Configuring Certificate Enrollment for a PKI

First Published: May 2, 2005
Last Updated: March 31, 2011

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.

Finding Feature Information in This Module

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 for PKI Certificate Enrollment” section on page 38.

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

Contents

- Prerequisites for PKI Certificate Enrollment, page 2
- Information About Certificate Enrollment for a PKI, page 2
- How to Configure Certificate Enrollment for a PKI, page 6
- Configuration Examples for PKI Certificate Enrollment Requests, page 27
- Additional References, page 36
- Feature Information for PKI Certificate Enrollment, page 38
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.”

Note: 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

Before configuring peers to request a certificate and enroll in the PKI, you should understand the following concepts:

- What Are CAs?, page 2
- Authentication of the CA, page 3
- Supported Certificate Enrollment Methods, page 3
- Registration Authorities, page 4
- Automatic Certificate Enrollment, page 5
- Certificate Enrollment Profiles, page 6

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.

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.

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.

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

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—The router sends HTTP-based enrollment requests directly to the CA server instead of to the RA-mode certificate server (CS). Enrollment profiles can be used if a CA server does not support SCEP.

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 Cisco IOS Security Configuration Guide: Secure Connectivity.

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.

*Note*

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.

**Note**
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, page 6
- Configuring Manual Certificate Enrollment, page 12
- Configuring a Persistent Self-Signed Certificate for Enrollment via SSL, page 21
- Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment, page 24

Configuring Certificate Enrollment or Autoenrollment

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

Prerequisites for Autoenrollment

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.


### 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.

### Restrictions for Autoenrollment

**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.

### SUMMARY STEPS

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:**  
  Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**  
  Router# configure terminal | |
| **Step 3** crypto pki trustpoint name | Declares the trustpoint and a given name and enters ca-trustpoint configuration mode. |
| **Example:**  
  Router(config)# crypto pki trustpoint mytp | |
| **Step 4** enrollment [mode] [retry period minutes] [retry count number] url url [pem] | Specifies the URL of the CA on which your router should send certificate requests.  
  • **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. For enrollment method options, see the enrollment command in the Cisco IOS Security Command Reference.  
  • **pem**—Adds privacy-enhanced mail (PEM) boundaries to the certificate request. |
| **Example:**  
  Router(ca-trustpoint)# enrollment url http://cat.example.com | |
| **Step 5** eckeypair label | (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. |
| **Example:**  
  Router(ca-trustpoint)# eckeypair Router_1_Key | |
### How to Configure Certificate Enrollment for a PKI

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td><code>subject-name</code> [x.500-name]</td>
<td>(Optional) Specifies the requested subject name that will be used in the certificate request.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(ca-trustpoint)# subject-name cat</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>ip address</code> {(ip-address</td>
<td>interface</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(ca-trustpoint)# ip address 192.168.1.66</code></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td><code>serial-number</code> [none]</td>
<td>(Optional) Specifies the router serial number in the certificate request, unless the <code>none</code> keyword is issued.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(ca-trustpoint)# serial-number</code></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><code>auto-enroll</code> [percent] [regenerate]</td>
<td>(Optional) Enables autoenrollment, allowing the client to automatically request a rollover certificate from the CA.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(ca-trustpoint)# auto-enroll regenerate</code></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td><code>usage</code> method1 [method2 [method3]] | Method2 [Method3]</td>
<td>(Optional) Specifies the intended use for the certificate.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(ca-trustpoint)# usage ssl-client</code></td>
<td></td>
</tr>
</tbody>
</table>

**Note**
- If autoenrollment is not enabled, the client must be manually reenrolled 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.”
- It is recommended that a new key pair be generated for security reasons.
### Configuring Certificate Enrollment for a PKI

