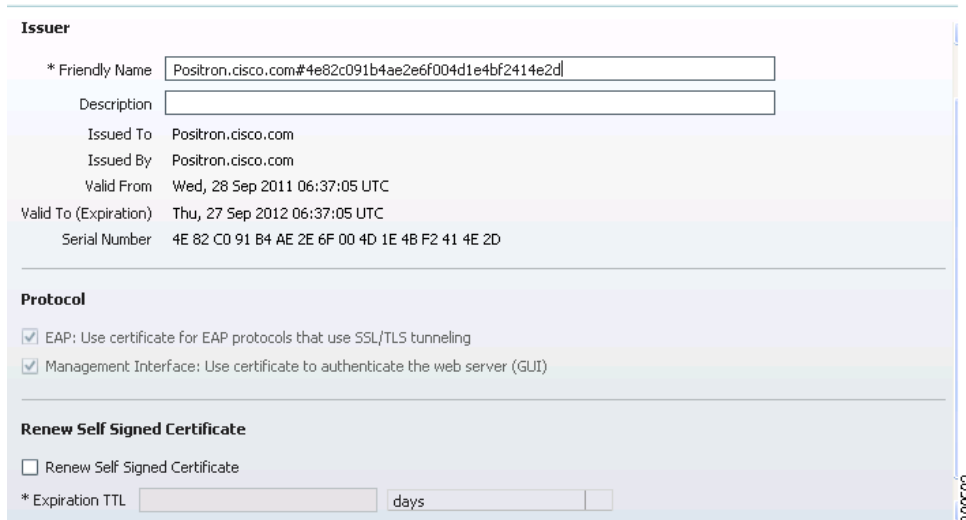


**Note** To edit a local certificate on a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

- Step 3** Check the check box next to the certificate that you want to edit, and click **Edit**.  
The page refreshes and lists the information for the local certificate as shown in [Figure 13-6](#).

**Figure 13-6 Local Certificate Edit Page**



**Issuer**

\* Friendly Name

Description

Issued To Positron.cisco.com

Issued By Positron.cisco.com

Valid From Wed, 28 Sep 2011 06:37:05 UTC

Valid To (Expiration) Thu, 27 Sep 2012 06:37:05 UTC

Serial Number 4E 82 C0 91 B4 AE 2E 6F 00 4D 1E 4B F2 41 4E 2D

---

**Protocol**

☒ EAP: Use certificate for EAP protocols that use SSL/TLS tunneling

☒ Management Interface: Use certificate to authenticate the web server (GUI)

---

**Renew Self Signed Certificate**

☐ Renew Self Signed Certificate

\* Expiration TTL  days

You can edit the following:

- Friendly Name
- Description
- Protocols
- Expiration TTL (if the certificate is self-signed)

- Step 4** Enter a friendly name to easily identify this certificate when you have many certificates with the same certificate subject.
- Step 5** Enter an optional description.
- Step 6** In the Protocol group box:
- Check the **EAP** check box to use this certificate for EAP protocols to identify the ISE node.
  - Check the **Management Interface** check box to use this certificate to authenticate the web server (GUI).



**Note** If you check the Management Interface check box, ensure that the CN value in the Certificate Subject is the FQDN of the node. Otherwise, the edit operation will fail.

For example, if local\_certificate\_1 is currently designated for EAP and you check the EAP check box while editing local\_certificate\_2, then after you save the changes to local\_certificate\_2, local\_certificate\_1 will no longer be associated with EAP.

- Step 7** To renew your self-signed certificate, check the **Renew Self Signed Certificate** check box and enter the expiration Time to Live (TTL) in days, weeks, months, or years.
- Step 8** Click **Save** to save your changes.

If the management interface option is enabled on the node in your deployment, Cisco ISE automatically restarts the application server on the node. Otherwise, you must restart the secondary nodes that are connected to your primary ISE node.

To restart the secondary nodes, from the command-line interface (CLI), enter the following commands:

- a. **application stop ise**
- b. **application start ise**

Refer to the [Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x](#) for more information on these commands.

---

## Deleting a Local Certificate

### Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To delete a local certificate, complete the following steps:

- 
- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **Local Certificates**.



**Note** To delete a local certificate from a secondary node, choose **Administration > System > Server Certificate**.

---

The Local Certificate page appears.

- Step 3** Check the check box next to the certificate or certificates that you want to delete, and click **Delete**.
- Step 4** The following message appears in a pop-up dialog box.
- Are you sure you want to delete the selected item(s)?
- Step 5** Click **OK** to delete the local certificate or certificates.
- 

## Exporting a Local Certificate

You can export the selected local certificate, or the certificate and the private key.

### Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To export a local certificate, complete the following steps:

**Step 1** Choose **Administration > System > Certificates**.

**Step 2** From the Certificate Operations navigation pane on the left, click **Local Certificates**.



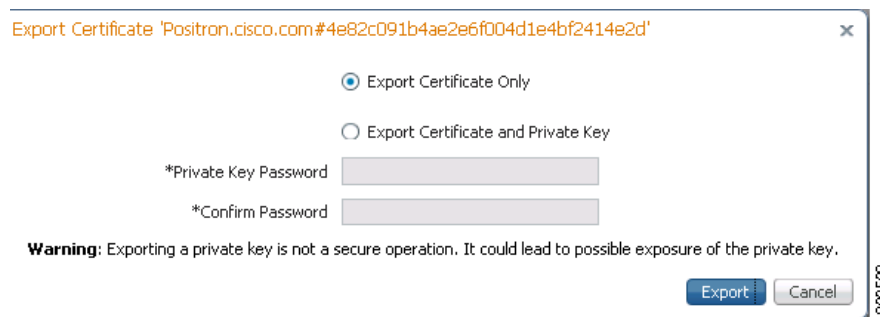
**Note** To export a local certificate from a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

**Step 3** Check the check box next to the certificate that you want to export, then click **Export**.

The Select Certificate Components to Export dialog box appears as shown in [Figure 13-7](#).

**Figure 13-7** Exporting a Local Certificate



You can choose to export only the certificate, or the certificate and the private key.

We do not recommend exporting the private key associated with the certificate because its value may be exposed. If you must export the private key, you must specify an encryption password for the private key. You will need to specify this password while importing this certificate into another Cisco ISE server to decrypt the private key.



**Note** If the certificate being exported was previously imported into Cisco ISE with an encrypted private key, you do not have to use the same password again while exporting it a second time.

**Step 4** Choose the certificate component that you want to export.

**Step 5** Enter the password if you have chosen to export the private key. The password should be at least 8 characters long.

**Step 6** Click **OK** to save the certificate to the file system that is running your client browser.

If you export only the certificate, the certificate is stored in the privacy-enhanced mail format. If you export both the certificate and the private key, the certificate is exported as a .zip file that contains the certificate in the privacy-enhanced mail format and the encrypted private key file.

# Certificate Signing Requests

The list of CSRs that you have created is available in the Certificate Signing Requests page. To obtain signatures from a CA, you must export the CSRs to the local file system that is running your client browser. You must then send the certificates to a CA. The CA will sign and return your certificates. The Certificate Signing Requests page allows you to export the CSRs to the local file system.

**Note**

If your Cisco ISE deployment has multiple nodes in a distributed setup, you must export the CSRs from each node in your deployment individually.

This section contains the following topics:

- [Viewing and Exporting Certificate Signing Requests, page 13-15](#)
- [Deleting a Certificate Signing Request, page 13-16](#)

## Viewing and Exporting Certificate Signing Requests

**Prerequisite:**

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To view the CSRs, complete the following steps:

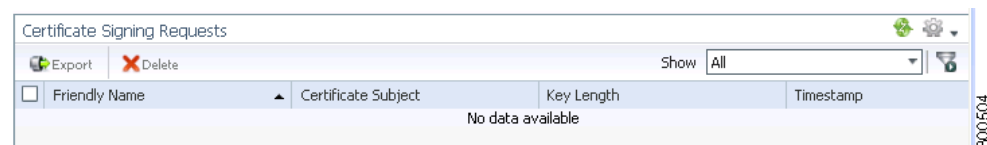
- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **Certificate Signing Requests**.

**Note**

If you want to view or export CSRs from a secondary node, choose **Administration > System > Certificate Signing Requests**.

The Certificate Signing Requests page appears with a list of CSRs as shown in [Figure 13-8](#).

**Figure 13-8** Certificate Signing Requests



- Step 3** Check the check box next to the certificates that you want to export, and click **Export**.
- Step 4** Click **OK** to save the file to the file system that is running the client browser.

## Deleting a Certificate Signing Request

### Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To delete a CSR, complete the following steps:

- 
- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **Certificate Signing Requests**.



---

**Note** If you want to delete a CSR from a secondary node, choose **Administration > System > Certificate Signing Requests**.

---

The Certificate Signing Requests page appears with a list of CSRs.

- Step 3** Check the check box next to the certificates that you want to delete, and click **Delete**.

The following message appears:

Are you sure you want to delete the selected item(s)?

- Step 4** Click **OK** to delete the CSR.
- 

## Certificate Authority Certificates

Certificate authority (CA) certificates are trusted certificates that are used to verify the identity of the client and server certificates that are presented to Cisco ISE. The digital certificates that are issued by a CA contain a public key and the identity of the user. You must request the certificate authority certificate from your CA and import it into Cisco ISE. When you import more than one certificate authority certificate, the certificate authority certificates form a Certificate Trust List (CTL). When a client sends an authentication request, Cisco ISE verifies the client certificate against the CTL. If the certificate of the client is issued by a CA that is present in the CTL, then Cisco ISE authenticates the client.

Cisco ISE does not support wildcard certificates.

Cisco ISE provides a web interface that allows you to do the following:

- Import a certificate authority certificate from a file residing on the system that is running the client browser. The certificate file must contain a privacy-enhanced mail or DER-formatted X509 certificate. After import, you can define the certificate as the Extensible Authentication Protocol-Certificate Trust List (EAP-CTL), which indicates that it is the immediate trust for TLS-related EAP protocols.
- Validate a certificate authority certificate.
- View the list of certificate authority certificates on the ISE node.
- Delete a certificate authority certificate.

