Configuring Certificate Enrollment for a PKI

This module describes the different methods available for certificate enrollment and how to set up each method for a participating PKI peer. Certificate enrollment, which is the process of obtaining a certificate from a certification authority (CA), occurs between the end host that requests the certificate and the CA. Each peer that participates in the public key infrastructure (PKI) must enroll with a CA.

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

- Finding Feature Information, on page 1
- Prerequisites for PKI Certificate Enrollment, on page 1
- Information About Certificate Enrollment for a PKI, on page 2
- How to Configure Certificate Enrollment for a PKI, on page 6
- Configuration Examples for PKI Certificate Enrollment Requests, on page 29
- Additional References, on page 38
- Feature Information for PKI Certificate Enrollment, on page 39

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for PKI Certificate Enrollment

Before configuring peers for certificate enrollment, you should have the following items:

- A generated Rivest, Shamir, and Adelman (RSA) key pair to enroll and a PKI in which to enroll.
- An authenticated CA.
Familiarity with the module “Cisco IOS PKI Overview: Understanding and Planning a PKI.”

Enable NTP on the device so that the PKI services such as auto enrollment and certificate rollover may function correctly.

As of Cisco IOS Release 12.3(7)T, all commands that begin with “crypto ca” have been changed to begin with “crypto pki.” Although the router will still accept crypto ca commands, all output will be displayed crypto pki.

Information About Certificate Enrollment for a PKI

What Are CAs

A CA is an entity that issues digital certificates that other parties can use. It is an example of a trusted third party. CAs are characteristic of many PKI schemes.

A CA manages certificate requests and issues certificates to participating network devices. These services provide centralized key management for the participating devices to validate identities and to create digital certificates. Before any PKI operations can begin, the CA generates its own public key pair and creates a self-signed CA certificate; thereafter, the CA can sign certificate requests and begin peer enrollment for the PKI.

You can use the Cisco IOS certificate server or a CA provided by a third-party CA vendor.

Framework for Multiple CAs

A PKI can be set up in a hierarchical framework to support multiple CAs. At the top of the hierarchy is a root CA, which holds a self-signed certificate. The trust within the entire hierarchy is derived from the RSA key pair of the root CA. The subordinate CAs within the hierarchy can be enrolled with either the root CA or with another subordinate CA. Multiple tiers of CAs are configured by either the root CA or with another subordinate CA. Within a hierarchical PKI, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA.

When to Use Multiple CAs

Multiple CAs provide users with added flexibility and reliability. For example, subordinate CAs can be placed in branch offices while the root CA is at the office headquarters. Also, different granting policies can be implemented per CA, so you can set up one CA to automatically grant certificate requests while another CA within the hierarchy requires each certificate request to be manually granted.

Scenarios in which at least a two-tier CA is recommended are as follows:

• Large and very active networks in which a large number of certificates are revoked and reissued. A multiple tier CA helps to control the size of the certificate revocation lists (CRLs).

• When online enrollment protocols are used, the root CA can be kept offline except to issue subordinate CA certificates. This scenario provides added security for the root CA.
Authentication of the CA

The certificate of the CA must be authenticated before the device will be issued its own certificate and before certificate enrollment can occur. Authentication of the CA typically occurs only when you initially configure PKI support at your router. To authenticate the CA, issue the `crypto pki authenticate` command, which authenticates the CA to your router by obtaining the self-signed certificate of the CA that contains the public key of the CA.

Note PKI does not support certificate with lifetime validity greater than the year 2099. So, It is recommended to choose a life time validity fewer than the value 2099.

Authentication via the fingerprint Command

Cisco IOS Release 12.3(12) and later releases allow you to issue the `fingerprint` command to preenter a fingerprint that can be matched against the fingerprint of a CA certificate during authentication.

If a fingerprint is not preentered for a trustpoint, and if the authentication request is interactive, you must verify the fingerprint that is displayed during authentication of the CA certificate. If the authentication request is noninteractive, the certificate will be rejected without a preentered fingerprint.

Note If the authentication request is made using the command-line interface (CLI), the request is an interactive request. If the authentication request is made using HTTP or another management tool, the request is a noninteractive request.

Note The SCEP will proceed for authentication even if GetCACaps returns any http failure message. Before enrollment, SCEP will initiate GetCACaps fetch. Enrollment will become successful only if GetCACaps is successful.

Supported Certificate Enrollment Methods

Cisco IOS software supports the following methods to obtain a certificate from a CA:

• Simple Certificate Enrollment Protocol (SCEP)--A Cisco-developed enrollment protocol that uses HTTP to communicate with the CA or registration authority (RA). SCEP is the most commonly used method for sending and receiving requests and certificates.

Note To take advantage of automated certificate and key rollover functionality, you must be running a CA that supports rollover and SCEP must be used as your client enrollment method. If you are running a Cisco IOS CA, you must be running Cisco IOS Release 12.4(2)T or a later release for rollover support.

• PKCS12--The router imports certificates in PKCS12 format from an external server.
• IOS File System (IFS)--The router uses any file system that is supported by Cisco IOS software (such as TFTP, FTP, flash, and NVRAM) to send a certificate request and to receive the issued certificate. Users may enable IFS certificate enrollment when their CA does not support SCEP.

Prior to Cisco IOS Release 12.3(4)T, only the TFTP file system was supported within IFS.

Note

• Manual cut-and-paste--The router displays the certificate request on the console terminal, allowing the user to enter the issued certificate on the console terminal. A user may manually cut-and-paste certificate requests and certificates when there is no network connection between the router and CA.

• Enrollment profiles--Enrollment profiles are primarily used for EST or terminal based enrollment. In case that the CA server does not support SCEP, the recommended methods for enrollment are EST based enrollment or terminal based enrollment.

• Self-signed certificate enrollment for a trustpoint--The secure HTTP (HTTPS) server generates a self-signed certificate that is to be used during the secure socket layer (SSL) handshake, establishing a secure connection between the HTTPS server and the client. The self-signed certificate is then saved in the router’s startup configuration (NVRAM). The saved, self-signed certificate can then be used for future SSL handshakes, eliminating the user intervention that was necessary to accept the certificate every time the router reloaded.

Note

To take advantage of autoenrollment and autoreenrollment, do not use either TFTP or manual cut-and-paste enrollment as your enrollment method. Both TFTP and manual cut-and-paste enrollment methods are manual enrollment processes, requiring user input.

Cisco IOS Suite-B Support for Certificate Enrollment for a PKI

Suite-B requirements comprise of four user interface suites of cryptographic algorithms for use with IKE and IPSec that are described in RFC 4869. Each suite consists of an encryption algorithm, a digital signature algorithm, a key agreement algorithm, and a hash or message digest algorithm.

Suite-B adds the following support for the certificate enrollment for a PKI:

• Elliptic Curve Digital Signature Algorithm (ECDSA) (256-bit and 384-bit curves) is used for the signature operation within X.509 certificates.

• PKI support for validation of for X.509 certificates using ECDSA signatures.

• PKI support for generating certificate requests using ECDSA signatures and for importing the issued certificates into IOS.

See the Configuring Security for VPNs with IPsec feature module for more detailed information about Cisco IOS Suite-B support.

Registration Authorities

A Cisco IOS certificate server can be configured to run in RA mode. An RA offloads authentication and authorization responsibilities from a CA. When the RA receives a SCEP or manual enrollment request, the
administrator can either reject or grant it on the basis of local policy. If the request is granted, it will be forwarded to the issuing CA, and the CA can be configured to automatically generate the certificate and return it to the RA. The client can later retrieve the granted certificate from the RA.

**Automatic Certificate Enrollment**

Automatic certificate enrollment allows the CA client to automatically request a certificate from its CA server. This automatic router request eliminates the need for operator intervention when the enrollment request is sent to the CA server. Automatic enrollment is performed on startup for any trustpoint CA that is configured and that does not have a valid client certificate. When the certificate expires, a new certificate is automatically requested.

---

**Note**

When automatic enrollment is configured, clients automatically request client certificates. The CA server performs its own authorization checks; if these checks include a policy to automatically issue certificates, all clients will automatically receive certificates, which is not very secure. Thus, automatic certificate enrollment should be combined with additional authentication and authorization mechanisms (such as Secure Device Provisioning (SDP), leveraging existing certificates, and one-time passwords).

