CHAPTER 12

Managing Certificates

The Cisco Identity Services Engine (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 would be logged in the *catalina.out* file. You can download this file as part of the support bundle (Monitor > 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 expiry warning:

  - 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 Cisco ISE node or primary Administration Cisco 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

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 512 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 in order to see the new certificate. This note applies for both Firefox and Internet Explorer 8 browsers.

You might want to install a CA-signed certificate and configure 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 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.

The 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 choose the import option when you have exported the certificate and key from another Cisco ISE server. You must specify a password to encrypt the 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 on 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.

This section covers the following topics:

Viewing Local Certificates

The Local Certificate page lists all the local certificates added to the 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 12-1:

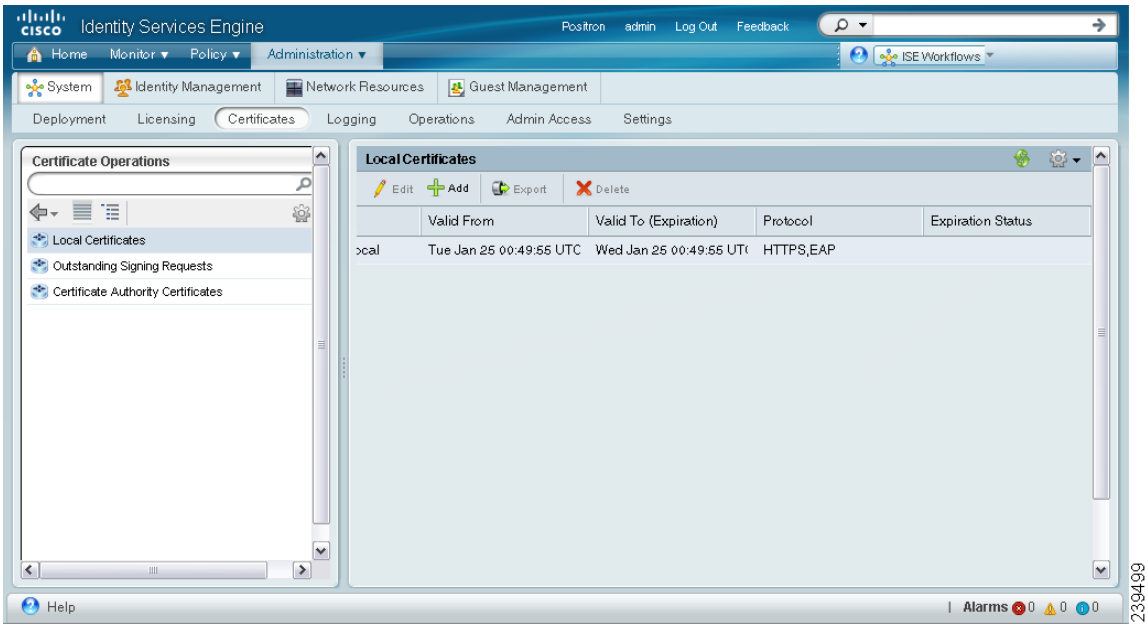
- Friendly Name—Name of the certificate.
- Issued To—Certificate subject or the CN to which the certificate is issued.

  The common name is usually the fully qualified domain name of the Cisco ISE node.
- Issued By—Server that issued this certificate.
- Valid From—Date on which the certificate was created.
- Valid To—Expiration date of the certificate.

- Protocol—Protocols for which to use this certificate.
- Expiration Status—Provides information about the status of the certificate expiration.

  If your certificate expires in less than 90 days, the status is displayed as “Expiring in *x* days.” If your certificate has already expired, the status is displayed as “Certificate has expired.”

Figure 12-1 Local Certificate List Page



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 12-4
- Generating a Self-Signed Certificate, page 12-7
- Generating a Certificate Signing Request, page 12-8 and Binding a CA-Signed Certificate, page 12-10

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 in order 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**.