- Edit the certificate authority certificate. You can edit the friendly name and description, the trust designation for EAP protocols, and the certificate revocation list (CRL) configuration.
- Export a certificate authority certificate to a file residing on the system that runs the client browser.

**Note**

When deregistering a node whose status has changed (for example, a node status that reverts to standalone), you must examine the Certificate Trust Store to verify if the certificate that is listed in the Certificate Authority Certificate table still applies or is still a valid certificate. Certificates that are no longer needed because the node is no longer part of a distributed deployment can be deleted. However, when a node is deregistered, the corresponding certificate stores are not automatically revised or updated by Cisco ISE. You would have to manually delete such certificates that you no longer need.

This section contains the following topics:

- [Viewing Certificate Authority Certificates, page 13-17](#)
- [Adding a Certificate Authority Certificate, page 13-18](#)
- [Editing a Certificate Authority Certificate, page 13-19](#)
- [Deleting a Certificate Authority Certificate, page 13-22](#)
- [Exporting a Certificate Authority Certificate, page 13-22](#)
- [Importing Certificate Chains, page 13-23](#)
- [Creating Certificate Trust Lists in the Primary ISE Node, page 13-23](#)

## Viewing Certificate Authority Certificates

The Certificate Store page lists all certificates that have been added to Cisco ISE.

**Prerequisite:**

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

**To view the certificate authority certificates, complete the following steps:**

- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **Certificate Store**. The Certificate Store page appears as shown in [Figure 13-9](#).

**Figure 13-9** Certificate Store

Friendly Name	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
Positron.cisco.com#	Positron.cisco.com	Positron.cisco.com	Wed, 28 Sep 2011	Thu, 27 Sep 2012	✓

This page provides the following information for the certificate authority certificates:

- Friendly Name—Name of the certificate authority certificate.
- Issued To—Certificate subject or the company name to which the certificate has been issued.
- Issued By—CA that issued the certificate.
- Valid From—Date on which the certificate was issued.
- Expiration—The expiration date of the certificate authority certificate.
- Expiration Status—Provides information about the status of the certificate expiration. There are five icons and categories of informational message that appear in this column:
  1. Active (green icon)
  2. Expiring in less than 90 days (blue icon)
  3. Expiring in less than 60 days (yellow icon)
  4. Expiring in less than 30 days (orange icon)
  5. Expired (red icon)

## Adding a Certificate Authority Certificate



### Note

Before you add a certificate authority certificate, ensure that the certificate authority certificate resides on the file system that is running the client browser.

### Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

**To add a certificate authority certificate, complete the following steps:**

- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **Certificate Store**.  
The Certificate Store page appears.
- Step 3** Click **Add**.  
The Import a new Trusted CA (Certificate Authority) Certificate page appears as shown in [Figure 13-10](#).

**Figure 13-10 Import a Trusted CA Page**

Certificate Authority Certificates > Import

### Import a new Trusted CA (Certificate Authority) Certificate

\* Certificate File

Friendly Name

All Certificate Authority Certificates are available for selection as the Root CA for secure LDAP connections. In addition, they may be enabled for EAP-TLS and administrative authentication below:

☐ Trust for client authentication

☐ Enable Validation of Certificate Extensions (recommended)

Description

300506

- Step 4** Click **Browse** to choose the certificate authority certificate from the file system that is running the client browser.
- Step 5** If you would like to specify a **Friendly Name** for the certificate, enter it in the field below the private key password. If you do not specify a name, Cisco ISE automatically creates a name in the format `<common name>#<issuer>#<nnnnn>` where `<nnnnn>` is a unique five-digit number.
- Step 6** Check the **Trust for client authentication** check box if you want to use this certificate in the trust list.



**Note** If you check both the **Trust for client authentication** and **Enable Validation of Certificate Extensions** options, ensure that the “keyUsage” extension is present and the “keyCertSign” bit is set, and that the basic constraints extension is present with the CA flag set to true.

- Step 7** Add an optional description.
- Step 8** Click **Submit** to save the certificate authority certificate.

If client certificate-based authentication is enabled, then Cisco ISE will restart the application server on each node in your deployment, starting with the application server on the primary Administration node and followed, one-by-one, by each additional node.

Refer to the [Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x](#) for more information on these commands.

## Editing a Certificate Authority Certificate

### Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To edit a certificate authority certificate, complete the following steps:

- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **Certificate Store**.  
The Certificate Store page appears.
- Step 3** Check the check box next to the certificate that you want to edit, and click **Edit**.  
The page refreshes and the information for the certificate authority certificate is listed as shown in [Figure 13-11](#).