---

**Automated Client Certificate and Key Rollover**

By default, the automatic certificate enrollment function requests a new client certificate and keys from the CS before the client’s current certificate expires. Certificate and key rollover allows the certificate renewal rollover request to be made before the certificate expires by retaining the current key and certificate until the new, or rollover, certificate is available. After a specified amount of time, the rollover certificate and keys will become the active certificate and keys. The expired certificate and keys are immediately deleted upon rollover and removed from the certificate chain and CRL.

The setup for automatic rollover is twofold: CA clients must be automatically enrolled and the client’s CAs must be automatically enrolled and have the **auto-rollover** command enabled. For more information on configuring your CA servers for automatic certificate rollover see the section “Automatic CA Certificate and Key Rollover” in the chapter “Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” of the *Public Key Infrastructure Configuration Guide*.

An optional renewal percentage parameter can be used with the **auto-enroll** command to allow a new certificate to be requested when a specified percentage of the lifetime of the certificate has passed. For example, if the renewal percentage is configured as 90 and the certificate has a lifetime of one year, a new certificate is requested 36.5 days before the old certificate expires. In order for automatic rollover to occur, the renewal percentage must be less than 100. The specified percent value must not be less than 10. If a client certificate is issued for less than the configured validity period due to the impending expiration of the CA certificate, the rollover certificate will be issued for the balance of that period. A minimum of 10 percent of the configured validity period, with an absolute minimum of 3 minutes, is required to allow rollover enough time to function.

---

**Tip**

If CA autoenrollment is not enabled, you may manually initiate rollover on an existing client with the **crypto pki enroll** command if the expiration time of the current client certificate is equal to or greater than the expiration time of the corresponding CA certificate. The client will initiate the rollover process, which occurs only if the server is configured for automated rollover and has an available rollover server certificate.
A key pair is also sent if configured by the **auto-enroll re-generate** command and keyword. It is recommended that a new key pair be issued for security reasons.

### Certificate Enrollment Profiles

Certificate enrollment profiles allow users to specify certificate authentication, enrollment, and reenrollment parameters when prompted. The values for these parameters are referenced by two templates that make up the profile. One template contains parameters for the HTTP request that is sent to the CA server to obtain the certificate of the CA (also known as certificate authentication); the other template contains parameters for the HTTP request that is sent to the CA for certificate enrollment.

Configuring two templates enables users to specify different URLs or methods for certificate authentication and enrollment; for example, authentication (getting the certificate of the CA) can be performed via TFTP (using the **authentication url** command) and enrollment can be performed manually (using the **enrollment terminal** command).

Prior to Cisco IOS Release 12.3(11)T, certificate requests could be sent only in a PKCS10 format; however, an additional parameter was added to the profile, allowing users to specify the PKCS7 format for certificate renewal requests.

A single enrollment profile can have up to three separate sections for each task--certificate authentication, enrollment, and reenrollment.

### How to Configure Certificate Enrollment for a PKI

This section contains the following enrollment option procedures. If you configure enrollment or autoenrollment (the first task), you cannot configure manual certificate enrollment. Also, if you configure TFTP or manual cut-and-paste certificate enrollment, you cannot configure autoenrollment, autoreenrollment, an enrollment profile, nor can you utilize the automated CA certificate rollover capability.

### Configuring Certificate Enrollment or Autoenrollment

Perform this task to configure certificate enrollment or autoenrollment for clients participating in your PKI.

**Before you begin**

Before configuring automatic certificate enrollment requests, you should ensure that all necessary enrollment information is configured.

**Prerequisites for Enabling Automated Client Certificate and Key Rollover**

CA client support for certificate rollover is automatically enabled when using autoenrollment. For automatic CA certificate rollover to run successfully, the following prerequisites are applicable:

- Your network devices must support shadow PKI.
• Your clients must be running Cisco IOS Release 12.4(2)T or a later release.

• The client’s CS must support automatic rollover. See the section “Automatic CA Certificate and Key Rollover” in the chapter “Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” of the Public Key Infrastructure Configuration Guide for more information on CA server automatic rollover configuration.

Prerequisites for Specifying Autoenrollment Initial Key Generation Location

To specify the location of the autoenrollment initial key generation, you must be running Cisco IOS Release 12.4(11)T or a later release.

RSA Key Pair Restriction for Autoenrollment

Trustpoints configured to generate a new key pair using the regenerate command or the regenerate keyword of the auto-enroll command must not share key pairs with other trustpoints. To give each trustpoint its own key pair, use the rsakeypair command in ca-trustpoint configuration mode. Sharing key pairs among regenerating trustpoints is not supported and will cause loss of service on some of the trustpoints because of key and certificate mismatches.

Restrictions for Automated Client Certificate and Key Rollover

In order for clients to run automatic CA certificate rollover successfully, the following restrictions are applicable:

• SCEP must be used to support rollover. Any device that enrolls with the PKI using an alternative to SCEP as the certificate management protocol or mechanism (such as enrollment profiles, manual enrollment, or TFTP enrollment) will not be able to take advantage of the rollover functionality provided by SCEP.

• If the configuration cannot be saved to the startup configuration after a shadow certificate is generated, rollover will not occur.

Note

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

SUMMARY STEPS

1. enable
2. configure terminal
3. crypto pki trustpoint name
4. enrollment [mode | retry period minutes | retry count number] url url [pem]
5. eckeypair label
6. subject-name [x.500-name]
7. vrf vrf-name
8. ip-address {ip-address | interface | none}
9. serial-number [none]
10. auto-enroll [percent] [regenerate]
11. usage method1 [method2 [method3]]
12. password string
13. rsakeypair key-label key-size encryption-key-size ]
14. fingerprint <ca-fingerprint>
15. on <devicename>
16. exit
17. crypto pki authenticate <name>
18. exit
19. copy system:running-config nvram:startup-config
20. show crypto pki certificates

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto pki trustpoint &lt;name&gt;</td>
<td>Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# crypto pki trustpoint mytp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> enrollment [mode</td>
<td>retry period minutes</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# enrollment url <a href="http://cat.example.com">http://cat.example.com</a></td>
<td></td>
</tr>
</tbody>
</table>

- **mode** -- Specifies RA mode if your CA system provides an RA.
- **retry period minutes** -- Specifies the wait period between certificate request retries. The default is 1 minute between retries.
- **retry count number** -- Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. (Specify from 1 to 100 retries.)
- **url** -- URL of the file system where your router should send certificate requests. An IPv6 address can be added in the URL enclosed in brackets. For example: http://[2001:DB8:1::1]:80.
- **pem** -- Adds privacy-enhanced mail (PEM) boundaries to the certificate request.
## Configuring Certificate Enrollment for a PKI

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>An enrollment method other than TFTP or manual cut-and-paste must be configured to support autoenrollment.</td>
</tr>
</tbody>
</table>

**Step 5**

**eckeypair label**

**Example:**

```
Router(ca-trustpoint)# eckeypair Router_1_Key
```

(Optional) Configures the trustpoint to use an Elliptic Curve (EC) key on which certificate requests are generated using ECDSA signatures. The `label` argument specifies the EC key label that is configured using the `crypto key generate rsa` or `crypto key generate ec keysize` command in global configuration mode. See the Configuring Internet Key Exchange for IPsec VPNs feature module for more information.

**Note** If an ECDSA signed certificate is imported without a trustpoint configuration, then the label defaults to the FQDN value.

**Step 6**

**subject-name [x.500-name]**

**Example:**

```
Router(ca-trustpoint)# subject-name cat
```

(Optional) Specifies the requested subject name that will be used in the certificate request.

- **x.500-name** --If it is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.

**Step 7**

**vrf vrf-name**

**Example:**

```
Router(ca-trustpoint)# vrf myvrf
```

(Optional) Specifies the the VRF instance in the public key infrastructure (PKI) trustpoint to be used for enrollment, certificate revocation list (CRL) retrieval, and online certificate status protocol (OCSP) status.

**Step 8**

**ip-address {ip-address | interface | none}**

**Example:**

```
Router(ca-trustpoint)# ip address 192.168.1.66
```

(Optional) Includes the IP address of the specified interface in the certificate request.

- Issue the `ip-address` argument to specify either an IPv4 or IPv6 address.
- Issue the `interface` argument to specify an interface on the router.
- Issue the `none` keyword if no IP address should be included.

