Managing Certificates

Certificates are used in a network to provide secure access. Certificates are used to identify Cisco ISE to an endpoint and also to secure the communication between that endpoint and the Cisco ISE node. Certificates are used for all HTTPS communication and the Extensible Authentication Protocol (EAP) communication.

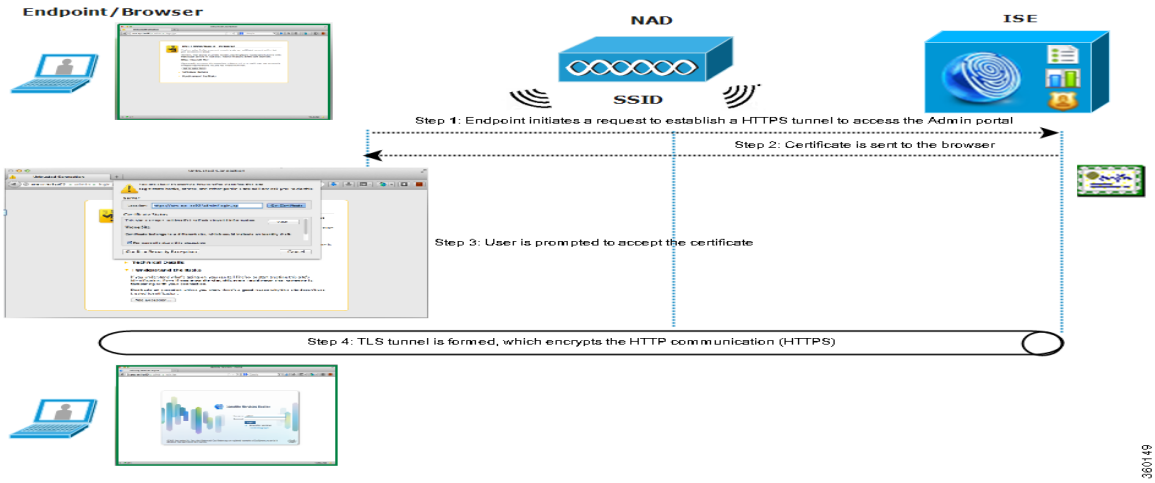
HTTPS Communication Using the Cisco ISE Certificate

All Cisco ISE web portals from release 1.1.0 onwards are secured using the HTTPS (TLS-encrypted HTTP communication) protocol:

- Administration Portal
- Centralized Web Authentication Portal
- Sponsor Portal
- Client Provisioning Portal
- My Devices Portal

Figure 8-1 shows an TLS-encrypted process when communicating with the Admin portal.

Figure 8-1 HTTPS (TLS-Encrypted HTTP Communication)



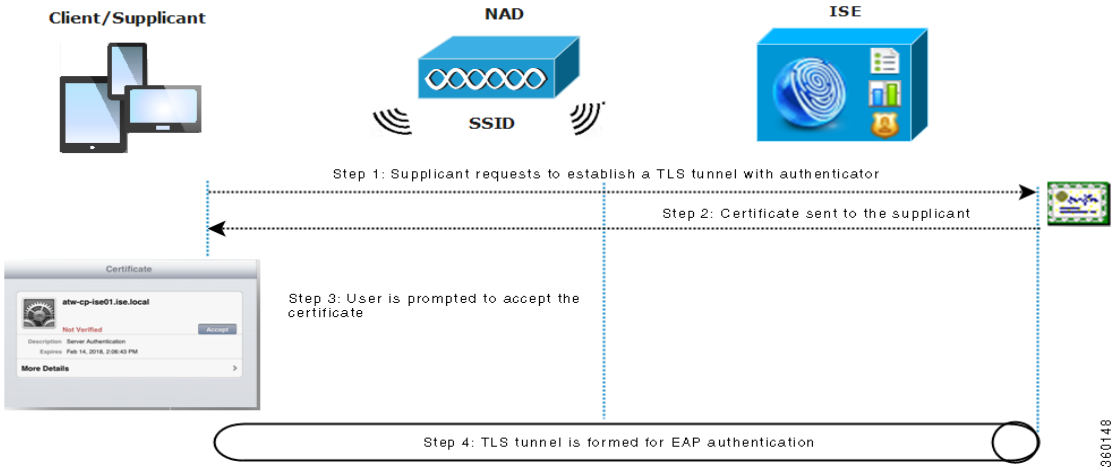
EAP Communication Using the Cisco ISE Certificate

Certificates are used with almost all EAP methods. The following EAP methods are commonly used:

- EAP-TLS
- PEAP
- EAP-FAST

For tunneled EAP methods, such as PEAP and FAST, Transport Layer Security (TLS) is used to secure the credential exchange. Similar to a request to a HTTPS web site, the client establishes a connection with the server. The server presents its certificate to the client. If the client trusts the certificate, the TLS tunnel is formed. The client's credentials are not sent to the server until after the tunnel is established, thereby ensuring a secure exchange. In a secure access deployment, the client is a supplicant, and the server is an ISE Policy Service node. Figure 8-2 shows an example using PEAP.

Figure 8-2 EAP Communication



Certificates Enable Cisco ISE to Provide Secure Access

The Cisco Identity Services Engine (ISE) relies on public key infrastructure (PKI) to provide secure communication with both endpoints and administrators, as well as 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. Cisco ISE provides the Admin Portal to manage the following two categories of X.509 certificates:

- Local certificates—These are server certificates that identify a Cisco ISE node to client applications. Every Cisco ISE node has its own local certificates, each of which are stored on the node along with the corresponding private key.
- Certificate Store certificates—These are certificate authority (CA) certificates used to establish trust for the public keys received from users and devices. The Certificate Store also contains certificates that are distributed by the Simple Certificate Enrollment Protocol (SCEP), which enables registration of mobile devices into the enterprise network. Certificates in the Certificate Store are managed on the primary Administration node, and are automatically replicated to all other nodes in an Cisco ISE deployment.

In a distributed deployment, you must import the certificate only in to the certificate trust list (CTL) of the primary Administration node. The certificate gets replicated to the secondary nodes.

In general, to ensure certificate authentication in Cisco ISE is not impacted by minor differences in certificate-driven verification functions, use lower case hostnames for all Cisco ISE nodes deployed in a network.

Enabling PKI in Cisco ISE

You should enable PKI in Cisco ISE in the following way:

Step 1 Establish local certificates on each deployment node for TLS-enabled authentication protocols (for example, EAP-TLS protocol), and for HTTPS, which is used by browser and REST clients to access the Cisco ISE web portals.

By default, a Cisco ISE node is preinstalled with a self-signed certificate that is used for both purposes. In a typical enterprise environment, this certificate is replaced with one or two server certificates that are signed by a trusted CA.