**Figure 13-11 Certificate Authority Certificate Edit Page**

Certificate Authority Certificates > Positron.cisco.com#4e8416a4630efeb2422df4df7f6ab27f

### Edit Certificate

**Issuer**

* Friendly Name	Positron.cisco.com#4e8416a4630efeb2422df4df7f6ab27f
Description	none
Issued To	Positron.cisco.com
Issued By	Positron.cisco.com
<b>Issuer</b> From	Thu, 29 Sep 2011 06:56:36 UTC
Valid To (Expiration)	Fri, 28 Sep 2012 06:56:36 UTC
Serial Number	4E 84 16 A4 63 0E FE B2 42 2D F4 DF 7F 6A B2 7F

**Usage**

All Certificate Authority Certificates are available for selection as the Root CA for secure LDAP connections. In addition, they may be enabled for EAP-TLS and administrative authentication below:

☒ Trust for client authentication

**Certificate Status Validation**

To verify certificates, enable the methods below. If both are enabled, OCSP will always be tried first.

**OCSP Configuration**

☐ Validate against OCSP Service  

☐ Reject the request if certificate status could not be determined by OCSP

**Certificate Revocation List Configuration**

☐ Download CRL

CRL Distribution URL  

Retrieve CRL

☒ Automatically before expiration. 5 Minutes

☐ Every 1 Hours

If download failed, wait 10 Minutes before retry.

☐ Bypass CRL Verification if CRL is not Received

☐ Ignore that CRL is not yet valid or expired

Save Reset

You can edit the following:

- Friendly Name
- Description
- Usage
- Certificate Revocation List Configuration

**Step 4** Enter a friendly name to easily identify this certificate.

**Step 5** Enter an optional description.

**Step 6** Check the **Trust for client authentication** check box if you want to use this certificate in the trust list.



**Note** If you check both the **Trust for client authentication** and **Enable Validation of Certificate Extensions** options, ensure that the “keyUsage” extension is present and the “keyCertSign” bit is set, and that the basic constraints extension is present with the CA flag set to true.

**Step 7** In the Certificate Status Validation group box, check the following check boxes so that OCSP services are always tried first for certificate validation:

- a. **Validate Against OCSP Service**
- b. **Reject the request if certificate status could not be determined by OCSP**

See “[OCSP Services](#)” section on page 13-27 for more information on OCSP services.

**Step 8** In the Certificate Revocation List Configuration group box, do the following:

- a. Check the **Download CRL** check box for Cisco ISE to download a CRL.
- b. Enter the URL to download the CRL from a CA in the URL Distribution text box. This field will be automatically populated if it is specified in the certificate authority certificate. The URL must begin with “http” or “https.”  
The CRL can be downloaded automatically or periodically.
- c. You can configure the time interval between downloads in minutes, hours, days, or weeks if you want the CRL to be downloaded automatically before the previous CRL update expires.
- d. Configure the time interval in minutes, hours, days, or weeks to wait before the Cisco ISE tries to download the CRL again.
- e. If you uncheck the Bypass CRL Verification if CRL is not Received check box, all client requests that use certificates signed by the selected CA will be rejected until Cisco ISE receives the CRL file. If you check this check box, the client requests will be accepted before the CRL is received.
- f. If you uncheck the Ignore CRL that is not yet valid or expired check box, Cisco ISE checks the CRL file for the start date in the Effective Date field and the expiration date in the Next Update field. If the CRL is not yet active or has expired, all authentications that use certificates signed by this CA are rejected. If you check this check box, Cisco ISE ignores the start date and expiration date and continues to use the not yet active or expired CRL and permits or rejects the EAP-TLS authentications based on the contents of the CRL.

**Step 9** Click **Save** to save the changes you have made to the certificate authority certificate.

Refer to the [Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x](#) for more information on these commands.

## Deleting a Certificate Authority Certificate

### Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

**To delete a certificate authority certificate, complete the following steps:**


- 
- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **Certificate Store**.  
The Certificate Store page appears.
- Step 3** Check the check box next to the certificate that you want to delete, and click **Delete**.  
The following message appears.  
Are you sure you want to delete?
- Step 4** Click **OK** to delete the certificate authority certificate.  
If client certificate-based authentication is enabled, then Cisco ISE will restart the application server on each node in your deployment, starting with the application server on the primary Administration node and followed, one-by-one, by each additional node.
- 

## Exporting a Certificate Authority Certificate

### Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

**To export a certificate authority certificate, complete the following steps:**

- 
- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **Certificate Store**.  
The Certificate Store page appears.
- Step 3** Check the check box next to the certificate that you want to export, and click **Export**.
-  **Note** You can export only one certificate at a time.
- 
- Step 4** Save the privacy-enhanced mail file to the file system that is running your client browser.
-

## Importing Certificate Chains

You can import certificates from a file that contains a certificate chain. Cisco ISE supports the privacy-enhanced mail format for importing chains, where each privacy-enhanced-mail-encoded certificate is ordered with the root CA certificate appearing first to the last certificate (end entity) in the correct order. For example, if there are  $n$  certificates, then certificates 1 to  $n - 1$  are assumed to be root or CA certificates that belong to the trust list, and the  $n$ th certificate is assumed to be an end entity certificate from the local certificate store. The associated private key file belongs to the  $n$ th (end entity) certificate. Ensure that this format and convention is strictly followed.