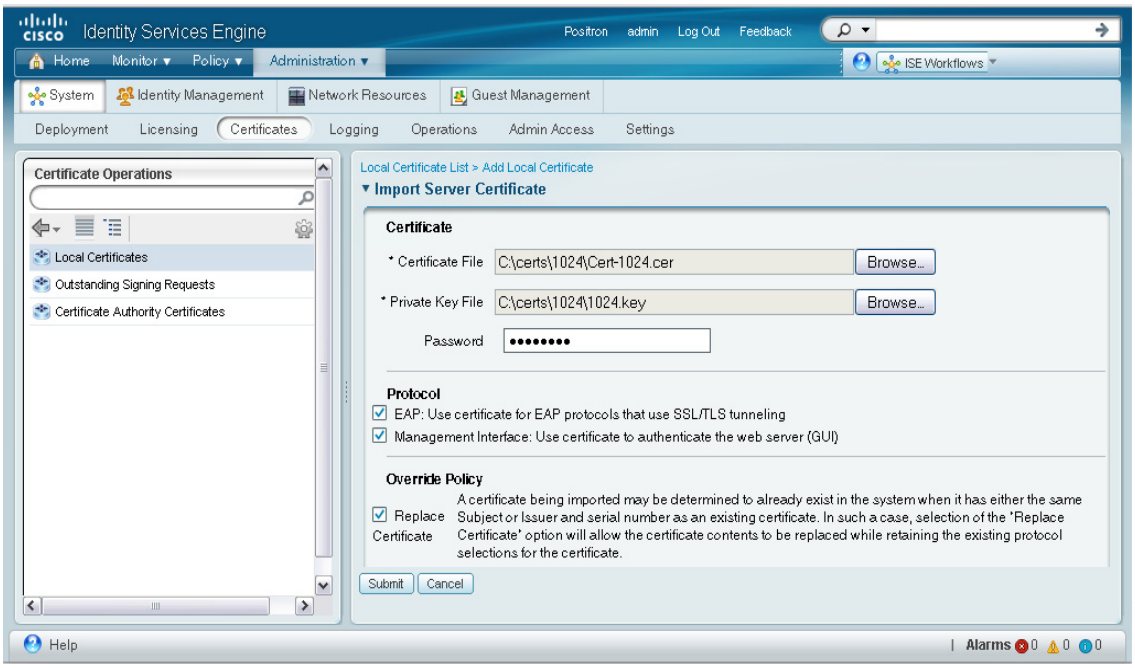
Note To import a local certificate to a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

Step 3 Choose **Add > Import**.

The Import Local Server Certificate page appears as shown in Figure 12-2.

Figure 12-2 Import 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 In the Protocol area:

- Check the **EAP** check box to use this certificate for EAP protocols to identify the Cisco 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 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 Cisco ISE node, you must restart the secondary nodes connected to your primary Cisco 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 1.0* 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**.

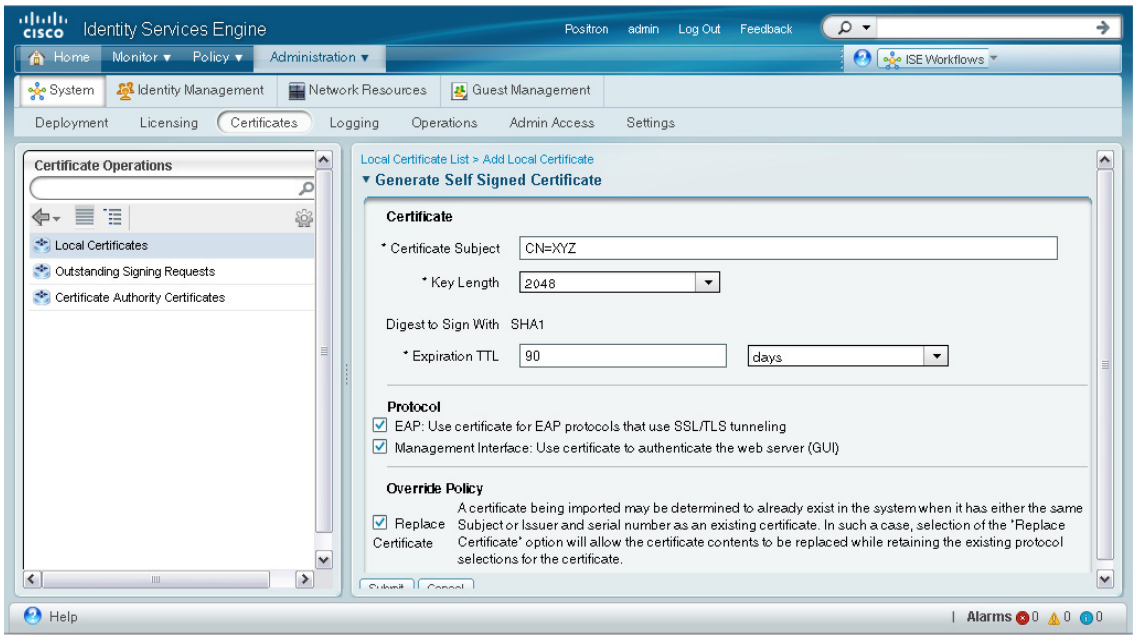
Note To generate a self-signed certificate from a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