**Note** If this command is enabled, you will not be prompted for an IP address during enrollment for this trustpoint.

**Step 9**

**serial-number [none]**

**Example:**

```
Router(ca-trustpoint)# serial-number
```

(Optional) Specifies the router serial number in the certificate request, unless the `none` keyword is issued.

- Issue the `none` keyword to specify that a serial number will not be included in the certificate request.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 10</strong></td>
<td>(Optional) Enables autoenrollment, allowing the client to automatically request a rollover certificate from the CA.</td>
</tr>
</tbody>
</table>
| **Example:** auto-enroll [percent] [regenerate] | - If autoenrollment is not enabled, the client must be manually re-enrolled in your PKI upon certificate expiration.  
    - By default, only the Domain Name System (DNS) name of the router is included in the certificate.  
    - Use the `percent` argument to specify that a new certificate will be requested after the percentage of the lifetime of the current certificate is reached.  
    - Use the `regenerate` keyword to generate a new key for the certificate even if a named key already exists. |
| **Note**                          | If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable: “! RSA key pair associated with trustpoint is exportable.” |
| **Note**                          | It is recommended that a new key pair be generated for security reasons.                        |
| **Step 11**                       | (Optional) Specifies the intended use for the certificate.                                          |
| **Example:** usage method[1 [method2 [method3]]] | - Available options are `ike`, `ssl-client`, and `ssl-server`; the default is `ike`. |
| **Step 12**                       | (Optional) Specifies the revocation password for the certificate.                                  |
| **Example:** password string       | - If this command is enabled, you will not be prompted for a password during enrollment for this trustpoint. |
| **Note**                          | When SCEP is used, this password can be used to authorize the certificate request--often via a one-time password or similar mechanism. |
| **Step 13**                       | (Optional) Specifies which key pair to associate with the certificate.                              |
| **Example:** rsakeypair key-label key-size encryption-key-size ] | - A key pair with the `key-label` argument will be generated during enrollment if it does not already exist or if the `auto-enroll regenerate` command was issued.  
    - Specify the `key-size` argument for generating the key, and specify the `encryption-key-size` argument to |
### Purpose

**Command or Action**  |  **Purpose**  
---|---
request separate encryption, signature keys, and certificates. The key-size and encryption-key-size must be the same size. Length of less than 2048 is not recommended.  

**Note**  
If this command is not enabled, the FQDN key pair is used.

### Step 14

**fingerprint ca-fingerprint**  
**Example:**

Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E

**(Optional) Specifies a fingerprint that can be matched against the fingerprint of a CA certificate during authentication.**

**Note**  
If the fingerprint is not provided and authentication of the CA certificate is interactive, the fingerprint will be displayed for verification.

### Step 15

**on devicename :**  
**Example:**

Router(ca-trustpoint)# on usbtoken0:  

**(Optional) Specifies that RSA keys will be created on the specified device upon autoenrollment initial key generation.**

- Devices that may be specified include NVRAM, local disks, and Universal Serial Bus (USB) tokens. USB tokens may be used as cryptographic devices in addition to a storage device. Using a USB token as a cryptographic device allows RSA operations such as key generation, signing, and authentication to be performed on the token.

### Step 16

**exit**  
**Example:**

Router(ca-trustpoint)# exit

**Exits ca-trustpoint configuration mode and returns to global configuration mode.**

### Step 17

**crypto pki authenticate name**  
**Example:**

Router(config)# crypto pki authenticate mytp

**Retrieves the CA certificate and authenticates it. Check the certificate fingerprint if prompted.**

**Note**  
This command is optional if the CA certificate is already loaded into the configuration.

### Step 18

**exit**  
**Example:**

Router(config)# exit

**Exits global configuration mode.**

### Step 19

**copy system:running-config nvram:startup-config**  
**Example:**

Router# copy system:running-config nvram:startup-config

**(Optional) Copies the running configuration to the NVRAM startup configuration.**

**Note**  
Autoenrollment will not update NVRAM if the running configuration has been modified but not written to NVRAM.
### Configuring Manual Certificate Enrollment

Manual certificate enrollment can be set up via TFTP or the manual cut-and-paste method. Both options can be used if your CA does not support SCEP or if a network connection between the router and CA is not possible. Perform one of the following tasks to set up manual certificate enrollment:

#### PEM-Formatted Files for Certificate Enrollment Request

Using PEM-formatted files for certificate requests can be helpful for customers who are using terminal or profile-based enrollment to request certificates from their CA server. Customers using PEM-formatted files can directly use existing certificates on their routers.

#### Restrictions for Manual Certificate Enrollment

**SCEP Restriction**

We do not recommend switching URLs if SCEP is used; that is, if the enrollment URL is “http://myca,” do not change the enrollment URL after getting the CA certificate and before enrolling the certificate. A user can switch between TFTP and manual cut-and-paste.

**Key Regeneration Restriction**

Do not regenerate the keys manually using the `crypto key generate` command; key regeneration will occur when the `crypto pki enroll` command is issued if the `regenerate` keyword is specified.

### Configuring Cut-and-Paste Certificate Enrollment

Perform this task to configure cut-and-paste certificate enrollment. This task helps you to configure manual certificate enrollment via the cut-and-paste method for peers participating in your PKI.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto pki trustpoint name`
4. `enrollment terminal pem`
5. `fingerprint ca-fingerprint`
6. `exit`
7. `crypto pki authenticate name`
8. `crypto pki enroll name`
9. `crypto pki import name certificate`
10. `exit`
## 11. show crypto pki certificates

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto pki trustpoint <em>name</em></td>
<td>Declares the trustpoint and a given name and enters</td>
</tr>
<tr>
<td>Example:</td>
<td>ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td>Router(config)# crypto pki trustpoint mytp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> enrollment terminal pem</td>
<td>Specifies the manual cut-and-paste certificate enrollment</td>
</tr>
<tr>
<td>Example:</td>
<td>method.</td>
</tr>
<tr>
<td>Router(ca-trustpoint)# enrollment terminal</td>
<td>• The certificate request will be displayed on the console terminal so</td>
</tr>
<tr>
<td></td>
<td>that it may be manually copied (or cut).</td>
</tr>
<tr>
<td></td>
<td>• pem --Configures the trustpoint to generate PEM-formatted certificate</td>
</tr>
<tr>
<td></td>
<td>requests to the console terminal.</td>
</tr>
<tr>
<td><strong>Step 5</strong> fingerprint <em>ca-fingerprint</em></td>
<td>(Optional) Specifies a fingerprint that can be matched</td>
</tr>
<tr>
<td>Example:</td>
<td>against the fingerprint of a CA certificate during authentication.</td>
</tr>
<tr>
<td>Router(ca-trustpoint)# fingerprint 12EF53FA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>355CD23E 12EF53FA 355CD23E</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits ca-trustpoint configuration mode and returns to global</td>
</tr>
<tr>
<td>Example:</td>
<td>configuration mode.</td>
</tr>
<tr>
<td>Router(ca-trustpoint)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> crypto pki authenticate <em>name</em></td>
<td>Retrieves the CA certificate and authenticates it.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# crypto pki authenticate mytp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> crypto pki enroll name</td>
<td>Generates certificate request and displays the request for</td>
</tr>
<tr>
<td>Example:</td>
<td>copying and pasting into the certificate server.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Router(config)# crypto pki enroll mytp                 | • You are prompted for enrollment information, such as whether to include the router FQDN and IP address in the certificate request. You are also given the choice about displaying the certificate request to the console terminal.  
• The base-64 encoded certificate with or without PEM headers as requested is displayed. |
| **Step 9** crypto pki import name certificate          | Imports a certificate manually at the console terminal (pasting).  
• The base-64 encoded certificate is accepted from the console terminal and inserted into the internal certificate database. |
| **Note** You must enter this command twice if usage keys, a signature key, and an encryption key are used. The first time the command is entered, one of the certificates is pasted into the router. The second time the command is entered, the other certificate is pasted into the router. It does not matter which certificate is pasted first. |
| **Note** Some CAs ignore the usage key information in the certificate request and issue general purpose usage certificates. If this applies to the certificate authority you are using, import the general purpose certificate. The router will not use one of the two key pairs generated. |

| Step 10 exit                                           | Exits global configuration mode. |
| **Example:**                                           | Router(config)# exit             |

| Step 11 show crypto pki certificates                    | (Optional) Displays information about your certificates, the certificates of the CA, and RA certificates. |
| **Example:**                                           | Router# show crypto pki certificates |

### Configuring TFTP Certificate Enrollment

Perform this task to configure TFTP certificate enrollment. This task helps you to configure manual certificate enrollment using a TFTP server.

