



## Certificate Management in Cisco ISE

---

A certificate is an electronic document that identifies an individual, a server, a company, or another entity, and associates that entity with a public key. A self-signed certificate is signed by its creator. Certificates can be self-signed or digitally signed by an external CA. A CA-signed digital certificate is considered an industry standard and more secure than a self-signed certificate.

Certificates are used in a network to provide secure access. Certificates identify a Cisco ISE node to an endpoint and secure the communication between that endpoint and the Cisco ISE node.

Cisco ISE uses certificates for:

- Communication between Cisco ISE nodes.
- Communication between Cisco ISE and external servers such as the syslog and feed servers.
- Communication between Cisco ISE and end user portals such as guest, sponsor and BYOD portals.

Manage certificates for all the nodes in your deployment through the Cisco ISE administration portal.

- [Configure Certificates in Cisco ISE to Enable Secure Access, on page 2](#)
- [Certificate Usage, on page 2](#)
- [Certificate Matching in Cisco ISE, on page 5](#)
- [Validity of X.509 Certificates, on page 5](#)
- [Enable Public Key Infrastructure in Cisco ISE, on page 6](#)
- [Wildcard Certificates, on page 7](#)
- [Certificate Hierarchy, on page 11](#)
- [System Certificates, on page 11](#)
- [Trusted Certificates Store, on page 20](#)
- [Default Trusted Certificates in Cisco ISE, on page 29](#)
- [Certificate-Signing Requests, on page 33](#)
- [Set Up Certificates for Portal Use, on page 40](#)
- [User and Endpoint Certificate Renewal, on page 42](#)
- [Extract a Certificate and Private Key from a .pfx File, on page 46](#)
- [Cisco ISE CA Service, on page 47](#)
- [OCSP Services, on page 74](#)

# Configure Certificates in Cisco ISE to Enable Secure Access

Cisco ISE relies on public key infrastructure (PKI) to provide secure communication with both endpoints and administrators and between Cisco ISE nodes in a multinode deployment. PKI relies on X.509 digital certificates to transfer public keys for encryption and decryption of messages, and to verify the authenticity of other certificates representing users and devices. Through the Cisco ISE administration portal, you can manage two categories of X.509 certificates:

- **System Certificates:** These are server certificates that identify a Cisco ISE node to client applications. Every Cisco ISE node has its own system certificates that are stored on the node along with the corresponding private keys.




---

**Note** Cisco ISE cannot import more than one certificate with the same private key. If the certificate is renewed and imported without changing the private key, then the existing certificate is replaced with the imported certificate.

---

- **Trusted Certificates:** These are CA certificates that are used to establish trust for the public keys that are received from users and devices. The Trusted Certificates store also contains certificates that are distributed by the Simple Certificate Enrollment Protocol (SCEP), which enables the registration of mobile devices into the enterprise network. Trusted certificates are managed on the primary PAN, and are automatically replicated to all the other nodes in a Cisco ISE deployment.

In a distributed deployment, you must import the certificate only into the Certificate Trust List (CTL) of the PAN. The certificate gets replicated to the secondary nodes.

To ensure certificate authentication in Cisco ISE is not impacted by minor differences in certificate-driven verification functions, use lowercase hostnames for all Cisco ISE nodes that are deployed in a network.

## Certificate Usage

When you import a certificate into Cisco ISE, specify the purpose for which the certificate is to be used. Choose **Administration > System > Certificates > System Certificates**, and click **Import**.

Choose one or more of the following uses:

- **Admin:** For internode communication and authenticating the administration portal.
- **EAP Authentication:** For TLS-based EAP authentication.
- **RADIUS DTLS:** For RADIUS DTLS server authentication.
- **Portal:** For communicating with all Cisco ISE end-user portals.
- **SAML:** For verifying that the SAML responses are being received from the correct identity provider.
- **pxGrid:** For communicating with the pxGrid controller.

Associate different certificates from each node for communicating with the administration portal (Admin usage), the pxGrid controller (pxGrid usage), and for TLS-based EAP authentication (EAP Authentication usage). However, you can associate only one certificate from each node for each of these purposes.

You must always use a new private key for each certificate that you import into Cisco ISE. When you reuse private keys across certificates, application initialization errors may occur due to a Red Hat NSS database limitation.

When a new certificate is imported into the Red Hat NSS database, any existing certificate that has the same private key is overridden. Cisco ISE application initialization is impacted if an admin certificate's private key is overridden.

With multiple PSNs in a deployment that can service a web portal request, Cisco ISE needs a unique identifier to identify the certificate that must be used for portal communication. When you add or import certificates that are designated for portal use, define a certificate group tag and associate it with the corresponding certificate on each node in your deployment. Associate this certificate group tag to the corresponding end-user portals (guest, sponsor, and personal devices portals). This certificate group tag is the unique identifier that helps Cisco ISE identify the certificate that must be used when communicating with each of these portals. You can only designate one certificate from each node for each of the portals.



---

**Note** An EAP-TLS client certificate should have KeyUsage=Key Agreement and ExtendedKeyUsage=Client Authentication for the following ciphers:

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384

An EAP-TLS client certificate should have KeyUsage=Key Encipherment and ExtendedKeyUsage=Client Authentication for the following ciphers:

- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

To bypass this requirement, choose **Administration > System > Settings > Security Settings** and check the **Accept certificates without validating purpose** checkbox.

---

# Certificate Matching in Cisco ISE

When you set up Cisco ISE nodes in a deployment, the nodes communicate with each other. The system checks the FQDN of each Cisco ISE node to ensure that they match (for example ise1.cisco.com and ise2.cisco.com or if you use wildcard certificates then \*.cisco.com). In addition, when an external machine presents a certificate to a Cisco ISE server, the external certificate that is presented for authentication is checked (or matched) against the certificate in the Cisco ISE server. If the two certificates match, the authentication succeeds.

For Cisco , matching is performed between the nodes (if there are two), and between Cisco and pxGrid.

Cisco ISE checks for a matching subject name as follows:

1. Cisco ISE looks at the subject alternative name extension of the certificate. If the subject alternative name contains one or more DNS names, then one of the DNS names must match the FQDN of the Cisco ISE node. If a wildcard certificate is used, then the wildcard domain name must match the domain in the Cisco ISE node's FQDN.
2. If there are no DNS names in the subject alternative name, or if the subject alternative name is missing entirely, then the common name in the **Subject** field of the certificate or the wildcard domain in the **Subject** field of the certificate must match the FQDN of the node.
3. If no match is found, the certificate is rejected.



---

**Note** X.509 certificates that are imported into Cisco ISE must be in privacy-enhanced mail (PEM) or distinguished encoding rule format. Files containing a certificate chain (a system certificate along with the sequence of trust certificates that sign it) can be imported, subject to certain restrictions.

---

## Validity of X.509 Certificates

X.509 certificates are valid until a specific date. When a system certificate expires, the Cisco ISE functionality that depends on the certificate is impacted. Cisco ISE notifies you about the pending expiration of a system certificate when the expiration date is within 90 days. This notification appears in several ways:

- Colored expiration status icons appear in the **System Certificates** window. The navigation path is **Administration > System > Certificate Management > System Certificates**.
- Expiration messages appear in the Cisco ISE System Diagnostic report. The navigation path is **Operations > Reports > Reports > Diagnostics > System Diagnostic**.
- Expiration alarms are generated 90 days, 60 days, and 30 days before expiration. Expiration alarms are generated every day in the final 30 days before expiration.

If the expiring certificate is a self-signed certificate, you can extend its expiration date by editing the certificate. For a certificate authority-signed certificate, you must allow sufficient time to acquire the replacement certificate from your certificate authority.

# Enable Public Key Infrastructure in Cisco ISE

PKI is a cryptographic technique that enables secure communication and verifies the identity of a user using digital signatures.

**Step 1** Configure system certificates on each node in your deployment for the following:

- TLS-enabled authentication protocols such as EAP-TLS.
- Administration portal authentication.
- Allow browser and REST clients to access Cisco ISE web portals.
- Allow access to pxGrid controller.

By default, a Cisco ISE node is preinstalled with a self-signed certificate that is used for EAP authentication, and for access to administration portal, end user portals, and pxGrid controller. In a typical enterprise environment, this self-signed certificate is replaced with server certificates that are signed by a trusted CA.

**Step 2** Populate the Trusted Certificates store with the CA-signed certificates that are used to establish trust with the user, and device certificates that will be presented to Cisco ISE.

To validate the authenticity of a user or device certificate with a certificate chain that consists of a root CA certificate and one or more intermediate CA certificates:

- Enable the relevant trust option for the root CA.

In the Cisco ISE GUI, choose **Administration > System > Certificates > Certificate Management > Trusted Certificates**. In this window, check the check box for the root CA certificate and click **Edit**. In the **Usage** area, check the necessary check boxes in the **Trusted For** area.

- If you do not want to enable the trust option for the root CA, import the entire CA-signed certificate chain into the Trusted Certificates store.

For inter-node communications, you must populate the Trusted Certificates store with the trust certificates that validate the Admin system certificate of each node in the Cisco ISE deployment. To use the default self-signed certificate for internode communication, export this certificate from the System Certificates window of each Cisco ISE node and import it into the Trusted Certificates store. If you replace the self-signed certificates with CA-signed certificates, it is only necessary to populate the Trusted Certificates store with the appropriate root CA and intermediate CA certificates. You cannot register a node in a Cisco ISE deployment until you complete this step.

If you use self-signed certificates to secure communication between a client and a PSN in a deployment, when BYOD users move from one location to another, EAP-TLS user authentication fails. For such authentication requests that have to be serviced between a few PSNs, you must secure communication between the client and the PSN with an externally-signed CA certificate or use wildcard certificates that are signed by an external CA.

If you intend to get a publicly signed certificate or if the Cisco ISE deployment is to be operated in FIPS mode, you must ensure that all system and trusted certificates are FIPS-compliant. This means that each certificate must have a minimum key size of 2048 bytes, and use SHA-1 or SHA-256 encryption.

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

## Wildcard Certificates

A wildcard certificate uses a wildcard notation (an asterisk and period before the domain name) and the certificate can be shared across multiple hosts in an organization. For example, the CN value for the certificate subject would be a generic hostname such as `aaa.ise.local` and the SAN field would include the same generic hostname and a wildcard notation such as `DNS.1=aaa.ise.local` and `DNS.2=*.ise.local`.

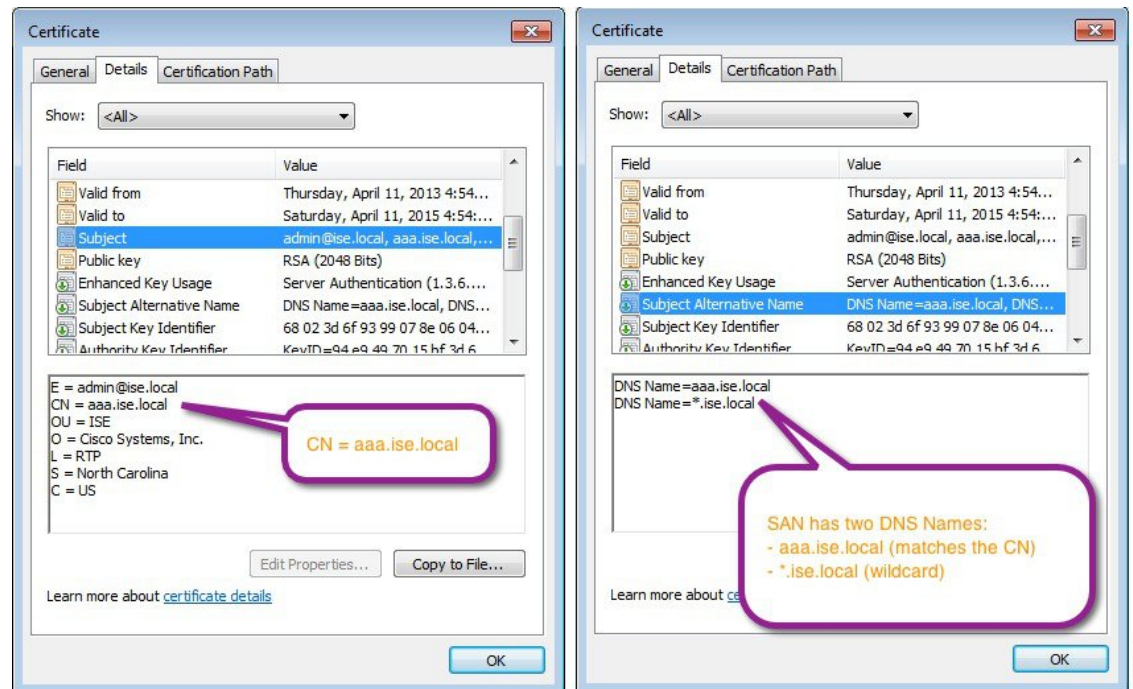
If you configure a wildcard certificate to use `*.ise.local`, you can use the same certificate to secure any other host whose DNS name ends with `“.ise.local,”` such as :

- `aaa.ise.local`
- `psn.ise.local`
- `mydevices.ise.local`
- `sponsor.ise.local`

Wildcard certificates secure communication in the same way as a regular certificate, and requests are processed using the same validation methods.

The following figure is an example of a wildcard certificate that is used to secure a website.

**Figure 1: Example of Wildcard Certificate**



## Wildcard Certificate Support in Cisco ISE

Cisco ISE supports wildcard certificates. In earlier releases, Cisco ISE verified any certificate enabled for HTTPS to ensure the common name field matches the FQDN of the host exactly. If the fields did not match, the certificate could not be used for HTTPS communication.

In earlier releases, Cisco ISE used that common name value to replace the variable in the url-redirect A-V pair string. For all centralized web authentication, onboarding, posture redirection, and so on, the common name value was used.

Cisco ISE uses the hostname of the ISE node as the common name.

## Wildcard Certificates for HTTPS and Extensible Authentication Protocol Communication

You can use wildcard server certificates in Cisco ISE for administration (web-based services) and EAP protocols that use SSL or TLS tunneling. When you use wildcard certificates, you do not need to generate a unique certificate for each Cisco ISE node. Also, you no longer have to populate the SAN field with multiple FQDN values to prevent certificate warnings. Use an asterisk (\*) in the SAN field to share a single certificate across multiple nodes in a deployment and prevent certificate name mismatch warnings. However, the use of wildcard certificates is considered less secure than assigning a unique server certificate to each Cisco ISE node.

When assigning public wildcard certificates to the guest portal and importing sub-CA with root-CA certificates, the certificate chain is not sent until Cisco ISE services are restarted.




---

**Note** If you use wildcard certificates, we recommend that you partition your domain space for greater security. For example, instead of \*.example.com, you can partition it as \*.amer.example.com. If you do not partition your domain, it could lead to serious security issues.

---

Wildcard certificates use an asterisk (\*) and a period before the domain name. For example, the common name value for a certificate's Subject Name would be a generic hostname such as aaa.ise.local and the SAN field would have the wildcard character such as \*.ise.local. Cisco ISE supports wildcard certifications in which the wildcard character (\*) is the left-most character in the presented identifier. For example, \*.example.com or \*.ind.example.com. Cisco ISE does not support certificates in which the presented identifier contains other characters along with the wildcard character. For example, abc\*.example.com, or a\*b.example.com, or \*abc.example.com.

## Fully Qualified Domain Name in URL Redirection

Authorization profile redirects are carried out for central web authentication, device registration web authentication, native supplicant provisioning, mobile device management, client provisioning, and posture services. When Cisco ISE builds an authorization profile redirect, the resulting cisco-av-pair includes a string similar to the following:

```
url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa
```

When processing this request, Cisco ISE substitutes actual values for some keywords in this string. For example, SessionIdValue is replaced with the actual session ID of the request. For an eth0 interface, Cisco ISE replaces the IP in the URL with the FQDN of the Cisco ISE node. For non-eth0 interfaces, Cisco ISE



uses the IP address in the URL. You can assign a host alias (name) for interfaces eth1 through eth3, which Cisco ISE can then substitute in place of IP address during URL redirection.

To do this, use the **ip host** command in the configuration mode from the Cisco ISE CLI ISE /admin(config)# prompt:

```
ip host IP_address host-alias FQDN-string
```

Where *IP\_address* is the IP address of the network interface (eth1 or eth2 or eth3) and *host-alias* is the name that you assign to the network interface. *FQDN-string* is the fully qualified domain name of the network interface. Using this command, you can assign a *host-alias* or an *FQDN-string* or both to a network interface.

Here is an example using the **ip host** command: ip host a.b.c.d sales sales.amerxyz.com

After you assign a host alias to the non-eth0 interface, restart the application services on Cisco ISE using the **application start ise** command.

Use the **no** form of this command to remove the association of the host alias with the network interface.

```
no ip host IP_address host-alias FQDN-string
```

Use the **show running-config** command to view the host alias definitions.

If you provide the *FQDN-string*, Cisco ISE replaces the IP address in the URL with the FQDN. If you provide only the host alias, Cisco ISE combines the host alias with the configured IP domain name to form a complete FQDN and replaces the IP address in the URL with the FQDN. If you do not map a network interface to a host alias, then Cisco ISE uses the IP address of the network interface in the URL.

When you use non-eth0 interfaces for client provisioning or native supplicant or guest flows, ensure that the IP address or host alias for non-eth0 interfaces are configured appropriately in the PSN certificate's SAN fields.

## Advantages of Using Wildcard Certificates

- **Cost savings:** Certificates that are signed by third-party CAs are expensive, especially as the number of servers increases. Wildcard certificates can be used on multiple nodes in the Cisco ISE deployment.
- **Operational efficiency:** Wildcard certificates allow all PSNs to share the same certificate for EAP and web services. In addition to significant cost savings, certificate administration is also simplified by creating the certificate once and applying it on all the PSNs.
- **Reduced authentication errors:** Wildcard certificates address issues seen with Apple iOS devices when the client stores trusted certificates within the profile and does not follow the iOS keychain where the signing root is trusted. When an iOS client first communicates with a PSN, it does not explicitly trust the PSN certificate, although a trusted CA has signed the certificate. Using a wildcard certificate, the certificate is the same across all PSNs, so the user only has to accept the certificate once and successive authentications to different PSNs proceed without errors or prompts.
- **Simplified supplicant configuration:** For example, a Microsoft Windows supplicant with PEAP-MSCHAPv2 and a trusted server certificate requires that you specify each of the server certificate to trust, or the user may be prompted to trust each PSN certificate when the client connects using a different PSN. With wildcard certificates, a single server certificate can be trusted rather than individual certificates from each PSN.
- **Wildcard certificates result in an improved user experience with less prompting and more seamless connectivity.**

## Disadvantages of Using Wildcard Certificates

The following are some of the security considerations that are related to the use of wildcard certificates:

- Loss of auditability and nonrepudiation.
- Increased exposure of the private key.
- Not common or understood by administrators.

