



Configuring Certificate Enrollment for a PKI

Last Updated: October 9, 2012

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.



Note

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

- [Finding Feature Information](#), page 1
- [Prerequisites for PKI Certificate Enrollment](#), page 1
- [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 32
- [Additional References](#), page 39
- [Feature Information for PKI Certificate Enrollment](#), page 41

Finding Feature Information

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

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

Prerequisites for PKI Certificate Enrollment

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



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- 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

- [What Are CAs, page 2](#)
- [Framework for Multiple CAs, page 2](#)
- [Authentication of the CA, page 3](#)
- [Supported Certificate Enrollment Methods, page 3](#)
- [Registration Authorities, page 4](#)
- [Automatic Certificate Enrollment, page 4](#)
- [Certificate Enrollment Profiles, page 5](#)

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, page 4](#)

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 sever. This automatic router request eliminates the need for operator intervention when the enrollment request is sent to the CA server. Automatic enrollment is performed on startup for any trustpoint CA that is

configured and that does not have a valid client certificate. When the certificate expires, a new certificate is automatically requested.

**Note**

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

Automated Client Certificate and Key Rollover

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

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

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

**Tip**

If CA autoenrollment is not enabled, you may manually initiate rollover on an existing client with the **crypto pki enroll** command if the expiration time of the current client certificate is equal to or greater than the expiration time of the corresponding CA certificate. The client will initiate the rollover process, which occurs only if the server is configured for automated rollover and has an available rollover server certificate.

**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 23](#)
- [Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment, page 28](#)

Configuring Certificate Enrollment or Autoenrollment

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

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

Prerequisites for Enabling Automated Client Certificate and Key Rollover

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

- Your network devices must support shadow PKI.
- Your clients must be running Cisco IOS Release 12.4(2)T or a later release.
- The client's CS must support automatic rollover. See the section "Automatic CA Certificate and Key Rollover" in the chapter "Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment" of the *Public Key Infrastructure Configuration Guide* for more information on CA server automatic rollover configuration.

Prerequisites for Specifying Autoenrollment Initial Key Generation Location

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

**Note****RSA Key Pair Restriction for Autoenrollment**

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

Restrictions for Automated Client Certificate and Key Rollover

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

- SCEP must be used to support rollover. Any device that enrolls with the PKI using an alternative to SCEP as the certificate management protocol or mechanism (such as enrollment profiles, manual enrollment, or TFTP enrollment) will not be able to take advantage of the rollover functionality provided by SCEP.
- If the configuration cannot be saved to the startup configuration after a shadow certificate is generated, rollover will not occur.

>

**Note**

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	crypto pki trustpoint <i>name</i> Example: <pre>Router(config)# crypto pki trustpoint mytp</pre>	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.

Command or Action	Purpose
<p>Step 4 enrollment [mode retry period <i>minutes</i> retry count <i>number</i>] url <i>url</i> [pem]</p> <p>Example:</p> <pre>Router(ca-trustpoint)# enrollment url http:// cat.example.com</pre>	<p>Specifies the URL of the CA on which your router should send certificate requests.</p> <ul style="list-style-type: none"> • mode --Specifies RA mode if your CA system provides an RA. • retry period <i>minutes</i> --Specifies the wait period between certificate request retries. The default is 1 minute between retries. • retry count <i>number</i> -- 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 <i>url</i> -- URL of the file system where your router should send certificate requests. An IPv6 address can be added in the URL enclosed in brackets. For example: <code>http:// [2001:DB8:1:1::1]:80</code>. For more enrollment method options, see the enrollment url (ca-trustpoint) command page. • pem -- Adds privacy-enhanced mail (PEM) boundaries to the certificate request. <p>Note An enrollment method other than TFTP or manual cut-and-paste must be configured to support autoenrollment.</p>
<p>Step 5 eckeypair <i>label</i></p> <p>Example:</p> <pre>Router(ca-trustpoint)# eckeypair Router_1_Key</pre>	<p>(Optional) Configures the trustpoint to use an Elliptic Curve (EC) key on which certificate requests are generated using ECDSA signatures. The <i>label</i> argument specifies the EC key label that is configured using the crypto key generate rsa or crypto key generate ec keysizes command in global configuration mode. See the Configuring Internet Key Exchange for IPsec VPNs feature module for more information.</p> <p>Note If an ECDSA signed certificate is imported without a trustpoint configuration, then the label defaults to the FQDN value.</p>
<p>Step 6 subject-name [<i>x.500-name</i>]</p> <p>Example:</p> <pre>Router(ca-trustpoint)# subject-name cat</pre>	<p>(Optional) Specifies the requested subject name that will be used in the certificate request.</p> <ul style="list-style-type: none"> • <i>x.500-name</i> --If it is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.
<p>Step 7 vrf <i>vrf-name</i></p> <p>Example:</p> <pre>Router(ca-trustpoint)# vrf myvrf</pre>	<p>(Optional) Specifies the the VRF instance in the public key infrastructure (PKI) trustpoint to be used for enrollment, certificate revocation list (CRL) retrieval, and online certificate status protocol (OCSP) status.</p>