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

The Generate Self-Signed Certificate page appears as shown in Figure 12-3.

Figure 12-3 Generating a Self-Signed Certificate Page



Step 4 Enter the following information:

- Certificate subject—A distinguished name (DN) identifying the entity associated with the certificate. The DN must include a common name (CN) value.
- Required key length. Valid values are 512, 1024, 2046, 4096.
- Certificate expiry time. You can specify a time period in days, weeks, months, or years.

Step 5 In the Protocol area:

- Check the **EAP** check box to use this certificate for EAP protocols to identify the Cisco 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 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 generate the self-signed certificate.

If you generate a self-signed certificate on your primary Cisco ISE node, you must restart the secondary nodes connected to your primary Cisco 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 1.0* for more information on these commands.

Note If you are using a self-signed certificate and you need to 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**.

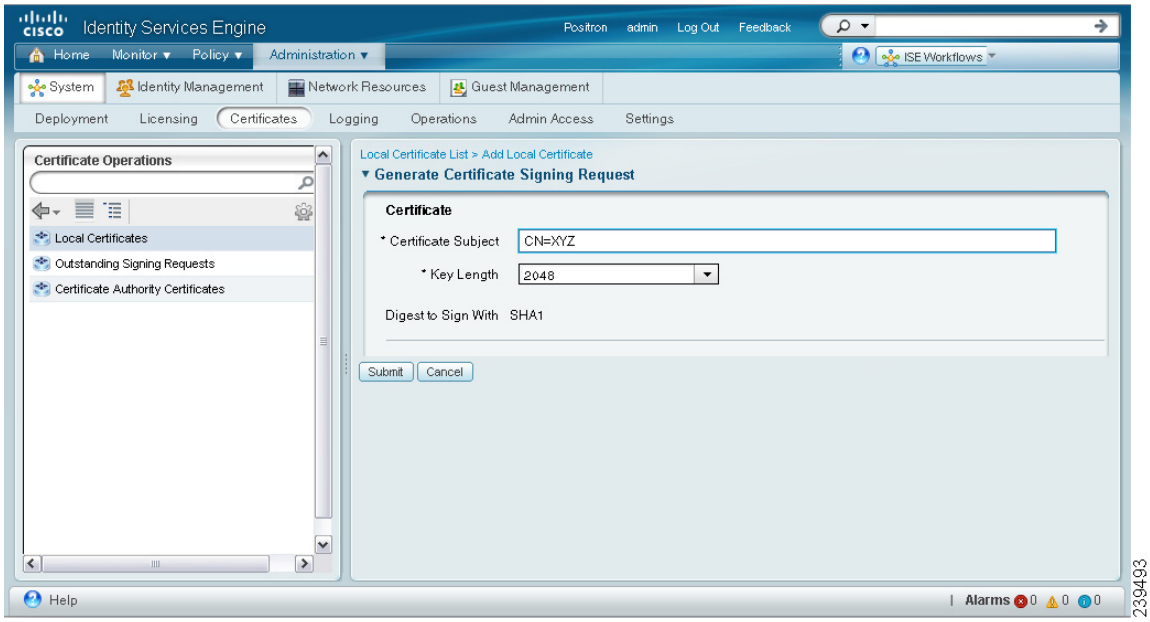
Note To generate a CSR from a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

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

The Generate Certificate Signing Request page appears as shown in Figure 12-4.

Figure 12-4 Generating a Certificate Signing Request



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

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 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.