Wildcard certificates are considered less secure than using a unique server certificate in each Cisco ISE node. But cost and other operational factors outweigh the security risk.

Security devices such as Cisco Adaptive Security Appliance also support wildcard certificates.

You must be careful when deploying wildcard certificates. For example, if you create a certificate with \*.company.local and an attacker is able to recover the private key, that attacker can spoof any server in the company.local domain. Therefore, it is considered a best practice to partition the domain space to avoid this type of compromise.

To address this possible issue and to limit the scope of use, wildcard certificates may also be used to secure a specific subdomain of your organization. Add an asterisk (\*) in the subdomain area of the common name where you want to specify the wildcard.

For example, if you configure a wildcard certificate for \*.ise.company.local, that certificate may be used to secure any host whose DNS name ends in “.ise.company.local”, such as:

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

## Wildcard Certificate Compatibility

Wildcard certificates are usually created with the wildcard listed as the common name of the certificate subject. Cisco ISE supports this type of construction. However, not all endpoint supplicants support the wildcard character in the certificate subject.

All the Microsoft native supplicants that were tested (including Windows Mobile which is now discontinued) do not support wildcard character in the certificate subject.

You can use another supplicant, such as Network Access Manager that might allow the use of wildcard characters in the Subject field.

You can also use special wildcard certificates such as DigiCert's Wildcard Plus that is designed to work with incompatible devices by including specific subdomains in the Subject Alternative Name of the certificate.

Although the Microsoft supplicant limitation appears to be a deterrent to using wildcard certificates, there are alternative ways to create the wildcard certificate that allow it to work with all the devices tested for secure access, including the Microsoft native supplicants.

To do this, instead of using the wildcard character in the Subject, you must use the wildcard character in the Subject Alternative Name field instead. The Subject Alternative Name field maintains an extension that is designed for checking the domain name (DNS name). See RFC 6125 and RFC 2128 for more information.

## Certificate Hierarchy

In the administration portal, view the certificate hierarchy or the certificate trust chain of all endpoint, system, and trusted certificates. The certificate hierarchy includes the certificate, all the intermediate CA certificates, and the root certificate. For example, when you choose to view a system certificate from the the administration portal, the details of the corresponding system certificate are displayed. The certificate hierarchy is displayed at the top of the certificate. Click a certificate in the hierarchy to view its details. The self-signed certificate does not have any hierarchy or trust chain.

In the certificate listing windows, you will see one of the following icons in the **Status** column:

- Green icon: Indicates a valid certificate (valid trust chain).
- Red icon: Indicates an error (for example, trust certificate missing or expired).
- Yellow icon: Warns that a certificate is about to expire and prompts renewal.

## System Certificates

Cisco ISE system certificates are server certificates that identify a Cisco ISE node to other nodes in the deployment and to client applications. System certificates are:

- Used for inter-node communication in a Cisco ISE deployment. Check the **Admin** check box in the **Usage** area of these certificates.
- Used by browser and REST clients who connect to Cisco ISE web portals. Check the **Portal** check box in the **Usage** area of these certificates.
- Used to form the outer TLS tunnel with PEAP and EAP-FAST. Check the **EAP Authentication** check box in the **Usage** area for mutual authentication with EAP-TLS, PEAP, and EAP-FAST.
- Used for RADIUS DTLS server authentication.
- Used to communicate with SAML identity providers. Check the **SAML** check box in the **Usage** area of this certificate. If you choose the SAML option, you cannot use this certificate for any other service.

A SAML certificate is used by multiple Cisco ISE services such as Posture services and licensing communication between Cisco ISE and the Cisco Smart Software Manager. If you delete the SAML certificate from your Cisco ISE, the associated services are disrupted.

- Used to communicate with the pxGrid controller. Check the **pxGrid** check box in the **Usage** area of these certificates.

Install valid system certificates on each node in your Cisco ISE deployment. By default, two self-signed certificates and one signed by the internal Cisco ISE CA are created on a Cisco ISE node during installation time:

- A self-signed server certificate designated for EAP, Admin, Portal, and RADIUS DTLS (it has a key size of 2048 and is valid for one year).
- A self-signed SAML server certificate that can be used to secure communication with a SAML identity provider (it has a key size of 2048 and is valid for one year).

- An internal Cisco ISE CA-signed server certificate that can be used to secure communication with pxGrid clients (it has a key size of 4096 and is valid for one year).

When you set up a deployment and register a secondary node, the certificate that is designated for pxGrid controller is automatically replaced with a certificate that is signed by the primary node's CA. Thus, all pxGrid certificates become part of the same PKI trust hierarchy.



#### Note

- When you export a wildcard system certificate to be imported into the other nodes (for inter-node communication), ensure that you export the certificate and the private key, and specify an encryption password. During import, you will need the certificate, private key, and encryption password.
- Cisco ISE supports the use of RSASSA-PSS algorithm only for trusted certificates and endpoint certificates for EAP-TLS authentication. When you view the certificate, the signature algorithm is listed as 1.2.840.113549.1.1.10 instead of the algorithm name.

Cisco ISE does not support system certificates that use RSASSA-PSS as the signature algorithm. This is applicable for the server certificate, root certificate, and intermediate CA certificate.

For supported key and cipher information for your release, see the appropriate version of the [Cisco Identity Services Engine Network Component Compatibility](#) guide.

We recommend that you replace the self-signed certificate with a CA-signed certificate for greater security. To obtain a CA-signed certificate, you must:

1. [Create a Certificate-Signing Request and Submit it to a Certificate Authority, on page 33](#)
2. [Import a Root Certificate into the Trusted Certificate Store, on page 27](#)
3. [Bind a CA-Signed Certificate to a Certificate Signing Request, on page 33](#)

#### ISE Community Resource

[How To: Implement ISE Server-Side Certificates](#)

[Certificate Renewal on Cisco Identity Services Engine Configuration Guide](#)

## View System Certificates

The **System Certificate** window lists all the system certificates added to Cisco ISE.

#### Before you begin

To perform the following task, you must be a Super Admin or System Admin.

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

**Step 2** The following columns are displayed in the **System Certificates** window:

- **Friendly Name:** Name of the certificate.
- **Usage:** The services for which this certificate is used.

- **Portal group tag:** Applicable only for certificates that are designated for portal use. This field specifies which certificate has to be used for portals.
- **Issued To:** Common Name of the certificate subject.
- **Issued By:** Common Name of the certificate issuer
- **Valid From:** Date on which the certificate was created, also known as the "Not Before" certificate attribute.
- **Valid To (Expiration):** Expiration date of the certificate, also known as the "Not After" certificate attribute. The following icons are displayed next to the expiration date:
  - Green icon: Expiring in more than 90 days.
  - Blue icon: Expiring in 90 days or less.
  - Yellow icon: Expiring in 60 days or less.
  - Orange icon: Expiring in 30 days or less.
  - Red icon: Expired.

---

## Import a System Certificate

You can import a system certificate for any Cisco ISE node from the administration portal.



---

**Note** Changing the certificate of the admin role certificate on a primary PAN node restarts services on all other nodes. The system restarts one node at a time, after the primary PAN restart is complete.

---

### Before you begin

- Ensure that you have the system certificate and the private key file on the system that is running on the client browser.
- If the system certificate that you import is signed by an external CA, import the relevant root CA and intermediate CA certificates into the Trusted Certificates store (**Administration > System > Certificates > Trusted Certificates**).
- If the system certificate that you import contains 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 perform the following task, you must be a Super Admin or System Admin.

---

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

**Step 2** Click **Import**.  
The **Import Server Certificate** window is displayed.

**Step 3** Enter the values for the certificate that you are going to import.

**Step 4** Click **Submit**.

## System Certificate Import Settings

*Table 1: System Certificate Import Settings*

Field Name	Description
<b>Select Node</b>	(Required) Choose the Cisco ISE node on which you want to import the system certificate from the drop-down list.
<b>Certificate File</b>	(Required) Click <b>Choose File</b> and choose the certificate file from your local system.
<b>Private Key File</b>	(Required) Click <b>Choose File</b> and choose the private key file from your local system.
<b>Password</b>	(Required) Enter the password to decrypt the private key file.
<b>Friendly Name</b>	Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the following format:  <common name> # <issuer> # <nnnnn> where <nnnnn> is a unique five-digit number.
<b>Allow Wildcard Certificates</b>	Check this check box if you want to import a wildcard certificate. A wildcard certificate uses a wildcard notation (an asterisk and period before the domain name). Wildcard certificates are shared across multiple hosts in an organization.  If you check this check box, Cisco ISE imports this certificate to all the other nodes in the deployment.
<b>Validate Certificate Extensions</b>	Check this check box if you want Cisco ISE to validate the certificate extensions. If you check this check box and the certificate that you import contains a basic constraints extension with the CA flag set to true, ensure that the key usage extension is present. The keyEncipherment bit or the keyAgreement bit, or both, must also be set.

Field Name	Description
Usage	<p>Choose the service for which this system certificate must be used:</p> <ul style="list-style-type: none"> <li>• <b>Admin:</b> Server certificate used to secure communication with the administration portal and between the Cisco ISE nodes in a deployment. <ul style="list-style-type: none"> <li><b>Note</b> Changing the certificate of the admin role certificate on the primary PAN restarts services on all other Cisco ISE nodes.</li> </ul> </li> <li>• <b>EAP Authentication:</b> Server certificate used for authentications that use the EAP protocol for SSL or TLS tunneling.</li> <li>• <b>RADIUS DTLS:</b> Server certificate used for RADIUS DTLS authentication.</li> <li>• <b>pxGrid:</b> Client and server certificate to secure communication between the pxGrid client and the server.</li> <li>• <b>:</b> Used by <b>Syslog Over Cisco ISE Messaging</b> feature, which enables MnT WAN survivability for built-in UDP syslog collection targets (LogCollector and LogCollector2).</li> <li>• <b>SAML:</b> Server certificate used to secure communication with the SAML identity provider. A certificate that is designated for SAML use cannot be used for any other service such as Admin, EAP authentication, and so on.</li> <li>• <b>Portal:</b> Server certificate used to secure communication with all Cisco ISE web portals</li> </ul>



**Note** If the certificate is generated by other third-party tools and not Cisco ISE, you cannot import the certificate or its private key into Cisco ISE.

#### Related Topics

[System Certificates](#), on page 11

[View System Certificates](#), on page 12

[Import a System Certificate](#), on page 13

## Generate a Self-Signed Certificate

Add a new local certificate by generating a self-signed certificate. Cisco recommends that you only employ self-signed certificates for your internal testing and evaluation needs. If you plan to deploy Cisco ISE in a production environment, use CA-signed certificates whenever possible to ensure more uniform acceptance around a production network.



**Note** If you use a self-signed certificate and you want to change the hostname of your Cisco ISE node, log in to the administration portal of the Cisco ISE node, delete the self-signed certificate that has the old hostname, and generate a new self-signed certificate. Otherwise, Cisco ISE continues to use the self-signed certificate with the old hostname.

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

**Self-Signed Certificate Settings***Table 2: Self-Signed Certificate Settings*

Field Name	Usage Guidelines
<b>Select Node</b>	(Required) Choose the node for which you want to generate the system certificate from the drop-down list.
<b>Common Name (CN)</b>	(Required if you do not specify a SAN) By default, the common name is the FQDN of the Cisco ISE node for which you are generating the self-signed certificate.
<b>Organizational Unit (OU)</b>	Organizational Unit name. For example, Engineering.
<b>Organization (O)</b>	Organization name. For example, Cisco.
<b>City (L)</b>	(Do not abbreviate) City name. For example, San Jose.
<b>State (ST)</b>	(Do not abbreviate) State name. For example, California.
<b>Country (C)</b>	Country name. Enter the two-letter ISO country code. For example, US.
<b>Subject Alternative Name (SAN)</b>	An IP address, DNS name, or Uniform Resource Identifier (URI) that is associated with the certificate.
<b>Key Type</b>	The algorithm to be used for creating the public key, either RSA or ECDSA.
<b>Key Length</b>	<p>The bit size for the public key. Choose one of the following options from the drop-down list for RSA:</p> <ul style="list-style-type: none"> <li>• 512</li> <li>• 1024</li> <li>• 2048</li> <li>• 4096</li> </ul> <p>Choose one of the following options from the drop-down list for ECDSA:</p> <ul style="list-style-type: none"> <li>• 256</li> <li>• 384</li> </ul> <p><b>Note</b> RSA and ECDSA public keys might have different key lengths for the same security level.</p> <p>Choose 2048 if you plan to get a public CA-signed certificate or deploy Cisco ISE as a FIPS-compliant policy management system.</p>



Field Name	Usage Guidelines
<b>Digest to Sign With</b>	Choose one of the following hashing algorithms from the drop-down list: <ul style="list-style-type: none"> <li>• SHA-1</li> <li>• SHA-256</li> </ul>
<b>Certificate Policies</b>	Enter the certificate policy OID or list of OIDs that the certificate should conform to. Use a comma or space to separate the OIDs.
<b>Expiration TTL</b>	Specify the number of days after which the certificate expires. Choose the value from the drop-down lists.
<b>Friendly Name</b>	Enter a friendly name for the certificate. 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.
<b>Allow Wildcard Certificates</b>	Check this check box if you want to generate a self-signed wildcard certificate. A wildcard certificate uses a wildcard notation (an asterisk and period before the domain name) and allows the certificate to be shared across multiple hosts in an organization.
<b>Usage</b>	Choose the service for which this system certificate must be used: <ul style="list-style-type: none"> <li>• <b>Admin:</b> Server certificate used to secure communication with the administration portal and between the Cisco ISE nodes in a deployment.</li> <li>• <b>EAP Authentication:</b> Server certificate used for authentications that use the EAP protocol for SSL or TLS tunneling.</li> <li>• <b>RADIUS DTLS:</b> Server certificate used for RADIUS DTLS authentication.</li> <li>• <b>pxGrid:</b> Client and server certificate to secure communication between the pxGrid client and the server.</li> <li>• <b>SAML:</b> Server certificate used to secure communication with the SAML identity provider. A certificate that is designated for SAML use cannot be used for any other service such as Admin, EAP authentication, and so on.</li> <li>• <b>Portal:</b> Server certificate used to secure communication with all Cisco ISE web portals.</li> </ul>

**Related Topics**

[System Certificates](#), on page 11

[View System Certificates](#), on page 12

[Generate a Self-Signed Certificate](#), on page 15

## Edit a System Certificate

Use this window to edit a system certificate and to renew a self-signed certificate. When you edit a wildcard certificate, the changes are replicated to all the nodes in the deployment. If you delete a wildcard certificate, that wildcard certificate is removed from all the nodes in the deployment.

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

- 
- Step 1** Choose **Administration > System > Certificates > System Certificates**.
  - Step 2** Check the check box next to the certificate that you want to edit, and click **Edit**.
  - Step 3** To renew a self-signed certificate, check the **Renewal Period** check box and enter the expiration Time to Live (TTL) in days, weeks, months, or years. Choose the required value from the drop-down lists.
  - Step 4** Click **Save**.

If the **Admin** check box is checked, then the application server on the Cisco ISE node restarts. In addition, if the Cisco ISE node is the PAN in a deployment, then the application server on all the other nodes in the deployment also restart. The system restarts one node at a time, after the primary PAN restart has completed.

For information on troubleshooting, see [Launching a BYOD Portal using Google Chrome 65, on page 18](#) [Configuring Wireless BYOD setup using Mozilla Firefox 64, on page 18](#).

**Launching a BYOD Portal using Google Chrome 65**

When using Chrome 65 and above to launch Cisco ISE, it can cause BYOD portal or Guest portal to fail to launch in the browser although the URL is redirected successfully. This is because of a new security feature introduced by Google that requires all certificates to have a **Subject Alternative Name** field. For Cisco ISE Release 2.4 and later, you must fill the **Subject Alternative Name** field.

To launch BYOD portal with Chrome 65 and above, follow the steps below:

- 
- Step 1** Generate a new self-signed certificate from the Cisco ISE GUI by filling the Subject Alternative Name field. Both DNS and IP Address must be filled.
  - Step 2** Cisco ISE services restart.
  - Step 3** Redirect the portal in Chrome browser.
  - Step 4** From browser, **View Certificate > Details > Copy the certificate by selecting base-64 encoded**
  - Step 5** Install the certificate in Trusted path.
  - Step 6** Close the Chrome browser and try to redirect the portal.
- 

**Configuring Wireless BYOD setup using Mozilla Firefox 64**

When configuring wireless BYOD setup for the browser Firefox 64 and later releases, with operating systems Win RS4 or RS5, you may not be able to add Certificate Exception. This behaviour is expected in case of fresh installs of Firefox 64 and later releases, and does not occur in case of upgrading to Firefox 64 and above from a previous version. The following steps allow you to add certificate exception in this case:

- 
- Step 1** Configure for BYOD flow single or dual PEAP or TLS.
  - Step 2** Configure CP Policy with Windows ALL option.
  - Step 3** Connect Dot1.x or MAB SSID in end client Windows RS4 or Windows RS5.

**Step 4** Type any URL in FF64 browser for redirection to Guest or BYOD portal.

**Step 5** Click **Add Exception > Unable to add certificate**, and proceed with flow.

As a workaround, add the certificate manually for Firefox 64. In the Firefox 64 browser, choose **Options > Privacy & Settings > View Certificates > Servers > Add Exception**.

---

## Delete a System Certificate

It is safe to delete system certificates that are tagged as *Not in use* in **Administration > System > Certificates > System Certificates**.

Although you can delete multiple certificates from the System Certificates store at a time, you must have at least one certificate to use for Admin and EAP authentication. Also, you cannot delete any certificate that is in use for Admin, EAP Authentication, Portals, or pxGrid controller. However, you can delete the pxGrid certificate when the service is disabled.

If you choose to delete a wildcard certificate, the certificate is removed from all the Cisco ISE nodes in the deployment.

---

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

**Step 2** Check the check boxes next to the certificates that you want to delete, and click **Delete**.

A warning message is displayed.

**Step 3** Click **Yes** to delete the certificate.

---

## Export a System Certificate

You can export a system certificate or a certificate and its associated private key. If you export a certificate and its private key for backup purposes, you can reimport them later if needed.