Command or Action	Purpose
<p>Step 8 <code>ip-address {ip-address interface none}</code></p> <p>Example:</p> <pre>Router(ca-trustpoint)# ip address 192.168.1.66</pre>	<p>(Optional) Includes the IP address of the specified interface in the certificate request.</p> <ul style="list-style-type: none"> • Issue the <i>ip-address</i> argument to specify either an IPv4 or IPv6 address. • Issue the <i>interface</i> argument to specify an interface on the router. • Issue the none keyword if no IP address should be included. <p>Note If this command is enabled, you will not be prompted for an IP address during enrollment for this trustpoint.</p>
<p>Step 9 <code>serial-number [none]</code></p> <p>Example:</p> <pre>Router(ca-trustpoint)# serial- number</pre>	<p>(Optional) Specifies the router serial number in the certificate request, unless the none keyword is issued.</p> <ul style="list-style-type: none"> • Issue the none keyword to specify that a serial number will not be included in the certificate request.
<p>Step 10 <code>auto-enroll [percent] [regenerate]</code></p> <p>Example:</p> <pre>Router(ca-trustpoint)# auto- enroll regenerate</pre>	<p>(Optional) Enables autoenrollment, allowing the client to automatically request a rollover certificate from the CA.</p> <ul style="list-style-type: none"> • If autoenrollment is not enabled, the client must be manually re-enrolled in your PKI upon certificate expiration. • By default, only the Domain Name System (DNS) name of the router is included in the certificate. • Use the <i>percent</i> 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. <p>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.”</p> <p>Note It is recommended that a new key pair be generated for security reasons.</p>
<p>Step 11 <code>usage method1 [method2 [method3]]</code></p> <p>Example:</p> <pre>Router(ca-trustpoint)# usage ssl-client</pre>	<p>(Optional) Specifies the intended use for the certificate.</p> <ul style="list-style-type: none"> • Available options are ike, ssl-client, and ssl-server; the default is ike.
<p>Step 12 <code>password string</code></p> <p>Example:</p> <pre>Router(ca-trustpoint)# password string1</pre>	<p>(Optional) Specifies the revocation password for the certificate.</p> <ul style="list-style-type: none"> • If this command is enabled, you will not be prompted for a password during enrollment for this trustpoint. <p>Note When SCEP is used, this password can be used to authorize the certificate request--often via a one-time password or similar mechanism.</p>

Command or Action	Purpose
<p>Step 13 <code>rsakeypair key-label key-size encryption-key-size []</code></p> <p>Example:</p> <pre>Router(ca-trustpoint)# rsakeypair key-label 2048 2048</pre>	<p>(Optional) Specifies which key pair to associate with the certificate.</p> <ul style="list-style-type: none"> A key pair with the <i>key-label</i> argument will be generated during enrollment if it does not already exist or if the auto-enroll regenerate command was issued. Specify the <i>key-size</i> argument for generating the key, and specify the <i>encryption-key-size</i> argument to request separate encryption, signature keys, and certificates. The key-size and encryption-key-size must be the same size. Length of less than 2048 is not recommended. <p>Note If this command is not enabled, the FQDN key pair is used.</p>
<p>Step 14 <code>fingerprint ca-fingerprint</code></p> <p>Example:</p> <pre>Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E</pre>	<p>(Optional) Specifies a fingerprint that can be matched against the fingerprint of a CA certificate during authentication.</p> <p>Note If the fingerprint is not provided and authentication of the CA certificate is interactive, the fingerprint will be displayed for verification.</p>
<p>Step 15 <code>on devicename :</code></p> <p>Example:</p> <pre>Router(ca-trustpoint)# on usbtoken0:</pre>	<p>(Optional) Specifies that RSA keys will be created on the specified device upon autoenrollment initial key generation.</p> <ul style="list-style-type: none"> 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.
<p>Step 16 <code>exit</code></p> <p>Example:</p> <pre>Router(ca-trustpoint)# exit</pre>	<p>Exits ca-trustpoint configuration mode and returns to global configuration mode.</p>
<p>Step 17 <code>crypto pki authenticate name</code></p> <p>Example:</p> <pre>Router(config)# crypto pki authenticate mytp</pre>	<p>Retrieves the CA certificate and authenticates it.</p> <ul style="list-style-type: none"> Check the certificate fingerprint if prompted. <p>Note This command is optional if the CA certificate is already loaded into the configuration.</p>
<p>Step 18 <code>exit</code></p> <p>Example:</p> <pre>Router(config)# exit</pre>	<p>Exits global configuration mode.</p>