#### How to Configure Certificate Enrollment for a PKI

<table>
<thead>
<tr>
<th>Step 11</th>
<th><strong>password string</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# password string1</td>
<td>(Optional) Specifies the revocation password for the certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- If this command is enabled, you will not be prompted for a password during enrollment for this trustpoint.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> When SCEP is used, this password can be used to authorize the certificate request—often via a one-time password or similar mechanism.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 12</th>
<th><strong>rsakeypair key-label [key-size [encryption-key-size]]</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# rsakeypair cat</td>
<td>(Optional) Specifies which key pair to associate with the certificate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- A key pair with the <code>key-label</code> argument will be generated during enrollment if it does not already exist or if the <code>auto-enroll regenerate</code> command was issued.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Specify the <code>key-size</code> argument for generating the key, and specify the <code>encryption-key-size</code> argument to request separate encryption, signature keys, and certificates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> If this command is not enabled, the FQDN key pair is used.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 13</th>
<th><strong>fingerprint ca-fingerprint</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E</td>
<td>(Optional) Specifies a fingerprint that can be matched against the fingerprint of a CA certificate during authentication.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> If the fingerprint is not provided and authentication of the CA certificate is interactive, the fingerprint will be displayed for verification.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 14</th>
<th><strong>on devicename:</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# on usbtoken0:</td>
<td>(Optional) Specifies that RSA keys will be created on the specified device upon autoenrollment initial key generation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 15</th>
<th><strong>exit</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# exit</td>
<td>Exits ca-trustpoint configuration mode and returns to global configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 16</th>
<th><strong>crypto pki authenticate name</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# crypto pki authenticate mytp</td>
<td>Retrieves the CA certificate and authenticates it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Check the certificate fingerprint if prompted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> This command is optional if the CA certificate is already loaded into the configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 17</th>
<th><strong>exit</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# exit</td>
<td>Exits global configuration mode.</td>
</tr>
</tbody>
</table>
How to Configure Certificate Enrollment for a PKI

Configuring Certificate Enrollment for a PKI

12

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:

- Configuring Cut-and-Paste Certificate Enrollment, page 12
- Configuring TFTP Certificate Enrollment, page 14
- Certifying a URL Link for Secure Communication with a Trend Micro Server, page 17

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 Cisco IOS 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 18 copy system:running-config nvram:startup-config</td>
<td>(Optional) Copies the running configuration to the NVRAM startup configuration.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# copy system:running-config nvram:startup-config</td>
</tr>
<tr>
<td>Step 19 show crypto pki certificates</td>
<td>(Optional) Displays information about your certificates, including any rollover certificates.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# show crypto pki certificates</td>
</tr>
</tbody>
</table>

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:

- Configuring Cut-and-Paste Certificate Enrollment, page 12
- Configuring TFTP Certificate Enrollment, page 14
- Certifying a URL Link for Secure Communication with a Trend Micro Server, page 17

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 Cisco IOS 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><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></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> <code>crypto pki trustpoint name</code></td>
<td>Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.</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><strong>Step 4</strong> <code>enrollment terminal [pem]</code></td>
<td>Specifies the manual cut-and-paste certificate enrollment method.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# enrollment terminal</td>
<td>• The certificate request will be displayed on the console terminal so that it may be manually copied (or cut).</td>
</tr>
<tr>
<td></td>
<td>• <code>pem</code>—Configures the trustpoint to generate PEM-formatted certificate requests to the console terminal.</td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>fingerprint ca-fingerprint</code></td>
<td>(Optional) Specifies a fingerprint that can be matched against the fingerprint of a CA certificate during authentication.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E</td>
<td><strong>Note</strong> If the fingerprint is not provided, it will be displayed for verification.</td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>exit</code></td>
<td>Exits ca-trustpoint configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# exit</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Certificate Enrollment for a PKI

#### Command or Action

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

<table>
<thead>
<tr>
<th>Step 8</th>
<th>crypto pki enroll name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# crypto pki enroll mytp</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Generates certificate request and displays the request for copying and pasting into the certificate server.</td>
</tr>
<tr>
<td>-</td>
<td>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.</td>
</tr>
<tr>
<td>-</td>
<td>The base-64 encoded certificate with or without PEM headers as requested is displayed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 9</th>
<th>crypto pki import name certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# crypto pki import mytp certificate</td>
</tr>
<tr>
<td><strong>Purpose:</strong></td>
<td>Imports a certificate manually at the console terminal (pasting).</td>
</tr>
<tr>
<td>-</td>
<td>The base-64 encoded certificate is accepted from the console terminal and inserted into the internal certificate database.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

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

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

### 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.
Prerequisites for TFTP Certificate Enrollment

- 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></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</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><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 3** crypto pki trustpoint name | Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.

**Example:**
Router(config)# crypto pki trustpoint mytp

**Step 4** enrollment [mode] [retry period minutes] [retry count number] url url [pem] | Specifies TFTP as the enrollment method to send the enrollment request and to retrieve the CA certificate and router certificate and any optional parameters.

**Example:**
Router(ca-trustpoint)# enrollment url tftp://certserver/file_specification

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.

**Step 5** fingerprint ca-fingerprint | (Optional) Specifies the fingerprint of the CA certificate received via an out-of-band method from the CA administrator.