### Before you begin

To perform the following task, you must be a Super Admin or System Admin.

---

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

**Step 2** Check the check box next to the certificate that you want to export and click **Export**.

**Step 3** Choose whether to export only the certificate, or the certificate and its associated private key.

**Tip** We do not recommend exporting the private key that is associated with a certificate because its value may be exposed. If you must export a private key (for example, when you export a wildcard system certificate to be imported into the other Cisco ISE nodes for inter-node communication), specify an encryption password for the private key. You must specify this password while importing this certificate into another Cisco ISE node to decrypt the private key.

**Step 4** Enter the password if you have chosen to export the private key. The password should be at least eight characters long.

---

**Step 5** Click **Export** 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 PEM format. If you export both the certificate and private key, the certificate is exported as a .zip file that contains the certificate in the PEM format and the encrypted private key file.

---

## Trusted Certificates Store

The Trusted Certificates store contains X.509 certificates that are used for trust and for Simple Certificate Enrollment Protocol (SCEP).

X.509 certificates imported to Cisco ISE must be in PEM or Distinguished Encoding Rule format. Files containing a certificate chain, a system certificate along with the sequence of trust certificates that sign it, are imported, subject to certain restrictions.

When assigning public wildcard certificates to the guest portal and importing sub-CA with root-CA certificates, the certificate chain is not sent until the Cisco ISE services restart.

The certificates in the Trusted Certificate store are managed on the primary PAN, and are replicated to every node in the Cisco ISE deployment. Cisco ISE supports wildcard certificates.

Cisco ISE uses the trusted certificates for the following purposes:

- To verify client certificates used for authentication by endpoints, and by Cisco ISE administrators accessing ISE-PICthe administration portal using certificate-based administrator authentication.
- To enable secure communication between Cisco ISE nodes in a deployment. The Trusted Certificates store must contain the chain of CA certificates needed to establish trust with the system certificate on each node in a deployment.
  - If a self-signed certificate is used for the system certificate, the self-signed certificate from each node must be placed in the Trusted Certificates store of the PAN.
  - If a CA-signed certificate is used for the system certificate, the CA root certificate, and any intermediate certificates in the trust chain, must be placed in the Trusted Certificates store of the PAN.
- To enable Secure LDAP authentication, a certificate from the certificate store must be selected when defining an LDAP identity source that will be accessed over SSL.
- To distribute to personal devices preparing to register in the network using the personal devices portals. Cisco ISE implements the SCEP on PSNs to support personal device registration. A registering device uses the SCEP protocol to request a client certificate from a PSN. The PSN contains a registration authority (RA) that acts as an intermediary. The RA receives and validates the request from the registering device and then forwards the request to an external CA or the internal Cisco ISE CA, which issues the client certificate. The CA sends the certificate back to the RA, which returns it to the device.

Each SCEP CA used by Cisco ISE is defined by a SCEP RA profile. When a SCEP RA profile is created, two certificates are automatically added to the Trusted Certificates store:

- A CA certificate (a self-signed certificate)
- An RA certificate (a Certificate Request Agent certificate), which is signed by the CA.

The SCEP protocol requires that these two certificates be provided by the RA to a registering device. By placing these two certificates in the Trusted Certificates store, they are replicated to all PSN nodes for use by the RA on those nodes.



**Note** When a SCEP RA profile is removed, the associated CA chain is also removed from the Trusted Certificates store. However, if the same certificates are referenced by secure syslog, LDAP, system, or trust certificates, only the SCEP profile is deleted.

### ISE Community Resource

[Install a Third-Party CA Certificate in ISE](#)

## Certificates in Trusted Certificates Store

The Trusted Certificate store is prepopulated with trusted certificates: manufacturing certificate, root certificate, and other trusted certificates. The Root certificate (Cisco Root CA) signs the Manufacturing (Cisco CA Manufacturing) certificate. These certificates are disabled by default. If you have Cisco IP phones as endpoints in your deployment, enable the root and manufacturing certificates so the Cisco-signed client certificates for the phones are authenticated.

## List of Trusted Certificates

*Table 3: Trusted Certificates Window Columns*

Field Name	Usage Guidelines
<b>Friendly Name</b>	Displays the name of the certificate.
<b>Status</b>	This column displays <b>Enabled</b> or <b>Disabled</b> . If the certificate is disabled, Cisco ISE will not use the certificate for establishing trust.
<b>Trusted for</b>	Displays one or more of the following services for which the certificate is used. <ul style="list-style-type: none"> <li>• <b>Infrastructure</b></li> <li>• <b>Cisco Services</b></li> <li>• <b>Endpoints</b></li> </ul>
<b>Issued To</b>	Displays the common name of the certificate subject.
<b>Issued By</b>	Displays the common name of the certificate issuer.
<b>Valid From</b>	Displays the date and time when the certificate was issued. This value is also known as the “Not Before” certificate attribute.
<b>Expiration Date</b>	Displays the date and time when the certificate expires. This value is also known as the “Not After” certificate attribute.

Field Name	Usage Guidelines
<b>Expiration Status</b>	<p>Provides information about the status of the certificate expiration. There are five icons and categories of informational message that are displayed in this column:</p> <ul style="list-style-type: none"> <li>• <b>Green:</b> Expiring in more than 90 days</li> <li>• <b>Blue:</b> Expiring in 90 days or less</li> <li>• <b>Yellow:</b> Expiring in 60 days or less</li> <li>• <b>Orange:</b> Expiring in 30 days or less</li> <li>• <b>Red:</b> Expired</li> </ul>

**Related Topics**

[Trusted Certificates Store](#), on page 20

[View Trusted Certificates](#), on page 23

[Change the Status of a Certificate in Trusted Certificates Store](#), on page 23

[Add a Certificate to Trusted Certificates Store](#), on page 23

## Trusted Certificate Naming Constraints

A trusted certificate in CTL may contain a name constraint extension. This extension defines a namespace for values of all subject name and subject alternative name fields of subsequent certificates in a certificate chain. Cisco ISE does not check constraints that are specified in a root certificate.

Cisco ISE supports the following name constraints:

- Directory name

The directory name constraint should be a prefix of the directory name in the subject or subject alternative name field. For example:

- Correct subject prefix:

CA certificate name constraint: Permitted: O=Cisco

Client certificate subject: O=Cisco,CN=Salomon

- Incorrect subject prefix:

CA certificate name constraint: Permitted: O=Cisco

Client certificate subject: CN=Salomon,O=Cisco

- DNS
- Email
- URI (The URI constraint must start with a URI prefix such as http://, https://, ftp://, or ldap://).

Cisco ISE does not support the following name constraints:

- IP Address
- OtherName

When a trusted certificate contains a constraint that is not supported and the certificate that is being verified does not contain the appropriate field, Cisco ISE rejects the certificate because it cannot verify unsupported constraints.

The following is an example of the name constraints definition within the trusted certificate:

```
X509v3 Name Constraints: critical
    Permitted:
      othername:<unsupported>
      email:.abcde.at
      email:.abcde.be
      email:.abcde.bg
      email:.abcde.by
      DNS:.dir
      DirName: DC = dir, DC = emea
      DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
      DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
      DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
      DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100
      URI:.dir
      IP:172.23.0.171/255.255.255.255
    Excluded:
      DNS:.dir
      URI:.dir
```

An acceptable client certificate subject that matches the above definition is as follows:

```
Subject: DC=dir, DC=emea, OU+=DE, OU=OU-Administration, OU=Users, OU=X1,
CN=cwinwell
```

## View Trusted Certificates

The **Trusted Certificates** window lists all the trusted certificates that are available in Cisco ISE. To view the trusted certificates, you must be a Super Admin or System Admin.

### Before you begin

To perform the following task, you must be a Super Admin or System Admin.

- 
- Step 1** To view all the certificates, choose **Administration > System > Certificates > Trusted Certificates**. The Trusted Certificates window displayed, listing all the trusted certificates.
- Step 2** Check the check box of the trusted certificate and click **Edit**, **View**, **Export**, or **Delete** to perform the required task.
- 

## Change the Status of a Certificate in Trusted Certificates Store

The status of a certificate must be enabled so that Cisco ISE can use the certificate for establishing trust. When a certificate is imported into the Trusted Certificates store, it is automatically enabled.

## Add a Certificate to Trusted Certificates Store

The **Trusted Certificate** store window allows you to add CA certificates to Cisco ISE.

**Before you begin**

- To perform the following task, you must be a Super Admin or System Admin.
- The certificate that you want to add must be in the file system of the computer where your browser is running. The certificate must be in PEM or DER format.
- To use the certificate for Admin or EAP authentication, define the basic constraints in the certificate and set the CA flag to true.

## Edit a Trusted Certificate

After you add a certificate to the Trusted Certificates store, you can further edit it by using the **Edit** options.

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

- 
- Step 1** Administration > System > Certificates > Trusted Certificates.
- Step 2** Check the check box next to the certificate that you want to edit, and click **Edit**.
- Step 3** (Optional) Enter a name for the certificate in the **Friendly Name** field. If you do not specify a friendly name, a default name is generated in the following format:
- common-name#issuer#nnnnn*
- Step 4** Define the usage of the certificate by checking the necessary check boxes in the **Trusted For** area.
- Step 5** (Optional) Enter a description for the certificate in the **Description** field.
- Step 6** Click **Save**.
- 

## Trusted Certificate Settings

The following table describes the fields in the **Edit** window of a Trusted Certificate. Edit the CA certificate attributes in this window. The navigation path for this page is **Administration > System > Certificates > Trusted Certificates**. Check the check box for the Trusted Certificate you want to edit, and click **Edit**.

**Table 4: Trusted Certificate Edit Settings**

Field Name	Usage Guidelines
Certificate Issuer	
<b>Friendly Name</b>	Enter a friendly name for the certificate. This is an optional field. If you do not enter a friendly name, a default name is generated in the following format: <i>common-name#issuer#nnnnn</i>
<b>Status</b>	Choose <b>Enabled</b> or <b>Disabled</b> from the drop-down list. If the certificate is disabled, Cisco ISE will not use the certificate for establishing trust.
<b>Description</b>	(Optional) Enter a description.



Field Name	Usage Guidelines
Usage	
<b>Trust for authentication within ISE</b>	Check this check box if you want this certificate to verify server certificates (from other Cisco ISE nodes or LDAP servers).
<b>Trust for client authentication and Syslog</b>	(Applicable only if you check the <b>Trust for authentication within ISE</b> check box) Check the check box if you want this certificate to be used to: <ul style="list-style-type: none"> <li>• Authenticate endpoints that connect to Cisco ISE using the EAP protocol.</li> <li>• Trust a Syslog server.</li> </ul>
<b>Trust for certificate based admin authentication</b>	You can check this check box only when <b>Trust for client authentication and Syslog</b> is selected.  Check this check box to enable usage for certificate-based authentications for admin access. Import the required certificate chains into the Trusted Certificate store.
<b>Trust for authentication of Cisco Services</b>	Check this check box if you want this certificate to be used to trust external Cisco services such as the Feed Service.
<b>Certificate Status Validation</b>	Cisco ISE supports two ways of checking the revocation status of a client or server certificate that is issued by a particular CA. The first way is to validate the certificate using the Online Certificate Status Protocol (OCSP), which makes a request to an OCSP service maintained by the CA. The second way is to validate the certificate against a CRL which is downloaded from the CA into Cisco ISE. Both of these methods can be enabled, in which case OCSP is used first and only if a status determination cannot be made then the CRL is used.
<b>Validate Against OCSP Service</b>	Check the check box to validate the certificate against OCSP services. You must first create an OCSP Service to be able to check this box.
<b>Reject the request if OCSP returns UNKNOWN status</b>	Check the check box to reject the request if certificate status is not determined by the OCSP service. If you check this check box, an unknown status value that is returned by the OCSP service causes Cisco ISE to reject the client or server certificate currently being evaluated.
<b>Reject the request if OCSP Responder is unreachable</b>	Check the check box for Cisco ISE to reject the request if the OCSP Responder is not reachable.
<b>Download CRL</b>	Check the check box for the Cisco ISE to download a CRL.
<b>CRL Distribution URL</b>	Enter the URL to download the CRL from a CA. This field is automatically populated if it is specified in the certificate authority certificate. The URL must begin with “http”, “https”, or “ldap.”
<b>Retrieve CRL</b>	The CRL can be downloaded automatically or periodically. Configure the time interval between downloads.

Field Name	Usage Guidelines
<b>If download failed, wait</b>	Configure the time interval that Cisco ISE must wait Cisco ISE tries to download the CRL again.
<b>Bypass CRL Verification if CRL is not Received</b>	Check this check box, for the client requests to be accepted before the CRL is received. If you uncheck this check box, all client requests that use certificates signed by the selected CA will be rejected until Cisco ISE receives the CRL file.
<b>Ignore that CRL is not yet valid or expired</b>	Check this check box if you want Cisco ISE to ignore the start date and expiration date and continue to use the not yet active or expired CRL and permit or reject the EAP-TLS authentications based on the contents of the CRL.  Uncheck this check box if you want Cisco ISE to check 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.

**Related Topics**

[Trusted Certificates Store](#), on page 20

[Edit a Trusted Certificate](#), on page 24

## Delete a Trusted Certificate

You can delete trusted certificates that you no longer need. However, you must not delete Cisco ISE internal CA certificates. Cisco ISE internal CA certificates can be deleted only when you replace the Cisco ISE root certificate chain for the entire deployment.

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

**Step 2** Check the check boxes next to the certificates that you want to delete, and click **Delete**.

A warning message is displayed. To delete the Cisco ISE Internal CA certificates, click one of the following options:

- **Delete:** To delete the Cisco ISE internal CA certificates. All endpoint certificates that are signed by the Cisco ISE internal CA become invalid and the endpoints cannot join the network. To allow the endpoints on the network again, import the same Cisco ISE internal CA certificates into the Trusted Certificates store.
- **Delete & Revoke:** Deletes and revokes the Cisco ISE internal CA certificates. All endpoint certificates that are signed by the Cisco ISE internal CA become invalid and the endpoints cannot get on to the network. This operation cannot be undone. You must replace the Cisco ISE root certificate chain for the entire deployment.

**Step 3** Click **Yes** to delete the certificate.

## Export a Certificate from Trusted Certificates Store

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.



---

**Note** If you export certificates from the internal CA and plan to use the exported certificates to restore from backup, use the CLI command **application configure ise**. See [Export Cisco ISE CA Certificates and Keys, on page 55](#).

---

- 
- Step 1** Choose **Administration > System > Certificates > Trusted Certificates**.
- Step 2** Check the check box next to the certificate that you want to export, and click **Export**. You can export only one certificate at a time.
- Step 3** The chosen certificate downloads in the PEM format into the file system that is running your client browser.
- 

## Import a Root Certificate into the Trusted Certificate Store

When you import the root CA and intermediate CA certificates, specify the services for which the trusted CA certificates are to be used.

When you import an external root CA certificate, enable the **Trust for certificate based admin authentication** usage option in Step 5 of the following task.

### Before you begin

You must have the root certificate and other intermediate certificates from the CA that signed your certificate signing requests and returned the digitally signed CA certificates.

- 
- Step 1** Choose **Administration > System > Certificates > Trusted Certificates**.
- Step 2** Click **Import**.
- Step 3** In the **Import a new Certificate into the Certificate Store** window, click **Choose File** to select the root CA certificate that is signed and returned by your CA.
- Step 4** Enter a **Friendly Name**.  
If you do not enter a **Friendly Name**, Cisco ISE autopopulates this field with a name of the format *common-name#issuer#nnnnn*, where *nnnnn* is a unique number. You can also edit the certificate later to change the **Friendly Name**.
- Step 5** Check the check boxes next to the services for which you want to use this trusted certificate.
- Step 6** (Optional) In the **Description** field, enter a description for your certificate.
- Step 7** Click **Submit**.
- 

### What to do next

Import the intermediate CA certificates into the Trusted Certificates store (if applicable).

## Trusted Certificate Import Settings

Table 5: Trusted Certificate Import Settings

Field Name	Description
<b>Certificate File</b>	Click <b>Browse</b> to choose the certificate file from the computer that is running the browser.
<b>Friendly Name</b>	Enter a friendly name for the certificate. 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.
<b>Trust for authentication within ISE</b>	Check the check box if you want this certificate to be used to verify server certificates (from other ISE nodes or LDAP servers).
<b>Trust for client authentication and Syslog</b>	(Applicable only if you check the Trust for authentication within ISE check box) Check the check box if you want this certificate to be used to: <ul style="list-style-type: none"> <li>• Authenticate endpoints that connect to ISE using the EAP protocol</li> <li>• Trust a Syslog server</li> </ul>
<b>Trust for authentication of Cisco Services</b>	Check this check box if you want this certificate to be used to trust external Cisco services such as the feed service.
<b>Validate Certificate Extensions</b>	(Only 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.
<b>Description</b>	Enter an optional description.

### Related Topics

[Trusted Certificates Store](#), on page 20

[Certificate Chain Import](#), on page 28

[Import a Root Certificate into the Trusted Certificate Store](#), on page 27

## Certificate Chain Import

You can import multiple certificates from a single file that contains a certificate chain received from a Certificate store. All certificates in the file must be in the PEM format, and the certificates must be arranged in the following order:

- The last certificate in the file must be the client or server certificate issued by the CA.
- All preceding certificates must be the root CA certificate plus any intermediate CA certificates in the signing chain for the issued certificate.

Importing a certificate chain is a two-step process:

1. Import the certificate chain file into the Trusted Certificate store in the Cisco ISE administration portal. This operation imports all certificates from the file except the last one into the Trusted Certificates store.
2. Import the certificate chain file using the Bind a CA-Signed Certificate operation. This operation imports the last certificate from the file as a local certificate.

## Install Trusted Certificates for Cisco ISE Inter Node Communication

When you set up the deployment, before you register a secondary node, you must populate the PAN's CTL with appropriate CA certificates that are used to validate the Admin certificate of the secondary node. The procedure to populate the CTL of the PAN is different for different scenarios:

- If the secondary node is using a CA-signed certificate to communicate with the Cisco ISE administration portal, you must import the CA-signed certificate of the secondary node, the relevant intermediate certificates (if any), and the root CA certificate (of the CA that signed the secondary node's certificate) into the CTL of the PAN.
- If the secondary node is using a self-signed certificate to communicate with the Cisco ISE administration portal, you can import the self-signed certificate of the secondary node into the CTL of the PAN.