Importing the certificate chain is a two-step process:

- Import the certificate chain file to the certificate authority certificate list. See the [“Adding a Certificate Authority Certificate” section on page 13-18](#) for information on how to import the certificate chain. Cisco ISE places all the certificates except the last one in the trusted certificate list.
- Import the certificate chain file to the local certificate store. See the [“Importing a Server Certificate” section on page 13-5](#) for information on how to import the certificate chain. Cisco ISE places the last certificate ( $n$ th certificate) in the local certificate store.

## Creating Certificate Trust Lists in the Primary ISE Node

In a distributed deployment, before registering a secondary node, you must populate the primary node's CTL with the appropriate CA certificates that can be used to validate the HTTPS certificate of the secondary node. The procedure to populate the CTL of the primary node is different for different scenarios:

- If the secondary node is using a CA-signed certificate for HTTPS communication, you can import the appropriate CA certificates into the CTL of the primary node. See [“Importing Root and CA Certificates into the CTL of the Primary Node” section on page 13-23](#) for more information.
- If the secondary node is using a CA-signed certificate for HTTPS communication, you can alternatively import the CA-signed certificate of the secondary node into the CTL of the primary node, instead of relying on CA certificates for trust. See [“Importing the CA-Signed Certificate from the Secondary Node into the Primary Node's CTL” section on page 13-24](#) for more information.
- If the secondary node is using a self-signed certificate for HTTPS communication, you can import the self-signed certificate of the secondary node into the CTL of the primary node. See [“Importing the Self-Signed Certificate from the Secondary Node into the CTL of the Primary Node” section on page 13-24](#) for more information.

**Note**

After registering your secondary node to the primary node, if you change the HTTPS certificate on the registered secondary node, you must obtain appropriate CA certificates that can be used to validate the secondary node's HTTPS certificate.

## Importing Root and CA Certificates into the CTL of the Primary Node

**Prerequisite:**

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To import root and CA certificates into the CTL of the primary node, complete the following steps:


- 
- Step 1** You must obtain the appropriate CA certificates from the certificate authority that has signed the server certificate of the secondary node and import them into the CTL of the primary node. You do not have to obtain the root and all the intermediate CA certificates. You must obtain the CA certificate from the CA that directly signed the server certificate of the secondary node. You can optionally import additional higher-level signer CA certificates. For example, in a three-tier hierarchy, if the server certificate of the secondary node is signed by a CA and then by a Root CA, you must import the CA certificate of the CA that signed the server certificate of the secondary node and not the Root CA. The certificate validation software should be able to construct the path from the server certificate of the secondary node to the topmost signing certificate in the CA store.
- Step 2** Log into the administrative user interface of your primary node, and import the appropriate CA certificates into the CTL of the primary node. See the [“Adding a Certificate Authority Certificate” section on page 13-18](#) for more information. Repeat this process to add additional CA certificates, if required.
- 

## Importing the CA-Signed Certificate from the Secondary Node into the Primary Node’s CTL

### Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To import the CA-signed certificate from the secondary node into the CTL of the primary node, complete the following steps:

- 
- Step 1** Log into the administrative user interface of the node that you are going to register as your secondary node, and export the CA-signed certificate that is used for HTTPS communication to the file system running your client browser. See the [“Exporting a Certificate Authority Certificate” section on page 13-22](#) for more information.
-  **Note** In the Export dialog box, click the **Export Certificate Only** radio button.
- 
- Step 2** Log into the administrative user interface of your primary node, and import the CA-signed certificate of the secondary node into the CTL of the primary node. See the [“Adding a Certificate Authority Certificate” section on page 13-18](#) for more information.
- 

## Importing the Self-Signed Certificate from the Secondary Node into the CTL of the Primary Node

### Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See [Cisco ISE Admin Group Roles and Responsibilities](#) for more information on the various administrative roles and the privileges associated with each of them.

To import the self-signed certificate from the secondary node into the CTL of the primary node, complete the following steps:

- Step 1** Log into the administrative user interface of the node that you are going to register as your secondary node and export the self-signed certificate that is used for HTTPS communication to the file system running your client browser. See the “[Exporting a Local Certificate](#)” section on page 13-13 for more information.



**Note** In the Export dialog box, click the **Export Certificate Only** radio button.

- Step 2** Log into the administrative user interface of your primary node, and import the self-signed certificate of the secondary node into the CTL of the primary node. See the “[Adding a Certificate Authority Certificate](#)” section on page 13-18 for more information.

## Simple Certificate Enrollment Protocol Profiles

- [Adding and Modifying Simple Certificate Enrollment Protocol Profiles](#), page 13-25
- [Deleting Simple Certificate Enrollment Protocol Profiles](#), page 13-26

## Adding and Modifying Simple Certificate Enrollment Protocol Profiles

To help enable certificate provisioning functions for the variety of mobile devices that users can register on the network, Cisco ISE enables you to configure one or more Simple Certificate Enrollment Protocol (SCEP) Certificate Authority (CA) profiles to point Cisco ISE to multiple CA locations. The benefit of allowing for multiple profiles is to help ensure high availability and perform load balancing across the CA locations that you specify. If a request to a particular SCEP CA goes unanswered three consecutive times, Cisco ISE declares that particular server unavailable and automatically moves to the CA with the next lowest known load and response times, then it begins periodic polling until the server comes back online.