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**.

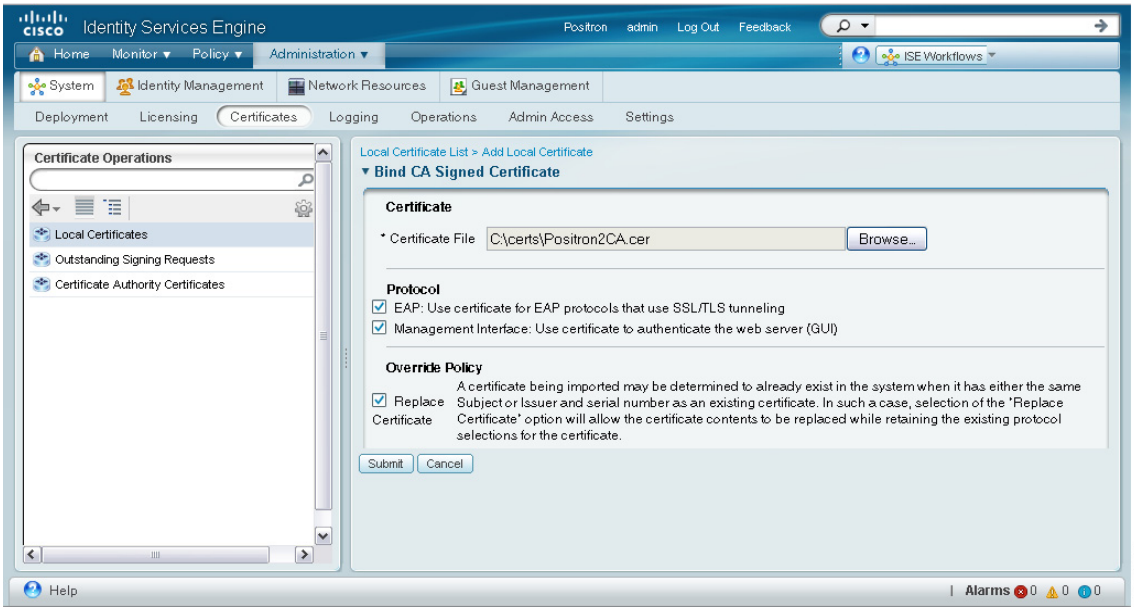
Note To bind a CA-signed certificate to a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

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

The Bind CA Signed Certificate page appears as shown in Figure 12-5.

Figure 12-5 Binding a CA-Signed Certificate



Step 4 Click **Browse** to choose the CA-signed certificate.

Step 5 In the Protocol area:

- Check the **EAP** check box to use this certificate for EAP protocols to identify the Cisco 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 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 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**.

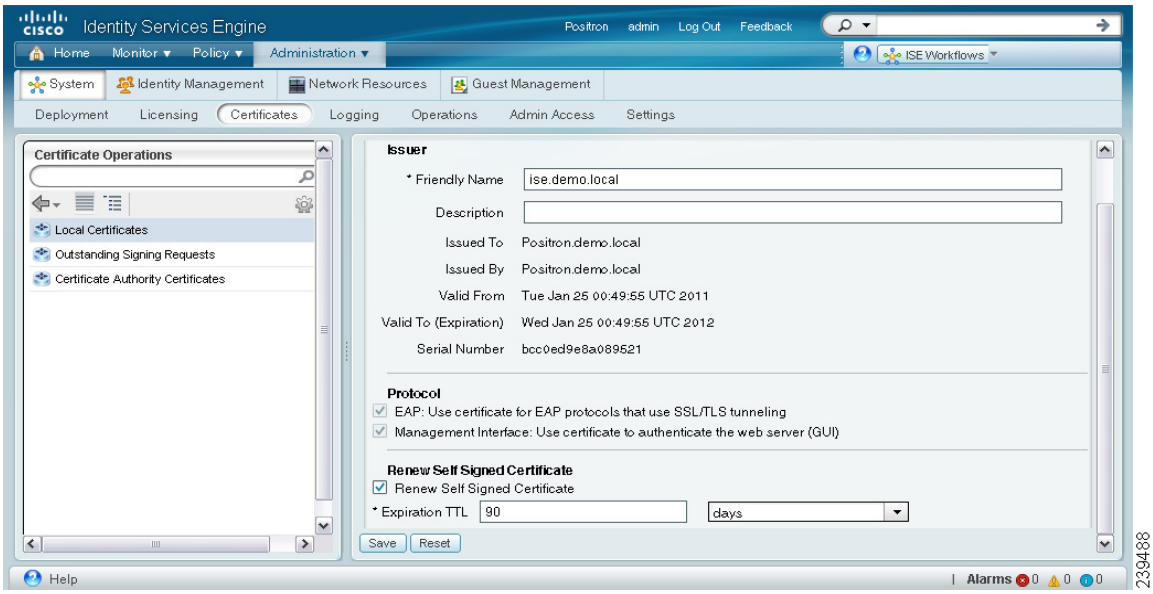
Note To edit a local certificate on a secondary node, choose **Administration > System > Server Certificate**.