Step 2 Populate the Certificate Store with the CA certificates that are necessary to establish trust with the user as well as device certificates that will be presented to Cisco ISE.

If a certificate chain consisting of a root CA certificate plus one or more intermediate CA certificates is required to validate the authenticity of a user or device certificate, you must import the entire chain into the Certificate Store.

Related Topics

- See Local Certificates, page 8-4 for details on how to generate a Certificate Signing Request and import a CA-signed certificate.
- See Certificate Store, page 8-24 for details on how to import these certificate chains.

The Cisco ISE nodes use HTTPS for inter-node communication, so an administrator must populate the Certificate Store with the trust certificate(s) needed to validate the HTTPS local certificate belonging to each node in the Cisco ISE deployment. If a default self-signed certificate is used for HTTPS, then you must export this certificate from each Cisco ISE node and import it into the certificate store. If you replace the self-signed certificates with CA-signed certificates, it is only necessary to populate the Certificate Store with the appropriate root CA and intermediate CA certificates. Be aware that you cannot register a node in a Cisco ISE deployment until you complete this step.

If a Cisco ISE deployment is to be operated in FIPS mode, you must ensure that all local and certificate store 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 or primary Administration node, 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.

This chapter contains the following sections:

Local Certificates

Cisco ISE local certificates are server certificates that identify a Cisco ISE node to client applications. Local certificates are:

- Used by browser and REST clients who connect to Cisco ISE web portals. You must use HTTPS protocol for these connections.
- Used to form the outer TLS tunnel with PEAP and EAP-FAST. These certificates can be used for mutual authentication with EAP-TLS, PEAP, and EAP-FAST.

You must install valid local certificates for HTTPS and EAP-TLS on each node in your Cisco ISE deployment. By default, a self-signed certificate is created on a Cisco ISE node during installation time, and this certificate is designated for HTTPS and EAP-TLS use (it has a key length of 1024 and is valid for one year). It is recommended that you replace the self-signed certificate with a CA-signed certificate for greater security.

Wildcard Certificates

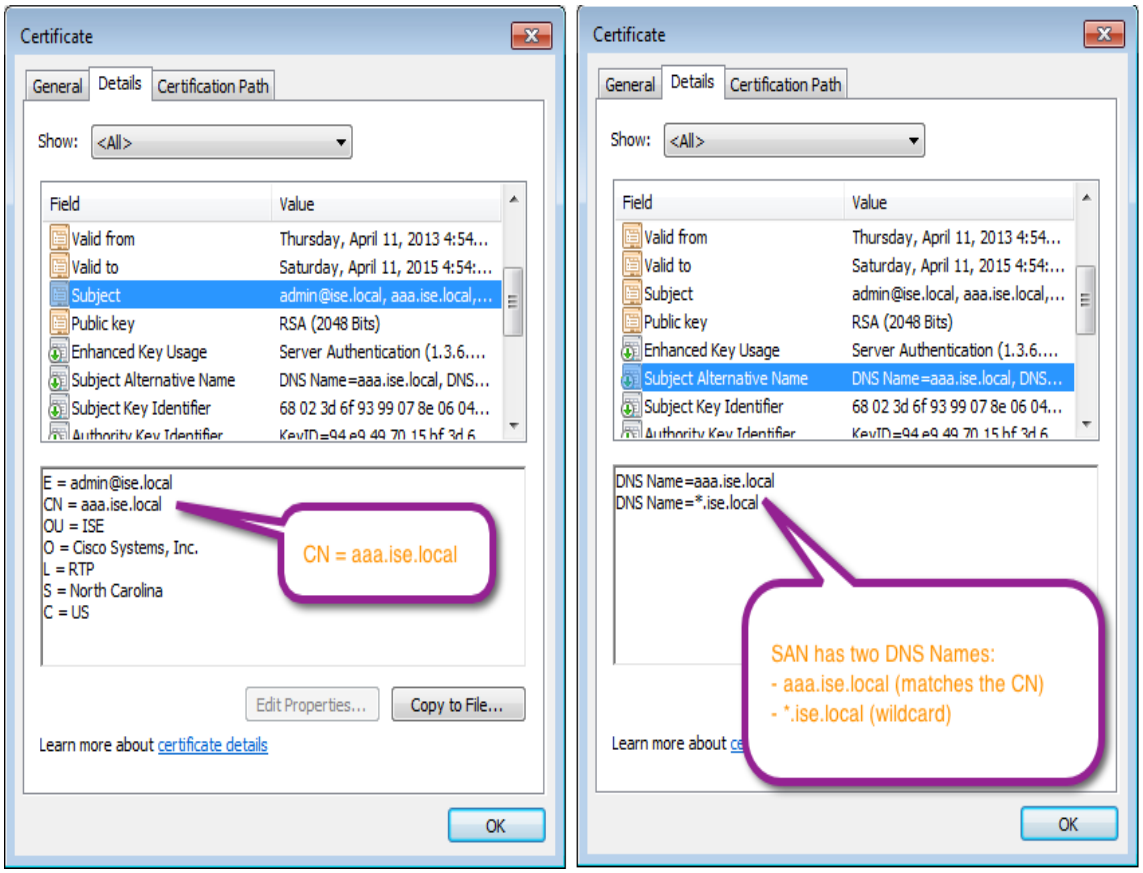
A wildcard certificate uses a wildcard notation (an asterisk and period before the domain name) and allows the certificate to be shared across multiple hosts in an organization. For example, the CN value for the Certificate Subject would be some generic hostname such as aaa.ise.local and the SAN field would include the same generic hostname and the 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

Figure 8-3 shows an example of a wildcard certificate that is used to secure a web site.

Figure 8-3 Wildcard Certificate Example



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

Related Topics

- Wildcard Certificates for HTTPS and EAP Communication, page 8-5
- Wildcard Certificate Support in Cisco ISE 1.2, page 8-6
- Fully Qualified Domain Name in URL Redirection, page 8-6
- Wildcard Certificate Compatibility, page 8-8
- Creating a Wildcard Certificate, page 8-8
- Installing Wildcard Certificates in Cisco ISE, page 8-10

Wildcard Certificates for HTTPS and EAP Communication

You can use wildcard server certificates in Cisco ISE for HTTPS (web-based services) and EAP protocols that use SSL/TLS tunneling. 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 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.

Note If you use wildcard certificates, we strongly 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 can lead to serious security issues.

Wildcard certificate uses an asterisk (*) and a period before the domain name. For example, the CN value for a certificate's Subject Name would be a generic host name 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 additional characters along with the wildcard character. For example, abc*.example.com or a*b.example.com or *abc.example.com.