For details on how to set up your Microsoft SCEP server to interoperate with Cisco ISE, see [http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto\\_60\\_byod\\_certificates.pdf](http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf).

To add a new SCEP CA profile, complete the following steps:

- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **SCEP CA Profile**. The SCEP CA Add Profile page appears, as shown in [Figure 13-12](#).

**Figure 13-12** Add a New SCEP CA Profile

SCEP Certificate Authority Certificates > New SCEP Profile

**Add Profile**

**SCEP Certificate Authority**

\* Name

Description

\* URL

- Step 3** Specify a **Name** for the profile to distinguish it from other SCEP CS profile names.
- Step 4** Enter an optional **Description** of the profile.
- Step 5** Specify the **URL** of the SCEP CA server in question, where Cisco ISE can direct SCEP CA requests when users access the network from their mobile devices.
- You can optionally use the adjacent **Test Connectivity** button to verify that Cisco ISE is able to reach the server at the URL that you specify, before clicking the Submit button to end the session. (Either way, Cisco ISE will test the URL before allowing you to save the profile.)
- Step 6** Click **Submit**.

**For Reference:**

Once users' devices receive their validated certificate, they reside on the device as described in [Table 13-1](#).

**Table 13-1** Device Certificate Location

Device	Certificate Storage Location	Access Method
iPhone/iPad	Standard certificate store	Settings > General > Profile
Android	Encrypted certificate store	Invisible to end users. <b>Note</b> Certificates can be removed using Settings > Location & Security > Clear Storage.
Windows	Standard certificate store	Launch mmc.exe from the <b>/cmd</b> prompt, or view in the certificate snap-in.
Mac	Standard certificate store	Application > Utilities > Keychain Access

## Deleting Simple Certificate Enrollment Protocol Profiles

To delete an existing SCEP CA profile, complete the following steps:

- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **SCEP CA Profile**.

**Step 3** Enable the checkboxes for the profiles you want to remove, and click **Delete**.

---

## OCSP Services

The Online Certificate Status Protocol (OCSP) is a protocol that is used for checking the status of x.509 digital certificates. This protocol is an alternative to the CRL (Certificate Revocation List) and addresses issues that result in handling CRLs.

Cisco ISE has the capability to communicate with OCSP servers over HTTP to validate the status of certificates in authentications. The OCSP configuration is configured in a reusable configuration object that can be referenced from any certificate authority (CA) certificate that is configured in Cisco ISE. See [Editing a Certificate Authority Certificate, page 13-19](#).

You can configure CRL and/or OCSP verification per CA. If both are selected, then Cisco ISE first performs verification over OCSP. If a communication problem is detected with both the primary and secondary OCSP servers, or if unknown status is returned for a given certificate, Cisco ISE will fail over to perform CRL checking.

This section contains the following topics:

- [OCSP Certificate Status Values, page 13-27](#)
- [OCSP High Availability, page 13-27](#)
- [Viewing OCSP Services, page 13-28](#)
- [Adding, Editing, or Duplicating OCSP Services, page 13-29](#)
- [Deleting an OCSP Service, page 13-32](#)
- [OCSP Statistics Counters, page 13-32](#)
- [Monitoring OCSP, page 13-33](#)

## OCSP Certificate Status Values

OCSP services return the following values for a given certificate request:

- **Good**—Indicates a positive response to the status inquiry. It means that the certificate is not revoked, and the state is good only until the next time interval (time to live) value.
- **Revoked**—The certificate was revoked.
- **Unknown**—The certificate status is unknown. This can happen if the OCSP is not configured to handle the given certificate CA.
- **Error**—No response was received for the OCSP request.

### Related Topics

[OCSP Statistics Counters, page 13-32](#)

## OCSP High Availability

Cisco ISE has the capability to configure up to two OCSP servers per CA, called primary and secondary OCSP servers. Each OCSP server configuration contains the following parameters:

- URL—The OCSP server URL.
- Nonce—A random number that is sent in the request. This option ensures that old communications cannot be reused in replay attacks.
- Validate Response—Cisco ISE validates the response signature that is received from the OCSP server.

In case of timeout (5 seconds), when Cisco ISE communicates with the primary OCSP server, it falls over to the secondary OCSP server.

Cisco ISE uses the secondary OCSP server for a configurable amount of time before attempting to use the primary server again.

## OCSP Failures

The three general OCSP failure scenarios are as follows:

1. Failed OCSP cache or OCSP client side (Cisco ISE) failures
2. Failed OCSP responder scenarios, for example:
  - a. The first primary OCSP responder not responding, and the secondary OCSP responder responding to the Cisco ISE OCSP request.
  - b. Errors, responses not received from Cisco ISE OCSP requests.