### Note

- If you change the Admin certificate on a registered secondary node, you must obtain appropriate CA certificates that can be used to validate the secondary node's Admin certificate and import it into the CTL of the PAN.
- If you use self-signed certificates to secure communication between a client and PSN in a deployment, when BYOD users move from one location to another, EAP-TLS user authentication fails. For such authentication requests that have to be serviced between a few PSNs, you must secure communication between the client and the PSN with an externally-signed CA certificate or use wildcard certificates signed by an external CA.

Ensure that the certificate issued by the external CA has basic constraints defined and the CA flag is set to true. To install CA-signed certificates for inter-node communication, carry out the following steps. For information on these tasks, refer to Chapter "Basic Setup" in the *Cisco ISE Administrator Guide*.

- 
- Step 1** Create a Certificate Signing Request (CSR) and submit the CSR to a Certificate Authority.
  - Step 2** Import the root certificates to the trusted certificate store.
  - Step 3** Bind the CA-signed certificate to the CSR.
- 

## Default Trusted Certificates in Cisco ISE

The Trusted Certificates store (**Administration > System > Certificates > Trusted Certificates**) in Cisco ISE includes some certificates that are available by default. These certificates are automatically imported into the store to meet security requirements. However, it is not mandatory for you to use all of them. Unless

mentioned otherwise in the following table, you can use certificates of your choice instead of the ones that are already available.

**Table 6: Default Trusted Certificates**

Trusted Certificate Name	Serial Number	Purpose of Certificate	Cisco ISE Releases with Certificate
<b>Baltimore CyberTrust Root CA</b>	02 00 00 B9	This certificate can serve as the root CA certificate in CA chains used by cisco.com in some geographies. The certificate was also used in ISE 2.4 posture/CP update XML files when they hosted at <a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a> .	Releases 2.4 and later.
<b>DST Root CA X3 Certificate Authority</b>	44 AF B0 80 D6 A3 27 BA 89 30 39 86 2E F8 40 6B	This certificate can serve as the root CA certificate for the CA chain used by cisco.com.	Releases 2.4 and later.
<b>Thawte Primary Root CA</b>	34 4E D5 57 20 D5 ED EC 49 F4 2F CE 37 DB 2B 6D	This certificate can serve as the root CA certificate for the CA chain used by cisco.com and perfigo.com.	Releases 2.4 and later.
<b>VeriSign Class 3 Public Primary Certification Authority</b>	18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A	This certificate serves as the root CA certificate for VeriSign Class 3 Secure Server CA-G3.  You must use this certificate when configuring profiler feed services in Cisco ISE.	Releases 2.4 and later.
<b>VeriSign Class 3 Secure Server CA - G3</b>	6E CC 7A A5 A7 03 20 09 B8 CE BC F4 E9 52 D4 91	This is an intermediate CA certificate that expires on February 7, 2020. You do not need to renew this certificate.  You can remove the certificate by following the task below.	Releases 2.4 and later.

Trusted Certificate Name	Serial Number	Purpose of Certificate	Cisco ISE Releases with Certificate
<b>Cisco CA Manufacturing</b>	6A 69 67 B3 00 00 00 00 00 03	This certificate may be used by certain Cisco devices connecting to Cisco ISE. The certificate is disabled by default.	Releases 2.4 and 2.6.
<b>Cisco Manufacturing CA SHA2</b>	02	This certificate can be used in CA chains for administrator authentications, endpoint authentications, and deployment infrastructure flows.	Releases 2.4 and later.
<b>Cisco Root CA 2048</b>	5F F8 7B 28 2B 54 DC 8D 42 A3 15 B5 68 C9 AD FF	This certificate can be used by certain Cisco devices connecting to Cisco ISE. The certificate is disabled by default.	Releases 2.4 and later.
<b>Cisco Root CA M2</b>	01	This certificate can be used in CA chains for administrator authentications, endpoint authentications, and deployment infrastructure flows.	Releases 2.4 and later.
<b>DigiCert Root CA</b>	02 AC 5C 26 6A 0B 40 9B 8F 0B 79 F2 AE 46 25 77	You must use this certificate for flows where guest login with Facebook is used.	Releases 2.4 and later.
<b>DigiCert SHA2 High Assurance Server CA</b>	04 E1 E7 A4 DC 5C F2 F3 6D C0 2B 42 B8 5D 15 9F	You must use this certificate for flows where guest login with Facebook is used.	Releases 2.4 and later.
<b>HydrantID SSL ICA G2</b>	75 17 16 77 83 D0 43 7E B5 56 C3 57 94 6E 45 63 B8 EB D3 AC	Trusted for Cisco services.	Releases 2.4 and 2.6.
<b>QuoVadis Root CA 2</b>	05 09	You must use this certificate in the profiler, posture, and client provisioning flows.	Releases 2.4 and later.

Trusted Certificate Name	Serial Number	Purpose of Certificate	Cisco ISE Releases with Certificate
Cisco ECC Root CA	01	This certificate is part of the Cisco Trust root store bundle that is used in Cisco ISE.	Release 2.6.
Cisco Licensing Root CA	01	This certificate is part of the Cisco Trust root store bundle that is used in Cisco ISE.	Releases 2.6 and later.
Cisco Root CA 2099	01 9A 33 58 78 CE 16 C1 C1	This certificate is part of the Cisco Trust root store bundle that is used in Cisco ISE.	Releases 2.6 and later.
Cisco Root CA M1	2E D2 0E 73 47 D3 33 83 4B 4F DD 0D D7 B6 96 7E	This certificate is part of the Cisco Trust Root Store bundle used in Cisco ISE.	Releases 2.6 and later.
Cisco RXC-R2	01	This certificate is part of the Cisco Trust root store bundle that is used in Cisco ISE.	Releases 2.6 and later.
DigiCert Global Root CA	08 3B E0 56 90 42 46 B1 A1 75 6A C9 59 91 C7 4A	This certificate is part of the Cisco Trust root store bundle that is used in Cisco ISE.	Releases 2.6 and later.
Cisco ECC Root CA 2099	03	This certificate is part of the Cisco Trust root store bundle that is used in Cisco ISE.	Releases 2.6 and later.

### Remove a Default Trusted Certificate from Cisco ISE

- 
- Export the certificate that you wish to delete and save it so that it can be imported again if needed.  
Check the check box against the certificate you wish to export, and click **Export** on the menu bar above. The key chain downloads to your system.
- Delete the certificate. Check the check box against the certificate you wish to delete, and click **Delete** on the menu bar above. You will not be allowed to delete the certificate if it is being used by any CA chain, Secure Syslog, or secure LDAP.
- Make the necessary configuration changes to remove the certificate from the CA chains, Secure Syslogs, and syslogs it is part of. Then, delete the certificate.
- After you delete the certificate, check that the related services (refer to the purpose of the certificate) are working as expected.



# Certificate-Signing Requests

For a CA to issue a signed certificate, you must create a certificate signing request and submit it to the CA.

The list of certificate-signing requests that you have created is available in the **Certificate-Signing Requests** window. Choose **Administration > System > Certificates > Certificate-Signing Requests**. To obtain signatures from a CA, you must export the certificate-signing request and then send the certificates to the CA. The CA signs and returns your certificates.

You can manage the certificates centrally from the Cisco ISE administration portal. You can create certificate-signing requests for all the nodes in your deployment and export them. Then, you should submit the certificate-signing requests to a CA, obtain the signed certificates from the CA, import the root and intermediary CA certificates given by the CA into the Trusted Certificates store, and bind the CA-signed certificates to the certificate-signing requests.

## Create a Certificate-Signing Request and Submit it to a Certificate Authority

You can generate a certificate-signing request to obtain a CA-signed certificate for the nodes in your deployment. You can generate the certificate-signing request for a specific node in the deployment or for all the nodes in your deployment.

- 
- Step 1** Choose **Administration > System > Certificates > Certificate-Signing Requests**.
  - Step 2** Click **Generate Certificate-Signing Requests (CSR)** to generate the certificate-signing request.
  - Step 3** Enter the values for generating a certificate-signing request. See [Trusted Certificate Settings, on page 24](#) for information on each of the fields in the window displayed.
  - Step 4** (Optional) Check the check box of the signing request that you want to download and click **Export** to download the request.
  - Step 5** Copy all the text from “-----BEGIN CERTIFICATE REQUEST-----” through “-----END CERTIFICATE REQUEST-----.” and paste the contents of the request in the certificate request of the chosen CA.
  - Step 6** Download the signed certificate.

Some CAs might email the signed certificate to you. The signed certificate is in the form of a .zip file that contains the newly issued certificate and the public signing certificates of the CA that you must add to the Cisco ISE trusted certificates store. The digitally-signed CA certificate, root CA certificate, and other intermediate CA certificate (if applicable) can be downloaded to the local system running your client browser.

---

## Bind a CA-Signed Certificate to a Certificate Signing Request

After the CA returns the digitally signed certificate, you must bind it to the certificate-signing request. You can perform the bind operation for all the nodes in your deployment, from the Cisco ISE administration portal.

### Before you begin

- You must have the digitally signed certificate, and the relevant root intermediate CA certificates sent by the CA.

- Import the relevant root and intermediate CA certificates to the Trusted Certificates store (**Administration > System > Certificates > Trusted Certificates**).

- 
- Step 1** Choose **Administration > System > Certificates > Certificate-Signing Requests**.
- Step 2** Check the check box next to the certificate signing request you must bind with the CA-signed certificate.
- Step 3** Click **Bind Certificate**.
- Step 4** In the **Bind CA Signed Certificate** window displayed, click **Choose File** to choose the CA-signed certificate.
- Step 5** Enter a value in the **Friendly Name** field.
- Step 6** Check the **Validate Certificate Extensions** check box if you want Cisco ISE to validate certificate extensions.
- If you enable the **Validate Certificate Extensions** option, and the certificate that you import contains a basic constraints extension with the 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.
- Note** Cisco ISE requires EAP-TLS client certificates to have digital signature key usage extension.
- Step 7** (Optional) Check the services for which this certificate will be used in the **Usage** area. This information is autopopulated if you have enabled the **Usage** option while generating the certificate signing request. You can also choose to edit the certificate at a later time to specify the usage.
- Changing the **Admin** usage certificate on a primary PAN restarts the services on all the other nodes. The system restarts one node at a time, after the primary PAN restarts.
- Step 8** Click **Submit** to bind the certificate-signing request with the CA-signed certificate.
- If this certificate is marked for Cisco ISE internode communication usage, the application server on the Cisco ISE node restarts.
- Repeat this process to bind the certificate-signing request with the CA-signed certificate on the other nodes in the deployment.
- 

### What to do next

[Import a Root Certificate into the Trusted Certificate Store, on page 27](#)

## Export a Certificate-Signing Request

### Before you begin

To perform the following task, you must be a Super Admin or System Admin.

- 
- Step 1** Choose **Administration > System > Certificates > Certificate-Signing Requests**.
- Step 2** Check the check box next to the certificates that you want to export, and click **Export**.
- Step 3** The certificate-signing request is downloaded to your local file system.
-

## Certificate-Signing Request Settings

Cisco ISE allows you to generate certificate-signing requests for all the nodes in your deployment from the administration portal in a single request. Also, you can choose to generate the certificate signing request for a single node or multiple both nodes in the deployment. If you choose to generate a certificate signing request for a single node, ISE automatically substitutes the Fully Qualified Domain Name (FQDN) of that particular node in the CN field of the certificate subject. If you enter a domain name other than the FQDN of that node in the CN field, Cisco ISE rejects authentication with that certificate. If you choose to include an entry in the Subject Alternative Name (SAN) field of the certificate, you must enter the FQDN of the ISE node in addition to other SAN attributes. If necessary, you can also add additional FQDNs in the SAN field. If you choose to generate certificate signing requests for all the nodes in your deployment, check the Allow Wildcard Certificates check box and enter the wildcard FQDN notation in the SAN field (DNS name), for example, \*.amer.example.com. If you plan to use the certificate for EAP Authentication, do not enter the wildcard value in the CN= field.

With the use of wildcard certificates, you no longer have to generate a unique certificate for each Cisco ISE node. Also, you no longer have to populate the SAN field with multiple FQDN values to prevent certificate warnings. Using an asterisk (\*) in the SAN field allows you to share a single certificate across multiple both nodes in a deployment and helps prevent certificate name mismatch warnings. However, use of wildcard certificates is considered less secure than assigning a unique server certificate for each Cisco ISE node.

Table 7: Certificate-Signing Request Settings

Field	Usage Guidelines
Certificate(s) will be used for	

Field	Usage Guidelines
	<p>Choose the service for which you are going to use the certificate:</p> <p><b>Cisco ISE Identity Certificates</b></p> <ul style="list-style-type: none"> <li>• <b>Multi-Use:</b> Used for multiple services (Admin, EAP-TLS Authentication, pxGrid, and Portal). Multi-use certificates use both client and server key usages. The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties: <ul style="list-style-type: none"> <li>• <b>Key Usage:</b> Digital Signature (Signing)</li> <li>• <b>Extended Key Usage:</b> TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)</li> </ul> </li> <li>• <b>Admin:</b> Used for server authentication (to secure communication with the Admin portal and between ISE nodes in a deployment). The certificate template on the signing CA is often called a Web Server certificate template. This template has the following properties: <ul style="list-style-type: none"> <li>• <b>Key Usage:</b> Digital Signature (Signing)</li> <li>• <b>Extended Key Usage:</b> TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)</li> </ul> </li> <li>• <b>EAP Authentication:</b> Used for server authentication. The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties: <ul style="list-style-type: none"> <li>• <b>Key Usage:</b> Digital Signature (Signing)</li> <li>• <b>Extended Key Usage:</b> TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)</li> </ul> </li> </ul> <p><b>Note</b> Digital signature key usage is required for EAP-TLS client certificates.</p> <ul style="list-style-type: none"> <li>• <b>RADIUS DTLS:</b> Used for RADIUS DTLS server authentication. This template has the following properties: <ul style="list-style-type: none"> <li>• <b>Key Usage:</b> Digital Signature (Signing)</li> <li>• <b>Extended Key Usage:</b> TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)</li> </ul> </li> <li>• <b>Portal:</b> Used for server authentication (to secure communication with all ISE web portals). The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties: <ul style="list-style-type: none"> <li>• <b>Key Usage:</b> Digital Signature (Signing)</li> <li>• <b>Extended Key Usage:</b> TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)</li> </ul> </li> <li>• <b>pxGrid:</b> Used for both client and server authentication (to secure communication between the pxGrid client and server). The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties: <ul style="list-style-type: none"> <li>• <b>Key Usage:</b> Digital Signature (Signing)</li> </ul> </li> </ul>

Field	Usage Guidelines
	<ul style="list-style-type: none"> <li>• <b>Extended Key Usage:</b> TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)</li> <li>• <b>SAML:</b> Server certificate used to secure communication with the SAML Identity Provider (IdP). A certificate designated for SAML use cannot be used for any other service such as Admin, EAP authentication, and so on.</li> <li>• <b>Key Usage:</b> Digital Signature (Signing)</li> <li>• <b>Extended Key Usage:</b> TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)</li> </ul> <p><b>Note</b> We recommend that you do not use a certificate that contains the value of 2.5.29.37.0 for the Any Purpose object identifier in the Extended Key Usage attribute. If you use a certificate that contains the value of 2.5.29.37.0 for the Any Purpose object identifier in the Extended Key Usage attribute, the certificate is considered invalid and the following error message is displayed:</p> <pre>source=local ; type=fatal ; message="unsupported certificate"</pre> <p><b>Cisco ISE Certificate Authority Certificates</b></p> <ul style="list-style-type: none"> <li>• <b>ISE Root CA:</b> (Applicable only for the internal CA service ) Used for regenerating the entire internal CA certificate chain including the root CA on the Primary PAN and subordinate CAs on the PSNs.</li> <li>• <b>ISE Intermediate CA:</b> (Applicable only for the internal CA service when ISE acts as an intermediate CA of an external PKI) Used to generate an intermediate CA certificate on the Primary PAN and subordinate CA certificates on the PSNs. The certificate template on the signing CA is often called a Subordinate Certificate Authority. This template has the following properties: <ul style="list-style-type: none"> <li>• <b>Basic Constraints:</b> Critical, Is a Certificate Authority</li> <li>• <b>Key Usage:</b> Certificate Signing, Digital Signature</li> <li>• <b>Extended Key Usage:</b> OCSP Signing (1.3.6.1.5.5.7.3.9)</li> </ul> </li> <li>• <b>Renew ISE OCSP Responder Certificates:</b> (Applicable only for the internal CA service) Used to renew the ISE OCSP responder certificate for the entire deployment (and is not a certificate signing request). For security reasons, we recommend that you renew the ISE OCSP responder certificates every six months.</li> </ul>
<p><b>Allow Wildcard Certificates</b></p>	<p>Check this check box to use a wildcard character (*) in the CN and/or the DNS name in the SAN field of the certificate. If you check this check box, all the nodes in the deployment are selected automatically. You must use the asterisk (*) wildcard character in the left-most label position. If you use wildcard certificates, we recommend that you partition your domain space for greater security. For example, instead of *.example.com, you can partition it as *.amer.example.com. If you do not partition your domain, it might lead to security issues.</p>

Field	Usage Guidelines
<b>Generate CSRs for these Nodes</b>	Check the check boxes next to the nodes for which you want to generate the certificate. To generate a CSR for select nodes in the deployment, you must uncheck the Allow Wildcard Certificates option.
<b>Common Name (CN)</b>	By default, the common name is the FQDN of the ISE node for which you are generating the certificate signing request. \$FQDN\$ denotes the FQDN of the ISE node. When you generate certificate signing requests for multiple nodes in the deployment, the Common Name field in the certificate signing requests is replaced with the FQDN of the respective ISE nodes.
<b>Organizational Unit (OU)</b>	Organizational Unit name. For example, Engineering.
<b>Organization (O)</b>	Organization name. For example, Cisco.
<b>City (L)</b>	(Do not abbreviate) City name. For example, San Jose.
<b>State (ST)</b>	(Do not abbreviate) State name. For example, California.
<b>Country (C)</b>	Country name. You must enter the two-letter ISO country code. For example, US.
<b>Subject Alternative Name (SAN)</b>	<p>An IP address, DNS name, Uniform Resource Identifier (URI), or Directory Name that is associated with the certificate.</p> <ul style="list-style-type: none"> <li>• <b>DNS Name:</b> If you choose the DNS name, enter the fully qualified domain name of the ISE node. If you have enabled the Allow Wildcard Certificates option, specify the wildcard notation (an asterisk and a period before the domain name). For example, *.amer.example.com.</li> <li>• <b>IP Address:</b> IP address of the ISE node to be associated with the certificate.</li> <li>• <b>Uniform Resource Identifier:</b> A URI that you want to associate with the certificate.</li> <li>• <b>Directory Name:</b> A string representation of distinguished name(s) (DNs) defined per RFC 2253. Use a comma (,) to separate the DN. For “dnQualifier” RDN, escape the comma and use backslash-comma “\,” as separator. For example, CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL</li> </ul>
<b>Key Type</b>	Specify the algorithm to be used for creating the public key: RSA or ECDSA.