Wildcard Certificate Support in Cisco ISE 1.2

Cisco ISE release 1.2 supports wildcard certificates. Prior to release 1.2, Cisco ISE verifies any certificate enabled for HTTPS to ensure the CN field matches the Fully Qualified Domain Name (FQDN) of the host exactly. If the fields did not match, the certificate could not be used for HTTPS communication.

Prior to release 1.2, Cisco ISE uses that CN value to replace the variable in the url-redirect A-V pair string. For all Centralized Web Authentication (CWA), onboarding, posture redirection, and so on, the CN value is used.

Cisco ISE 1.2 uses the hostname as the CN instead of relying on the CN field.

Fully Qualified Domain Name in URL Redirection

When Cisco ISE builds an authorization profile redirect (for central web authentication, device registration web authentication, native supplicant provisioning, mobile device management, and client provisioning and posture services), 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 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, you can use the **ip host** command in the configuration mode from the Cisco ISE CLI:

ISE /admin(config)# **ip host** *IP_address host-alias FQDN-string*

where *IP_address* is the IP address of the network interface (eth1 or eth2 or eth3)

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:

```
ISE/admin(config)# ip host a.b.c.d sales sales.amer.xyz.com
```

After you assign a host alias to the non-eth0 interface, you must 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:

ISE/admin(config)# **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 make use of non-eth0 interfaces for client provisioning or native supplicant or guest flows, you have to make sure that the IP address or host alias for non-eth0 interfaces should be configured appropriately in the Policy Service node certificate's SAN fields.

Advantages of Using Wildcard Certificates

- Cost savings. Certificates signed by a third party Certificate Authority is expensive, especially as the number of servers increase. Wildcard certificates may be used on multiple nodes in the Cisco ISE deployment.
- Operational efficiency. Wildcard certificates allow all Policy Service Node (PSN) EAP and web services to share the same certificate. 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 where 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, even though a trusted Certificate Authority has signed the certificate. Using a wildcard certificate, the certificate will be the same across all PSNs, so the user only has to accept the certificate once and successive authentications to different PSNs proceed without error or prompting.
- Simplified supplicant configuration. For example, Microsoft Windows supplicant with PEAP-MSCHAPv2 and server certificate trust enabled 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 related to 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 a unique server certificate per ISE node. But, cost and other operational factors outweigh the security risk.

Security devices such as ASA 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 (CN) of the Certificate Subject, such as the example in Figure 8-3. Cisco ISE release 1.2 supports this type of construction. However, not all endpoint supplicants support the wildcard character in the Certificate Subject.

All Microsoft native supplicants tested (including Windows Mobile) do not support wildcard character in the Certificate Subject.

You can use another supplicant, such as Cisco AnyConnect Network Access Manager (NAM) that might allow the use of wildcard character 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 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 Alterative Name (SAN) field instead. The SAN field maintains an extension designed for checking the domain name (DNS name). See RFCs 6125 and 2128 for more information.

For more information on Microsoft support of wildcard certificates, see:
http://technet.microsoft.com/en-US/cc730460

Creating a Wildcard Certificate

This section describes how to create a wildcard certificate. This procedure would work for most SSL certificate providers.

However, if your SSL certificate provider does not support wildcard values in the SAN field of the certificate, then you must populate the certificate SAN with the FQDN of each ISE node and interface (per the alias specified using the ip host command). This certificate is known as a multi-domain certificate. FQDNs for specific service aliases such as those used for the My Devices and Sponsor portals should also be included in the certificate SAN. Some services such as Local Web Authentication to the

ISE Admin portal, Sponsor portal, and the My Devices portal can use a load balancer. In these cases, the FQDN assigned to the virtual IP address of the load-balanced service should be included in the SAN field of the certificate.

Note It is possible to have separate certificates for HTTPS and EAP authentication. The certificate designated for HTTPS is used to secure inter-node communications and all web portal services including Central Web Authentication, DRW, Posture Discovery and Assessment, Mobile Device Management, Native Supplicant Provisioning, Sponsor, and My Devices portals. The certificate designated for EAP is used to secure all client authentication using EAP protocols including PEAP, EAP-TLS, and EAP-FAST.

For example, if you have an ISE deployment with two PSN nodes (psn1 and psn2 with eth0, eth1, and eth2 interfaces enabled) and you want to create a multi-domain certificate without wildcards, then your values would be:

CN=aaa.company.local (FQDN of an ISE node in the deployment)

SAN=DNS.1=aaa.company.local, DNS.2=psn1.company.local, DNS.3=psn2.company.local, DNS.4=psn1-e1.company.local, DNS.5=psn2-e1.company.local, DNS.6=psn1-e2.company.local, DNS.7=psn2-e2.company.local.

Tip If you are planning to deploy additional Policy Service nodes in the future, then you can add additional DNS name entries in the SAN field so that you can reuse the same certificate at the time of deploying the new nodes.

For cases where an IP address needs to be specified in the SAN field of the certificate (for example, DMZ with a static IP address for URL re-direction), ensure that you specify the IP address of the policy service node as the DNS Name and IP Address in the SAN field of the certificate. For example, CN=psn.ise.local and SAN=DNS.1=psn.ise.local, DNS.2=*.ise.local, DNS.3=10.1.1.20, IP.1=10.1.1.20.

Before You Begin

For Microsoft native supplicants, use the wildcard character in the SAN field of the certificate.

Step 1 Enter a generic hostname for the CN field of the Subject. For example, CN=aaa.ise.local.

Step 2 Enter the same generic hostname and a wildcard notation in the SAN field of the certificate. For example, DNS Name=aaa.ise.local, DNS Name=*.ise.local. See Figure 8-3.

This method is successful with the majority of the tested public Certificate Authorities such as Comodo.com and SSL.com. With these public CAs, you must request a “Unified Communications Certificate (UCC).”

What To Do Next

Import the wildcard certificates in to the Policy Service nodes.

Related Topics

Installing Wildcard Certificates in Cisco ISE, page 8-10

Installing Wildcard Certificates in Cisco ISE

Before You Begin

If you have enabled non-eth0 interfaces, ensure that you map a host alias to that interface using the **ip host** command from the CLI. See Fully Qualified Domain Name in URL Redirection for more information.

To install wildcard certificates, you must perform the following tasks:

Step 1 Create the Certificate Signing Request for Wildcard Certificates. See Creating a Certificate Signing Request for Wildcard Certificates, page 8-10.

Step 2 Export the Certificate Signing Request. See Exporting the Certificate Signing Request, page 8-11.

Step 3 Submit the Certificate Signing Request to a Certificate Authority. See Submitting the CSR to a Certificate Authority, page 8-11.