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

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

**Step 6** exit | Exits ca-trustpoint configuration mode and returns to global configuration mode.

**Example:**
Router(ca-trustpoint)# exit

**Step 7** crypto pki authenticate name | Retrieves the CA certificate and authenticates it from the specified TFTP server.

**Example:**
Router(config)# crypto pki authenticate mytp

**Step 8** crypto pki enroll name | Generates certificate request and writes the request out to the TFTP server.

**Example:**
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 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.
Configuring Certificate Enrollment for a PKI

How to Configure Certificate Enrollment for a PKI

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.

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 9: crypto pki import name certificate</td>
<td>Imports a certificate via TFTP at the console terminal, which retrieves the granted certificate.</td>
</tr>
<tr>
<td>Example:</td>
<td>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.</td>
</tr>
<tr>
<td>Step 10: exit</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>The router will parse the received files, verify the certificates, and insert the certificates into the internal certificate database on the router.</td>
</tr>
<tr>
<td>Step 11: show crypto pki certificates</td>
<td>(Optional) Displays information about your certificates, the certificates of the CA, and RA certificates.</td>
</tr>
</tbody>
</table>

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.
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> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>clock set hh:mm:ss date month year</code></td>
<td>Sets the clock on the router.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# clock set 23:22:00 22 Dec 2009</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>clock timezone zone hours-offset [minutes-offset]</code></td>
<td>Sets the time zone.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# clock timezone PST -08</td>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>ip http server</code></td>
<td>Enables the HTTP server.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# ip http server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> <code>hostname name</code></td>
<td>Configures the hostname of the router.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# hostname hostname1</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command/Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td><code>ip domain-name name</code></td>
<td>Defines the domain name for the router.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Router(config)# <code>ip domain-name example.com</code></td>
</tr>
<tr>
<td>8</td>
<td><code>crypto key generate rsa general-keys modulus modulus-size</code></td>
<td>Generates the crypto keys.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Router(config)# <code>crypto key generate rsa general-keys modulus general</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>The <code>general-keys</code> keyword specifies that a general purpose key pair is generated, which is the default. The <code>modulus</code> keyword and <code>modulus-size</code> argument specify the IP size of the key modulus. By default, the modulus of a CA key is 1024 bits. Choose the size of the key modulus in the range of 360 to 2048 for your general purpose keys. If you choose a key modulus value greater than 512, the router may require a few minutes to process the command.</td>
</tr>
<tr>
<td>9</td>
<td><code>crypto pki trustpoint name</code></td>
<td>Declares the CA that your router should use and enters ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Router(config)# <code>crypto pki trustpoint mytp</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>Effective with Cisco IOS Release 12.3(8)T, the <code>crypto pki trustpoint</code> command replaced the <code>crypto ca trustpoint</code> command.</td>
</tr>
<tr>
<td>10</td>
<td><code>enrollment terminal</code></td>
<td>Specifies the manual cut-and-paste certificate enrollment method.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# <code>enrollment terminal</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></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><code>crypto ca authenticate name</code></td>
<td>Takes the name of the CA as the argument and authenticates it.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td>Router(ca-trustpoint)# <code>crypto ca authenticate mytp</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
**Command or Action**

**Purpose**

**Step 12** Copy the following block of text containing the base 64 encoded CA certificate and paste it at the prompt.

```
MIIDIDCCAomgAwIBAgIENd70zzANBgkqhkiG9w0BAQUFADBOMQs
wCQYDVQQGEwJV
UzEQMA4GA1UEChMHRXF1aW2heDhEcMAsGA1UECxMkRXF1aW2heCB
TZWN1cnUgUmQwMQ0wCwYDVQQDEwRDUkwxMBoGA1UdEwQFMBwMB
A4GA1UdEwEB/wQCMAAwMB0GA1UdDgQMBwEB/wQCMAAwMB0GA1UdDgQ
MBwMBAAoadDQG

The following command output displays:

Certificate has the following attributes:
Fingerprint MD5: 67CB9DC0 13248A82 9BB2171E D11BECD4
Fingerprint SHA1: D23209AD 23D31423 2174E40D 7F9D6213 9786633A
```

**Step 13** Enter yes to accept this certificate.

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

The following command output displays:

Trustpoint CA certificate accepted.
```
Certificate successfully imported
```

**Step 14** serial-number

*Example:*

```
hostname1(ca-trustpoint)# serial-number
```

Specifies the router serial number in the certificate request.