Field	Usage Guidelines
<b>Key Length</b>	<p>Specify the bit size for the public key.</p> <p>The following options are available for RSA:</p> <ul style="list-style-type: none"> <li>• 512</li> <li>• 1024</li> <li>• 2048</li> <li>• 4096</li> </ul> <p>The following options are available for ECDSA:</p> <ul style="list-style-type: none"> <li>• 256</li> <li>• 384</li> </ul> <p><b>Note</b> RSA and ECDSA public keys might have different key length for the same security level.</p> <p>Choose 2048 or greater if you plan to get a public CA-signed certificate or deploy Cisco ISE as a FIPS-compliant policy management system.</p>
<b>Digest to Sign With</b>	Choose one of the following hashing algorithm: SHA-1 or SHA-256.
<b>Certificate Policies</b>	Enter the certificate policy OID or list of OIDs that the certificate should conform to. Use comma or space to separate the OIDs.

**Related Topics**

[Certificate-Signing Requests](#), on page 33

[Create a Certificate-Signing Request and Submit it to a Certificate Authority](#), on page 33

[Bind a CA-Signed Certificate to a Certificate Signing Request](#), on page 33

## Set Up Certificates for Portal Use

With multiple PSNs in a deployment that can service a web portal request, Cisco ISE needs a unique identifier to identify the certificate that must be used for portal communication. When you add or import certificates that are designated for portal use, define a certificate group tag and associate it with the corresponding certificate on each node in your deployment. Associate this certificate group tag to the corresponding end-user portals (guest, sponsor, and personal devices portals). This certificate group tag is the unique identifier that helps Cisco ISE identify the certificate that must be used when communicating with each of these portals. You can only designate one certificate from each node for each of the portals.



**Note** Cisco ISE presents the Portal certificate on TCP port 8443 (or the port that you have configured for portal use).

**Step 1** [Create a Certificate-Signing Request and Submit it to a Certificate Authority](#), on page 33.



You must choose a Certificate Group Tag that you have already defined or create a new one for the portal. For example, mydevicesportal.

**Step 2** [Import a Root Certificate into the Trusted Certificate Store, on page 27.](#)

**Step 3** [Bind a CA-Signed Certificate to a Certificate Signing Request, on page 33.](#)

---

## Reassign Default Portal Certificate Group Tag to CA-Signed Certificate

By default, all Cisco ISE portals use the self-signed certificate. If you want to use a CA-signed certificate for portals, you can assign the default portal certificate group tag to a CA-signed certificate. You can use an existing CA-signed certificate or generate a CSR and obtain a new CA-signed certificate for portal use. You can reassign any portal group tag from one certificate to another.

The following procedure describes how to reassign the default portal certificate group tag to a CA-signed certificate.

---

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

Hover the mouse over the **i** icon next to the Default Portal Certificate Group tag to view the list of portals that use this tag. You can also view the ISE nodes in the deployment that have portal certificates which are assigned this tag.

**Step 2** Check the check box next to the CA-signed certificate that you want to use for portals, and click **Edit**.

Be sure to choose a CA-signed certificate that is not in use by any of the portals.

**Step 3** Under the **Usage** area, check the **Portal** check box and choose the Default Portal Certificate Group Tag.

**Step 4** Click **Save**.

A warning message appears.

**Step 5** Click **Yes** to reassign the default portal certificate group tag to the CA-signed certificate.

---

## Associate Portal Certificate Tag Before You Register a Node

If you use the "Default Portal Certificate Group" tag for all the portals in your deployment, before you register a new ISE node, ensure that you import the relevant CA-signed certificate, choose "Portal" as a service, and associate the "Default Portal Certificate Group" tag with this certificate.

When you add a new node to a deployment, the default self-signed certificate is associated with the "Default Portal Certificate Group" tag and the portals are configured to use this tag.

After you register a new node, you cannot change the Certificate Group tag association. Therefore, before you register the node to the deployment, you must do the following:

---

**Step 1** Create a self-signed certificate, choose "Portal" as a service, and assign a different certificate group tag (for example, tempportaltag).

**Step 2** Change the portal configuration to use the newly created certificate group tag (tempportaltag).

**Step 3** Edit the default self-signed certificate and remove the Portal role.

This option removes the Default Portal Certificate Group tag association with the default self-signed certificate.

**Step 4**

Do one of the following:

Option	Description
Generate a CSR	<p>When you generate the CSR:</p> <ol style="list-style-type: none"> <li>a. Choose "Portal" as a service for which you will use this certificate and associate the "Default Portal Certificate Group" tag.</li> <li>b. Send the CSR to a CA and obtain the signed certificate.</li> <li>c. Import the root and any other intermediate certificates of the CA that signed your certificate in to the Trusted Certificates store.</li> <li>d. Bind the CA-signed certificate with the CSR.</li> </ol>
Import the private key and the CA-signed certificate	<p>When you import the CA-signed certificate:</p> <ol style="list-style-type: none"> <li>a. Choose "Portal" as a service for which you will use this certificate and associate the "Default Portal Certificate Group" tag.</li> <li>b. Import the root and any other intermediate certificates of the CA that signed your certificate in to the Trusted Certificates store.</li> </ol>
Edit an existing CA-signed certificate.	<p>When you edit the existing CA-signed certificate:</p> <p>Choose "Portal" as a service for which you will use this certificate and associate the "Default Portal Certificate Group" tag.</p>

**Step 5**

Register the ISE node to the deployment.

The portal configuration in the deployment is configured to the "Default Portal Certificate Group" tag and the portals are configured to use the CA-signed certificate associated with the "Default Portal Certificate Group" tag on the new node.

## User and Endpoint Certificate Renewal

By default, Cisco ISE rejects a request that comes from a device whose certificate has expired. However, you can change this default behavior and configure ISE to process such requests and prompt the user to renew the certificate.

If you choose to allow the user to renew the certificate, Cisco recommends that you configure an authorization policy rule which checks if the certificate has been renewed before processing the request any further. Processing a request from a device whose certificate has expired may pose a potential security threat. Hence, you must configure appropriate authorization profiles and rules to ensure that your organization's security is not compromised.

Some devices allow you to renew the certificates before and after their expiry. But on Windows devices, you can renew the certificates only before it expires. Apple iOS, Mac OSX, and Android devices allow you to renew the certificates before or after their expiry.

## Dictionary Attributes Used in Policy Conditions for Certificate Renewal

Cisco ISE certificate dictionary contains the following attributes that are used in policy conditions to allow a user to renew the certificate:

- **Days to Expiry:** This attribute provides the number of days for which the certificate is valid. You can use this attribute to create a condition that can be used in authorization policy. This attribute can take a value from 0 to 15. A value of 0 indicates that the certificate has already expired. A value of 1 indicates that the certificate has less than 1 day before it expires.
- **Is Expired:** This Boolean attribute indicates whether a certificate has expired or not. If you want to allow certificate renewal only when the certificate is near expiry and not after it has expired, use this attribute in authorization policy condition.

## Authorization Policy Condition for Certificate Renewal

You can use the CertRenewalRequired simple condition (available by default) in authorization policy to ensure that a certificate (expired or about to expire) is renewed before Cisco ISE processes the request further.

## CWA Redirect to a Renew Certificate

If a user certificate is revoked before its expiry, Cisco ISE checks the CRL published by the CA and rejects the authentication request. In case, if a revoked certificate has expired, the CA may not publish this certificate in its CRL. In this scenario, it is possible for Cisco ISE to renew a certificate that has been revoked. To avoid this, before you renew a certificate, ensure that the request gets redirected to Central Web Authentication (CWA) for a full authentication. You must create an authorization profile to redirect the user for CWA.

## Configure Cisco ISE to Allow Users to a Renew Certificate

You must complete the tasks listed in this procedure to configure Cisco ISE to allow users to renew certificates.

### Before you begin

Configure a limited access ACL on the WLC to redirect a CWA request.

- 
- Step 1** [Update the Allowed Protocol Configuration, on page 43](#)
  - Step 2** [Create an Authorization Policy Profile for CWA Redirection, on page 44](#)
  - Step 3** [Create an Authorization Policy Rule to Renew a Certificate, on page 44](#)
  - Step 4** [Enable BYOD Settings in Guest Portal, on page 45](#)
- 

## Update the Allowed Protocol Configuration

- 
- Step 1** Choose **Policy > Policy Elements > Results > Authentication > Allowed Protocols > Default Network Access**.

- Step 2** Check the **Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy** check box under the EAP-TLS protocol and EAP-TLS inner methods for PEAP and EAP-FAST protocols.
- Requests that use the EAP-TLS protocol will go through the NSP flow.
- For PEAP and EAP-FAST protocols, you must manually install and configure Cisco AnyConnect for Cisco ISE to process the request.
- Step 3** Click **Submit**.
- 

#### What to do next

[Create an Authorization Policy Profile for CWA Redirection, on page 44](#)

## Create an Authorization Policy Profile for CWA Redirection

#### Before you begin

Ensure that you have configured a limited access ACL on the WLC.

---

- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.
- Step 2** Click **Add**.
- Step 3** Enter a name for the authorization profile. For example, CertRenewal\_CWA.
- Step 4** Check the **Web Redirection (CWA, DRW, MDM, NSP, CPP)** check box in the Common Tasks area.
- Step 5** Choose **Centralized Web Auth** from the drop-down list and the limited access ACL.
- Step 6** Check the **Display Certificates Renewal Message** check box.
- The URL-redirect attribute value changes and includes the number of days for which the certificate is valid.
- Step 7** Click **Submit**.
- 

#### What to do next

[Create an Authorization Policy Rule to Renew a Certificate, on page 44](#)

## Create an Authorization Policy Rule to Renew a Certificate

#### Before you begin

Ensure that you have created an authorization profile for central web authentication redirection.

Enable Policy Sets on **Administration > System > Settings > Policy Settings**.

---

- Step 1** Choose **Work Centers > Device Administration > Policy Sets**.
- Step 2** Click **Create Above**.
- Step 3** Enter a name for the new rule.

- Step 4** Choose the following simple condition and result:  
If CertRenewalRequired EQUALS True, then choose the authorization profile that you created earlier (CertRenewal\_CWA) for the permission.
- Step 5** Click **Save**.

---

#### What to do next

When you access the corporate network with a device whose certificate has expired, click **Renew** to reconfigure your device.

## Enable BYOD Settings in Guest Portal

For a user to be able to renew a personal device certificate, you must enable the BYOD settings in the chosen guest portal.

- Step 1** Choose **Work Centers > Guest Access > Portals & Components > Guest Portals**.
- a) Select the chosen CWA portal and click **Edit**.
- Step 2** From BYOD Settings, check the **Allow employees to use personal devices on the network** check box.
- Step 3** Click **Save**.

## Certificate Renewal Fails for Apple iOS Devices

When you use ISE to renew the endpoint certificates on Apple iOS devices, you might see a “Profiled Failed to Install” error message. This error message appears if the expiring or expired network profiles were signed by a different Admin HTTPS certificate than the one that is used in processing the renewal, either on the same Policy Service Node (PSN) or on another PSN.

As a workaround, use a multi-domain SSL certificate, which is commonly referred to as Unified Communications Certificate (UCC), or a wildcard certificate for Admin HTTPS on all PSNs in the deployment.

## Certificate Periodic Check Settings

Cisco ISE checks the Certificate Revocation Lists (CRL) periodically. Using this window, you can configure Cisco ISE to check ongoing sessions against CRLs that are downloaded automatically. You can specify the time of the day when the OCSP or CRL checks should begin each day and the time interval in hours that Cisco ISE waits before checking the OCSP server or CRLs again.

**Table 8: Certificate Periodic Check Settings**

Field Name	Usage Guidelines
Certificate Check Settings	

Field Name	Usage Guidelines
<b>Check ongoing sessions against automatically retrieved CRL</b>	Check this check box if you want Cisco ISE to check ongoing sessions against CRLs that are automatically downloaded.
<b>CRL/OCSP Periodic Certificate Checks</b>	
<b>First check at</b>	Specify the time of the day when the CRL or OCSP check should begin each day. Enter a value between 00:00 and 23:59 hours.
<b>Check every</b>	Specify the time interval in hours that Cisco ISE waits before checking the CRL or OCSP server again.

**Related Topics**

[OCSP Services](#), on page 74

[Add OCSP Client Profiles](#), on page 76

## Extract a Certificate and Private Key from a .pfx File

Cisco ISE does not allow import of certificates in .pfx format. Hence, if the certificate intended for import is in the .pfx format, you must convert it to .pem or .key file formats before import.

**Before you begin**

Ensure that OpenSSL is installed in the server that contains the SSL certificate.

- 
- Step 1** Start OpenSSL from the OpenSSL\bin folder.
- Step 2** Open the command prompt and go to the folder that contains your .pfx file.
- Step 3** Run the following command to extract the private key in .pem format: **openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes**
- You will be prompted to type the import password. Type the password that you used to protect your keypair when you created the .pfx file. You will be prompted again to provide a new password to protect the .pem file that you are creating. Store the password to your key file in a secure place to avoid misuse.
- Step 4** Run the following command to extract the certificate in .pem format: **openssl pkcs12 -in certname.pfx -nokeys -out cert.pem**
- Step 5** Run the following command to decrypt the private key: **openssl rsa -in key.pem -out server.key**
- Type the password that you created to protect the private key file in the previous step.
- The .pem file and the decrypted and the encrypted .key files are available in the path, where you started OpenSSL.
-

## Cisco ISE CA Service

Certificates can be self-signed or digitally signed by an external Certificate Authority (CA). The Cisco ISE Internal Certificate Authority (ISE CA) issues and manages digital certificates for endpoints from a centralized console to allow employees to use their personal devices on the company's network. A CA-signed digital certificate is considered industry standard and more secure. The Primary PAN is the Root CA. The Policy Service Nodes (PSNs) are subordinate CAs to the Primary PAN (SCEP RA). The ISE CA offers the following functionalities:

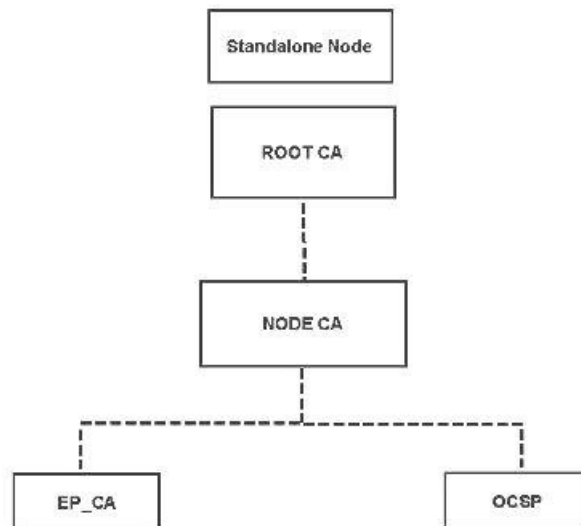
- **Certificate Issuance:** Validates and signs Certificate Signing Requests (CSRs) for endpoints that connect to your network.
- **Key Management:** Generates and securely stores keys and certificates on both PAN and PSN nodes.
- **Certificate Storage:** Stores certificates issued to users and devices.
- **Online Certificate Status Protocol (OCSP) Support:** Provides an OCSP responder to check for the validity of certificates.

When a CA Service is disabled on the primary administrative node, the CA service is still seen as running on the secondary administration node's CLI. Ideally, the CA service should be seen as disabled. This is a known Cisco ISE issue.

## Cisco ISE CA Certificates Provisioned on Administration and Policy Service Nodes

After installation, a Cisco ISE node is provisioned with a Root CA certificate, and a Node CA certificate to manage certificates for endpoints.

*Figure 2: Cisco ISE CA Certificates Provisioned on a Standalone Node*

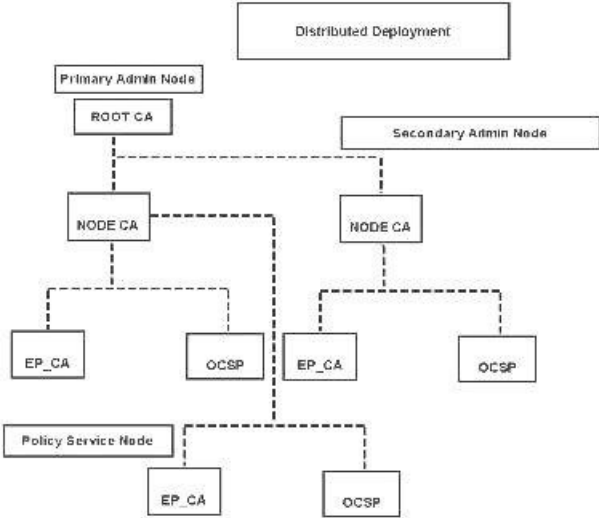


When you set up a deployment, the node that you designate as the Primary Administration Node (PAN) becomes the Root CA. The PAN has a Root CA certificate and a Node CA certificate that is signed by the Root CA.

When you register a Secondary Administration Node to the PAN, a Node CA certificate is generated and is signed by the Root CA on the Primary Administration Node.

Any Policy Service Node (PSN) that you register with the PAN is provisioned an Endpoint CA and an OCSP certificate signed by the Node CA of the PAN. The Policy Service Nodes (PSNs) are subordinate CAs to the PAN. When you use the ISE CA, the Endpoint CA on the PSN issues the certificates to the endpoints that access your network.

Figure 3: Cisco ISE CA Certificates Provisioned on Administration and Policy Service Nodes in a Deployment



### Cisco ISE CA Chain Regeneration

When you regenerate the Cisco ISE CA chain, all the certificates including the Root CA, Node CA, and Endpoint CA certificates are regenerated. You must regenerate the ISE CA chain when you change the domain name or hostname of your PAN or PSN.

### Elliptical Curve Cryptography Certificates Support

Cisco ISE CA service supports certificates that are based on Elliptical Curve Cryptography (ECC) algorithms. ECC offers more security and better performance than other cryptographic algorithms even when using a much smaller key size.

The following table compares the key sizes of ECC and RSA and security strength.