Step 4 Import the Root Certificates to the Certificate Store. See Importing the Root Certificates to the Certificate Store, page 8-12.

Step 5 Bind the Certificate Signing Request with the new public certificate. See Binding the CSR With the New Public Certificate, page 8-13.

Step 6 Export the CA-Signed Certificate and Private Key. See Exporting the CA-Signed Certificate and Private Key, page 8-13.

Step 7 Import the CA-Signed Certificate and Private Key in to all the Policy Service nodes. See Importing the CA-Signed Certificate to the Policy Service Nodes, page 8-13.

Creating a Certificate Signing Request for Wildcard Certificates

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

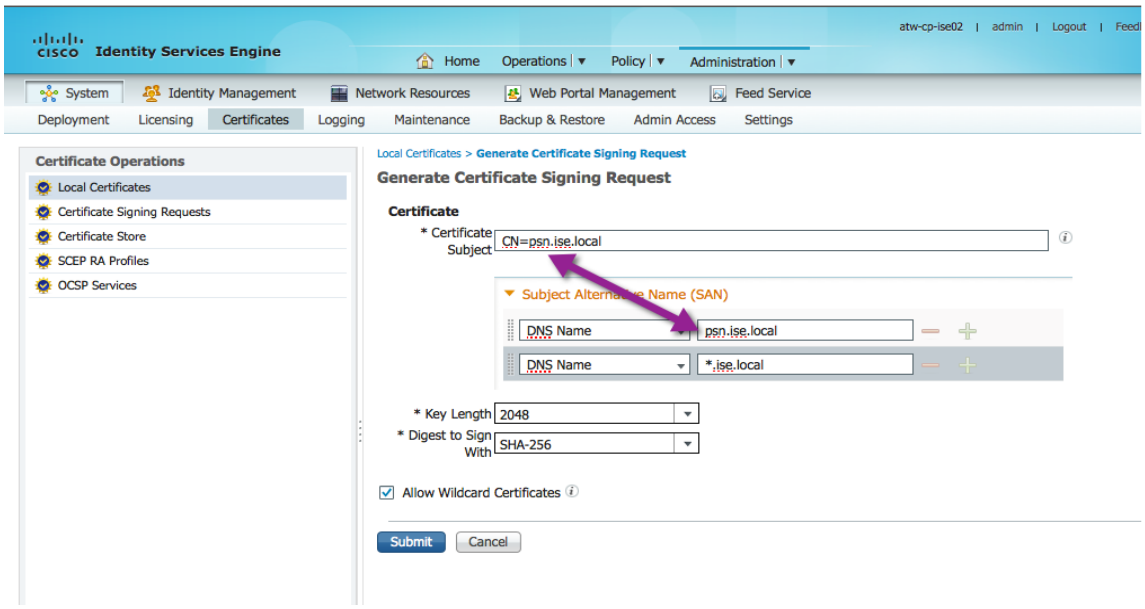
Step 2 Click **Add > Generate Certificate Signing Request**.

Step 3 In the Certificate Subject, enter the generic FQDN of any one of your Policy Service nodes. For example, CN=psn.ise.local.

Step 4 Enter two values for the SAN. One of the values must be same as the CN that you entered for the Certificate Subject. The other value is the wildcard notation. For example, DNS name=psn.ise.local, DNS name=*.ise.local.

Step 5 Check the **Allow Wildcard Certificates** check box.

Figure 8-4 Certificate Signing Request Using a Wildcard Notation



Step 6 Click **Submit**.

Exporting the Certificate Signing Request

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

Step 2 Check the check box next to the CSR that you generated. For example, psn.ise.local.

Step 3 Click **Export**.

Step 4 Save the CSR to your local system.

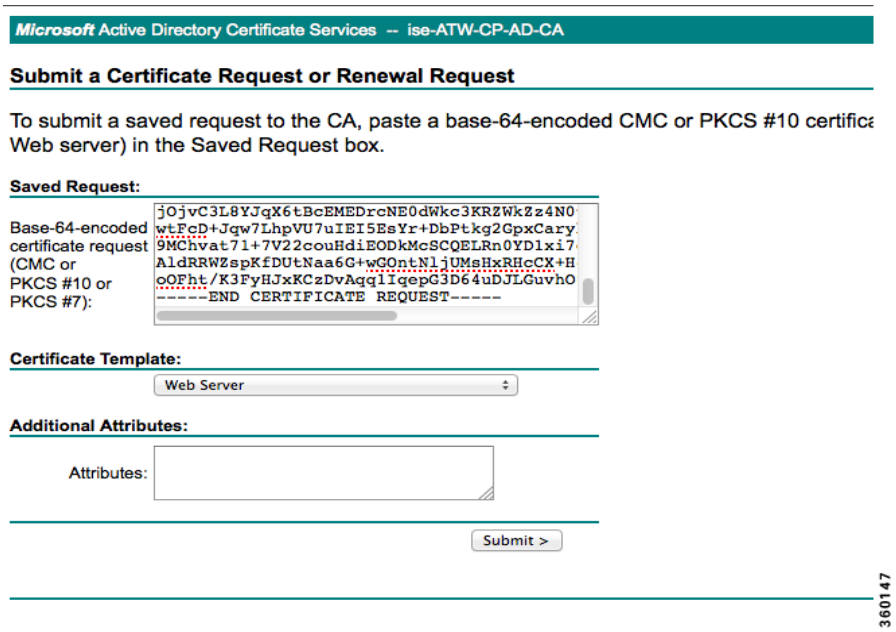
Submitting the CSR to a Certificate Authority

Step 1 Open the CSR in a text editor such as Notepad.

Step 2 Copy all the text from "-----BEGIN CERTIFICATE REQUEST-----" through "-----END CERTIFICATE REQUEST-----."

Step 3 Paste the contents of the CSR in to the certificate request of a chosen CA. See Figure 8-5.