**Step 15** revocation-check none

*Example:*

```
hostname1(ca-trustpoint)# revocation-check none
```

Specifies that certificate checking is ignored.
Configuring Certificate Enrollment for a PKI

How to Configure Certificate Enrollment for a PKI

This section contains the following tasks:

- Configuring a Trustpoint and Specifying Self-Signed Certificate Parameters, page 22
- Enabling the HTTPS Server, page 23

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

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.
Configuring Certificate Enrollment for a PKI

**How to Configure Certificate Enrollment for a PKI**

**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**

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>
</table>
| **Step 1** `enable` | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
| **Example:**  
  `Router> enable` |  |
| **Step 2** `configure terminal` | Enters global configuration mode. |
| **Example:**  
  `Router# configure terminal` |  |
| **Step 3** `crypto pki trustpoint name` | Declares the CA that your router should use and enters ca-trustpoint configuration mode.  
  **Note** Effective with Cisco IOS Release 12.3(8)T, the `crypto pki trustpoint` command replaced the `crypto ca trustpoint` command. |
| **Example:**  
  `Router(config)# crypto pki trustpoint local` |  |
| **Step 4** `enrollment selfsigned` | Specifies self-signed enrollment. |
| **Example:**  
  `Router(ca-trustpoint)# enrollment selfsigned` |  |
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 5    | subject-name [x.500-name] | (Optional) Specifies the requested subject name to be used in the certificate request.  
- If no value for the x.500-name argument is specified, the FQDN, which is the default subject name, is used. |
| 6    | rsakeypair key-label [key-size [encryption-key-size]] | (Optional) Specifies which key pair to associate with the certificate.  
- The value for 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 a value for the key-size argument for generating the key, and specify a value for the encryption-key-size argument to request separate encryption, signature keys, and certificates.  
**Note** If this command is not enabled, the FQDN key pair is used. |
| 7    | crypto pki enroll name | Tells the router to generate the persistent self-signed certificate. |
| 8    | end | (Optional) Exits ca-trustpoint configuration mode.  
- Enter this command a second time to exit global configuration mode. |
| 9    | show crypto pki certificates [trustpoint-name [verbose]] | Displays information about your certificate, the certification authority certificate, and any registration authority certificates. |
| 10   | show crypto pki trustpoints [status | label [status]] | Displays the trustpoints that are configured in the router. |

### Enabling the HTTPS Server

Perform the following task to enable the HTTPS server.

### Prerequisites

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><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> ip http secure-server</td>
<td>Enables the HTTPS web server.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip http secure-server</td>
<td>Note: A key pair (modulus 1024) and a certificate are generated.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> copy system:running-config nvram: startup-config</td>
<td>Saves the self-signed certificate and the HTTPS server in enabled mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# copy system:running-config nvram: startup-config</td>
<td></td>
</tr>
</tbody>
</table>

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.
Prerequisites

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.

Restrictions

- 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. authentication url url
   or
   authentication terminal
8. authentication command
9. enrollment url url
   or
   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>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</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></td>
<td></td>
</tr>
<tr>
<td>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></td>
<td></td>
</tr>
<tr>
<td>crypto pki trustpoint name</td>
<td>Declares the trustpoint and a given name and enters ca-trustpoint</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>configuration mode.</td>
</tr>
<tr>
<td>Router(config)# crypto pki trustpoint Entrust</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>enrollment profile label</td>
<td>Specifies that an enrollment profile is to be used for certificate</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>authentication and enrollment.</td>
</tr>
<tr>
<td>Router(ca-trustpoint)# enrollment profile E</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits ca-trustpoint configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(ca-trustpoint)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>crypto pki profile enrollment label</td>
<td>Defines an enrollment profile and enters ca-profile-enroll</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>configuration mode.</td>
</tr>
<tr>
<td>Router(config)# crypto pki profile enrollment E</td>
<td>• label—Name for the enrollment profile; the enrollment profile name</td>
</tr>
<tr>
<td></td>
<td>must match the name specified in the enrollment profile command.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>authentication url url or</td>
<td>Specifies the URL of the CA server to which to send certificate</td>
</tr>
<tr>
<td></td>
<td>authentication requests.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• url—URL of the CA server to which your router should send authentication requests.</td>
</tr>
<tr>
<td>Router(ca-profile-enroll)# authentication url <a href="http://entrust:81">http://entrust:81</a></td>
<td>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.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Router(ca-profile-enroll)# authentication terminal</td>
<td>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.)</td>
</tr>
<tr>
<td></td>
<td>Specifies manual cut-and-paste certificate authentication.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>authentication command</td>
<td>(Optional) Specifies the HTTP command that is sent to the CA for</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>authentication.</td>
</tr>
<tr>
<td>Router(ca-profile-enroll)# authentication command</td>
<td></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.”