**Before you begin**

- You must know the correct URL to use if you are configuring certificate enrollment via TFTP.
- The router must be able to write a file to the TFTP server for the `crypto pki enroll` command.
- If you are using a file specification with the `enrollment` command, the file must contain the CA certificate either in binary format or be base-64 encoded.
- You must know if your CA ignores key usage information in a certificate request and issues only a general purpose usage certificate.

Caution

Some TFTP servers require that the file must exist on the server before it can be written. Most TFTP servers require files that can be written over. This requirement may pose a risk because any router or other device may write or overwrite the certificate request; thus, the replacement certificate request will not be used by the CA administrator, who must first check the enrollment request fingerprint before granting the certificate request.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. crypto pki trustpoint name
4. enrollment [mode] [retry period minutes] [retry count number] url url [pem]
5. fingerprint ca-fingerprint
6. exit
7. crypto pki authenticate name
8. crypto pki enroll name
9. crypto pki import name certificate
10. exit
11. show crypto pki certificates

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> crypto pki trustpoint name</td>
<td>Declares the trustpoint and a given name and enters ca-trustpoint config</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# crypto pki trustpoint mytp</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>--------</td>
<td>----------------------</td>
</tr>
<tr>
<td><strong>enrollment [mode] [retry period minutes] [retry count number] url url [pem]</strong></td>
<td>Specifies TFTP as the enrollment method to send the enrollment request and to retrieve the CA certificate and router certificate and any optional parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# enrollment url tftp://certserver/file_specification</td>
<td></td>
</tr>
</tbody>
</table>

**Note** For TFTP enrollment, the URL must be configured as a TFTP URL, tftp://example_tftp_url.
- An optional file specification filename may be included in the TFTP URL. If the file specification is not included, the FQDN will be used. If the file specification is included, the router will append the extension “.ca” to the specified filename.

<table>
<thead>
<tr>
<th>Step 5</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>fingerprint ca-fingerprint</strong></td>
<td>(Optional) Specifies the fingerprint of the CA certificate received via an out-of-band method from the CA administrator.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note** If the fingerprint is not provided, it will be displayed for verification.

<table>
<thead>
<tr>
<th>Step 6</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>exit</strong></td>
<td>Exits ca-trustpoint configuration mode and returns to global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# exit</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>crypto pki authenticate name</strong></td>
<td>Retrieves the CA certificate and authenticates it from the specified TFTP server.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config)# crypto pki authenticate mytp</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 8</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>crypto pki enroll name</strong></td>
<td>Generates certificate request and writes the request out to the TFTP server.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router(config)# crypto pki enroll mytp</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- You are prompted for enrollment information, such as whether to include the router FQDN and IP address in the certificate request. You are queried about whether to display the certificate request to the console terminal.
- The filename to be written is appended with the extension “.req”. For usage keys, a signature key and an encryption key, two requests are generated and sent. The usage key request filenames are appended with the extensions “-sign.req” and “-encr.req”, respectively.

<table>
<thead>
<tr>
<th>Step 9</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>crypto pki import name certificate</strong></td>
<td>Imports a certificate via TFTP at the console terminal, which retrieves the granted certificate.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| `crypto pki import mytp certificate` | • The router will attempt to retrieve the granted certificate via TFTP using the same filename used to send the request, except the extension is changed from “.req” to “.crt”. For usage key certificates, the extensions “-sign.crt” and “-encr.crt” are used.  
• The router will parse the received files, verify the certificates, and insert the certificates into the internal certificate database on the router. |

**Note** Some CAs ignore the usage key information in the certificate request and issue general purpose usage certificates. If your CA ignores the usage key information in the certificate request, only import the general purpose certificate. The router will not use one of the two key pairs generated.

<table>
<thead>
<tr>
<th>Step 10</th>
<th>exit</th>
<th>Exits global configuration mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>exit</code></td>
<td>Router(config)# exit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th>show crypto pki certificates</th>
<th>(Optional) Displays information about your certificates, the certificates of the CA, and RA certificates.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td><code>show crypto pki certificates</code></td>
<td>Router# show crypto pki certificates</td>
</tr>
</tbody>
</table>

**Certifying a URL Link for Secure Communication with a Trend Micro Server**

Perform this task to certify a link used in URL filtering that allows secure communication with a Trend Micro Server.

**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the *Next Generation Encryption* (NGE) white paper.

**SUMMARY STEPS**

1. enable  
2. `clock set hh : mm : ss date month year`  
3. `configure terminal`  
4. `clock timezone zone hours-offset [minutes-offset ]`  
5. `ip http server`  
6. `hostname name`  
7. `ip domain-name name`
8. `crypto key generate rsa general-keys modulus`  `modulus-size`
9. `crypto pki trustpoint`  `name`
10. `enrollment terminal`
11. `crypto ca authenticate`  `name`
12. Copy the following block of text containing the base 64 encoded CA certificate and paste it at the prompt.
13. Enter yes to accept this certificate.
14. `serial-number`
15. `revocation-check none`
16. `end`
17. `trm register`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>clock set</strong> <code>hh : mm : ss date month year</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Router# clock set 23:22:00 22 Dec 2009</td>
</tr>
<tr>
<td></td>
<td><strong>Sets the clock on the router.</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td><strong>Enters global configuration mode.</strong></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>clock timezone</strong> <code>zone hours-offset [minutes-offset]</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>Router(config)# clock timezone PST -08</td>
</tr>
<tr>
<td></td>
<td><strong>Sets the time zone.</strong></td>
</tr>
<tr>
<td></td>
<td>• The <code>zone</code> argument is the name of the time zone (typically a standard acronym). The <code>hours-offset</code> argument is the number of hours the time zone is different from Universal Time Coordinated (UTC). The <code>minutes-offset</code> argument is the number of minutes the time zone is different from UTC.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The <code>minutes-offset</code> argument of the <code>clock timezone</code> command is available for those cases where a local time zone is a percentage of an hour different from UTC or Greenwich Mean Time (GMT). For example, the time zone for some sections of Atlantic Canada (AST) is UTC-3.5. In this case, the necessary command would be <code>clock timezone AST -3 30</code>.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>5</td>
<td>ip http server</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config)# ip http server</td>
</tr>
<tr>
<td>6</td>
<td>hostname name</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config)# hostname hostname1</td>
</tr>
<tr>
<td>7</td>
<td>ip domain-name name</td>
</tr>
<tr>
<td></td>
<td>Example: Router(config)# ip domain-name example.com</td>
</tr>
<tr>
<td>8</td>
<td>crypto key generate rsa general-keys modulus modulus-size</td>
</tr>
<tr>
<td></td>
<td>• The general-keys keyword specifies that a general purpose key pair is generated, which is the default.</td>
</tr>
<tr>
<td></td>
<td>• The modulus keyword and modulus-size argument specify the IP size of the key modulus. By default, the modulus of a CA key is 1024 bits. When generating RSA keys, you will be prompted to enter a modulus length. A longer modulus could offer stronger security but takes longer to generate and to use. A length of less than 2048 is not recommended.</td>
</tr>
<tr>
<td></td>
<td>Note The name for the general keys that are generated are based on the domain name that is configured in Step 7. For example, the keys will be called “example.com.”</td>
</tr>
<tr>
<td>9</td>
<td>crypto pki trustpoint name</td>
</tr>
<tr>
<td></td>
<td>Note Effective with Cisco IOS Release 12.3(8)T, the crypto pki trustpoint command replaced the crypto ca trustpoint command.</td>
</tr>
<tr>
<td>10</td>
<td>enrollment terminal</td>
</tr>
<tr>
<td></td>
<td>• The certificate request will be displayed on the console terminal so that you may manually copy (or cut).</td>
</tr>
<tr>
<td>11</td>
<td>crypto ca authenticate name</td>
</tr>
</tbody>
</table>
### Command or Action

```
Router(ca-trustpoint)# crypto ca authenticate mytp
```

### Purpose

- The following command output displays:

```
Enter the base 64 encoded CA certificate. End with a blank line or the word "quit" on a line by itself.
```

**Step 12**

Copy the following block of text containing the base 64 encoded CA certificate and paste it at the prompt.

```
MIIBIDCCChongPopEaPqgEuB3l/02zaN8zgjqhjicGw3eO6AUIVp9sAJOaw5QDQpQcQVYMQOeXAV
UmMQAwGAMxBW1h/hQF1eB2e5EMduzAIUEBMA4i50F1eB2e5Z28N8icfiG2svy
<...>
```