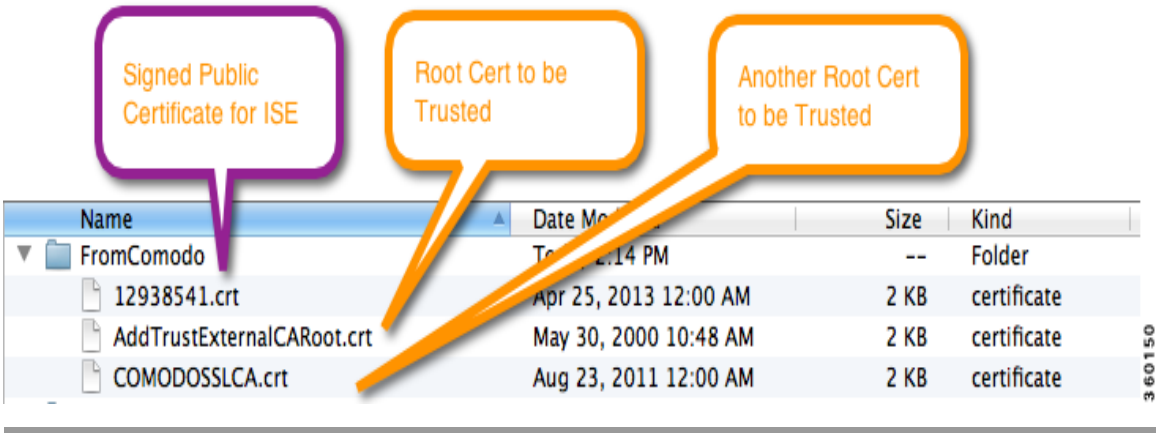
Figure 8-5 CSR Content in a Certificate Request Form - Active Directory CA



Step 4 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 certificate store. See Figure 8-6.

Figure 8-6 Certificates Returned By the CA



Importing the Root Certificates to the Certificate Store

Before You Begin

Before we bind the newly signed certificate to the CSR on Cisco ISE, ensure that the signing root certificates exist in the Cisco ISE Certificate Store.

Step 1 Choose **Administration > Certificates > Certificate Store**.

Step 2 Click **Import**.

Step 3 Choose the root certificates returned by your CA.

Binding the CSR With the New Public Certificate

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

Step 2 Click **Add > Bind CA signed Certificate**.

Step 3 Choose the CA-signed certificate.

Step 4 Check the **Allow Wildcard Certificates** check box.

Step 5 Choose the protocol.

Step 6 Click **Submit**.

Exporting the CA-Signed Certificate and Private Key

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

Step 2 Check the check box next to the CA-signed certificate and click **Export**.

Step 3 Save the file to your local system.

Importing the CA-Signed Certificate to the Policy Service Nodes

Step 1 Choose **Administration > Certificates > Certificate Store**.

Step 2 Choose the CA-signed certificate that you exported.

Step 3 Click **Submit**.

Installing a CA-Signed Certificate in Cisco ISE

The procedure for installing a CA-signed certificate is as follows:

Step 1 In the Cisco ISE administration interface of the node requiring the CA-signed certificate, generate a Certificate Signing Request (CSR).

Step 2 Export the CSR into a file.

Step 3 Provide the CSR file to the Certificate Authority and request the CA to create and sign a certificate using the attributes specified in the CSR. The CA should return the certificate in a file.

Step 4 In the Cisco ISE administration interface of the same node, bind the CA-signed certificate to its private key, which is kept with the CSR on the node. Designate the certificate for HTTPS and/or EAP-TLS use.

Note If you are going to use the CA-signed certificate for HTTPS, the subject Common Name value specified for the CSR must match the fully qualified domain name (FQDN) of the Cisco ISE node, or must match the wildcard domain name specified in the SAN/CN field of the certificate.

Cisco ISE checks for a matching subject name as follows:

1. Cisco ISE looks at the subject alternative name (SAN) extension of the certificate. If the SAN 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 SAN, or if the SAN is missing entirely, then the Common Name (CN) 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 imported to Cisco ISE must be in privacy-enhanced mail (PEM) or distinguished encoding rule (DER) format. Files containing a certificate chain, which is a local certificate along with the sequence of trust certificates that sign it, can be imported, subject to certain restrictions. See Importing Certificate Chains, page 8-28 for more information.

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

- Colored expiration status icons appear in the Local Certificates page.
- Expiration messages appear in the Cisco ISE System Diagnostic report.
- Expiration alarms are generated at 90 days, 60 days, and 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 CA-signed certificate, you must allow sufficient time to acquire replacement certificate from your CA.

You can perform the following tasks from the Cisco ISE administration interface to manage local certificates:

- View a list of the local certificates stored on an Cisco ISE node. The list shows the protocol assignment (HTTPS, EAP-TLS) of each certificate, along with its expiration status.
- Generate a CSR
- Export a CSR
- Bind a CA-signed certificate to its private key
- Export a local certificate and, optionally, its private key
- Import a local certificate and its private key

- Generate a self-signed local certificate
- Edit a local certificate, which includes extending the expiration date if the certificate is self-signed
- Delete a local certificate
- Delete a CSR

This section contains the following topics:

Related Topics

- Wildcard Certificates, page 8-4
- Fully Qualified Domain Name in URL Redirection, page 8-6
- Importing a Local Certificate, page 8-16
- Generating a Certificate Signing Request, page 8-19
- Binding a CA-Signed Certificate, page 8-20

Viewing Local Certificates

The Local Certificate page lists all the local 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 > Local Certificates**.

The Local Certificate page appears and provides the following information for the local certificates:

- Friendly Name—Name of the certificate.
- Protocol—Protocols for which to use this certificate.
- 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 know as the Not Before certificate attribute.
- Expiration Date—Expiration date of the certificate, also known as the Not After certificate attribute.
- Expiration Status—Indicates when the certificate expires. There are five categories along with an associated icon that appear here:
  1. Expiring in more than 90 days (green icon)
  2. Expiring in 90 days or less (blue icon)
  3. Expiring in 60 days or less (yellow icon)
  4. Expiring in 30 days or less (orange icon)

5. Expired (red icon)

Related Topics

- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Wildcard Certificates, page 8-4

Adding a Local Certificate

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

- Importing a Local Certificate, page 8-16
- Generating a Self-Signed Certificate, page 8-18
- Generating a Certificate Signing Request, page 8-19 and Binding a CA-Signed Certificate, page 8-20

If you are planning to import a wildcard certificate, ensure that you have read the following sections:

- Wildcard Certificates, page 8-4
- Creating a Wildcard Certificate, page 8-8
- Installing Wildcard Certificates in Cisco ISE, page 8-10

Note If you are using Firefox and Internet Explorer 8 browsers and you change the HTTPS local certificate on a node, existing browser sessions connected to that node do not automatically switch over to the new certificate. You must restart your browser to see the new certificate.

Importing a Local Certificate

You can add a new local certificate by importing a local certificate.

Before You Begin

Ensure that you have the local certificate and the private key file on the system that is running the client browser.

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

If the local certificate that you import contains the basic constraints extension with the CA flag set to true, ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set.

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

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

Step 2 Choose **Add > Import Local Server Certificate**.

Step 3 Click **Browse** to choose the certificate file and the private key from the system that is running your client browser.

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

Step 4 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.

Step 5 Check the **Enable Validation of Certificate Extensions** check box if you want Cisco ISE to validate certificate extensions.

If you check the **Enable Validation of Certificate Extensions** check box and the certificate that you are importing 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.