An OCSP responder may not provide a response to the Cisco ISE OCSP request or it may return an OCSP Response Status as “not successful.” OCSP Response Status values can be as follows:

- tryLater
- signRequired
- unauthorized
- internalError
- malformedRequest

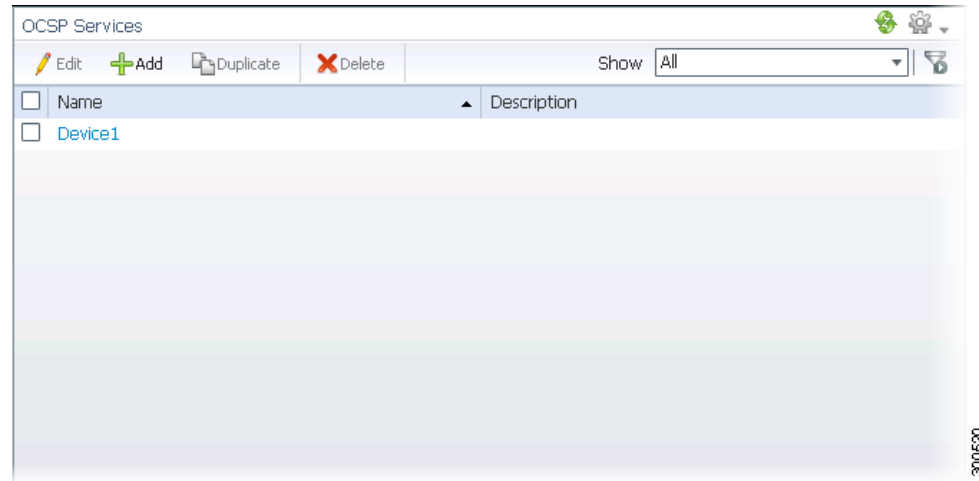
There are many date-time checks, signature validity checks and so on, on the OCSP request. For more details, refer to *RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP* which describes all the possible states, including the error states.

3. Failed OCSP reports

## Viewing OCSP Services

To view OCSP services, complete the following steps:

- 
- Step 1** Choose **Administration > System > Certificates**.
  - Step 2** From the Certificate Operations navigation pane on the left, click **OCSP Services**.  
The OCSP Service List page appears, as shown in [Figure 13-13](#).
  - Step 3** The OCSP Service List page displays the following information for the configured OCSP service:
    - Name
    - Description

**Figure 13-13** OCSP Service List Page

## Adding, Editing, or Duplicating OCSP Services

To add or edit OCSP services, complete the following steps:

- 
- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **OCSP Services**.  
The OCSP Service List page appears. See [Figure 13-13](#).
- Step 3** Click one of the following:
- **Add**
  - **Edit**
  - **Duplicate**

The New OCSP Service page appears. See [Figure 13-14](#).

**Figure 13-14** OCSP Services Add or Edit Page

**Step 4** Provide the following information for the OCSP service:

- Name
- Description

**Step 5** Check the **Enable Secondary Server** check box if you want to enable high availability.

**Step 6** Select one of the following options for high availability:

- **Always Access Primary Server First**—Use this option to check the primary server before trying to move to the secondary server. Even if the primary was checked earlier and found to be unresponsive, Cisco ISE will try to send a request to the primary server before moving to the secondary server.
- **Fallback to Primary Server After Interval**—Use this option when you want Cisco ISE to move to the secondary server and then fall back to the primary server again. In this case, all other requests are skipped, and the secondary server is used for the amount of time that is configured in the text box. The allowed time range is 1-999 minutes.

**Step 7** Provide the URLs or IP addresses of the primary and secondary OCSP servers.

**Step 8** Check or uncheck the following options:

- **Nonce**—You can configure a nonce to be sent as part of the OCSP request. This includes a pseudo-random number in the OCSP request. It is verified that the number that is received in the response is the same as the number that is included in the request. This option ensures that old communications cannot be reused in replay attacks.
- **Validate Response Signature**—The OCSP responder signs the response with one of the following signatures:
  - The CA certificate
  - A different certificate from the CA certificate

In order for Cisco ISE to validate the response signature, the OCSP responder needs to send the response along with the certificate, otherwise the response verification fails, and the status of the certificate cannot be relied on. According to the RFC, OCSP can sign the response using different

certificates. This is true as long as OCSP sends the certificate that signed the response for Cisco ISE to validate it. If OCSP signs the response with a different certificate which is not configured in Cisco ISE, the response verification will fail.

**Step 9** Provide the number of minutes for the Cache Entry Time to Live.

Each response from the OCSP server holds a “nextUpdate” value. This value shows when the status of this certificate will be updated next on the server. When the OCSP response is cached, the two values (one from the configuration and another from response) are compared, and the response is cached for the period of time that is the lowest value of these two. If the “nextUpdate” value is 0, the response is not cached at all.

Cisco ISE will cache OCSP responses for the configured time. The cache is not replicated nor persistent, thus when Cisco ISE restarts the cache is cleared.