**The following command output displays:**

Certificate has the following attributes:

- **Fingerprint** MD5: 67CB9DC0 13248A82 9BB2171E D118EC04

Certificate has the following attributes:
### Configuring a Persistent Self-Signed Certificate for Enrollment via SSL

This section contains the following tasks:

- **Note**: These tasks are optional because if you enable the HTTPS server, it generates a self-signed certificate automatically using default values.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 13</strong></td>
<td>Enter yes to accept this certificate.</td>
</tr>
<tr>
<td></td>
<td>% Do you accept this certificate? [yes/no]: yes</td>
</tr>
<tr>
<td></td>
<td>The following command output displays:</td>
</tr>
<tr>
<td></td>
<td>Trustpoint CA certificate accepted.</td>
</tr>
<tr>
<td></td>
<td>% Certificate successfully imported</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>serial-number</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>specifies the router serial number in the certificate request.</td>
</tr>
<tr>
<td></td>
<td>hostname1(ca-trustpoint)# serial-number</td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>revocation-check none</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>specifies that certificate checking is ignored.</td>
</tr>
<tr>
<td></td>
<td>hostname1(ca-trustpoint)# revocation-check none</td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td>end</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>exits ca-trustpoint configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>hostname1(ca-trustpoint)# end</td>
</tr>
<tr>
<td><strong>Step 17</strong></td>
<td>trm register</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>manually starts the Trend Micro Server registration process.</td>
</tr>
<tr>
<td></td>
<td>hostname1# trm register</td>
</tr>
</tbody>
</table>
Persistent Self-Signed Certificates Overview

The SSL protocol can be used to establish a secure connection between an HTTPS server and a client (web browser). During the SSL handshake, the client expects the SSL server’s certificate to be verifiable using a certificate the client already possesses.

If Cisco IOS software does not have a certificate that the HTTPS server can use, the server generates a self-signed certificate by calling a PKI application programming interface (API). When the client receives this self-signed certificate and is unable to verify it, intervention is needed. The client asks you if the certificate should be accepted and saved for future use. If you accept the certificate, the SSL handshake continues.

Future SSL handshakes between the same client and the server use the same certificate. However, if the router is reloaded, the self-signed certificate is lost. The HTTPS server must then create a new self-signed certificate. This new self-signed certificate does not match the previous certificate, so you are once again asked to accept it.

Requesting acceptance of the router’s certificate each time that the router reloads may present an opportunity for an attacker to substitute an unauthorized certificate when you are being asked to accept the certificate. Persistent self-signed certificates overcome all these limitations by saving a certificate in the router’s startup configuration.

Restrictions

- You can configure only one trustpoint for a persistent self-signed certificate.
- The maximum lifetime of a self-signed certificate is 00:00:00 GMT Jan 1, 2030.

Note

Do not change the IP domain name or the hostname of the router after creating the self-signed certificate. Changing either name triggers the regeneration of the self-signed certificate and overrides the configured trustpoint. WebVPN ties the SSL trustpoint name to the WebVPN gateway configuration. If a new self-signed certificate is triggered, then the new trustpoint name does not match the WebVPN configuration, causing the WebVPN connections to fail.

Configuring a Trustpoint and Specifying Self-Signed Certificate Parameters

Note

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Perform the following task to configure a trustpoint and specify self-signed certificate parameters.

SUMMARY STEPS

1. enable
2. configure terminal
3. crypto pki trustpoint name
4. enrollment selfsigned
5. subject-name [x.500-name]
6. `rsakeypair key-label [key-size [encryption-key-size]]`
7. `crypto pki enroll name`
8. `end`
9. `show crypto pki certificates [trustpoint-name [verbose]]`
10. `show crypto pki trustpoints [status | label [status]]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>crypto pki trustpoint name</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(config)# crypto pki trustpoint local</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>enrollment selfsigned</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(ca-trustpoint)# enrollment selfsigned</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><code>subject-name [x.500-name]</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(ca-trustpoint)# subject-name</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><code>rsakeypair key-label [key-size [encryption-key-size]]</code>&lt;br&gt;<strong>Example:</strong>&lt;br&gt;Router(ca-trustpoint)# rsakeypair examplekey 2048</td>
</tr>
</tbody>
</table>
Enabling the HTTPS Server

Perform the following task to enable the HTTPS server.

Before you begin
To specify parameters, you must create a trustpoint and configure it. To use default values, delete any existing self-signed trustpoints. Deleting all self-signed trustpoints causes the HTTPS server to generate a persistent self-signed certificate using default values as soon as the server is enabled.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip http secure-server
4. end
5. copy system:running-config nvram:startup-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

---

**Configuring Certificate Enrollment for a PKI**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>crypto pki enroll name</td>
<td>Tells the router to generate the persistent self-signed certificate.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# crypto pki enroll local</td>
<td></td>
</tr>
</tbody>
</table>

| Step 8 end | (Optional) Exits ca-trustpoint configuration mode. |
| Example:   | • Enter this command a second time to exit global configuration mode. |
| Router(ca-trustpoint)# end |         |

| Step 9 show crypto pki certificates [trustpoint-name[verbose]] | Displays information about your certificate, the certification authority certificate, and any registration authority certificates. |
| Example: |         |
| Router# show crypto pki certificates local verbose |         |

| Step 10 show crypto pki trustpoints [status | label [status]] | Displays the trustpoints that are configured in the router. |
| Example: |         |
| Router# show crypto pki trustpoints status |         |
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router&gt; enable</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

#### Step 2

**configure terminal**

**Example:**

Router# configure terminal

#### Step 3

**ip http secure-server**

**Example:**

Router(config)# ip http secure-server

**Note**

A key pair (modulus 1024) and a self-signed certificate are automatically generated.

#### Step 4

**end**

**Example:**

Router(config)# end

#### Step 5

**copy system:running-config nvram: startup-config**

**Example:**

Router# copy system:running-config nvram: startup-config

### Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment

Perform this task to configure a certificate enrollment profile for enrollment or reenrollment. This task helps you to configure an enrollment profile for certificate enrollment or reenrollment of a router with a Cisco IOS CA that is already enrolled with a third-party vendor CA.

Enable a router that is enrolled with a third-party vendor CA to use its existing certificate to enroll with the Cisco IOS certificate server so the enrollment request is automatically granted. To enable this functionality, you must issue the **enrollment credential** command. Also, you cannot configure manual certificate enrollment.

#### Before you begin

Perform the following tasks at the client router before configuring a certificate enrollment profile for the client router that is already enrolled with a third-party vendor CA so that the router can reenroll with a Cisco IOS certificate server:

- Defined a trustpoint that points to the third-party vendor CA.
- Authenticated and enrolled the client router with the third-party vendor CA.
To use certificate profiles, your network must have an HTTP interface to the CA.

If an enrollment profile is specified, an enrollment URL may not be specified in the trustpoint configuration. Although both commands are supported, only one command can be used at a time in a trustpoint.