Command or Action	Purpose
<p>Step 19 <code>copy system:running-config nvram:startup-config</code></p> <p>Example:</p> <pre>Router# copy system:running-config nvram:startup-config</pre>	<p>(Optional) Copies the running configuration to the NVRAM startup configuration.</p> <p>Note Autoenrollment will not update NVRAM if the running configuration has been modified but not written to NVRAM.</p>
<p>Step 20 <code>show crypto pki certificates</code></p> <p>Example:</p> <pre>Router# show crypto pki certificates</pre>	<p>(Optional) Displays information about your certificates, including any rollover certificates.</p>

Configuring Manual Certificate Enrollment

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

- [PEM-Formatted Files for Certificate Enrollment Request, page 12](#)
- [Restrictions for Manual Certificate Enrollment, page 12](#)
- [Configuring Cut-and-Paste Certificate Enrollment, page 13](#)
- [Configuring TFTP Certificate Enrollment, page 15](#)
- [Certifying a URL Link for Secure Communication with a Trend Micro Server, page 18](#)

PEM-Formatted Files for Certificate Enrollment Request

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

Restrictions for Manual Certificate Enrollment

SCEP Restriction

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

Key Regeneration Restriction

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

Configuring Cut-and-Paste Certificate Enrollment

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>crypto pki trustpoint <i>name</i></p> <p>Example:</p> <pre>Router(config)# crypto pki trustpoint mytp</pre>	<p>Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.</p>

Command or Action	Purpose
<p>Step 4 enrollment terminal pem</p> <p>Example:</p> <pre>Router(ca-trustpoint)# enrollment terminal</pre>	<p>Specifies the manual cut-and-paste certificate enrollment method.</p> <ul style="list-style-type: none"> The certificate request will be displayed on the console terminal so that it may be manually copied (or cut). pem --Configures the trustpoint to generate PEM-formatted certificate requests to the console terminal.
<p>Step 5 fingerprint <i>ca-fingerprint</i></p> <p>Example:</p> <pre>Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E</pre>	<p>(Optional) Specifies a fingerprint that can be matched against the fingerprint of a CA certificate during authentication.</p> <p>Note If the fingerprint is not provided, it will be displayed for verification.</p>
<p>Step 6 exit</p> <p>Example:</p> <pre>Router(ca-trustpoint)# exit</pre>	<p>Exits ca-trustpoint configuration mode and returns to global configuration mode.</p>
<p>Step 7 crypto pki authenticate <i>name</i></p> <p>Example:</p> <pre>Router(config)# crypto pki authenticate mytp</pre>	<p>Retrieves the CA certificate and authenticates it.</p>
<p>Step 8 crypto pki enroll <i>name</i></p> <p>Example:</p> <pre>Router(config)# crypto pki enroll mytp</pre>	<p>Generates certificate request and displays the request for copying and pasting into the certificate server.</p> <ul style="list-style-type: none"> You are prompted for enrollment information, such as whether to include the router FQDN and IP address in the certificate request. You are also given the choice about displaying the certificate request to the console terminal. The base-64 encoded certificate with or without PEM headers as requested is displayed.

Command or Action	Purpose
<p>Step 9 <code>crypto pki import name certificate</code></p> <p>Example:</p> <pre>Router(config)# crypto pki import mytp certificate</pre>	<p>Imports a certificate manually at the console terminal (pasting).</p> <ul style="list-style-type: none"> The base-64 encoded certificate is accepted from the console terminal and inserted into the internal certificate database. <p>Note You must enter this command twice if usage keys, a signature key, and an encryption key are used. The first time the command is entered, one of the certificates is pasted into the router. The second time the command is entered, the other certificate is pasted into the router. It does not matter which certificate is pasted first.</p> <p>Note Some CAs ignore the usage key information in the certificate request and issue general purpose usage certificates. If this applies to the certificate authority you are using, import the general purpose certificate. The router will not use one of the two key pairs generated.</p>
<p>Step 10 <code>exit</code></p> <p>Example:</p> <pre>Router(config)# exit</pre>	<p>Exits global configuration mode.</p>
<p>Step 11 <code>show crypto pki certificates</code></p> <p>Example:</p> <pre>Router# show crypto pki certificates</pre>	<p>(Optional) Displays information about your certificates, the certificates of the CA, and RA certificates.</p>

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.

- 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

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint <i>name</i> Example: Router(config)# crypto pki trustpoint mytp	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.
Step 4	enrollment [mode] [retry period minutes] [retry count number] url url [pem] Example: Router(ca-trustpoint)# enrollment url tftp://certserver/ file_specification	Specifies TFTP as the enrollment method to send the enrollment request and to retrieve the CA certificate and router certificate and any optional parameters. Note For TFTP enrollment, the URL must be configured as a TFTP URL, tftp://example_tftp_url. <ul style="list-style-type: none"> • 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.