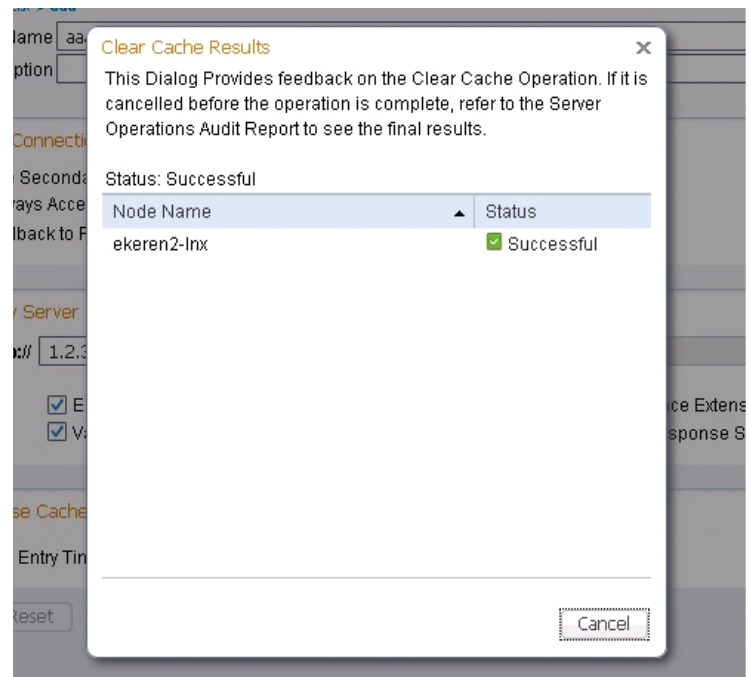
The OCSP cache is used in order to maintain the OCSP responses, for the following reasons:

- To reduce network traffic and load from the OCSP servers on an already known certificate
- To increase the performance of Cisco ISE by caching already known certificate statuses

**Step 10** Click **Clear Cache** to clear entries of all the certificate authorities that are connected to the OCSP service.

In a deployment, Clear Cache interacts with all the nodes and performs the operation. This mechanism updates every node in the deployment. [Figure 13-15](#) shows the Clear Cache Status Message dialog box.

**Figure 13-15** Clear Cache Status Message



## Deleting an OCSP Service

To delete an OCSP service, complete the following steps:

- 
- Step 1** Choose **Administration > System > Certificates**.
- Step 2** From the Certificate Operations navigation pane on the left, click **OCSP Services**.  
The OCSP Service List page appears.
- Step 3** Check the check box next to the OCSP service that you want to delete, and click **Delete**.  
The following message appears: Are you sure you want to delete?
- Step 4** Click **OK** to delete the OCSP service.
- 

## OCSP Statistics Counters

The OCSP counters are used for logging and monitoring the data and health of the OCSP servers. Logging occurs every five minutes. A syslog message is sent to the Cisco ISE Monitoring node and is preserved in the local store, which contains the data for the previous five minutes. After the message is sent, the counters are recalculated for the next interval. This means, after five minutes, a new five minute window interval starts again.

[Table 13-2](#) lists the OCSP syslog messages and their descriptions.

**Table 13-2** OCSP Syslog Messages

Attribute Name	Attribute Description
OCSPPrimaryNotResponsiveCount	The number of nonresponsive primary requests
OCSPSecondaryNotResponsiveCount	The number of nonresponsive secondary requests
OCSPPrimaryCertsGoodCount	The number of 'good' certificates that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsGoodCount	The number of 'good' statuses that are returned for a given CA using the primary OCSP server
OCSPPrimaryCertsRevokedCount	The number of 'revoked' statuses that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsRevokedCount	The number of 'revoked' statuses that are returned for a given CA using the secondary OCSP server
OCSPPrimaryCertsUnknownCount	The number of 'Unknown' statuses that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsUnknownCount	The number of 'Unknown' statuses that are returned for a given CA using the secondary OCSP server
OCSPPrimaryCertsFoundCount	The number of certificates that were found in cache from a primary origin
OCSPSecondaryCertsFoundCount	The number of certificates that were found in cache from a secondary origin

**Table 13-2 OCSP Syslog Messages**

Attribute Name	Attribute Description
ClearCacheInvokedCount	How many times clear cache was triggered since the interval
OCSPCertsCleanedUpCount	How many cached entries were cleaned since the t interval
NumOfCertsFoundInCache	Number of the fulfilled requests from the cache
OCSPCacheCertsCount	Number of certificates that were found in the OCSP cache

## Monitoring OCSP

You can view the OCSP services data in the form of an [OCSP Monitoring Report](#). The OCSP services data is stored in ocspp\_notice database table.

This section describes the process of running this report. For more information on Cisco ISE reports, see [Chapter 25, “Reporting.”](#)

### OCSP Monitoring Report

To view OCSP services data, complete the following steps:

- 
- Step 1** From the Cisco ISE Admin dashboard, select **Operations > Reports > Catalog**.
  - Step 2** In the Reports list, select **Server Instance**.
  - Step 3** In the Reports panel on the right, click the **OCSP Monitoring** radio button.
  - Step 4** From the **Run** drop-down menu, choose a time period over which the report data will be collected:
    - Last 30 minutes
    - Last hour
    - Last 12 hours
    - Today
    - Yesterday
    - Last 7 days
    - Last 30 days
    - Query and run—Use this to get data of more than last 30 days.

The report runs upon choosing the time period, and the **Server Instance > OCSP Monitoring report** data appears.

---