ECC Key Size (in bits)	RSA Key Size (in bits)
160	1024
224	2048
256	3072



ECC Key Size (in bits)	RSA Key Size (in bits)
384	7680
521	15360

Because of the smaller key size, encryption is quicker.

Cisco ISE supports the following ECC curve types. The higher the curve type or key size, the greater is the security.

- P-192
- P-256
- P-384
- P-521

ISE does not support explicit parameters in the EC part of a certificate. If you try to import a certificate with explicit parameters, you get the error: Validation of certificate failed: Only named ECParameters supported.

Cisco ISE CA service supports ECC certificates for devices connecting through the BYOD flow. You can also generate ECC certificates from the Certificate Provisioning Portal.



**Note** The following table lists the operating systems and versions that support ECC along with the supported curve types. If your devices are not running a supported operating system or on a supported version, you can use RSA-based certificates instead.

Operating System	Supported Versions	Supported Curve Types
Windows	8 and later	P-256, P-384, and P-521
Android	4.4 and later <b>Note</b> Android 6.0 requires May 2016 patch to support ECC certificates.	All curve types (except Android 6.0, which does not support the P-192 curve type).

Windows 7 and Apple iOS do not natively support ECC for authentication over EAP-TLS. This release of Cisco ISE does not support the use of ECC certificates on MAC OS X devices.

If the BYOD flow with Enrollment over Secure Transport (EST) protocol is not working properly, check the following:

- Certificate Services Endpoint Sub CA certificate chain is complete. To check whether the certificate chain is complete:
  1. Choose **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**.
  2. Check the check box next to the certificate that you want to check and click **View**.

- Ensure that the CA and EST services are up and running. If the services are not running, go to **Administration > System > Certificates > Certificate Authority > Internal CA Settings** to enable the CA service.

**Note**

- This release of Cisco ISE does not support EST clients to authenticate directly against the EST Server residing within Cisco ISE. While on-boarding an Android or a Windows endpoint, ISE triggers an EST flow if the request is for an ECC-based certificate.
- BYOD flow with Android clients might fail when using EST protocol along with a static IP address, an FQDN or a hostname in the authorization profile. The workaround is to use SCEP instead of EST. You can configure SCEP in the native supplicant profile. See [Creating Native Supplicant Profiles](#) for more information.

## Cisco ISE Certificate Authority Certificates

The Certificate Authority (CA) Certificates page lists all the certificates related to the internal Cisco ISE CA. In previous releases, these CA certificates were present in the Trusted Certificates store and are now moved to the CA Certificates page. These certificates are listed node wise in this page. You can expand a node to view all the ISE CA certificates of that particular node. The Primary and Secondary Administration nodes have the root CA, node CA, subordinate CA, and OCSP responder certificates. The other nodes in the deployment have the endpoint subordinate CA and OCSP certificates.

When you enable the Cisco ISE CA service, these certificates are generated and installed on all the nodes automatically. Also, when you replace the entire ISE Root CA Chain, these certificates are regenerated and installed on all the nodes automatically. There is no manual intervention required.

The Cisco ISE CA certificates follow the following naming convention: **Certificate Services <Endpoint Sub CA/Node CA/Root CA/OCSP Responder>-<node\_hostname>#certificate\_number**.

From the CA Certificates page, you can edit, import, export, delete, and view the Cisco ISE CA certificates.

### Edit a Cisco ISE CA Certificate

After you add a certificate to the Cisco ISE CA Certificates Store, you can further edit it by using the edit settings.

#### Before you begin

To perform the following task, you must be a Super Admin or System Admin.

- 
- Step 1** Choose **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**.
  - Step 2** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose .
  - Step 3** Check the check box next to the certificate that you want to edit, and click **Edit**.
  - Step 4** Modify the editable fields as required. See [Trusted Certificate Settings, on page 24](#) for a description of the fields.
  - Step 5** Click **Save** to save the changes you have made to the certificate store.
-

## Export a Cisco ISE CA Certificate

To export the Cisco ISE root CA and node CA certificates:

### Before you begin

To perform the following task, you must be a Super Admin or System Admin.

- 
- Step 1** Choose **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**.
- Step 2** In the ISE-PIC GUI, click the **Menu** icon (☰) and choose .
- Step 3** Check the check box next to the certificate that you want to export, and click **Export**. 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.
- 

## Import a Cisco ISE CA Certificate

If an endpoint tries to authenticate to your network using a certificate issued by Cisco ISE CA from another deployment, you must import the Cisco ISE root CA, node CA, and endpoint sub CA certificates from that deployment in to the Cisco ISE Trusted Certificates store.

### Before you begin

- To perform the following task, you must be a Super Admin or System Admin.
- Export the ISE root CA, node CA, and endpoint sub CA certificates from the deployment where the endpoint certificate is signed and store it on the file system of the computer where your browser is running.

- 
- Step 1** Log in to the Admin Portal of the deployment where the endpoint is getting authenticated.
- Step 2** Choose **Administration > System > Certificates > Trusted Certificates**.
- Step 3** Click **Import**.
- Step 4** Configure the field values as necessary. See [Trusted Certificate Import Settings, on page 28](#) for more information.
- 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 PAN and followed, one-by-one, by each additional node.
- 

## Certificate Templates

Certificate templates contain properties that are common to all certificates issued by the Certificate Authority (CA) based on that template. The certificate template defines the Subject, Subject Alternative Name (SAN), key type, key size, SCEP RA profile that must be used, validity period of the certificate, and the extended key usage (EKU) that specifies whether the certificate has to be used for client or server authentication or both. The internal Cisco ISE CA (ISE CA) uses a certificate template to issue certificates based on that template.

Cisco ISE comes with the following default certificate templates for the ISE CA. You can create additional certificate templates, if needed. The default certificate templates are:

- **CA\_SERVICE\_Certificate\_Template**—For other network services that use Cisco ISE as the Certificate Authority. For example, use this certificate template while configuring ISE to issue certificates for ASA VPN users. You can modify only the validity period in this certificate template.
- **EAP\_Authentication\_Certificate\_Template**—For EAP authentication.
- **pxGrid\_Certificate\_Template**—For the pxGrid controller while generating the certificate from the Certificate Provisioning Portal.

## Certificate Template Name Extension

The Cisco ISE Internal CA includes an extension to represent the certificate template that was used to create the endpoint certificate. All endpoint certificates issued by the internal CA contain a certificate template name extension. This extension represents the certificate template that was used to create that endpoint certificate. The extension ID is 1.3.6.1.4.1.9.21.2.5. You can use the **CERTIFICATE: Template Name** attribute in authorization policy conditions and assign appropriate access privileges based on the results of the evaluation.

## Use Certificate Template Name in Authorization Policy Conditions

You can use the certificate template name extension in authorization policy rules.

- 
- Step 1** Choose **Policy > Policy Sets**, and expand the Default policy set to view the authorization policy rules.
- Step 2** Add a new rule or edit an existing rule. This example describes editing the **Compliant\_Device\_Access** rule:
- Edit the **Compliant\_Device\_Access** rule.
  - Choose **Add Attribute/Value**.
  - From Dictionaries, choose the **CERTIFICATE: Template Name** attribute and **Equals** operator.
  - Enter the value of the certificate template name. For example, **EAP\_Authentication\_Certificate\_Template**.
- Step 3** Click **Save**.
- 

## Deploy Cisco ISE CA Certificates for pxGrid Controller

Cisco ISE CA provides a certificate template for the pxGrid controller to generate a certificate from the Certificate Provisioning Portal.

### Before you begin

Generate a certificate signing request (CSR) for the pxGrid client and copy the contents of the CSR in to the clipboard.

- 
- Step 1** Create a network access user account (**Administration > Identity Management > Identities > Users > Add**). Make note of the user group to which the user is assigned.
- Step 2** Edit the Certificate Provisioning Portal Settings (**Administration > Device Portal Management > Certificate Provisioning**).
- Select the certificate provisioning portal and click **Edit**.
  - Click the **Portal Settings** drop-down list. From the Configure authorized groups Available list, select the user group to which the network access user belongs to and move it to Chosen list.

- c) Click the **Certificate Provisioning Portal Settings** drop-down list. Choose the pxGrid\_Certificate\_Template. See the Portal Settings for Certificate Provisioning Portal section in *Cisco ISE Admin Guide: Guest and BYOD* for more information.
- d) Save the portal settings.

**Step 3**

Launch the Certificate Provisioning Portal. Click the Portal Test URL link.

- a) Log in to the Certificate Provisioning Portal using the user account created in step 1.
- b) Accept the AUP and click **Continue**.
- c) From the **I want to** drop-down list, choose **Generate a single certificate (with certificate signing request)**.
- d) In the Certificate Signing Request Details field, paste the contents of the CSR from the clipboard.
- e) From the **Certificate Download Format** drop-down list, choose **PKCS8 format**.

**Note** If you choose the PKCS12 format, you must convert the single certificate file in to separate certificate and key files. The certificate and key files must be in binary DER encoded or PEM format before you can import them in to Cisco ISE.

- f) From the **Choose Certificate Template** drop-down list, choose **pxGrid\_Certificate\_Template**.
- g) Enter a certificate password.
- h) Click **Generate**.  
The certificate is generated.
- i) Export the certificate.  
The certificate along with the certificate chain is exported.

**Step 4**

Import the Cisco ISE CA chain in to the Trusted Certificates store in the pxGrid client.

## 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 (called as Cisco ISE External CA Settings) 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).

## Issued Certificates

The Admin portal lists all the certificates issued by the internal ISE CA to endpoints (Administration > System > Certificates > Endpoint Certificates). The Issued Certificates page provides you an at-a-glance view of the certificate status. You can mouse over the Status column to find out the reason for revocation if a certificate has been revoked. You can mouse over the Certificate Template column to view additional details such as Key Type, Key Size or Curve Type, Subject, Subject Alternative Name (SAN), and Validity of the certificate. You can click on the endpoint certificate to view the certificate.

All certificates issued by the ISE CA (certificates automatically provisioned through the BYOD flow and certificates obtained from the Certificate Provisioning portal) are listed in the Endpoint Certificates page. You can manage these certificates from this page.

For example, if you want to view the certificates issued to user7, enter user7 in the text box that appears below the Friendly Name field. All the certificates issued by Cisco ISE to this user appear. Remove the search term from the text box to cancel the filter. You can also use the Advanced Filter option to view records based on various search criteria.

This Endpoint Certificates page also provides you the option to revoke an endpoint certificate, if necessary.

The Certificate Management Overview page displays the total number of endpoint certificates issued by each PSN node in your deployment. You can also view the total number of revoked certificates per node and the total number of certificates that have failed. You can filter the data on this page based on any of the attributes.

## Issued and Revoked Certificates



**Note** Expired or revoked issued certificates will be automatically deleted after 30 days.

**Table 9: Issued and Revoked Certificates**

Fields	Usage Guidelines
<b>Node Name</b>	Name of the Policy Service node (PSN) that issued the certificate.
<b>Certificates Issued</b>	Number of endpoint certificates issued by the PSN node.
<b>Certificates Revoked</b>	Number of revoked endpoint certificates (certificates that were issued by the PSN node).
<b>Certificates Requests</b>	Number of certificate-based authentication requests processed by the PSN node.
<b>Certificates Failed</b>	Number of failed authentication requests processed by the PSN node.

### Related Topics

[Issued Certificates](#), on page 53

[User and Endpoint Certificate Renewal](#), on page 42

[Configure Cisco ISE to Use Certificates for Authenticating Personal Devices](#), on page 58

[Configure Cisco ISE to Allow Users to a Renew Certificate](#), on page 43

[Revoke an Endpoint Certificate](#), on page 74

## Backup and Restoration of Cisco ISE CA Certificates and Keys

You must back up the Cisco ISE CA certificates and keys securely to be able to restore them back on a Secondary Administration Node in case of a PAN failure and you want to promote the Secondary Administration Node to function as the root CA or intermediate CA of an external PKI. The Cisco ISE configuration backup does not include the CA certificates and keys. Instead, you should use the Command Line Interface (CLI) to

export the CA certificates and keys to a repository and to import them. The **application configure ise** command now includes export and import options to backup and restore CA certificates and keys.

The following certificates from the Trusted Certificates Store are restored on the Secondary Administration Node:

- Cisco ISE Root CA certificate
- Cisco ISE Sub CA certificate
- Cisco ISE Endpoint RA certificate
- Cisco ISE OCSP Responder certificate

You must back up and restore Cisco ISE CA certificates and keys when you:

- Have a Secondary Administration Node in the deployment
- Replace the entire Cisco ISE CA root chain
- Configure Cisco ISE root CA to act as a subordinate CA of an external PKI
- Restore data from a configuration backup. In this case, you must first regenerate the Cisco ISE CA root chain and then back up and restore the ISE CA certificates and keys.

## Export Cisco ISE CA Certificates and Keys

You must export the CA certificates and keys from the PAN to import them on the Secondary Administration Node. This option enables the Secondary Administration Node to issue and manage certificates for endpoints when the PAN is down and you promote the Secondary Administration Node to be the PAN.

### Before you begin

Ensure that you have created a repository to store the CA certificates and keys.

- 
- Step 1** Enter **application configure ise** command from the Cisco ISE CLI.
  - Step 2** Enter 7 to export the certificates and keys.
  - Step 3** Enter the repository name.
  - Step 4** Enter an encryption key.

A success message appears with the list of certificates that were exported, along with the subject, issuer, and serial number.

### Example:

```
The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x621867df-568341cd-944cc77f-c9820765

Subject:CN=Cisco ISE Endpoint CA of ise-vm1
Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa

Subject:CN=Cisco ISE Endpoint RA of ise-vm1
Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
```

```

Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fbl
ISE CA keys export completed successfully

```

## Import Cisco ISE CA Certificates and Keys

After you register the Secondary Administration Node, you must export the CA certificates and keys from the PAN and import them in to the Secondary Administration Node.

- Step 1** Enter **application configure ise** command from the Cisco ISE CLI.
- Step 2** Enter 8 to import the CA certificates and keys.
- Step 3** Enter the repository name.
- Step 4** Enter the name of the file that you want to import. The file name should be in the format **ise\_ca\_key\_pairs\_of\_<vm hostname>**.
- Step 5** Enter the encryption key to decrypt the file.

A success message appears.

### Example:

```

The following 4 CA key pairs were imported:
  Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
  Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
  Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4

  Subject:CN=Cisco ISE Endpoint CA of ise-vm1
  Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
  Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56

  Subject:CN=Cisco ISE Endpoint RA of ise-vm1
  Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
  Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

  Subject:CN=Cisco ISE OSCP Responder Certificate of ise-vm1
  Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
  Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully

```

**Note** Encryption of exported keys file was introduced in Cisco ISE Release 2.6. The export of keys from Cisco ISE Release 2.4 and earlier versions and import of keys in Cisco ISE Release 2.6 and later versions will not be successful.

## Generate Root CA and Subordinate CAs on the Primary PAN and PSN

When you set up the deployment, Cisco ISE generates a root CA on the primary PAN and subordinate CA certificates on the PSNs for the Cisco ISE CA service. However, when you change the domain name or the



hostname of the primary PAN or PSN, you must regenerate root CA on the primary PAN and sub CAs on the PSNs respectively.

If you want to change the hostname on a PSN, instead of regenerating the root CA and subordinate CAs on the primary PAN and PSNs respectively, you can deregister the PSN before changing the hostname, and register it back. A new subordinate certificate gets provisioned automatically on the PSN.

---

**Step 1** Choose **Administration > System > Certificates > Certificate Signing Requests**

**Step 2** Click **Generate Certificate Signing Requests (CSR)**.

**Step 3** Choose ISE Root CA from the **Certificate(s) will be used for** drop-down list.

**Step 4** Click **Replace ISE Root CA Certificate chain**.

The root CA and subordinate CA certificates get generated for all the nodes in your deployment.

---

#### What to do next

If you have a secondary PAN in the deployment, obtain a backup of the Cisco ISE CA certificates and keys from the primary PAN and restore it on the secondary PAN. This ensures that the secondary PAN can function as the root CA in case of a primary PAN failure and you promote the secondary PAN to be the primary PAN.

## Configure Cisco ISE Root CA as Subordinate CA of an External PKI

If you want the root CA on the primary PAN to act as a subordinate CA of an external PKI, generate an ISE intermediate CA certificate signing request, send it to the external CA, obtain the root and CA-signed certificates, import the root CA certificate in to the Trusted Certificates Store, and bind the CA-signed certificate to the CSR. In this case, the external CA is the root CA, the Primary PAN is a subordinate CA of the external CA, and the PSNs are subordinate CAs of the primary PAN.

---

**Step 1** Choose **Administration > System > Certificates > Certificate Signing Requests**.

**Step 2** Click **Generate Certificate Signing Requests (CSR)**.

**Step 3** Choose ISE Intermediate CA from the **Certificate(s) will be used for** drop-down list.

**Step 4** Click **Generate**.

**Step 5** Export the CSR, send it to the external CA, and obtain the CA-signed certificate.

**Step 6** Import the root CA certificate from the external CA in to the Trusted Certificates store.

**Step 7** Bind the CA-signed certificate with the CSR.

---

#### What to do next

If you have a secondary PAN in the deployment, obtain a backup of the Cisco ISE CA certificates and keys from the primary PAN and restore it on the secondary PAN. Server and root certificates are then automatically replicated in the secondary PAN. This ensures that the secondary PAN can function as subordinate CA of the external PKI in case of administration node failover.

# Configure Cisco ISE to Use Certificates for Authenticating Personal Devices

You can configure Cisco ISE to issue and manage certificates for endpoints (personal devices) that connect to your network. You can use the internal Cisco ISE CA service to sign the certificate signing request from endpoints or forward the CSR to an external CA.

## Before you begin

- Obtain a backup of the Cisco ISE CA certificates and keys from the primary PAN and store them in a secure location for disaster recovery purposes.
- If you have a secondary PAN in the deployment, back up the Cisco ISE CA certificates and keys from the primary PAN and restore them on the secondary PAN.

---

**Step 1** [Add Users to Employee User Group, on page 58.](#)

You can add users to the internal identity store or to an external identity store such as Microsoft Active Directory.