Step 6 Check the **Allow Wildcard Certificates** check box if you want to import a wildcard certificate (a certificate that contains an asterisk (*) in any Common Name in the Subject and/or the DNS name in the Subject Alternative Name.

Step 7 In the Protocol group box:

- Check the **EAP** check box to use this certificate for EAP protocols to identify the Cisco ISE node.
- Check the **HTTPS** check box to use this certificate to authenticate the web server.

  If you check the Management Interface check box, ensure that the Common Name value in the Certificate Subject matches the fully qualified domain name (FQDN) of the node or a wildcard notation if a wildcard certificate is used. Otherwise, the import process will fail.

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

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

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

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

To restart the secondary nodes from the CLI, enter the following commands in the given order:

a. **application stop ise**

b. **application start ise**

Refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.2* for more information on these commands.

Related Topics

- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Wildcard Certificates, page 8-4
- Creating a Wildcard Certificate, page 8-8
- Installing Wildcard Certificates in Cisco ISE, page 8-10

Generating a Self-Signed Certificate

You can 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 are planning to deploy Cisco ISE in a production environment, be sure to use CA-signed certificates whenever possible to ensure more uniform acceptance around a production network.

Before You Begin

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

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

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

Step 2 Choose **Add > Generate Self Signed Certificate**.

Step 3 Enter the following information in the Generate Self Signed Certificate page:

- **Certificate Subject**—A distinguished name (DN) identifying the entity that is associated with the certificate. The DN must include a Common Name (CN) value.
- **Subject Alternative Name**—A DNS name or IP Address that is associated with the certificate.
- Required **Key Length**—Valid values are 512, 1024, 2048, and 4096. If you are deploying Cisco ISE as a FIPS-compliant policy management-engine, you must specify a 2048-bit or larger key length.
- **Digest to Sign With**—You can choose to encrypt and decrypt certificates using either SHA-1 or SHA-256.
- Certificate **Expiration TTL**. You can specify an expiration time period in days, weeks, months, or years.
- If you would like to specify a **Friendly Name** for the certificate, enter it in the field below the private key password. If you do not specify a name, Cisco ISE automatically creates a name in the format <*common name*>#<*issuer*>#<*nnnnn*> where <*nnnnn*> is a unique five-digit number.

Step 4 Check the **Allow Wildcard Certificates** check box if you want to generate a self-signed wildcard certificate (a certificate that contains an asterisk (*) in any Common Name in the Subject and/or the DNS name in the Subject Alternative Name. For example, DNS name assigned to the SAN can be *.amer.cisco.com.

Step 5 In the Protocol group box:

- Check the **EAP** check box to use this certificate for EAP protocols that use SSL/TLS tunneling.
- Check the **HTTPS** check box to use this certificate to authenticate the Cisco ISE portals.

  If you check the Management Interface check box, ensure that the Common Name value in the Certificate Subject matches the fully qualified domain name (FQDN) of the node. Otherwise, the self-signed certificate will not be generated.

  If the HTTPS check box is checked, then the Primary Administration node in a deployment will be restarted.

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

Step 7 Click **Submit** to generate the certificate.

Note If you are using a self-signed certificate and you must change the hostname of your Cisco ISE node, you must log in to the Admin 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 will continue to use the self-signed certificate with the old hostname.

Related Topics

- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Wildcard Certificates, page 8-4
- Installing Wildcard Certificates in Cisco ISE, page 8-10

Generating a Certificate Signing Request

You can add a new local certificate by generating a certificate signing request and then binding a CA-signed certificate.

Before You Begin

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

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

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

Step 2 Choose **Add > Generate Certificate Signing Request**.

Step 3 Enter the certificate subject and the required key length. The certificate subject is a distinguished name (DN) identifying the entity that is associated with the certificate. The DN must include a common name value. Elements of the distinguished name are:

- C = Country
- ST = Test state or province
- L = Test locality (City)
- O = Organization name
- OU = Organizational unit name
- CN = Common name
- E = E-mail address

For example, the Certificate Subject in a CSR can take the following values: “CN=Host-ISE.cisco.com, OU=Cisco, O=security, C=US, ST=NC, L=RTP, e=test@test.com” or “CN=aaa.amer.cisco.com, DNS name in SAN=*.amer.cisco.com, OU=Cisco, O=security, C=US, ST=NC, L=RTP, e=abc@xyz.com.”

Note When populating the Certificate Subject field, do not encapsulate the string in quotation marks.

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

Step 4 **Subject Alternative Name**—A DNS name or IP Address that is associated with the certificate.

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

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

Step 6 Check the **Allow Wildcard Certificates** check box if the Certificate Subject contains a CN or SAN with a wildcard FQDN.

Step 7 Click **Submit** to generate a CSR.

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

Related Topics

- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Wildcard Certificates, page 8-4
- Creating a Certificate Signing Request for Wildcard Certificates, page 8-10

Binding a CA-Signed Certificate

After a Certificate Signing Request is signed by a Certificate Authority and returned to you, you must bind the CA-signed certificate with its private key to complete the process of adding a local certificate in 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** > **Local Certificates**.

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

Step 2 Choose **Add > Bind CA Certificate**.

Step 3 Click **Browse** to choose the CA-signed certificate and choose the appropriate CA-signed certificate.

Step 4 Specify 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.

Step 5 Check the **Enable Validation of Certificate Extensions** check box if you want Cisco ISE to validate certificate extensions.

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

Step 6 Check the **Allow Wildcard Certificates** check box to bind a certificate that contains the wildcard character, asterisk (*) in any CN in the Subject or DNS in the Subject Alternative Name.

Step 7 In the Protocol group box:

- Check the **EAP** check box to use this certificate for EAP protocols that use SSL/TLS tunneling.
- Check the **HTTPS** check box to use this certificate to authenticate the Cisco ISE web portal.

  If you check the Management Interface check box, ensure that the Common Name value in the Certificate Subject matches the fully qualified domain name (FQDN) of the node or a wildcard notation if a wildcard certificate is used. Otherwise, the bind operation will fail.

  If the HTTPS check box is checked, then the Primary Administration node in a deployment will be restarted.

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

Step 9 Click **Submit** to bind the CA-signed certificate.

Related Topics

- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Wildcard Certificates, page 8-4
- Installing Wildcard Certificates in Cisco ISE, page 8-10

Editing a Local Certificate

You can use this page to edit local certificates.

Before You Begin

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

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

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

Step 2 Check the check box next to the certificate that you want to edit, and click **Edit**.

Step 3 You can edit the following:

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

Step 4 Enter an optional friendly name and description to identify this certificate.