	Command or Action	Purpose
Step 5	<p>fingerprint <i>ca-fingerprint</i></p> <p>Example:</p> <pre>Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E</pre>	<p>(Optional) Specifies the fingerprint of the CA certificate received via an out-of-band method from the CA administrator.</p> <p>Note If the fingerprint is not provided, it will be displayed for verification.</p>
Step 6	<p>exit</p> <p>Example:</p> <pre>Router(ca-trustpoint)# exit</pre>	<p>Exits ca-trustpoint configuration mode and returns to global configuration mode.</p>
Step 7	<p>crypto pki authenticate <i>name</i></p> <p>Example:</p> <pre>Router(config)# crypto pki authenticate mytp</pre>	<p>Retrieves the CA certificate and authenticates it from the specified TFTP server.</p>
Step 8	<p>crypto pki enroll <i>name</i></p> <p>Example:</p> <pre>Router(config)# crypto pki enroll mytp</pre>	<p>Generates certificate request and writes the request out to the TFTP server.</p> <ul style="list-style-type: none"> 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.
Step 9	<p>crypto pki import <i>name certificate</i></p> <p>Example:</p> <pre>Router(config)# crypto pki import mytp certificate</pre>	<p>Imports a certificate via TFTP at the console terminal, which retrieves the granted certificate.</p> <ul style="list-style-type: none"> The router will attempt to retrieve the granted certificate via TFTP using the same filename used to send the request, except the extension is changed from “.req” to “.crt”. For usage key certificates, the extensions “-sign.crt” and “-encr.crt” are used. The router will parse the received files, verify the certificates, and insert the certificates into the internal certificate database on the router. <p>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.</p>

Command or Action	Purpose
Step 10 <code>exit</code> Example: <pre>Router(config)# exit</pre>	Exits global configuration mode.
Step 11 <code>show crypto pki certificates</code> Example: <pre>Router# show crypto pki certificates</pre>	(Optional) Displays information about your certificates, the certificates of the CA, and RA certificates.

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

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



Note

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>clock set <i>hh : mm : ss date month year</i></p> <p>Example:</p> <pre>Router# clock set 23:22:00 22 Dec 2009</pre>	<p>Sets the clock on the router.</p>
Step 3	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>

Command or Action	Purpose
<p>Step 4 clock timezone <i>zone</i> <i>hours-offset</i> [<i>minutes-offset</i>]</p> <p>Example:</p> <pre>Router(config)# clock timezone PST -08</pre>	<p>Sets the time zone.</p> <ul style="list-style-type: none"> The <i>zone</i> argument is the name of the time zone (typically a standard acronym). The <i>hours-offset</i> argument is the number of hours the time zone is different from Universal Time Coordinated (UTC). The <i>minutes-offset</i> argument is the number of minutes the time zone is different from UTC. <p>Note The <i>minutes-offset</i> argument of the clock timezone 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 clock timezone AST -3 30.</p>
<p>Step 5 ip http server</p> <p>Example:</p> <pre>Router(config)# ip http server</pre>	<p>Enables the HTTP server.</p>
<p>Step 6 hostname <i>name</i></p> <p>Example:</p> <pre>Router(config)# hostname hostname1</pre>	<p>Configures the hostname of the router.</p>
<p>Step 7 ip domain-name <i>name</i></p> <p>Example:</p> <pre>Router(config)# ip domain-name example.com</pre>	<p>Defines the domain name for the router.</p>
<p>Step 8 crypto key generate rsa general-keys modulus <i>modulus-size</i></p> <p>Example:</p> <pre>Router(config)# crypto key generate rsa general-keys modulus general</pre>	<p>Generates the crypto keys.</p> <ul style="list-style-type: none"> The general-keys keyword specifies that a general purpose key pair is generated, which is the default. The modulus keyword and <i>modulus-size</i> argument specify the IP size of the key modulus. By default, the modulus of a CA key is 1024 bits. When generating RSA keys, you will be prompted to enter a modulus length. A longer modulus could offer stronger security but takes longer to generate and to use. A length of less than 2048 is not recommended. <p>Note The name for the general keys that are generated are based on the domain name that is configured in Step 7. For example, the keys will be called “example.com.”</p>

Command or Action	Purpose
<p>Step 9 crypto pki trustpoint <i>name</i></p> <p>Example:</p> <pre>Router(config)# crypto pki trustpoint mytp</pre>	<p>Declares the CA that your router should use and enters ca-trustpoint configuration mode.</p> <p>Note Effective with Cisco IOS Release 12.3(8)T, the crypto pki trustpoint command replaced the crypto ca trustpoint command.</p>
<p>Step 10 enrollment terminal</p> <p>Example:</p> <pre>Router(ca- trustpoint)# enrollment terminal</pre>	<p>Specifies the manual cut-and-paste certificate enrollment method.</p> <ul style="list-style-type: none"> The certificate request will be displayed on the console terminal so that you may manually copy (or cut).
<p>Step 11 crypto ca authenticate <i>name</i></p> <p>Example:</p> <pre>Router(ca- trustpoint)# crypto ca authenticate mytp</pre>	<p>Takes the name of the CA as the argument and authenticates it.</p> <ul style="list-style-type: none"> The following command output displays: <pre>Enter the base 64 encoded CA certificate. End with a blank line or the word "quit" on a line by itself.</pre>