### Configuration Examples for PKI Certificate Enrollment Requests

This section contains the following configuration examples:

- Configuring Certificate Enrollment or Autoenrollment: Example, page 28
- Configuring Autoenrollment: Example, page 28
• Configuring Certificate Autoenrollment with Key Regeneration: Example, page 29
• Configuring Cut-and-Paste Certificate Enrollment: Example, page 29
• Configuring Manual Certificate Enrollment with Key Regeneration: Example, page 32
• Creating and Verifying a Persistent Self-Signed Certificate: Example, page 33
• Configuring Direct HTTP Enrollment: Example, page 35

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
  revocation-check none
  rsakeypair myTP-A
  storage usbtoken0:
! Specifies that keys will be stored on usbtoken0:
  on usbtoken0:
! Specifies that keys generated on initial auto enroll will be generated on and stored on
  ! usbtoken0:

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
certificate pki 0B
  30820293 3082023D A0030201 0202010B 300D0609 2A864886 F70D0101 04050030
  79310B30 09060355 04061302 5553310B 30090603 55040813 02434131 15301306
  0355040A 130C4369 73366F20 53797374 656D706C 69676E20 6966617368696E6720
  6573697374 69737320 301E0603 55040B13 17737562
  6E726F6D 61642D 3433352E 636F6E6C7973737465727370726f6e657221 49140E22
  06035504 0A130543 6973636F 3120301E 06092A86 4886F70D 01090216 170706B9
  2D143562 2E36973 63F2DE6 6F6D305C 30006D20 2A864886 F70D0101 01050003
  4B003408 241008B3 0512A01 3B4243E1 378A9703 8AC5E3CE F77AF987 B5A422C4
  15E947F6 70997393 70CF34D6 63A86B9C 4347A81A 0551FC02 ABA62360 01EF7DD2
Configuring Certificate Enrollment for a PKI

Configuration Examples for PKI Certificate Enrollment Requests

In this example, keys are neither regenerated nor rolled over.

---

**Configuring Certificate Autoenrollment with Key Regeneration: Example**

The following example shows how to configure the router to automatically enroll with the CA named “trustme1” on startup and enable automatic rollover. The `regenerate` keyword is issued, so a new key will be generated for the certificate and reissued when the automatic rollover process is initiated. The renewal percentage is configured as 90 so if the certificate has a lifetime of one year, a new certificate is requested 36.5 days before 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:

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

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

-----BEGIN CERTIFICATE-----
MIICNDCCAd6gAwIBAgIQOsCmXpVHwodKrYRoqULV7jANBgkqhkiG9w0BAQUFADA5
MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1yb290MB4XDTAyMDIxNDAwNDYwMVoXDTA3MDIxNDAwNTQ0OFowOTELMAkGA1UEBhMCVVMxFjAUBgNVBAMTCW1zY2Etcm9vdDBcMA0GCSqGSIb3DQEBAQUAA4NAYGh0dHA6Ly9jcmwvMjUvMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1yb290MB4XDTAyMDIxNDAwNDYwMVoXDTA3MDIxNDAwNTQ0OFowOTELMAkGA1UEBhMCVVMxFjAUBgNVBAMTCW1zY2Etcm9vdDBcMA0GCSqGSIb3DQEBAQUAA4NAYGh0dHA6Ly9jcmwvMjUv
```

quit
AAGjcEwgb4wCVYDVR0PBQAqDAQHcGMAAGA1gDDwEB/wQFMMAAFA8wHtQYDVOR0JBBgYF
K1acm16D4SuDQOqYm1S9n5eSF8jM3G0A1HwmmQQQwL6AnOcUCuK8H0dHAl4Ly9t
c2NhLXvb3QVoQVYdVYEcUm9eb9tC2NhKXvb3QUj3aNDGqL6AthimaWx1oi8v
XFeRtsc2NhLXvb3QrcV2yvEyEcum9ebFsc2NhLXvb3QUj3sMBAGCSgQAQQbjcV
AQDDAgEAMsARcSgDI3DQEBQUA0A1EeuZ2kZX9qkoLHefTytPvWJ2Q0QmwwNRA
oJDSYdJL3bCI/ULL5Q7EmOyDyfLItYyxuhqYx5r/40a5QqLcrgq+y==
------END CERTIFICATE------

Certificate has the following attributes:
Fingerprint: D6C12961 CD78808A 0790082A
% 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]: n
% Include an IP address in the subject name? [no]: n
% Display Certificate Request to terminal? [yes/no]: y
Signature key certificate request -
Certificate Request follows:
MIIBhTCB7wIBADAlMwYIKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBznANBgkgklh10Wg0BAQFFEPAABBjAQwYKCGYeAxdhXFD1WAn/hI2z9zf0tsKKA
da0wYu0m59F/Pe0Wdl9h14XvQx0M02Pr5wk6jLOPpxv0JHMYN6ipLmyVxv
0jtyLxTrcohhDnmqevaGHzv/90has99fRXwCNXw042qChFnx9EKMuC7evrwRKEqR
mBHxZ80mF3jYqjwS8KCAwEAAAAMBB88C6gS1bDQ2dA1jRQ5jgESMBAwDyVlR0EAgH/
BAQDDAgeAMA0GCSqGSlbDQEBBAAA4AGBAR76WtcFw95POY7UcP+YIYN1XUUF4Cq/
hrA1RjL1tePeloU1hyPULpnt83j1Z5P8H3MfgPRaqodaWb6mubkzahb1j0G06
087fnLcR1d5Tv5J9kgFHtki2iEGZxBoUw9Uj1lenQdNdpBjcS5lYxwFdvcia6j0
N8rOtKnt8Q+
 ! !

Disdisplay enrollment request? [yes/no]: Encryption key certificate request -
Certificate Request follows:
MIIBhTCB7wIBADAlMwYIKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBznANBgkgklh10Wg0BAQFFEPAABBjAQwYKCGYeAxdhXFD1WAn/hI2z9zf0tsKKA
da0wYu0m59F/Pe0Wdl9h14XvQx0M02Pr5wk6jLOPpxv0JHMYN6ipLmyVxv
0jtyLxTrcohhDnmqevaGHzv/90has99fRXwCNXw042qChFnx9EKMuC7evrwRKEqR
mBHxZ80mF3jYqjwS8KCAwEAAAAMBB88C6gS1bDQ2dA1jRQ5jgESMBAwDyVlR0EAgH/
BAQDDAgeAMA0GCSqGSlbDQEBBAAA4AGBAR76WtcFw95POY7UcP+YIYN1XUUF4Cq/
hrA1RjL1tePeloU1hyPULpnt83j1Z5P8H3MfgPRaqodaWb6mubkzahb1j0G06
087fnLcR1d5Tv5J9kgFHtki2iEGZxBoUw9Uj1lenQdNdpBjcS5lYxwFdvcia6j0
N8rOtKnt8Q+
 ! !

Redisplay enrollment request? [yes/no]: Encryption key certificate request -
Certificate Request follows:
MIIBhTCB7wIBADAlMwYIKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBznANBgkgklh10Wg0BAQFFEPAABBjAQwYKCGYeAxdhXFD1WAn/hI2z9zf0tsKKA
da0wYu0m59F/Pe0Wdl9h14XvQx0M02Pr5wk6jLOPpxv0JHMYN6ipLmyVxv
0jtyLxTrcohhDnmqevaGHzv/90has99fRXwCNXw042qChFnx9EKMuC7evrwRKEqR
mBHxZ80mF3jYqjwS8KCAwEAAAAMBB88C6gS1bDQ2dA1jRQ5jgESMBAwDyVlR0EAgH/
BAQDDAgeAMA0GCSqGSlbDQEBBAAA4AGBAR76WtcFw95POY7UcP+YIYN1XUUF4Cq/
hrA1RjL1tePeloU1hyPULpnt83j1Z5P8H3MfgPRaqodaWb6mubkzahb1j0G06
087fnLcR1d5Tv5J9kgFHtki2iEGZxBoUw9Uj1lenQdNdpBjcS5lYxwFdvcia6j0
N8rOtKnt8Q+
 ! !

Redisplay enrollment request? [yes/no]: Encryption key certificate request -
Certificate Request follows:
MIIBhTCB7wIBADAlMwYIKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBznANBgkgklh10Wg0BAQFFEPAABBjAQwYKCGYeAxdhXFD1WAn/hI2z9zf0tsKKA
da0wYu0m59F/Pe0Wdl9h14XvQx0M02Pr5wk6jLOPpxv0JHMYN6ipLmyVxv
0jtyLxTrcohhDnmqevaGHzv/90has99fRXwCNXw042qChFnx9EKMuC7evrwRKEqR
mBHxZ80mF3jYqjwS8KCAwEAAAAMBB88C6gS1bDQ2dA1jRQ5jgESMBAwDyVlR0EAgH/
BAQDDAgeAMA0GCSqGSlbDQEBBAAA4AGBAR76WtcFw95POY7UcP+YIYN1XUUF4Cq/
hrA1RjL1tePeloU1hyPULpnt83j1Z5P8H3MfgPRaqodaWb6mubkzahb1j0G06
087fnLcR1d5Tv5J9kgFHtki2iEGZxBoUw9Uj1lenQdNdpBjcS5lYxwFdvcia6j0
N8rOtKnt8Q+
 !!

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

30
cb5jc3N0cml0ZVh1c3RuJmdlLm9uZ2VuZ21cOl9mZG5zOl9wYXJpZ2h0MS9oZWFsLm5ldDAM

% Router Certificate successfully imported

You can verify that the certificate was successfully imported by issuing the command:

Routere# show crypto pki certificates

Certificate
Status: Available
Certificate Serial Number: 14DBECE0000000000000C48
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

% Router Certificate successfully imported

You can verify that the certificate was successfully imported by issuing the command:

Routere# show crypto pki certificates

Certificate
Status: Available
Certificate Serial Number: 14DBECE0000000000000C48
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
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 2048s
  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)#