Step 5 In the Protocol group box:

- Check the **EAP** check box to use this certificate for EAP protocols that use SSL/TLS tunneling.
- Check the **HTTPS** check box to use this certificate to authenticate the Cisco ISE web portal.

If the HTTPS check box is checked, then the Primary Administration node in a deployment will be restarted.

Note If you check the Management Interface check box, ensure that the Common Name value in the Certificate Subject matches the fully qualified domain name (FQDN) of the node or a wildcard notation if a wildcard certificate is used. If the Common Name value is blank, the edit operation will fail.
For example, if local_certificate_1 is currently designated for EAP and you check the EAP check box while editing local_certificate_2, then after you save the changes to local_certificate_2, local_certificate_1 will no longer be associated with EAP.

Step 6 Check the **Renew Self Signed Certificate** check box if you are editing a self-signed certificate and want to extend the Expiration Date.

Step 7 Enter the Expiration TTL (Time to Live) in days, weeks, months, or years.

Step 8 Click **Save** to save your changes.

Related Topics

- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Wildcard Certificates, page 8-4
- Creating a Wildcard Certificate, page 8-8
- Installing Wildcard Certificates in Cisco ISE, page 8-10

Exporting a Local Certificate

You can export a selected local 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 Choose **Administration > System > Certificates > Local Certificates**.

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

Step 2 Check the check box next to the certificate that you want to export and then 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 associated with a certificate because its value may be exposed. If you must export a private key, specify an encryption password for the private key. You will need to specify this password while importing this certificate into another Cisco ISE server to decrypt the private key.

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

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

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

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

Related Topics

- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Importing a Local Certificate, page 8-16

Certificate Signing Requests

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

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

Related Topic

Exporting Certificate Signing Requests, page 8-23

Exporting Certificate Signing Requests

You can use this page to export certificate signing requests.

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**.

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

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

Step 3 Click **OK** to save the file to the file system that is running the client browser.

Related Topics

- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Wildcard Certificates, page 8-4

Certificate Store

The Cisco ISE Certificate Store contains X.509 certificates that are used for trust and for Simple Certificate Enrollment Protocol (SCEP). The certificates in the Certificate Store are managed on the primary administration node, and are replicated to every node in the Cisco ISE deployment.

Cisco ISE supports wildcard certificates.

Cisco ISE uses the Certificate Store certificates for the following purposes:

- To verify client certificates used for authentication by endpoints, and by Cisco ISE administrators accessing the Admin Portal using certificate-based administrator authentication.
- To enable secure communication between Cisco ISE nodes in a deployment. The Certificate Store must contain the chain of CA certificates needed to establish trust with the local HTTPS server certificate on each node in a deployment.
  - If a self-signed certificate is used for the server certificate, the self-signed certificate from each node must be placed in the Certificate Store of the primary Administration node.
  - If a CA-signed certificate is used for the server certificate, the CA root certificate, as well as any intermediate certificates in the trust chain, must be placed in the Certificate Store of the primary Administration node.
- 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.
- For distribution to mobile devices preparing to register in the network using the My Devices portal. Cisco ISE implements the SCEP on Policy Service Nodes (PSN) to support mobile 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; it receives and validates the request from the registering device, and then forwards the request to a CA, which actually 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 Certificate Store:

  a. A CA certificate (a self-signed certificate)
  b. 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 Certificate Store, they are replicated to all PSN nodes for use by the RA on those nodes.

Note X.509 certificates imported to Cisco ISE must be in Privacy-Enhanced Mail (PEM) or Distinguished Encoding Rule (DER) format. Files containing a certificate chain, that is, a local certificate along with the sequence of trust certificates that sign it, can be imported, subject to certain restrictions.

Note Performance Issues:
The default configuration of the maximum processes for SCEP module on the Windows CA server is set as 1. Increasing the value of maximum processes (say to 20) would improve the device registration performance. The performance could further be improved with a faster disk, for example an SSD.

Related Topics

- Configuring a Password Policy for Administrator Accounts, page 6-14
- Adding LDAP Identity Sources, page 14-24
- Simple Certificate Enrollment Protocol Profiles, page 8-30
- Importing Certificate Chains, page 8-28
- Expiration of X.509 Certificates, page 8-25
- CA Certificate Naming Constraint, page 8-25
- Viewing Certificate Store Certificates, page 8-27
- Changing the Status of a Certificate in Certificate Store, page 8-27
- Adding a Certificate to Certificate Store, page 8-27
- Editing a Certificate Store Certificate, page 8-28
- Exporting a Certificate from the Certificate Store, page 8-28

Expiration of X.509 Certificates

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

- Colored expiration status icons appear in the Certificate Store page.
- Expiration messages appear in the Cisco ISE System Diagnostic report.
- Expiration alarms are generated at 90 days, 60 days, and every day in the final 30 days before expiration.

The Certificate Store is prepopulated with two Cisco CA certificates: a Manufacturing certificate and a Root certificate. The Root certificate signs the Manufacturing certificate. These certificates are disabled by default. If you have Cisco IP phones as endpoints in your deployment, you should enable these two certificates so the Cisco-signed client certificates for the phones can be authenticated.

This section contains the following topics:

- Viewing Certificate Store Certificates, page 8-27
- Adding a Certificate to Certificate Store, page 8-27
- Editing a Certificate Store Certificate, page 8-28
- Exporting a Certificate from the Certificate Store, page 8-28
- Importing Certificate Chains, page 8-28
- Installation of CA Certificates for Cisco ISE Inter-node Communication, page 8-29

CA Certificate Naming Constraint

A CA 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 specified in a root certificate.

The following name constraints are supported:

- Directory name

  The Directory name constraint should be a prefix of the directory name in subject/SAN. 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
- E-mail
- URI (The URI constraint must start with a URI prefix such as http://, https://, ftp://, or ldap://).

The following name constraints are not supported:

- IP address
- Othername

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

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

```
X509v3 Name Constraints: critical
                Permitted:
                  othername:<unsupported>
                  email:.stihl.at
                  email:.stihl.be
                  email:.stihl.bg
                  email:.stihl.by
                  DNS:.dir
                  DirName: DC = dir, DC = emea
                  DirName: C = AT, ST = EMEA, L = AT, O = STIHL Group, OU = Domestic
                  DirName: C = BG, ST = EMEA, L = BG, O = STIHL Group, OU = Domestic
                  DirName: C = BE, ST = EMEA, L = BN, O = STIHL Group, OU = Domestic
                  DirName: C = CH, ST = EMEA, L = CH, O = STIHL 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=flovison
```

Viewing Certificate Store Certificates

The Certificate Store page lists all the CA certificates that have been added to Cisco ISE. To view the CA certificates, you must be a Super Admin or System Admin.