Command or Action	Purpose
<p>Step 12 Copy the following block of text containing the base 64 encoded CA certificate and paste it at the prompt.</p>	<pre>MIIDIDCCAomgAwIBAgIENd70zzANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJV UzEQMA4GA1UEChMHRXF1aWZheDEtMCsGA1UECxMkRXFlaWZheCBTZWN1cmUgQ2Vy dG1maWNhdGUgQXV0aG9yaXR5MjE2NDU1MVoXDTE4MDgyMjE2NDU1 MVowTjELMAkGA1UEBhMCVVMxEDAoBgNVBAoTB0VxdWlmYXgxLTArBgNVBAsTJEVx dWlmYXggU2VjdXJlIENlcnRpZmljYXRlIEF1dGhvcml0eTCBnzANBgkqhkiG9w0B AQEFAAOBjQAwgYkCgYEAwV2xWGCiYu6gmi0fCG2RFGiYCh7+2grvE4RiIcPRfM6f BeC4AfBONOziipUEZKzxa1NfBbPLZ4C/QgKO/t0BCezhABRP/PvwdN1Dulsr4R+A cJkVV5MW8Q+XarfCaCmczElZMKxRHjuvK9buY0V7xdlfUNLjUA86i0e/FP3gx7kC AwEAAaOCAQkwggEFMHAGAlUdHwRpMGcwZaBjOGGkXzBdMQswCQYDVQQGEwJVUzEQ MA4GA1UEChMHRXF1aWZheDEtMCsGA1UECxMkRXFlaWZheCBTZWN1cmUgQ2Vydg1m aWNhdGUgQXV0aG9yaXR5MjE2NDU1MVoXDTE4MDgyMjE2NDU1 ODIyMTY0MTUxWjALBgNVHQ8EBAMCAQYwHwYDVR0jBBgwFoAUSOZo+SvSspXXR9gj IBBPM5iQn9QwHQYDVR0OBBYEFjmaPkr0rKV10fYIyAQZtOYkJ/UMAWGAlUdEwQF MAMBAf8wGgYJKoZIhVZ9B0EABA0wCxsFVjMuMGMDAgbAMA0GCSqGSIb3DQEBBQUA A4GBAFjOKer89961zgK5F7WF0bnj4JXMJTENAKaSbn+2kmOeUJXRmm/kEd5jhW6Y 7qj/WsjTVbJmcVfewChrPSqnI0kBBIZCe/zuf6IWUrVnZ9NA2zsmWLIodz2uFHdh lvoqZiegDfqnc1zqcPGUIWVEX/r87yloqaKHee9570+sB3c4</pre> <p>The following command output displays:</p> <pre>Certificate has the following attributes: Fingerprint MD5: 67CB9DC0 13248A82 9BB2171E D11BEC4 Fingerprint SHA1: D23209AD 23D31423 2174E40D 7F9D6213 9786633A</pre>
<p>Step 13 Enter yes to accept this certificate.</p>	<pre>% Do you accept this certificate? [yes/no]: yes</pre> <p>The following command output displays:</p> <pre>Trustpoint CA certificate accepted. % Certificate successfully imported</pre>

	Command or Action	Purpose
Step 14	serial-number Example: <pre>hostname1(ca-trustpoint)# serial-number</pre>	Specifies the router serial number in the certificate request.
Step 15	revocation-check none Example: <pre>hostname1(ca-trustpoint)# revocation-check none</pre> Example:	Specifies that certificate checking is ignored.
Step 16	end Example: <pre>hostname1(ca-trustpoint)# end</pre>	Exits ca-trustpoint configuration mode and returns to privileged EXEC mode.
Step 17	trm register Example: <pre>hostname1# trm register</pre>	Manually starts the Trend Micro Server registration process.

Configuring a Persistent Self-Signed Certificate for Enrollment via SSL

This section contains the following tasks:



Note

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

- [Persistent Self-Signed Certificates Overview, page 24](#)
- [Restrictions, page 24](#)
- [Configuring a Trustpoint and Specifying Self-Signed Certificate Parameters, page 24](#)
- [Enabling the HTTPS Server, page 27](#)

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.



Note

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

Configuring a Trustpoint and Specifying Self-Signed Certificate Parameters



Note

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint name**
4. **enrollment selfsigned**
5. **subject-name** [*x.500-name*]
6. **rsa keypair** *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

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto pki trustpoint name Example: Router(config)# crypto pki trustpoint local	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.
Step 4	enrollment selfsigned Example: Router(ca-trustpoint)# enrollment selfsigned	Specifies self-signed enrollment.