**Step 2** [Create a Certificate Authentication Profile for TLS-Based Authentication, on page 59 .](#)

**Step 3** [Create an Identity Source Sequence for TLS-Based Authentication, on page 59.](#)

**Step 4** Create a client provisioning policy:

- [Configure Certificate Authority Settings, on page 60](#)
- [Create a CA Template, on page 61](#)
- [Create a Native Supplicant Profile to be Used in Client-Provisioning Policy, on page 63](#)
- [Download Agent Resources from Cisco for Windows and MAC OS X Operating Systems, on page 63](#)
- [Create Client-Provisioning Policy Rules for Apple iOS, Android, and MAC OS X Devices, on page 64](#)

**Step 5** [Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication, on page 64](#)

**Step 6** Configure authorization policy rules for TLS-based authentications.

- [Create Authorization Profiles for Central Web Authentication and Supplicant-Provisioning Flows, on page 65](#)
- [Create Authorization Policy Rules, on page 66](#)

When you use ECDHE-RSA based certificates, while connecting to the wireless SSID from your personal device, you will be prompted to enter the password a second time.

---

## Add Users to Employee User Group

The following procedure describes how to add users to the Employee user group in the Cisco ISE identity store. If you are using an external identity store, make sure that you have an Employee user group to which you can add users.

---

**Step 1** Choose **Administration > Identity Management > Identities > Users**.

**Step 2** Click **Add**.

**Step 3** Enter the user details.

**Step 4** In the **Passwords** section, choose the **Login Password** and TACACS+ **Enable Password** to set the access level to a network device.

**Step 5** Select Employee from the User Group drop-down list.

All users who belong to the Employee user group share the same set of privileges.

**Step 6** Click **Submit**.

---

#### What to do next

[Create a Certificate Authentication Profile for TLS-Based Authentication, on page 59](#)

## Create a Certificate Authentication Profile for TLS-Based Authentication

To use certificates for authenticating endpoints that connect to your network, you must define a certificate authentication profile in Cisco ISE or edit the default Preloaded\_Certificate\_Profile. The certificate authentication profile includes the certificate field that should be used as the principal username. For example, if the username is in the Common Name field, then you can define a certificate authentication profile with the Principal Username being the Subject - Common Name, which can be verified against the identity store.

---

**Step 1** Choose **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile**.

**Step 2** Enter a name for your certificate authentication profile. For example, CAP.

**Step 3** Choose Subject - Common Name as the **Principal Username X509 Attribute**.

**Step 4** Click **Save**.

---

#### What to do next

[Create an Identity Source Sequence for TLS-Based Authentication, on page 59](#)

## Create an Identity Source Sequence for TLS-Based Authentication

After you create a certificate authentication profile, you must add it to the identity source sequence so that Cisco ISE can obtain the attribute from the certificate and match it against the identity sources that you have defined in the identity source sequence.

#### Before you begin

Ensure that you have completed the following tasks:

- Add users to the Employee user group.
  - Create a certificate authentication profile for certificate-based authentication.
- 

**Step 1** Choose **Administration > Identity Management > Identity Source Sequences**.

**Step 2** Click **Add**.

**Step 3** Enter a name for the identity source sequence. For example, Dot1X.

**Step 4** Check the **Select Certificate Authentication Profile** check box and select the certificate authentication profile that you created earlier, namely CAP.

**Step 5** Move the identity source that contains your user information to the **Selected** list box in the Authentication Search List area.

You can add additional identity sources and Cisco ISE searches these data stores sequentially until a match is found.

**Step 6** Click the **Treat as if the user was not found and proceed to the next store in the sequence** radio button.

**Step 7** Click **Submit**.

### What to do next

[Configure Certificate Authority Settings, on page 60](#)

## Configure Certificate Authority Settings

You must configure the external CA settings if you are going to use an external CA for signing the CSRs. The external CA settings was known as the SCEP RA profile in previous releases of Cisco ISE. If you are using the Cisco ISE CA, then you do not have to explicitly configure the CA settings. You can review the Internal CA settings at Administration > System > Certificates > Internal CA Settings.

Once users' devices receive their validated certificate, they reside on the device as described in the following table.

**Table 10: 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

### Before you begin

If you are going to use an external Certificate Authority (CA) for signing the certificate signing request (CSR), then you must have the URL of the external CA.

**Step 1** Choose **Administration > System > Certificates > External CA Settings**.

**Step 2** Click **Add**.

**Step 3** Enter a name for the external CA setting. For example, EXTERNAL\_SCEP.

**Step 4** Enter the external CA server URL in the URL text box.

Click **Test Connection** to check if the external CA is reachable. Click the + button to enter additional CA server URLs.

**Step 5** Click **Submit**.

**What to do next**

[Create a CA Template, on page 61](#)

**Create a CA Template**

The certificate template defines the SCEP RA profile that must be used (for the internal or external CA), Key Type, Key Size or Curve Type, Subject, Subject Alternative Name (SAN), validity period of the certificate, and the Extended Key Usage. This example assumes that you are going to use the internal Cisco ISE CA. For an external CA template, the validity period is determined by the external CA and you cannot specify it.

You can create a new CA template or edit the default certificate template, EAP\_Authentication\_Certificate\_Template.

By default, the following CA templates are available in Cisco ISE:

- CA\_SERVICE\_Certificate\_Template—For other network services that use the ISE CA. For example, use this certificate template while configuring ISE to issue certificates for ASA VPN users.
- EAP\_Authentication\_Certificate\_Template—For EAP authentication.
- pxGrid\_Certificate\_Template—For pxGrid controller while generating the certificate from the Certificate Provisioning Portal.




---

**Note** Certificate templates that use the ECC key type can be used only with the internal Cisco ISE CA.

---

**Before you begin**

Ensure that you have configured the CA settings.

---

**Step 1** Choose **Administration > System > CA Service > Internal CA Certificate Template**.

**Step 2** Enter a name for the internal CA template. For example, Internal\_CA\_Template.

**Step 3** (Optional) Enter values for the Organizational Unit, Organization, City, State, and Country fields.

We do not support UTF-8 characters in the certificate template fields (Organizational Unit, Organization, City, State, and Country). Certificate provisioning fails if UTF-8 characters are used in the certificate template.

The username of the internal user generating the certificate is used as the Common Name of the certificate. Cisco ISE Internal CA does not support "+" or "\*" characters in the Common Name field. Ensure that your username does not include "+" or "\*" special characters.

**Step 4** Specify the Subject Alternative Name (SAN) and the validity period of the certificate.

**Step 5** Specify a Key Type. Choose RSA or ECC.

The following table lists the operating systems and versions that support ECC along with the curve types that are supported. If your devices are not running a supported operating system or on a supported version, you can use RSA-based certificates instead.

Operating System	Supported Versions	Supported Curve Types
Windows	8 and later	P-256, P-384, and P-521

Operating System	Supported Versions	Supported Curve Types
Android	4.4 and later  <b>Note</b> Android 6.0 requires May 2016 patch to support ECC certificates.	All curve types (except Android 6.0, which does not support the P-192 curve type).

Windows 7 and Apple iOS do not natively support ECC for EAP-TLS authentication. This release of Cisco ISE does not support the use of ECC certificates on MAC OS X devices.

If the devices in your network run an operating system that is not supported (Windows 7, MAC OS X, or Apple iOS, we recommend that you choose RSA as the Key Type.

- Step 6** (Applicable if you choose the RSA Key Type) Specify a key size. You must choose 1024 or a higher key size.
- Step 7** (Applicable only if you choose the ECC Key Type) Specify the Curve Type. The default is P-384.
- Step 8** Choose ISE Internal CA as the SCEP RA Profile.
- Step 9** Enter the validity period in days. The default is 730 days. Valid range is between 1 and 730.
- Step 10** Specify the Extended Key Usage. Check the **Client Authentication** check box if you want the certificate to be used for client authentication. Check the **Server Authentication** check box if you want the certificate to be used for server authentication.
- Step 11** Click **Submit**.

---

The internal CA certificate template is created and will be used by the client provisioning policy.

#### What to do next

[Create a Native Supplicant Profile to be Used in Client-Provisioning Policy, on page 63](#)

## Internal CA Settings

*Table 11: Internal CA Settings*

Field Name	Usage Guidelines
<b>Disable Certificate Authority</b>	Click this button to disable the internal CA service.
<b>Host Name</b>	Host name of the Cisco ISE node that is running the CA service.
<b>Personas</b>	Cisco ISE node personas that are enabled on the node running the CA service. For example, Administration, Policy Service, etc.
<b>Role(s)</b>	The role(s) assumed by the Cisco ISE node running the CA service. For example, Standalone or Primary or Secondary.
<b>CA, EST &amp; OCSP Responder Status</b>	Enabled or disabled
<b>OCSP Responder URL</b>	URL for Cisco ISE node to access the OCSP server.

Field Name	Usage Guidelines
SCEP URL	URL for the Cisco ISE node to access the SCEP server.

**Related Topics**

[Cisco ISE CA Service](#), on page 47

[Configure Cisco ISE to Use Certificates for Authenticating Personal Devices](#), on page 58

## Create a Native Supplicant Profile to be Used in Client-Provisioning Policy

You can create native supplicant profiles to enable users to bring personal devices to your Corporate network. Cisco ISE uses different policy rules for different operating systems. Each client provisioning policy rule contains a native supplicant profile, which specifies which provisioning wizard is to be used for which operating system.

**Before you begin**

- Configure the CA certificate template in Cisco ISE.
- Open up TCP port 8905 and UDP port 8905 to enable client agents and supplicant provisioning wizard installation. For more information about port usage, see the "Cisco ISE Appliance Ports Reference" appendix in the *Cisco Identity Services Engine Hardware Installation Guide*.

---

**Step 1** Choose **Policy** > **Policy Elements** > **Results** > **Client Provisioning** > **Resources**.

**Step 2** Choose **Add** > **Native Supplicant Profile**.

**Step 3** Enter a name for the native supplicant profile. For example, EAP\_TLS\_INTERNAL.

**Step 4** Choose ALL from the **Operating System** drop-down list.

**Note** The MAC OS version 10.10 user should manually connect to the provisioned SSID for dual-SSID PEAP flow.

**Step 5** Check the **Wired** or **Wireless** check box.

**Step 6** Choose TLS from the **Allowed Protocol** drop-down list.

**Step 7** Choose the CA certificate template that you created earlier.

**Step 8** Click **Submit**.

---

**What to do next**

[Download Agent Resources from Cisco for Windows and MAC OS X Operating Systems](#), on page 63

## Download Agent Resources from Cisco for Windows and MAC OS X Operating Systems

For Windows and MAC OS X operating systems, you must download the remote resources from the Cisco site.

**Before you begin**

Ensure that you are able to access the appropriate remote location to download client provisioning resources to Cisco ISE, by verifying that the proxy settings for your network are correctly configured.

- 
- Step 1** Choose **Policy** > **Policy Elements** > **Resources** > **Client Provisioning** > **Resources**.
- Step 2** Choose **Add** > **Agent resources from Cisco site**.
- Step 3** Check the check boxes next to the **Windows** and **MAC OS X** packages. Be sure to include the latest versions.
- Step 4** Click **Save**.
- 

**What to do next**

[Create Client-Provisioning Policy Rules for Apple iOS, Android, and MAC OS X Devices, on page 64](#)

## Create Client-Provisioning Policy Rules for Apple iOS, Android, and MAC OS X Devices

Client provisioning resource policies determine which users receive which version (or versions) of resources (agents, agent compliance modules, and agent customization packages/profiles) from Cisco ISE upon login and user session initiation.

When you download the agent compliance module, it always overwrites the existing one, if any, available in the system.

To enable employees to bring iOS, Android, MAC OS X devices, you must create policy rules for each of these devices on the Client Provisioning Policy page.

**Before you begin**

You must have configured the required native supplicant profiles and downloaded the required agents from the Client Provisioning Policy pages.

- 
- Step 1** Choose **Policy** > **Client Provisioning**.
- Step 2** Create client provisioning policy rules for Apple iOS, Android, and MAC OS X devices.
- Step 3** Click **Save**.
- 

**What to do next**

[Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication, on page 64](#)



## Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication

This task shows how to update the Dot1X authentication policy rule for TLS-based authentications.

**Before you begin**

Ensure that you have the certificate authentication profile created for TLS-based authentication.



- 
- Step 1** Choose **Policy > Policy Sets**.
- Step 2** Click the arrow icon  from the **View** column to open the Set view screen and view, manage, and update the authentication policy.
- The default rule-based authentication policy includes a rule for Dot1X authentication.
- Step 3** To edit the conditions for the Dot1X authentication policy rule, hover over the cell in the **Conditions** column and click . The Conditions Studio opens.
- Step 4** From the **Actions** column in the Dot1X policy rule, click the cog icon and then from the drop-down menu, insert a new policy set by selecting any of the insert or duplicate options, as necessary.
- A new row appears in the Policy Sets table.
- Step 5** Enter a name for the rule. For example, eap-tls.
- Step 6** From the **Conditions** column, click the (+) symbol.
- Step 7** Create the required conditions in the **Conditions Studio Page**. In the **Editor** section, click the **Click To Add an Attribute** text box, and select the required Dictionary and Attribute (for example, Network Access:UserName Equals User1).
- You can drag and drop a Library condition to the **Click To Add An Attribute** text box.
- Step 8** Click **Use**.
- Step 9** Leave the default rule as is.
- Step 10** Click **Save**.
- 

#### What to do next

[Create Authorization Profiles for Central Web Authentication and Supplicant-Provisioning Flows, on page 65](#)

## Create Authorization Profiles for Central Web Authentication and Supplicant-Provisioning Flows

You must define authorization profiles to determine the access that must be granted to the user after the certificate-based authentication is successful.

#### Before you begin

Ensure that you have configured the required access control lists (ACLs) on the wireless LAN controller (WLC). Refer to the *TrustSec How-To Guide: Using Certificates for Differentiated Access* for information on how to create the ACLs on the WLC.

This example assumes that you have created the following ACLs on the WLC.

- NSP-ACL - For native supplicant provisioning
- BLACKHOLE - For restricting access to block listed devices
- NSP-ACL-Google - For provisioning Android devices

- 
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

- Step 2** Click **Add** to create a new authorization profile.
- Step 3** Enter a name for the authorization profile.
- Step 4** From the **Access Type** drop-down list, choose ACCESS\_ACCEPT.
- Step 5** Click **Add** to add the authorization profiles for central web authentication, central web authentication for Google Play, native supplicant provisioning, and native supplicant provisioning for Google.
- Step 6** Click **Save**.

### What to do next

[Create Authorization Policy Rules, on page 66](#)

## Create Authorization Policy Rules

Cisco ISE evaluates the authorization policy rules and grants the user access to the network resources based on the authorization profile specified in the policy rule.

### Before you begin

Ensure that you have created the required authorization profiles.

- Step 1** Choose **Policy > Policy Sets**, and expand the policy set to view the authorization policy rules.
- Step 2** Insert additional policy rules above the default rule.
- Step 3** Click **Save**.

## CA Service Policy Reference

This section provides reference information for the authorization and client provisioning policy rules that you must create before you can enable the Cisco ISE CA service.

### Client-Provisioning Policy Rules for Certificate Services

This section lists the client provisioning policy rules that you must create while using the Cisco ISE certificate services. The following table provides the details.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
iOS	Any	Apple iOS All	Condition(s)	EAP_TLS_INTERNAL (the native supplicant profile that you created earlier). If you are using an external CA, select the native supplicant profile that you have created for the external CA.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
Android	Any	Android	Condition(s)	EAP_TLS_INTERNAL (the native supplicant profile that you created earlier). If you are using an external CA, select the native supplicant profile that you have created for the external CA.
MAC OS X	Any	MACOSX	Condition(s)	Under the Native Supplicant Configuration, specify the following: <ol style="list-style-type: none"> <li>1. Config Wizard: Select the MAC OS X supplicant wizard that you downloaded from the Cisco site.</li> <li>2. Wizard Profile: Choose the EAP_TLS_INTERNAL native supplicant profile that you created earlier. If you are using an external CA, select the native supplicant profile that you have created for the external CA.</li> </ol>

## Authorization Profiles for Certificate Services

This section lists the authorization profiles that you must create for enabling certificate-based authentication in Cisco ISE. You must have already created the ACLs (NSP-ACL and NSP-ACL-Google) on the wireless LAN controller (WLC).

- CWA - This profile is for devices that go through the central web authentication flow. Check the **Web Authentication** check box, choose Centralized from the drop-down list, and enter NSP-ACL in the ACL text box.

- CWA\_GooglePlay - This profile is for Android devices that go through the central web authentication flow. This profile enables Android devices to access Google Play Store and download the Cisco Network Setup Assistant. Check the **Web Authentication** check box, choose Centralized from the drop-down list, and enter NSP-ACL-Google in the ACL text box.
- NSP - This profile is for non-Android devices that go through the supplicant provisioning flow. Check the **Web Authentication** check box, choose Supplicant Provisioning from the drop-down list, and enter NSP-ACL in the ACL text box.
- NSP-Google - This profile is for Android devices that go through the supplicant provisioning flow. Check the **Web Authentication** check box, choose Supplicant Provisioning from the drop-down list, and enter NSP-ACL-Google in the ACL text box.

Review the default Blackhole\_Wireless\_Access authorization profile. The Advanced Attributes Settings should be:

- Cisco:cisco-av-pair = url-redirect=https://ip:port/blacklistportal/gateway?portal=PortalID
- Cisco:cisco-av-pair = url-redirect-acl=BLACKHOLE

## Authorization Policy Rules for Certificate Services

This section lists the authorization policy rules that you must create while enabling the Cisco ISE CA service.

- Corporate Assets-This rule is for corporate devices that connect to the corporate wireless SSID using 802.1X and MSCHAPV2 protocol.
- Android\_SingleSSID-This rule is for Android devices that access the Google Play Store to download the Cisco Network Setup Assistant for provisioning. This rule is specific to single SSID setup.
- Android\_DualSSID-This rule is for Android devices that access the Google Play Store to download the Cisco Network Setup Assistant for provisioning. This rule is specific to dual SSID setup.
- CWA-This rule is for devices that go through the central web authentication flow.
- NSP-This rule is for devices that go through the native supplicant provisioning flow using a certificate for EAP-TLS authentication.
- EAP-TLS-This rule is for devices that have completed the supplicant provisioning flow and are provisioned with a certificate. They will be given access to the network.

The following table lists the attributes and values that you must choose while configuring authorization policy rules for the Cisco ISE CA service. This example assumes that you have the corresponding authorization profiles configured in Cisco ISE as well.