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 12-6.

Figure 12-6 Local Certificate Edit Page



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 area:

- Check the **EAP** check box to use this certificate for EAP protocols to identify the Cisco 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 you edit a local certificate on your primary Cisco ISE node, you must restart the secondary nodes connected to your primary Cisco 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 1.0* 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**.

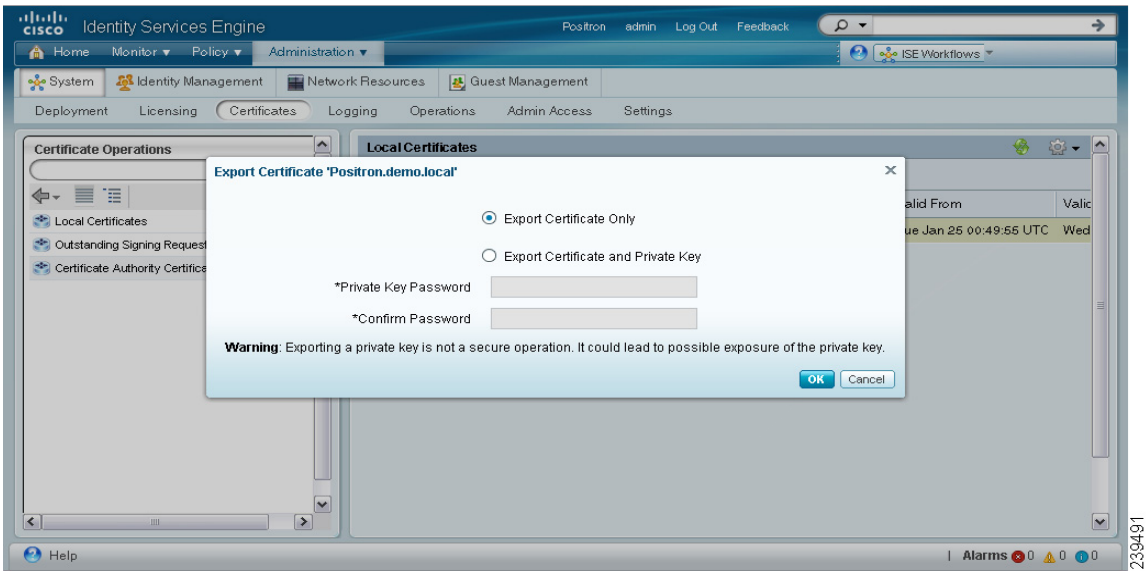
Note To export a local certificate from a secondary node, choose **Administration > System > Server Certificate**.

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 12-7.

Figure 12-7 Exporting a Local Certificate



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

Cisco does 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

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:

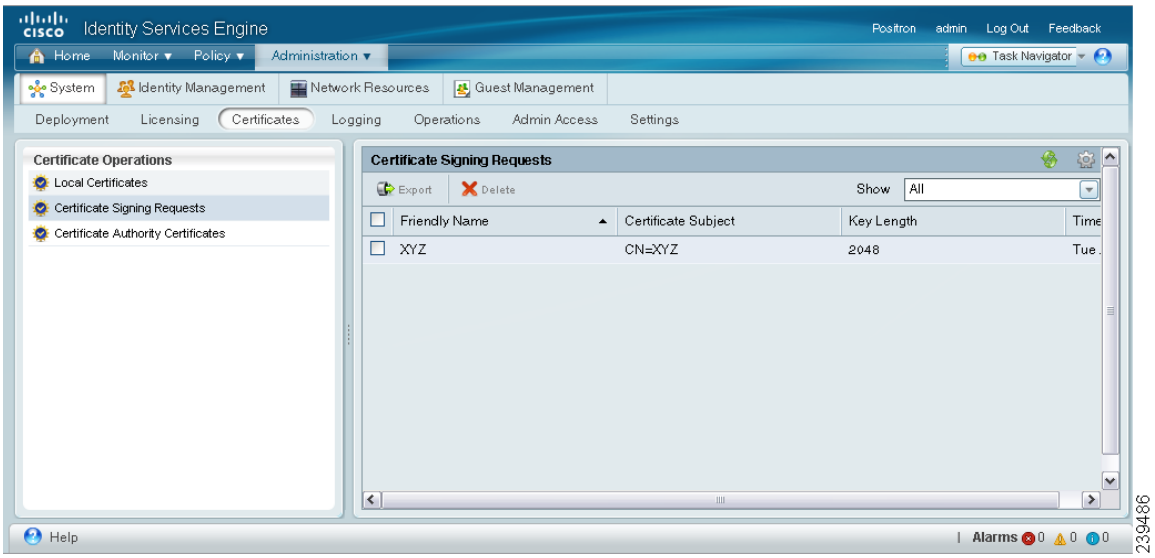
Step 1 Choose **Administration > System > Certificates**.

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 12-8.

Figure 12-8 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 certificates are certificates that are signed by a CA. A CA is a trusted third party that issues digital certificates for use by clients and servers so that they can identify themselves to each other. The digital certificates 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 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 Cisco 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 need to 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 covers the following topics:

Viewing Certificate Authority Certificates

The certificate authority certificates page lists all the 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.

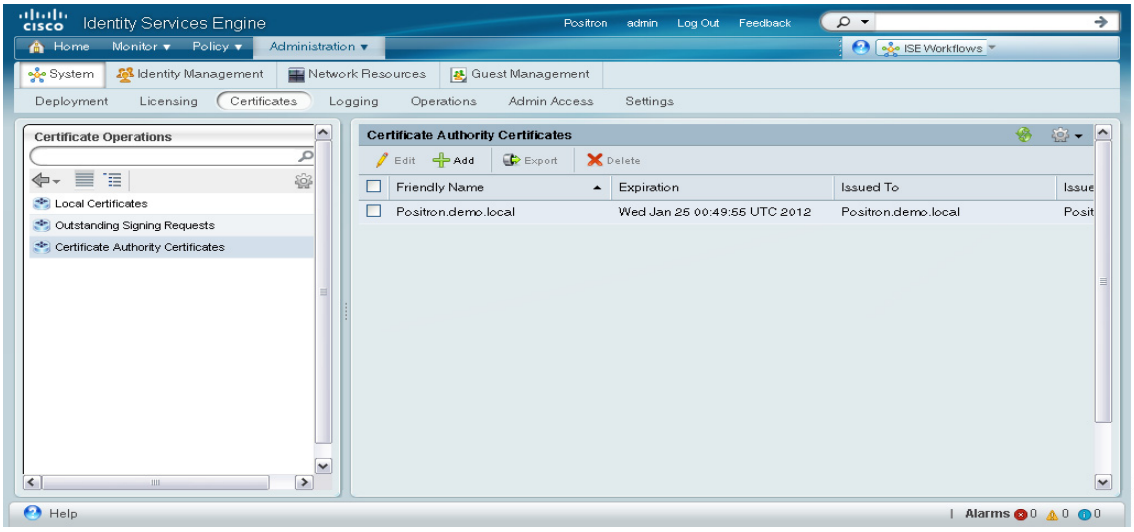
To view the certificate authority certificates, complete the following steps:

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

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

The Certificate Authority Certificates page appears as shown in Figure 12-9.

Figure 12-9 Certificate Authority Certificate List Page



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

- Friendly Name—Name of the certificate authority certificate
- Expiration—The expiration date 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
- Description—Description of the certificate authority certificate

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**.