Command or Action	Purpose
<p>Step 5 <code>subject-name</code> [<i>x.500-name</i>]</p> <p>Example:</p> <pre>Router(ca-trustpoint)# subject-name</pre>	<p>(Optional) Specifies the requested subject name to be used in the certificate request.</p> <ul style="list-style-type: none"> If no value for the <i>x-500-name</i> argument is specified, the FQDN, which is the default subject name, is used.
<p>Step 6 <code>rsa-keypair</code> <i>key-label</i> [key-size [encryption-key-size]]</p> <p>Example:</p> <pre>Router(ca-trustpoint)# rsa-keypair examplekey 2048</pre>	<p>(Optional) Specifies which key pair to associate with the certificate.</p> <ul style="list-style-type: none"> The value for the <i>key-label</i> 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 <i>key-size</i> argument for generating the key, and specify a value for the <i>encryption-key-size</i> argument to request separate encryption, signature keys, and certificates. The key-size and encryption-key-size must be the same size. Length of less than 2048 is not recommended. <p>Note If this command is not enabled, the FQDN key pair is used.</p>
<p>Step 7 <code>crypto pki enroll</code> name</p> <p>Example:</p> <pre>Router(ca-trustpoint)# crypto pki enroll local</pre>	<p>Tells the router to generate the persistent self-signed certificate.</p>
<p>Step 8 <code>end</code></p> <p>Example:</p> <pre>Router(ca-trustpoint)# end</pre>	<p>(Optional) Exits ca-trustpoint configuration mode.</p> <ul style="list-style-type: none"> Enter this command a second time to exit global configuration mode.
<p>Step 9 <code>show crypto pki certificates</code> [<i>trustpoint-name</i>][<i>verbose</i>]</p> <p>Example:</p> <pre>Router# show crypto pki certificates local verbose</pre>	<p>Displays information about your certificate, the certification authority certificate, and any registration authority certificates.</p>
<p>Step 10 <code>show crypto pki trustpoints</code> [<i>status</i> <i>label</i> [<i>status</i>]]</p> <p>Example:</p> <pre>Router# show crypto pki trustpoints status</pre>	<p>Displays the trustpoints that are configured in the router.</p>

Enabling the HTTPS Server

Perform the following task to enable the HTTPS server.

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

Command or Action	Purpose
<p>Step 1 enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
<p>Step 2 configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 ip http secure-server</p> <p>Example:</p> <pre>Router(config)# ip http secure-server</pre>	<p>Enables the HTTPS web server.</p> <p>Note A key pair (modulus 1024) and a self-signed certificate are automatically generated.</p>
<p>Step 4 end</p> <p>Example:</p> <pre>Router(config)# end</pre>	<p>Exits global configuration mode.</p>

Command or Action	Purpose
Step 5 <code>copy system:running-config nvram: startup-config</code>	Saves the self-signed certificate and the HTTPS server in enabled mode.
Example:	
<pre>Router# copy system:running-config nvram: startup-config</pre>	

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.

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.



Note

- To use certificate profiles, your network must have an HTTP interface to the CA.
- If an enrollment profile is specified, an enrollment URL may not be specified in the trustpoint configuration. Although both commands are supported, only one command can be used at a time in a trustpoint.
- Because there is no standard for the HTTP commands used by various CAs, the user is required to enter the command that is appropriate to the CA that is being used.

>

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>crypto pki trustpoint <i>name</i></p> <p>Example:</p> <pre>Router(config)# crypto pki trustpoint Entrust</pre>	<p>Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.</p>

Command or Action	Purpose
<p>Step 4 enrollment profile label</p> <p>Example:</p> <pre>Router(ca-trustpoint)# enrollment profile E</pre>	<p>Specifies that an enrollment profile is to be used for certificate authentication and enrollment.</p>
<p>Step 5 exit</p> <p>Example:</p> <pre>Router(ca-trustpoint)# exit</pre>	<p>Exits ca-trustpoint configuration mode.</p>
<p>Step 6 crypto pki profile enrollment <i>label</i></p> <p>Example:</p> <pre>Router(config)# crypto pki profile enrollment E</pre>	<p>Defines an enrollment profile and enters ca-profile-enroll configuration mode.</p> <ul style="list-style-type: none"> <i>label</i> --Name for the enrollment profile; the enrollment profile name must match the name specified in the enrollment profile command.
<p>Step 7 Do one of the following:</p> <ul style="list-style-type: none"> authentication url <i>url</i> authentication terminal <p>Example:</p> <pre>Router(ca-profile-enroll)# authentication url http://entrust:81</pre> <p>Example:</p> <pre>Router(ca-profile-enroll)# authentication terminal</pre>	<p>Specifies the URL of the CA server to which to send certificate authentication requests.</p> <ul style="list-style-type: none"> <i>url</i> --URL of the CA server to which your router should send authentication requests. If you are using HTTP, the URL should read “http://CA_name,” where CA_name is the host DNS name or IP address of the CA. If you are using TFTP, the URL should read “tftp://certserver/file_specification.” (If the URL does not include a file specification, the FQDN of the router will be used.) <p>Specifies manual cut-and-paste certificate authentication.</p>
<p>Step 8 authentication command</p> <p>Example:</p> <pre>Router(ca-profile-enroll)# authentication command</pre>	<p>(Optional) Specifies the HTTP command that is sent to the CA for authentication.</p>