Rule Name	Conditions	Permissions (Authorization Profiles to be Applied)
Corporate Assets	Corp_Assets AND (Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	PermitAccess
Android_SingleSSID	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android)	NSP_Google

Rule Name	Conditions	Permissions (Authorization Profiles to be Applied)
Android_DualSSID	(Wireless_MAB AND Session:Device-OS EQUALS Android)	CWA_GooglePlay
CWA	Wireless_MAB	CWA
NSP	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	NSP
EAP-TLS	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI)	PermitAccess

## Cisco ISE CA Issues Certificates to ASA VPN Users

ISE CA issues certificates to client machines connecting over ASA VPN. Using this feature, you can automatically provision certificates to end devices that connect over ASA VPN.

Cisco ISE uses the Simple Certificate Enrollment Protocol (SCEP) for enrollment and to provision certificates to the client machines. The AnyConnect client sends the SCEP request to the ASA over an HTTPS connection. The ASA evaluates the request and enforces policies before it relays the request to Cisco ISE over an HTTP connection established between Cisco ISE and ASA. The response from the Cisco ISE CA is relayed back to the client. The ASA cannot read the contents of the SCEP message and functions as a proxy for the Cisco ISE CA. The Cisco ISE CA decrypts the SCEP message from the client and sends the response in an encrypted form.

The ISE CA SCEP URL is `http://<IP Address or FQDN of ISE CA server>:9090/auth/caservice/pkiclient.exe`. If you are using FQDN of the ISE node, the DNS server connected to ASA must be able to resolve the FQDN.

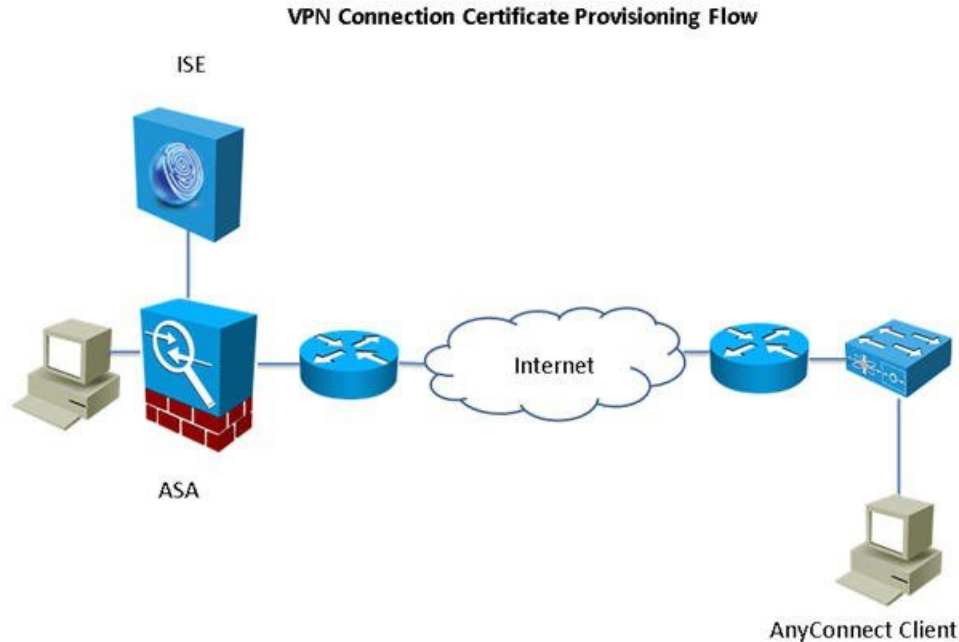
You can configure certificate renewal before expiration in the AnyConnect client profile. If the certificate has already expired, the renewal flow is similar to a new enrollment.

Supported versions include:

- Cisco ASA 5500 Series Adaptive Security Appliances that run software version 8.x
- Cisco AnyConnect VPN version 2.4 or later

## VPN Connection Certificate-Provisioning Flow

Figure 4: Certificate Provisioning for ASA VPN Users



1. The user initiates a VPN connection.
2. The AnyConnect client scans the client machine and sends the attributes such as the unique device identifier (for example, IMEI) to the ASA.
3. The ASA requests certificate-based authentication from the client. The authentication fails because there is no certificate.
4. The ASA proceeds to primary user authentication (AAA) using the username/password and passes the information to the authentication server (ISE).
  - a. If authentication fails, the connection is terminated immediately.
  - b. If authentication passes, limited access is granted. You can configure dynamic access policies (DAP) for client machines that request a certificate using the `aaa.cisco.sceprequired` attribute. You can set the value for this attribute to “true” and apply ACLs and web ACLs.
5. The VPN connection is established after the relevant policies and ACLs are applied. The client starts key generation for SCEP only after AAA authentication succeeds and the VPN connection is established.
6. The client starts the SCEP enrollment and sends SCEP requests to ASA over HTTP.
7. ASA looks up the session information of the request and relays the request to ISE CA, if the session is allowed for enrollment.
8. ASA relays the response from ISE CA back to the client.
9. If enrollment succeeds, the client presents a configurable message to the user and disconnects the VPN session.

10. The user can again authenticate using the certificate and a normal VPN connection is established.

## Configure Cisco ISE CA to Issue Certificates to ASA VPN Users

You must perform the following configurations on Cisco ISE and ASA to provision certificates to ASA VPN users.

### Before you begin

- Ensure that the VPN user account is present in Cisco ISE internal or external identity source.
- Ensure that the ASA and the Cisco ISE Policy Service Nodes are synchronized using the same NTP server.

- 
- Step 1** Define the ASA as a network access device in Cisco ISE. See [Add a Network Device in Cisco ISE, on page 71](#) for information on how to add ASA as a network device.
  - Step 2** [Configure Group Policy in ASA, on page 72.](#)
  - Step 3** [Configure AnyConnect Connection Profile for SCEP Enrollment, on page 72.](#)
  - Step 4** [Configure a VPN Client Profile in ASDM, on page 73.](#)
  - Step 5** [Import Cisco ISE CA Certificates into ASA.](#)
- 

### Add a Network Device in Cisco ISE

You can add a network device in Cisco ISE or use the default network device.

You can also add a network device in the **Network Devices (Work Centers > Device Administration > Network Resources > Network Devices)** window.

### Before you begin

The AAA function must be enabled on the network device to be added. See the section “Command to Enable AAA Functions” in chapter the “Integrations” in the *Cisco ISE Administrator Guide* for your release.

- 
- Step 1** Choose **Administration > Network Resources > Network Devices**.
  - Step 2** Click **Add**.
  - Step 3** Enter the corresponding values in the **Name**, **Description**, and **IP Address** fields.  
**Note** IPv4 and IPv6 are both supported for network device (TACACS and RADIUS) configurations and for external RADIUS server configuration. Ranges and subnet masks are supported for IPv4 addresses. Ranges are not supported for IPv6 addresses.
  - Step 4** Choose the required values from the **Device Profile**, **Model Name**, **Software Version**, and **Network Device Group** drop-down lists.
  - Step 5** (Optional) Check the **RADIUS Authentication Settings** check box to configure the RADIUS protocol for authentication.
  - Step 6** (Optional) Check the **TACACS Authentication Settings** check box to configure the TACACS protocol for authentication.
  - Step 7** (Optional) Check the **SNMP Settings** check box to configure SNMP for the Cisco ISE profiling service to collect information from the network device.

**Step 8** (Optional) Check the **Advanced Trustsec Settings** check box to configure a Cisco TrustSec-enabled device.

**Step 9** Click **Submit**.

### Configure Group Policy in ASA

Configure a group policy in ASA to define the ISE CA URL for AnyConnect to forward the SCEP enrollment request.

**Step 1** Log in to Cisco ASA ASDM.

**Step 2** From the Remote Access VPN navigation pane on the left, click **Group Policies**.

**Step 3** Click **Add** to create a group policy.

**Step 4** Enter a name for the group policy. For example, ISE\_CA\_SCEP.

**Step 5** In the SCEP forwarding URL field, uncheck the **Inherit** check box and enter the ISE SCEP URL with port number.

If you are using the FQDN of the ISE node, the DNS server connected to ASA must be able to resolve the FQDN of the ISE node.

**Example:**

http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe.

**Step 6** Click **OK** to save the group policy.

### Configure AnyConnect Connection Profile for SCEP Enrollment

Configure an AnyConnect connection profile in ASA to specify the ISE CA server, authentication method, and ISE CA SCEP URL.

**Step 1** Log in to Cisco ASA ASDM.

**Step 2** From the Remote Access VPN navigation pane on the left, click **AnyConnect Connection Profiles**.

**Step 3** Click **Add** to create a connection profile.

**Step 4** Enter a name for the connection profile. For example, Cert-Group.

**Step 5** (Optional) Enter a description for the connection profile in the Aliases field. For example, SCEP-Call-ASA.

**Step 6** In the Authentication area, specify the following:

- Method—Click the **Both** radio button
- AAA Server Group—Click **Manage** and choose your ISE server

**Step 7** In the Client Address Assignment area, select the DHCP server and client address pools to use.

**Step 8** In the Default Group Policy area, click **Manage** and select the Group Policy that you have created with the ISE SCEP URL and port number.

**Example:**

For example, ISE\_CA\_SCEP.

**Step 9** Choose **Advanced** > **General** and check the **Enable Simple Certificate Enrollment Protocol** check box for this connection profile.

**Step 10** Click **OK**.



Your AnyConnect connection profile is created.

---

### What to do next

#### Configure a VPN Client Profile in ASDM

Configure a VPN client profile in AnyConnect for SCEP enrollment.

---

- Step 1** Log in to Cisco ASA ASDM.
- Step 2** From the Remote Access VPN navigation pane on the left, click **AnyConnect Client Profile**.
- Step 3** Select the client profile that you want to use and click **Edit**.
- Step 4** Click **Certificate Enrollment** from the Profile navigation pane on the left.
- Step 5** Check the **Certificate Enrollment** check box.
- Step 6** Enter the values in the following fields:
- **Certificate Expiration Threshold**—The number of days before the certificate expiration date that AnyConnect warns users their certificate is going to expire (not supported when SCEP is enabled). The default is zero (no warning displayed). The range of values is zero to 180 days.
  - **Automatic SCEP Host**—Enter the host name and connection profile (tunnel group) of the ASA that has SCEP certificate retrieval configured. Enter a Fully Qualified Domain Name (FQDN) or a connection profile name of the ASA. For example, the hostname `asa.cisco.com` and the connection profile name `Cert_Group`.
  - **CA URL**—Identifies the SCEP CA server. Enter the FQDN or IP Address of the ISE server. For example, `http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe`.
- Step 7** Enter values for the Certificate Contents that define how the client requests the contents of the certificate.
- Step 8** Click **OK**.
- The AnyConnect client profile is created. Refer to the [Cisco AnyConnect Secure Mobility Client](#) for your version of AnyConnect for additional information.
- 

#### Import Cisco ISE CA Certificates into ASA

Import the Cisco ISE internal CA certificates into the ASA.

#### Before you begin

Export the Cisco ISE internal CA certificates. Go to **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**. Check the check boxes next to **Certificate Services Node CA** and **Certificate Services Root CA** certificates and export them, one certificate at a time.

---

- Step 1** Log in to Cisco ASA ASDM.
- Step 2** From the Remote Access VPN navigation pane on the left, choose **Certificate Management > CA Certificates**.
- Step 3** Click **Add** and select the Cisco ISE internal CA certificates to import them in to ASA.
-

## Revoke an Endpoint Certificate

If you need to revoke a certificate issued to an employee's personal device, you can revoke it from the Endpoint Certificates page. For example, if an employee's device has been stolen or lost, you can log in to the Cisco ISE Admin portal and revoke the certificate issued to that device from the Endpoint Certificates page. You can filter the data on this page based on the Friendly Name, Device Unique Id, or Serial Number.

If a PSN (sub CA) is compromised, you can revoke all certificates issued by that PSN by filtering on the Issued By field from the Endpoint Certificates page.

When you revoke a certificate issued to an employee, if there is an active session (authenticated using that certificate), the session is terminated immediately. Revoking a certificate ensures that unauthorized users do not have any access to resources as soon as the certificate is revoked.

- 
- Step 1** Choose **Administration > System > Certificates > Certificate Authority > Issued Certificates**.
  - Step 2** Check the check box next to the endpoint certificate that you want to revoke and click **Revoke**.  
You can search for the certificate based on the Friendly Name and Device Type.
  - Step 3** Enter the reason for revoking the certificate.
  - Step 4** Click **Yes**.
- 

## 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 Certificate Revocation List (CRL) 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.

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 an unknown status is returned for a given certificate, Cisco ISE switches to checking the CRL.

## Cisco ISE CA Service Online Certificate Status Protocol Responder

The Cisco ISE CA OCSP responder is a server that communicates with OCSP clients. The OCSP clients for the Cisco ISE CA include the internal Cisco ISE OCSP client and OCSP clients on the Adaptive Security Appliance (ASA). The OCSP clients should communicate with the OCSP responder using the OCSP request/response structure defined in RFC 2560, 5019.

The Cisco ISE CA issues a certificate to the OCSP responder. The OCSP responder listens on port 2560 for any incoming requests. This port is configured to allow only OCSP traffic.

The OCSP responder accepts a request that follows the structure defined in RFC 2560, 5019. Nonce extension is supported in the OCSP request. The OCSP responder obtains the status of the certificate and creates an OCSP response and signs it. The OCSP response is not cached on the OCSP responder, although you can

cache the OCSP response on the client for a maximum period of 24 hours. The OCSP client should validate the signature in the OCSP response.

The self-signed CA certificate (or the intermediate CA certificate if ISE acts as an intermediate CA of an external CA) on the PAN issues the OCSP responder certificate. This CA certificate on the PAN issues the OCSP certificates on the PAN and PSNs. This self-signed CA certificate is also the root certificate for the entire deployment. All the OCSP certificates across the deployment are placed in the Trusted Certificates Store for ISE to validate any response signed using these certificates.



---

**Note** Cisco ISE receives from OCSP responder servers a `thisUpdate` value, which indicates the time since the last certificate revocation. If the `thisUpdate` value is greater than 7 days, the OCSP certificate verification fails in Cisco ISE.

---

## 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. OCSP service returns this value if the certificate was not issued by the CA of this OCSP responder.
- **Error**—No response was received for the OCSP request.

## OCSP High Availability

Cisco ISE has the capability to configure up to two OCSP servers per CA, and they are 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 (which is 5 seconds), when Cisco ISE communicates with the primary OCSP server, it switches 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:

- Failed OCSP cache or OCSP client side (Cisco ISE) failures.

- Failed OCSP responder scenarios, for example:

The first primary OCSP responder not responding, and the secondary OCSP responder responding to the Cisco ISE OCSP request.

Errors or 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, in 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.

- Failed OCSP reports

## Add OCSP Client Profiles

You can use the OCSP Client Profile page to add new OCSP client profiles to Cisco ISE.

### Before you begin

If the Certificate Authority (CA) is running the OCSP service on a nonstandard port (other than 80 or 443), you must configure ACLs on the switch to allow for communication between Cisco ISE and the CA on that port. For example:

```
permit tcp <source ip> <destination ip> eq <OCSP port number>
```

- 
- Step 1** Choose **Administration > System > Certificates > Certificate Management > OCSP Client Profile**.
  - Step 2** Enter the values to add an OCSP Client Profile.
  - Step 3** Click **Submit**.
- 

## OCSP Client Profile Settings

Table 12: OCSP Client Profile Settings

Field Name	Usage Guidelines
Name	Name of the OCSP Client Profile.
Description	Enter an optional description.

Field Name	Usage Guidelines
<b>Configure OCSP Responder</b>	
<b>Enable Secondary Server</b>	Check this check box to enable a secondary OCSP server for high availability.
<b>Always Access Primary Server First</b>	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.
<b>Fallback to Primary Server After Interval <i>n</i> Minutes</b>	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 to 999 minutes.
<b>Primary and Secondary Servers</b>	
<b>URL</b>	Enter the URL of the primary and/or secondary OCSP server.
<b>Enable Nonce Extension Support</b>	You can configure a nonce to be sent as part of the OCSP request. The Nonce 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.
<b>Validate Response Signature</b>	<p>The OCSP responder signs the response with one of the following certificates:</p> <ul style="list-style-type: none"> <li>• The CA certificate</li> <li>• A certificate different from the CA certificate</li> </ul> <p>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 that is not configured in Cisco ISE, the response verification will fail.</p>

Field Name	Usage Guidelines
<p><b>Use OCSP URLs specified in Authority Information Access (AIA)</b></p>	<p>Click the radio button to use the OCSP URLs specified in the Authority Information Access extension.</p>
<p><b>Response Cache</b></p>	
<p><b>Cache Entry Time To Live <i>n</i> Minutes</b></p>	<p>Enter the time in minutes after which the cache entry expires. Each response from the OCSP server holds a nextUpdate value. This value shows when the status of the 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 or persistent, so when Cisco ISE restarts, the cache is cleared. The OCSP cache is used in order to maintain the OCSP responses and for the following reasons:</p> <ul style="list-style-type: none"> <li>• To reduce network traffic and load from the OCSP servers on an already-known certificate</li> <li>• To increase the performance of Cisco ISE by caching already-known certificate statuses</li> </ul> <p>By default, the cache is set to 2 minutes for the internal CA OCSP client profile. If an endpoint authenticates a second time within 2 minutes of the first authentication, the OCSP cache is used and the OCSP responder is not queried. If the endpoint certificate has been revoked within the cache period, the previous OCSP status of Good will be used and the authentication succeeds. Setting the cache to 0 minutes prevents any responses from being cached. This option improves security, but decreases authentication performance.</p>
<p><b>Clear Cache</b></p>	<p>Click <b>Clear Cache</b> to clear entries of all the certificate authorities that are connected to the OCSP service.</p> <p>In a deployment, <b>Clear Cache</b> interacts with all the nodes and performs the operation. This mechanism updates every node in the deployment.</p>

**Related Topics**

- [OCSP Services](#), on page 74
- [Cisco ISE CA Service Online Certificate Status Protocol Responder](#), on page 74
- [OCSP Certificate Status Values](#), on page 75
- [OCSP High Availability](#), on page 75

[OCSP Failures](#), on page 75

[OCSP Statistics Counters](#), on page 79

[Add OCSP Client Profiles](#), on page 76

## OCSP Statistics Counters

Cisco ISE uses OCSP counters to log and monitor the data and health of the OCSP servers. Logging occurs every five minutes. Cisco ISE sends a syslog message to the Monitoring node and it is preserved in the local store. The local store contains data from the previous five minutes. After Cisco ISE sends the syslog message, the counters are recalculated for the next interval. This means, after five minutes, a new five-minute window interval starts again.

The following table lists the OCSP syslog messages and their descriptions.

**Table 13: OCSP Syslog Messages**

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