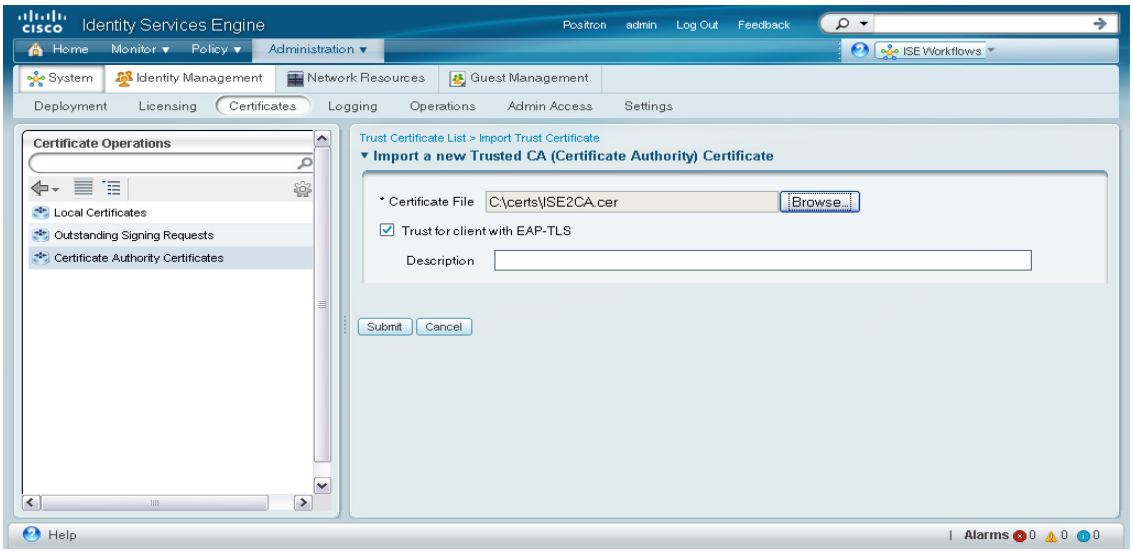
Step 2 From the Certificate Operations navigation pane on the left, click **Certificate Authority Certificates**.

The Certificate Authority Certificates page appears.

Step 3 Click **Add**.

The Import a new Trusted CA (Certificate Authority) Certificate page appears as shown in Figure 12-10.

Figure 12-10 Import a Trusted CA Page



Step 4 Click **Browse** to choose the certificate authority certificate from the file system that is running the client browser.

Step 5 Check the **Trust for client with EAP-TLS** check box if you want to use this certificate in the trust list for EAP-TLS protocols.

Note If you check the Trust for client with EAP-TLS check box, ensure that the keyUsage extension is present and the keyCertSign bit is set, and the basic constraints extension is present with the CA flag set to true.

Step 6 Add an optional description.

Step 7 Click **Submit** to save the certificate authority certificate.

If you add a certificate authority certificate to your primary Cisco ISE node, you must restart the secondary nodes connected to your primary Cisco 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 1.0* 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**.

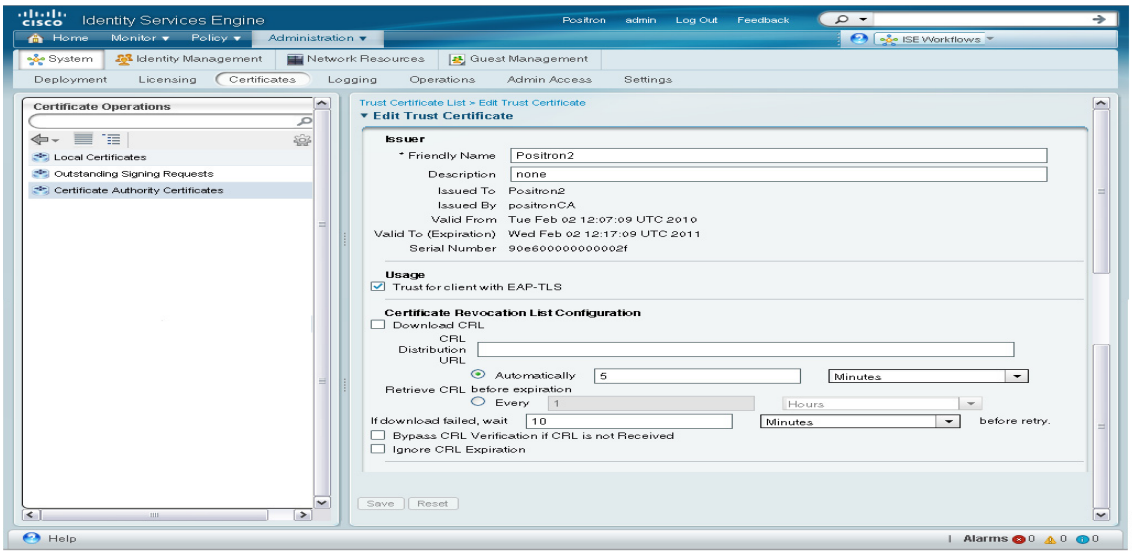
Step 2 From the Certificate Operations navigation pane on the left, click **Certificate Authority Certificates**.