Note
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 8D003081 89028181 00B88F70
  6BC78B6D 67D6CFF3 135C1D91 8F360292 CA44A032 5AC1A8FD 095E8465 F8C95A2B
  BFD1C2B7 E64A3804 9BBD7326 207BD456 19BAB788 D075E78E 0D2560C0 B09289AE
  6DECB8B0 6672FB3A 5CDAE929 9D4C4F71 F3BEB269 214F6293 4B88FBAB 9486BCFC
  2B941B9A 550999A7 2EFE12A9 6B7B669A 2D8BAB77 3FB38E0E 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 0D010101 05000381 8D003081 89028181 00B88F70
  6BC78B6D 67D6CFF3 135C1D91 8F360292 CA44A032 5AC1A8FD 095E8465 F8C95A2B
  BFD1C2B7 E64A3804 9BBD7326 207BD456 19BAB788 D075E78E 0D2560C0 B09289AE
  6DECB8B0 6672FB3A 5CDAE929 9D4C4F71 F3BEB269 214F6293 4B88FBAB 9486BCFC
  2B941B9A 550999A7 2EFE12A9 6B7B669A 2D8BAB77 3FB38E0E AA23CB8C B7020301 0001

Note
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
authentication command GET /certs/cacert.der
enrollment url http://entrust:81/cda-cgi/clientcgi.exe
enrollment command POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
parameter 1 value aaaa-bbbb-cccc
parameter 2 value 5001
## 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 <em>Cisco IOS Security Configuration Guide: Secure Connectivity</em></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 <em>Cisco IOS Security Configuration Guide: Secure Connectivity</em></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 <em>Cisco IOS Security Configuration Guide: Secure Connectivity</em></td>
</tr>
<tr>
<td>RSA key generation and deployment</td>
<td>“Deploying RSA Keys Within a PKI” module in the <em>Cisco IOS Security Configuration Guide: Secure Connectivity</em></td>
</tr>
<tr>
<td>Cisco IOS certificate server overview information and configuration tasks</td>
<td>“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” module in the <em>Cisco IOS Security Configuration Guide: Secure Connectivity</em></td>
</tr>
<tr>
<td>Setting up and using a USB token</td>
<td>“Storing PKI Credentials” module in the <em>Cisco IOS Security Configuration Guide: Secure Connectivity</em></td>
</tr>
<tr>
<td>Cisco IOS security commands</td>
<td><em>Cisco IOS Security Command Reference</em></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>
<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>
</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,</td>
</tr>
<tr>
<td></td>
<td>and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
<tr>
<td>download documentation, software, and tools. Use these resources to install</td>
<td></td>
</tr>
<tr>
<td>and configure the software and to troubleshoot and resolve technical</td>
<td></td>
</tr>
<tr>
<td>issues with Cisco products and technologies. Access to most tools on the</td>
<td></td>
</tr>
<tr>
<td>Cisco Support and Documentation website requires a Cisco.com user ID and</td>
<td></td>
</tr>
<tr>
<td>password.</td>
<td></td>
</tr>
</tbody>
</table>
Feature Information for PKI Certificate Enrollment

Table 1 lists the release history for this feature.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 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.

<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. The following section provides information about this feature:  
  - Configuring Certificate Enrollment or Autoenrollment  
  Note: This document describes the use of utilizing USB tokens for RSA operations during initial autoenrollment for a trustpoint. For other documents on this topic, see the “Related Documents” section. |
| 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 sections provide information about this feature:  
  - Automatic Certificate Enrollment  
  - Configuring Certificate Enrollment or Autoenrollment  
  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. |
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.

The following sections provide information about this feature:
- Automatic Certificate Enrollment
- Configuring Certificate Enrollment or Autoenrollment

The following commands were introduced by this feature: `auto-enroll`, `rsakeypair`, `show crypto ca timers`.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Autoenrollment</td>
<td>12.2(8)T</td>
<td>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. The following sections provide information about this feature: - Automatic Certificate Enrollment - Configuring Certificate Enrollment or Autoenrollment The following commands were introduced by this feature: <code>auto-enroll</code>, <code>rsakeypair</code>, <code>show crypto ca timers</code>.</td>
</tr>