Because there is no standard for the HTTP commands used by various CAs, the user is required to enter the command that is appropriate to the CA that is being used.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `crypto pki trustpoint name`
4. `enrollment profile label`
5. `exit`
6. `crypto pki profile enrollment label`
7. Do one of the following:
   - `authentication url url`
   - `authentication terminal`
8. `authentication command`
9. Do one of the following:
   - `enrollment url url`
   - `enrollment terminal`
10. `enrollment credential label`
11. `enrollment command`
12. `parameter number {value value | prompt string}`
13. `exit`
14. `show crypto pki certificates`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
</tr>
</tbody>
</table>
| 3    | `crypto pki trustpoint name`  
   **Example:**  
   ```bash
   Router(config)# crypto pki trustpoint Entrust
   ``` | Declares the trustpoint and a given name and enters ca-trustpoint configuration mode. |
| 4    | enrollment profile label  
   **Example:**  
   ```bash
   Router(ca-trustpoint)# enrollment profile E
   ``` | Specifies that an enrollment profile is to be used for certificate authentication and enrollment. |
| 5    | `exit`  
   **Example:**  
   ```bash
   Router(ca-trustpoint)# exit
   ``` | Exits ca-trustpoint configuration mode. |
| 6    | `crypto pki profile enrollment label`  
   **Example:**  
   ```bash
   Router(config)# crypto pki profile enrollment E
   ``` | Defines an enrollment profile and enters ca-profile-enroll configuration mode.  
       - `label` --Name for the enrollment profile; the enrollment profile name must match the name specified in the `enrollment profile` command. |
| 7    | Do one of the following:  
   • `authentication url url`  
   • `authentication terminal`  
   **Example:**  
   ```bash
   Router(ca-profile-enroll)# authentication url http://entrust:81
   ```  
   **Example:**  
   ```bash
   Router(ca-profile-enroll)# authentication terminal
   ``` | Specifies the URL of the CA server to which to send certificate authentication requests.  
       - `url` --URL of the CA server to which your router should send authentication requests. If you are using HTTP, the URL should read “http://CA_name,” where CA_name is the host DNS name or IP address of the CA. If you are using TFTP, the URL should read “tftp://certserver/file_specification.” (If the URL does not include a file specification, the FQDN of the router will be used.)  
       Specifies manual cut-and-paste certificate authentication. |
| 8    | `authentication command`  
   **Example:**  
   ```bash
   Router(ca-profile-enroll)# authentication command
   ``` | (Optional) Specifies the HTTP command that is sent to the CA for authentication. |
| 9    | Do one of the following:  
   • `enrollment url url`  
   • `enrollment terminal`  
   **Example:**  
   ```bash
   ``` | Specifies the URL of the CA server to which to send certificate enrollment requests via HTTP or TFTP.  
       Specifies manual cut-and-paste certificate enrollment. |
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>Router(ca-profile-enroll)# enrollment url <a href="http://entrust:81/cda-cgi/clientcgi.exe">http://entrust:81/cda-cgi/clientcgi.exe</a></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Router(ca-profile-enroll)# enrollment terminal</td>
</tr>
<tr>
<td><strong>Step 10</strong> enrollment credential <em>label</em></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Router(ca-profile-enroll)# enrollment credential Entrust</td>
</tr>
<tr>
<td><strong>Step 11</strong> enrollment command</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Router(ca-profile-enroll)# enrollment command</td>
</tr>
<tr>
<td><strong>Step 12</strong> parameter *number {value value</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Router(ca-profile-enroll)# parameter 1 value aaaa-bbbb-cccc</td>
</tr>
<tr>
<td><strong>Step 13</strong> exit</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Router(ca-profile-enroll)# exit</td>
</tr>
<tr>
<td><strong>Step 14</strong> show crypto pki certificates</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td>Router# show crypto pki certificates</td>
</tr>
</tbody>
</table>

### What to Do Next

If you configured the router to reenroll with a Cisco IOS CA, you should configure the Cisco IOS certificate server to accept enrollment requests only from clients already enrolled with the specified third-party vendor CA trustpoint to take advantage of this functionality. For more information, see the module “Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment.”
Configuring Certificate Enrollment in a Two-Tier PKI Environment

The feature enables sub-CAs to issue certificates to their clients when a root CA is offline. The root certificate can be imported through the CLI first, and then it is used to validate the issuing sub CA certificate configured under the trustpoint.

Note

Enable revocation checking as per your environment before performing the following tasks.

For importing the ROOT-CA through terminal, perform the following steps:

```
enable
configure terminal
crypto pki trustpoint ROOT-CA
revocation-check none
enrollment terminal
crypto pki authenticate ROOT-CA
exit
```

For authenticating SUB-CA without specifying or accepting the fingerprint.

```
enable
configure terminal
crypto pki trustpoint SUB-CA
revocation-check none
enrollment url url
chain-validation continue ROOT-CA
exit
crypto pki authenticate SUB-CA
exit
```

Configuration Examples for PKI Certificate Enrollment Requests

Configuring Certificate Enrollment or Autoenrollment Example

The following example shows the configuration for the “mytp-A” certificate server and its associated trustpoint, where RSA keys generated by the initial autoenrollment for the trustpoint will be stored on a USB token, “usbtoken0”:

```
crypto pki server mytp-A
database level complete
issuer-name CN=company, L=city, C=country
grant auto
! Specifies that certificate requests will be granted automatically.
! crypto pki trustpoint mytp-A
```
Configuring Autoenrollment Example

The following example shows how to configure the router to automatically enroll with a CA on startup, enabling automatic rollover, and how to specify all necessary enrollment information in the configuration:

```
crypto pki trustpoint trustpt1
enrollment url http://trustpt1.example.com/
subject-name OU=Spiral Dept., O=example.com
ip-address ethernet-0
serial-number none
usage ike
auto-enroll regenerate
password password1
rsa-key trustpt1 2048

crypto pki certificate chain trustpt1
```
the old certificate expires. The changes made to the running configuration are saved to the NVRAM startup configuration because autoenrollment will not update NVRAM if the running configuration has been modified but not written to NVRAM.

crypto pki trustpoint trustme1
  enrollment url http://trustme1.example.com/
  subject-name OU=Spiral Dept., O=example.com
  ip-address ethernet0
  serial-number none
  auto-enroll 90 regenerate
  password password1
  rsakeypair trustme1 2048
  exit

crypto pki authenticate trustme1

copy system:running-config nvram:startup-config

Configuring Cut-and-Paste Certificate Enrollment Example

The following example shows how to configure certificate enrollment using the manual cut-and-paste enrollment method:

Route(config)#
crypto pki trustpoint TP
Router(config-trustpoint)#
enrollment terminal
Router(config-trustpoint)#
crypto pki authenticate TP

% Do you accept this certificate? [yes/no]:
y
Trustpoint CA certificate accepted.
% Certificate successfully imported
Router(config)#
crypto pki enroll TP

% Start certificate enrollment..
% The subject name in the certificate will be:
Router.example.com

% Include the router serial number in the subject name? [yes/no]:
no
% Include an IP address in the subject name? [no]:
no
% Display Certificate Request to terminal? [yes/no]:
y
Configuring Certificate Enrollment for a PKI

Configuring Cut-and-Paste Certificate Enrollment Example

Signature key certificate request -
Certificate Request follows:
MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQcKgFhRTYW5kQmFzV2U2M2FmNmE5NzjdNjIwMzI2NjViZjUxa3BkNjYiMjEyMXzqYjQ5OTk0YzZlZmE2MDtjYmRyZjM2OTg5ZmUwMDMyZjI3MDNkZmIwM2FmNzUxODk5Y2FiNzI5MDA=

Redisplay enrollment request? [yes/no]:

Encryption key certificate request -
Certificate Request follows:
MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQcKgFhRTYW5kQmFzV2U2M2FmNmE5NzjdNjIwMzI2NjViZjUxa3BkNjYiMjEyMXzqYjQ5OTk0YzZlZmE2MDtjYmRyZjM2OTg5ZmUwMDMyZjI3MDNkZmIwM2FmNzUxODk5Y2FiNzI5MDA=

Redisplay enrollment request? [yes/no]:

Router(config)#
crypto pki import TP certificate
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

% Router Certificate successfully imported

Router(config)#
crypto pki import TP cert
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

Router(config)#
crypto pki import TP certificate
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

Configuring Certificate Enrollment for a PKI
You can verify that the certificate was successfully imported by issuing the `show crypto pki certificates` command:

```
Router# show crypto pki certificates
Certificate
Status: Available
Certificate Serial Number: 14DECE05000000000C48
Certificate Usage: Encryption
Issuer:
  CN = TPCA-root
  O = Company
  C = US
Subject:
  Name: Router.example.com
  OID.1.2.840.113549.1.9.2 = Router.example.com
CRL Distribution Point:
  http://tpca-root/CertEnroll/tpca-root.crl
Validity Date:
  start date: 18:16:45 PDT Jun 7 2002
  end date: 18:26:45 PDT Jun 7 2003
  renew date: 16:00:00 PST Dec 31 1969
Associated Trustpoints: TP

Certificate
Status: Available
Certificate Serial Number: 14DEC2E9000000000C47
Certificate Usage: Signature
Issuer:
  CN = tpca-root
  O = company
  C = US
Subject:
  Name: Router.example.com
  OID.1.2.840.113549.1.9.2 = Router.example.com
CRL Distribution Point:
  http://tpca-root/CertEnroll/tpca-root.crl
Validity Date:
  start date: 18:16:42 PDT Jun 7 2002
  end date: 18:26:42 PDT Jun 7 2003
  renew date: 16:00:00 PST Dec 31 1969
Associated Trustpoints: TP

CA Certificate
Status: Available
Certificate Serial Number: 3AC0A65E9547C2874AAF2468A942D5EE
Certificate Usage: Signature
Issuer:
  CN = tpca-root
  O = company
  C = US
```
Configuring Manual Certificate Enrollment with Key Regeneration Example