To view all the certificates, choose **Administration > System > Certificates > Certificate Store**. The Certificate Store page appears, listing all the CA certificates.

Related Topics

- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Certificate Store Page, page A-11

Changing the Status of a Certificate in Certificate 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 Certificate Store, it is automatically enabled.

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

Step 2 Check the check box next to the certificate you want to enable or disable, and click **Change Status**.

Adding a Certificate to Certificate Store

The Certificate Store page 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.
- Ensure that the certificate store certificate resides on the file system of the computer where your browser is running. The certificate must be in PEM or DER format.

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

Step 2 Click **Import**.

Step 3 Configure the field values as necessary.

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

Related Topics

- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Certificate Store Import Settings, page A-11

Editing a Certificate Store Certificate

After you add a certificate to the Certificate 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 Store**.

Step 2 Check the check box next to the certificate that you want to edit, and click **Edit**.

Step 3 Modify the editable fields as required.

Step 4 Click **Save** to save the changes you have made to the certificate store.

Related Topics

- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Certificate Store Edit Settings, page A-12

Exporting a Certificate from the Certificate Store

Before You Begin

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

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

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 Save the privacy-enhanced mail file to the file system that is running your client browser.

Related Topics

Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions

Importing Certificate Chains

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 Privacy-Enhanced Mail (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 being 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:

Step 1 Import the certificate chain file into the Certificate Store using the Adding a Certificate to Certificate Store operation. This operation will import all certificates from the file except the last one into the Certificate Store. You can perform this step only on the primary Administration node.

Step 2 Import the certificate chain file using the Binding a CA-Signed Certificate operation. This operation will import the last certificate from the file as a local certificate.

Installation of CA Certificates for Cisco ISE Inter-node Communication

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

- If the secondary node is using a CA-signed certificate for HTTPS communication, you must import the CA-signed certificate of the secondary node into the CTL of the primary node.
- If the secondary node is using a self-signed certificate for HTTPS communication, you can import the self-signed certificate of the secondary node into the CTL of the primary node.

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

Related Topics

- Importing a CA-Signed Certificate from a Secondary Node into the Primary Node's CTL, page 8-29
- Importing a Self-Signed Certificate from a Secondary Node into the CTL of the Primary Node, page 8-30

Importing a CA-Signed Certificate from a Secondary Node into the Primary Node's CTL

Before You Begin

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

Step 1 Log in to the Admin portal of the node that you are going to register as your secondary node, and export the CA-signed certificate that is used for HTTPS communication to the file system running your client browser.

Step 2 In the Export dialog box, click the **Export Certificate Only** radio button.

Step 3 Log in to the Admin portal of your primary node, and import the CA-signed certificate of the secondary node into the CTL of the primary node.

Related Topics

- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Exporting a Certificate from the Certificate Store, page 8-28
- Adding a Certificate to Certificate Store, page 8-27

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

Before You Begin

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

Step 1 Log in to the Admin portal of the node that you are going to register as your secondary node and export the self-signed certificate that is used for HTTPS communication to the file system running your client browser.

Step 2 In the Export dialog box, click the **Export Certificate Only** radio button.

Step 3 Log in to the Admin portal of your primary node, and import the self-signed certificate of the secondary node into the CTL of the primary node.

Related Topics

- Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions
- Exporting a Local Certificate, page 8-22
- Adding a Certificate to Certificate Store, page 8-27

Simple Certificate Enrollment Protocol Profiles

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

For details on how to set up your Microsoft SCEP server to interoperate with Cisco ISE, see

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf.

Related Topics

- Adding Simple Certificate Enrollment Protocol Profiles, page 8-30
- OCSP Services, page 8-31

Adding Simple Certificate Enrollment Protocol Profiles

Step 1 Choose **Administration > System > Certificates > SCEP CA Profile**.

Step 2 Specify a **Name** for the profile to distinguish it from other SCEP CS profile names.

Step 3 Enter an optional **Description** of the profile.

Step 4 Specify the **URL** of the SCEP CA server in question, where Cisco ISE can direct SCEP CA requests when users access the network from their mobile devices.

You can optionally use the adjacent **Test Connectivity** button to verify that Cisco ISE is able to reach the server at the URL that you specify, before clicking the Submit button to end the session. (Either way, Cisco ISE will test the URL before allowing you to save the profile.)

Step 5 Click **Submit**.

For Reference:

Once users' devices receive their validated certificate, they reside on the device as described in Table 8-1.

Table 8-1 Device Certificate Location

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

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. See Editing a Certificate Store Certificate, page 8-28.

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.

This section contains the following topics:

OCSP Certificate Status Values

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

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

Related Topics

OCSP Statistics Counters, page 8-34

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 reply 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:

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

3. Failed OCSP reports

Adding OCSP Services

You can use the add OCSP page to add new OCSP services to Cisco ISE.

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

Step 2 Click **Add**

Step 3 Provide a name and description for the OCSP service.

Step 4 Check the **Enable Secondary Server** check box if you want to enable high availability.

Step 5 Select one of the following options for high availability:

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

Step 6 Provide the URLs or IP addresses of the primary and secondary OCSP servers.

Step 7 Check or uncheck the following options:

- Nonce—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.
- Validate Response Signature—The OCSP responder signs the response with one of the following signatures:
  - The CA certificate
  - A certificate different from the CA certificate

  In order for Cisco ISE to validate the response signature, the OCSP responder needs to send the response along with the certificate, otherwise the response verification fails, and the status of the certificate cannot be relied on. According to the RFC, OCSP can sign the response using different certificates. This is true as long as OCSP sends the certificate that signed the response for Cisco ISE to validate it. If OCSP signs the response with a different certificate that is not configured in Cisco ISE, the response verification will fail.

Step 8 Provide the number of minutes for the Cache Entry Time to Live.

Each response from the OCSP server holds a nextUpdate value. This value shows when the status of 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:

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

Step 9 Click **Clear Cache** to clear entries of all the certificate authorities that are connected to the OCSP service.

In a deployment, Clear Cache interacts with all the nodes and performs the operation. This mechanism updates every node in the deployment.

OCSP Statistics Counters

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

Table 8-2 lists the OCSP syslog messages and their descriptions.

Table 8-2 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

Table 8-2 OCSP Syslog Messages

Message	Description
OCSPCertsCleanedUpCount	How many cached entries were cleaned since the t interval
NumOfCertsFoundInCache	Number of the fulfilled requests from the cache
OCSPCacheCertsCount	Number of certificates that were found in the OCSP cache

Monitoring OCSP

You can view the OCSP services data in the form of an OCSP Monitoring Report. For more information on Cisco ISE reports, see Chapter 26, "Reporting."