Command or Action	Purpose
<p>Step 9 Do one of the following:</p> <ul style="list-style-type: none"> • enrollment url <i>url</i> • • enrollment terminal <p>Example:</p> <pre>Router(ca-profile-enroll)# enrollment url http://entrust:81/cda-cgi/ clientcgi.exe</pre> <p>Example:</p> <p>Example:</p> <pre>Router(ca-profile-enroll)# enrollment terminal</pre>	<p>Specifies the URL of the CA server to which to send certificate enrollment requests via HTTP or TFTP.</p> <p>Specifies manual cut-and-paste certificate enrollment.</p>
<p>Step 10 enrollment credential <i>label</i></p> <p>Example:</p> <pre>Router(ca-profile-enroll)# enrollment credential Entrust</pre>	<p>(Optional) Specifies the third-party vendor CA trustpoint that is to be enrolled with the Cisco IOS CA.</p> <p>Note This command cannot be issued if manual certificate enrollment is being used.</p>
<p>Step 11 enrollment command</p> <p>Example:</p> <pre>Router(ca-profile-enroll)# enrollment command</pre>	<p>(Optional) Specifies the HTTP command that is sent to the CA for enrollment.</p>
<p>Step 12 parameter <i>number</i> {value <i>value</i> prompt <i>string</i>}</p> <p>Example:</p> <pre>Router(ca-profile-enroll)# parameter 1 value aaaa-bbbb-cccc</pre>	<p>(Optional) Specifies parameters for an enrollment profile.</p> <ul style="list-style-type: none"> • This command can be used multiple times to specify multiple values.

Command or Action	Purpose
Step 13 <code>exit</code> Example: <pre>Router(ca-profile-enroll)# exit</pre>	(Optional) Exits ca-profile-enroll configuration mode. <ul style="list-style-type: none"> Enter this command a second time to exit global configuration mode.
Step 14 <code>show crypto pki certificates</code> Example: <pre>Router# show crypto pki certificates</pre>	(Optional) Displays information about your certificates, the certificates of the CA, and RA certificates.

- [What to Do Next, page 32](#)

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

- [Configuring Certificate Enrollment or Autoenrollment Example, page 32](#)
- [Configuring Autoenrollment Example, page 33](#)
- [Configuring Certificate Autoenrollment with Key Regeneration Example, page 33](#)
- [Configuring Cut-and-Paste Certificate Enrollment Example, page 34](#)
- [Configuring Manual Certificate Enrollment with Key Regeneration Example, page 36](#)
- [Creating and Verifying a Persistent Self-Signed Certificate Example, page 37](#)
- [Configuring Direct HTTP Enrollment Example, page 39](#)

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
rsa-key-pair 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 73636F20 53797374 656D3120 301E0603 55040B13 17737562
6F726420 746F206B 6168756C 75692049 50495355 31243022 06035504 03131B79
6E692D75 31302043 65727469 66696361 7465204D 616E6167 6572301E 170D3030
30373134 32303536 32355A17 0D303130 37313430 31323834 335A3032 310E300C
06035504 0A130543 6973636F 3120301E 06092A86 4886F70D 01090216 11706B69
2D343562 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
4B003048 024100B3 0512A201 3B4243E1 378A9703 8AC5E3CE F77AF987 B5A422C4
15E947F6 70997393 70CF34D6 63A86B9C 4347A81A 0551FC02 ABA62360 01EF7DD2
6C136AEB 3C6C3902 03010001 A381F630 81F3300B 0603551D 0F040403 02052030
1C060355 1D110415 30138211 706B692D 3435622E 63697363 6F2E636F 6D301D06
03551D0E 04160414 247D9558 169B9A21 23D289CC 2DDA2A9A 4F77C616 301F0603
551D2304 18301680 14BD742C E892E819 1D551D91 683F6DB2 D8847A6C 73308185
0603551D 1F047E30 7C307AA0 3CA03AA4 38303631 0E300C06 0355040A 13054369
73636F31 24302206 03550403 131B796E 692D7531 30204365 72746966 69636174
65204D61 6E616765 72A23AA4 38303631 0E300C06 0355040A 13054369 73636F31
24302206 03550403 131B796E 692D7531 30204365 72746966 69636174 65204D61
6E616765 72300D06 092A8648 86F70D01 01040500 03410015 BC7CECF9 696697DF
E887007F 7A8DA24F 1ED5A785 C5C60452 47860061 0C18093D 08958A77 5737246B
0A25550A 25910E27 8B8B428E 32F8D948 3DD1784F 954C70
quit

```



Note

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 “trustm1” 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 trustm1