The following example shows how to regenerate new keys with a manual certificate enrollment from the CA named “trustme2”:

crypto pki trustpoint trustme2
  enrollment url http://trustme2.example.com/
  subject-name OU=Spiral Dept., O=example.com
  ip-address ethernet0
  serial-number none
  regenerate
  password password1
  rsakeypair trustme2 2048
  exit

crypto pki authenticate trustme2

crypto pki enroll trustme2

Creating and Verifying a Persistent Self-Signed Certificate Example

The following example shows how to declare and enroll a trustpoint named “local” and generate a self-signed certificate with an IP address:

crypto pki trustpoint local
  enrollment selfsigned
  end
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
crypto pki enroll local
Nov 29 20:51:13.067: %SSH-5-ENABLED: SSH 1.99 has been enabled
Nov 29 20:51:13.267: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: ethernet 0
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created

Note
A router can have only one self-signed certificate. If you attempt to enroll a trustpoint configured for a self-signed certificate and one already exists, you receive a notification and are asked if you want to replace it. If so, a new self-signed certificate is generated to replace the existing one.
Enabling the HTTPS Server Example

The following example shows how to enable the HTTPS server and generate a default trustpoint because one was not previously configured:

```
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ip http secure-server
% Generating 1024 bit RSA keys ...[OK]
*Dec 21 19:14:15.421:%PKI-4-NOAUTOSAVE:Configuration was modified. Issue "write memory"
to save new certificate
Router(config)#
```

You need to save the configuration to NVRAM if you want to keep the self-signed certificate and have the HTTPS server enabled following router reloads.

The following message also appears:

```
*Dec 21 19:14:10.441:%SSH-5-ENABLED:SSH 1.99 has been enabled
```

Note

Creation of the key pair used with the self-signed certificate causes the Secure Shell (SSH) server to start. This behavior cannot be suppressed. You may want to modify your Access Control Lists (ACLs) to permit or deny SSH access to the router. You can use the `ip ssh rsa keypair-name unexisting-key-pair-name` command to disable the SSH server.

Verifying the Self-Signed Certificate Configuration Example

The following example displays information about the self-signed certificate that you just created:

```
Router# show crypto pki certificates
Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: General Purpose
  Issuer:
    cn=IOS-Self-Signed-Certificate-3326000105
  Subject:
    Name: IOS-Self-Signed-Certificate-3326000105
    cn=IOS-Self-Signed-Certificate-3326000105
  Validity Date:
    start date: 19:14:14 GMT Dec 21 2004
    end date: 00:00:00 GMT Jan 1 2020
  Associated Trustpoints: TP-self-signed-3326000105
```

Note

The number 3326000105 is the router’s serial number and varies depending on the router’s actual serial number.

The following example displays information about the key pair corresponding to the self-signed certificate:
```
Router# show crypto key mypubkey rsa
% Key pair was generated at: 19:14:10 GMT Dec 21 2004
Key name: TP-self-signed-3326000105
Usage: General Purpose Key
Key is not exportable.
Key Data:
30819F30 0D06092A 864886F7 0D010101 05000381 89028181 00B88F70
6BC78B6D 67D66CF3 135C1D91 8F360292 CA44A032 5AC1A8FD 095E4865 F8C95A2B
BF8C47B7 E64A3804 9BBD7326 207BD456 19BAB78B D075E78E 00D2560C B09289AE
6DEC8B56 672F2B3A 5CDAE092 9D4C4F71 F38CB269 214F6293 4BA8FABF 9486BCFC
2B941BC8 5509999A7 2EFE12A5 6B7B669A 2D80AB77 39B38E0E AA23CB8C B7020301 0001
% Key pair was generated at: 19:14:13 GMT Dec 21 2004
Key name: TP-self-signed-3326000105.server
Usage: Encryption Key
Key is not exportable.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00C5680E 89777B42
463E5783 FE95EA9E F4456C7B 70499AF3 EA266651 56E29F4 5B003D93 2FC9F81D
8A461172 3FBAC2F3 046ED9DD C5F27C20 1BBA689B 08F16E45 C346337 F683D605
34E30F0E B4921BC5 DAC9E8BA 50C54AA0 BF551BDD 88453F50 61020301 0001
```

The second key pair with the name TP-self-signed-3326000105.server is the SSH key pair and is generated when any key pair is created on the router and SSH starts up.

The following example displays information about the trustpoint named “local”:

```
Router# show crypto pki trustpoints
Trustpoint local:
  Subject Name:
    serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.example.com
    Serial Number: 01
    Persistent self-signed certificate trust point
```

### Configuring Direct HTTP Enrollment Example

The following example show how to configure an enrollment profile for direct HTTP enrollment with a CA server:

```
crypto pki trustpoint Entrust
enrollment profile E
  serial
crypto pki profile enrollment E
  authentication url http://entrust:81/cda-cgi/clientcgi.exe
  enrollment command GET /certs/acert.der
  enrollment command POST reference_number=$P2&authcode=$P1
  &retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
  parameter 1 value aaaa-bbbb-cccc
  parameter 2 value 5001
```

### Configuring Certificate Enrollment in a Two-Tier PKI Environment Example

Example of importing the ROOT-CA via terminal.
(config)#crypto pki trustpoint ROOT-CA
(ca-trustpoint)#revocation-check none
(ca-trustpoint)#enrollment terminal

(config)#crypto pki authenticate ROOT-CA

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgIQIfTArEE1yKZFXHaAVgDk5jANBgkqhkiG9w0BAQsFADBN
MRwEQQYKZ2ImIzPyLGQBGRYDYz29cMRwGqfY1CZ5miZPyLGQBGRYIDnBuLWNvc3Qx
HDAaBgWVBAEMT3Zwbi11YXN0LXphY2ttY2ttkQ0EwRhcNMTgxMjIwMDAwMjNyWxNC
MjgxMjIwMDAwMjNyWxNCBNMwEQQYKZ5miZPyLGQBGRYDYz29cMRwGqfY1CZ5miZPy
LGQBGRYIDnBuLWNvc3QxHDAaBgWVBAEMT3Zwbi11YXN0LXphY2ttY2ttkQ0EwRhc
MAOGCSqGSIb3DQEBAQUAA4MCAw==END CERTIFICATE-----
quit
Certificate has the following attributes:
Fingerprint MD5: 99182E1E 96FB0595 DF86BFCE 3C781CF5
Fingerprint SHA1: 6E55B878 9AA3B603 D689AC25 F027615E 0C88E6E4

% Do you accept this certificate? [yes/no]: yes

Authenticating SUB-CA without having to specify or accept the fingerprint.

(config)#crypto pki trustpoint SUB-CA

(Config)#enrollment url http://<SUBCA_IP/FQDN>:80/certsrv/mscep/mscep.dll
(config)#chain-validation continue ROOT-CA
(config)#revocation-check none

(config)#crypto pki authenticate SUB-CA

Certificate has the following attributes:
Fingerprint MD5: 5C38CB0A 050A8E87 84A08A75 5F7084B8
Fingerprint SHA1: EB829470 B8B9E26E 4457F346 7A3E957C C623C6F9
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.
## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB token RSA operations: Benefits of using USB tokens</td>
<td>“Storing PKI Credentials” module in the Cisco IOS Security Configuration Guide: Secure Connectivity</td>
</tr>
<tr>
<td>Overview of PKI, including RSA keys, certificate enrollment, and CAs</td>
<td>“Cisco IOS PKI Overview: Understanding and Planning a PKI ” module in the Cisco IOS Security Configuration Guide: Secure Connectivity</td>
</tr>
<tr>
<td>Secure Device Provisioning: functionality overview and configuration tasks</td>
<td>“Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI ” module in the Cisco IOS Security Configuration Guide: Secure Connectivity</td>
</tr>
<tr>
<td>RSA key generation and deployment</td>
<td>“Deploying RSA Keys Within a PKI ” module in the Cisco IOS Security Configuration Guide: Secure Connectivity</td>
</tr>
<tr>
<td>Setting up and using a USB token</td>
<td>“Storing PKI Credentials ” module in the Cisco IOS Security Configuration Guide: Secure Connectivity</td>
</tr>
<tr>
<td>Cisco IOS security commands</td>
<td>Cisco IOS Security Command Reference</td>
</tr>
<tr>
<td>Suite-B ESP transforms</td>
<td>Configuring Security for VPNs with IPsec feature module.</td>
</tr>
<tr>
<td>Suite-B SHA-2 family (HMAC variant) and Elliptic Curve (EC) key pair configuration.</td>
<td>Configuring Internet Key Exchange for IPsec VPNs feature module.</td>
</tr>
<tr>
<td>Suite-B Integrity algorithm type transform configuration.</td>
<td>Configuring Internet Key Exchange Version 2 (IKEv2) feature module.</td>
</tr>
<tr>
<td>Suite-B Elliptic Curve Digital Signature Algorithm (ECDSA) signature (ECDSA-sig) authentication method configuration for IKEv2.</td>
<td>Configuring Internet Key Exchange Version 2 (IKEv2) feature module.</td>
</tr>
</tbody>
</table>
Configuring Certificate Enrollment for a PKI