<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 section provides information about this feature: - Configuring Certificate Enrollment or Autoenrollment The following commands were introduced by this feature: <code>ip-address</code> (ca-trustpoint), <code>password</code> (ca-trustpoint), <code>serial-number</code>, <code>subject-name</code>, <code>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 sections provide information about this feature: - Certificate Enrollment Profiles - Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment The following commands were introduced by this feature: <code>authentication command</code>, <code>authentication terminal</code>, <code>authentication url</code>, <code>crypto ca profile enrollment</code>, <code>enrollment command</code>, <code>enrollment profile</code>, <code>enrollment terminal</code>, <code>enrollment url</code>, <code>parameter</code>.</td>
</tr>
</tbody>
</table>
### Table 1  Feature Information for PKI Certificate Enrollment (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Import of RSA Key Pair and Certificates in PEM Format | 12.3(4)T | This feature allows customers to issue certificate requests and receive issued certificates in PEM-formatted files. The following section provides information about this feature:  
  - Configuring Manual Certificate Enrollment  
  The following commands were modified by this feature: enrollment, enrollment terminal. |
| Key Rollover for Certificate Renewal               | 12.3(7)T | 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 sections provide information about this feature:  
  - Automatic Certificate Enrollment  
  - Configuring Certificate Enrollment or Autoenrollment  
  - Configuring Manual Certificate Enrollment  
  The following commands were introduced or modified by this feature: auto-enroll, regenerate. |
| Manual Certificate Enrollment (TFTP Cut-and-Paste) | 12.2(13)T| 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 sections provide information about this feature:  
  - Supported Certificate Enrollment Methods  
  - Configuring Manual Certificate Enrollment  
  The following commands were introduced or modified by this feature: crypto ca import, enrollment, enrollment terminal. |
| Multiple-Tier CA Hierarchy                        | 12.2(15)T| 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.  
The following section provides information about this enhancement:  
  - Framework for Multiple CAs  
  **Note** This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator. |
Table 1  Feature Information for PKI Certificate Enrollment (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Persistent Self-Signed Certificates | 12.2(33)SXH 12.2(33)SRA 12.3(14)T | 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 sections provide information about this feature:  
  - Supported Certificate Enrollment Methods  
  - Configuring a Persistent Self-Signed Certificate for Enrollment via SSL  
    The following commands were introduced or modified by this feature: `enrollment selfsigned`, `show crypto pki certificates`, `show crypto pki trustpoints`. |
| PKI Status                          | 12.3(11)T        | This enhancement adds the `status` keyword to the `show crypto pki trustpoints` command, which allows you to display the current status of the trustpoint. Prior to this enhancement, you had to issue the `show crypto pki certificates` and the `show crypto pki timers` commands for the current status. The following section provides information about this enhancement:  
  - How to Configure Certificate Enrollment for a PKI  
    **Note** This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator. |
| Reenroll Using Existing Certificates| 12.3(11)T        | This feature allows users to reenroll a router with a Cisco IOS CA via existing certificates from a third-party vendor CA. The following section provides information about this enhancement:  
  - Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment  
    The following commands were introduced by this feature: `enrollment credential`, `grant auto trustpoint`. |
Trustpoint CLI

Suite-B support in IOS SW crypto

Table 1  Feature Information for PKI Certificate Enrollment (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<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>
<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>
</tbody>
</table>

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.

The following sections provide information about this feature:

- Cisco IOS Suite-B Support for Certificate Enrollment for a PKI, page 4
- Configuring Certificate Enrollment or Autoenrollment, page 6

The following commands were introduced or modified:
Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005–2010 Cisco Systems, Inc. All rights reserved.