The Certificate Authority Certificates 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 12-11.

Figure 12-11 Certificate Authority Certificate Edit Page



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 with EAP-TLS** check box if you want to use this certificate in the trust list for EAP-TLS protocols.

Note If you check the Trust for client with EAP-TLS check box, ensure that the keyUsage extension is present and the keyCertSign bit is set, and the basic constraints extension is present with the CA flag set to true.

Step 7 In the Certificate Revocation List Configuration area, do the following:

a. Check the **Download CRL** check box for the 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 8 Click **Save** to save the changes you have made to the certificate authority certificate.

If you edit a certificate authority certificate on your primary Cisco ISE node, you must restart the secondary nodes connected to your primary Cisco 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 1.0* 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 Authority Certificates**.

The Certificate Authority Certificates 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.

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 Authority Certificates**.

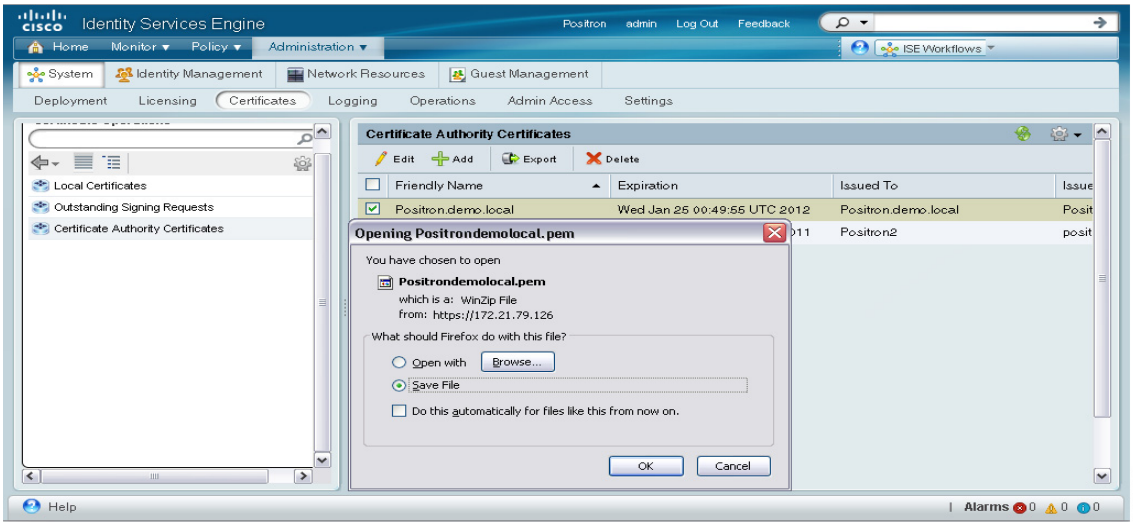
The Certificate Authority Certificates page appears.

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

Note You can only export one certificate at a time.

A pop-up appears as shown in Figure 12-12.

Figure 12-12 Exporting a Certificate Authority Certificate



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 12-19 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 12-4 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 Cisco 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 12-24 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 12-25 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 12-25 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 12-19 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 12-22 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 12-19 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 12-13 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 12-19 for more information.