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suite-B Elliptic curve Diffie-Hellman (ECDH) support for IPsec SA negotiation</td>
<td>Configuring Internet Key Exchange for IPsec VPNs and Configuring Internet Key Exchange Version 2 (IKEv2) feature modules.</td>
</tr>
<tr>
<td>Recommended cryptographic algorithms</td>
<td>Next Generation Encryption</td>
</tr>
</tbody>
</table>

**MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
</tbody>
</table>

**Technical Assistance**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
</tr>
</tbody>
</table>

**Link**


---

**Feature Information for PKI Certificate Enrollment**

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Table 1: Feature Information for PKI Certificate Enrollment

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Cisco IOS USB Token PKI Enhancements--Phase 2     | 12.4(11)T | This feature enhances USB token functionality by using the USB token as a cryptographic device. USB tokens may be used for RSA operations such as key generation, signing, and authentication.  
|                                                   |           | **Note**: This document describes the use of utilizing USB tokens for RSA operations during initial autoenrollment for a trustpoint.                   |
| Certificate Authority Key Rollover                | 12.4(2)T  | This feature introduces the ability for root CAs to roll over expiring CA certificates and keys and to have these changes propagate through the PKI network without manual intervention.  
|                                                   |           |  The following commands were introduced or modified by this feature: **auto-rollover, crypto pki certificate chain, crypto pki export pem, crypto pki server, crypto pki server info request, show crypto pki certificates, show crypto pki server, show crypto pki trustpoint.** |
| Certificate Autoenrollment                        | 12.2(8)T  | This feature introduces certificate autoenrollment, which allows the router to automatically request a certificate from the CA that is using the parameters in the configuration.  
<p>|                                                   |           | The following commands were introduced by this feature: <strong>auto-enroll, rsakeypair, show crypto ca timers.</strong>                                           |</p>
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Enrollment Enhancements</td>
<td>12.2(8)T</td>
<td>This feature introduces five new <code>crypto ca trustpoint</code> commands that provide new options for certificate requests and allow users to specify fields in the configuration instead of having to go through prompts. The following commands were introduced by this feature: <code>ip-address(ca-trustpoint), password(ca-trustpoint), serial-number, subject-name, usage</code>.</td>
</tr>
<tr>
<td>Direct HTTP Enrollment with CA Servers</td>
<td>12.3(4)T</td>
<td>This feature allows users to configure an enrollment profile if their CA server does not support SCEP and they do not want to use an RA-mode CS. The enrollment profile allows users to send HTTP requests directly to the CA server instead of to an RA-mode CS. The following commands were introduced by this feature: <code>authentication command, authentication terminal, authentication url, crypto ca profile enrollment, enrollment command, enrollment profile, enrollment terminal, enrollment url, parameter</code>.</td>
</tr>
<tr>
<td>Import of RSA Key Pair and Certificates in PEM Format</td>
<td>12.3(4)T</td>
<td>This feature allows customers to issue certificate requests and receive issued certificates in PEM-formatted files. The following commands were modified by this feature: <code>enrollment, enrollment terminal</code>.</td>
</tr>
<tr>
<td>Key Rollover for Certificate Renewal</td>
<td>12.3(7)T</td>
<td>This feature allows the certificate renewal request to be made before the certificate expires and retains the old key and certificate until the new certificate is available. The following commands were introduced or modified by this feature: <code>auto-enroll, regenerate</code>.</td>
</tr>
<tr>
<td><strong>Feature Name</strong></td>
<td><strong>Releases</strong></td>
<td><strong>Feature Information</strong></td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td><strong>Manual Certificate Enrollment (TFTP Cut-and-Paste)</strong></td>
<td>12.2(13)T</td>
<td>This feature allows users to generate a certificate request and accept CA certificates and the router’s certificates via a TFTP server or manual cut-and-paste operations. The following commands were introduced or modified by this feature: <strong>crypto ca import, enrollment, enrollment terminal</strong>.</td>
</tr>
<tr>
<td><strong>Multiple-Tier CA Hierarchy</strong></td>
<td>12.2(15)T</td>
<td>This enhancement enables users to set up a PKI in a hierarchical framework to support multiple CAs. Within a hierarchical PKI, all enrolled peers can validate the certificate of one another as long as the peers share a trusted root CA certificate or a common subordinate CA. <strong>Note</strong> This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.</td>
</tr>
<tr>
<td><strong>Persistent Self-Signed Certificates</strong></td>
<td>12.2(33)SXH 12.2(33)SRA 12.3(14)T</td>
<td>This feature allows the HTTPS server to generate and save a self-signed certificate in the router startup configuration. Thus, future SSL handshakes between the client and the HTTPS server can use the same self-signed certificate without user intervention. The following commands were introduced or modified by this feature: <strong>enrollment selfsigned, show crypto pki certificates, show crypto pki trustpoints</strong>.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PKI Status</td>
<td>12.3(11)T</td>
<td>This enhancement adds the <code>status</code> keyword to the <code>show crypto pki trustpoints</code> command, which allows you to display the current status of the trustpoint.</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.</td>
</tr>
<tr>
<td>Public Key Infrastructure (PKI) IPv6 Support for VPN Solutions</td>
<td>15.2(1)T</td>
<td>The <code>enrollment url (ca-trustpoint)</code> command was modified to allow the specification of an IPv6 address in the URL for the CA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The <code>ip-address (ca-trustpoint)</code> command was modified to allow the specification of an IPv6 address that is included as “unstructuredAddress” in the certificate request.</td>
</tr>
<tr>
<td>Public Key Infrastructure (PKI) IPv6 Support for VPN Solutions</td>
<td>15.2(1)T</td>
<td>The <code>enrollment url (ca-trustpoint)</code> command was modified to allow the specification of an IPv6 address in the URL for the CA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The <code>ip-address (ca-trustpoint)</code> command was modified to allow the specification of an IPv6 address that is included as “unstructuredAddress” in the certificate request.</td>
</tr>
<tr>
<td>Reenroll Using Existing Certificates</td>
<td>12.3(11)T</td>
<td>This feature allows users to reenroll a router with a Cisco IOS CA via existing certificates from a third-party vendor CA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following commands were introduced by this feature: <code>enrollment credential, grant auto trustpoint</code>.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Suite-B support in IOS SW crypto</td>
<td>15.1(2)T</td>
<td>Suite-B adds the following support for certificate enrollment for a PKI:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Elliptic Curve Digital Signature Algorithm (ECDSA) (256 bit and 384 bit curves) is used for the signature operation within X.509 certificates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PKI support for validation of X.509 certificates using ECDSA signatures.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PKI support for generating certificate requests using ECDSA signatures and for importing the issued certificates into IOS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suite-B requirements comprise of four user interface suites of cryptographic algorithms for use with IKE and IPsec that are described in RFC 4869. Each suite consists of an encryption algorithm, a digital signature algorithm, a key agreement algorithm, and a hash or message digest algorithm. See the Configuring Security for VPNs with IPsec feature module for more detailed information about Cisco IOS Suite-B support.</td>
</tr>
<tr>
<td>Trustpoint CLI</td>
<td>12.2(8)T</td>
<td>This feature introduces the <code>crypto pki trustpoint</code> command, which adds support for trustpoint CAs.</td>
</tr>
</tbody>
</table>