```

```

enrollment url http://trustmel.example.com/
subject-name OU=Spiral Dept., O=example.com
ip-address ethernet0
serial-number none
auto-enroll 90 regenerate
password password1
rsakeypair trustmel 2048
exit
crypto pki authenticate trustmel
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
MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2l2Y28gU3lzdGVtczESMBAGA1UEAxMJ
bXNjYSl1b290MB4XDTAyMDIxNDAwNDYwMVoXDTA3MDIxNDAwNTQ0FowOTELMAKG
A1UEBhMCMVVMxFejAUBgNVBAoTDUNpc2NvIFN5c3RlbXMxEjAQBGNVBAMTCW1zY2Et
cm9vdDcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCix8nIGFg+wvy3BjFbVi25wYoG
K2N0HWWHpqxFuFhgyBnIC00shIn9Ctrdn3JvUNHrONIKocEwNKUGYmPwWGTFAgMB
AAGjgcEwgb4wCwYDVR0PBAQDAgHGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYE
FKIacs16dKAfuNDVQymlSp7esf8jMG0GA1UdHwRmMGQwL6AtocCuGKWh0dHA6Ly9t
c2NhLXJvb3QvQ2VydEVucm9sbC9tc2NhLXJvb3QuY3J3SMDGg6L6AthitmaWxlOi8v
XFxtc2NhLXJvb3R3c2VydEVucm9sbC9tc2NhLXJvb3QuY3J3SMBAGCSsGAQQBjcV
AQQDAGEAMA0GCSqGSIb3DQEBBQUAA0EAeuZkZMX9qkoLHFETYPVWjZPQbBmwNRA
oJDSdYdtL3BcI/uLL5q7EmODyGfLyMGxuhQYx5r/40aSQgLCqBq+yg==
-----END CERTIFICATE-----
Certificate has the following attributes:
Fingerprint: D6C12961 CD78808A 4E02193C 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:
MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQkCFhRtYw5kQmFnZ2VyLmNpc2NvLmNv
bTcBbnZANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEAxdhXFDiWAn/hIZs9zfOtssKA
daoWYu0ms9Fe/Pew0ldh14vXdxgacstOs2Pr5wk6jLOPxpvxOJPWyQM6ipLmyVxv
ojhyLTrVohrh6Dnqcvk+G/5ohss9o9RxvONwx042pQchFnX9EkMuZC7evwRxJEgR
mBHXBZ8GmP3jYQsjs8MCaWAAaAhMB8GCSqGSIb3DQEJdjesMBAwDgYDVR0PAQH/
BAQDAGEAMA0GCSqGSIb3DQEBAUAA4GBAMT6WtyFw95POY7UtF+YIYHiVRUf4SCq
hRIAGrljUePlo9iTqyPULPnt8JnIZ5P5BHU3MfgP8sqodaWub6mubkzaohJ1qD06
O87fnLCnid5Tov5jKogFHIki2EGGZxBosUw91JlenQdNdDPbJc5LIWdfDvcIA6j0
Nl8rOtKnt8Q+
!
!
!
Redisplay enrollment request? [yes/no]:
Encryption key certificate request -

```



```

Issuer:
  CN = TPCA-root
  O = Company
  C = US
Subject:
  Name: Router.example.com
  OID.1.2.840.113549.1.9.2 = Router.example.com
CRL Distribution Point:
  http://tpca-root/CertEnroll/tpca-root.crl
Validity Date:
  start date: 18:16:45 PDT Jun 7 2002
  end   date: 18:26:45 PDT Jun 7 2003
  renew date: 16:00:00 PST Dec 31 1969
Associated Trustpoints: TP
Certificate
Status: Available
Certificate Serial Number: 14DEC2E9000000000C47
Certificate Usage: Signature
Issuer:
  CN = tpca-root
  O = company
  C = US
Subject:
  Name: Router.example.com
  OID.1.2.840.113549.1.9.2 = Router.example.com
CRL Distribution Point:
  http://tpca-root/CertEnroll/tpca-root.crl
Validity Date:
  start date: 18:16:42 PDT Jun 7 2002
  end   date: 18:26:42 PDT Jun 7 2003
  renew date: 16:00:00 PST Dec 31 1969
Associated Trustpoints: TP
CA Certificate
Status: Available
Certificate Serial Number: 3AC0A65E9547C2874AAF2468A942D5EE
Certificate Usage: Signature
Issuer:
  CN = tpca-root
  O = Company
  C = US
Subject:
  CN = tpca-root
  O = company
  C = US
CRL Distribution Point:
  http://tpca-root/CertEnroll/tpca-root.crl
Validity Date:
  start date: 16:46:01 PST Feb 13 2002
  end   date: 16:54:48 PST Feb 13 2007
Associated Trustpoints: TP

```

Configuring Manual Certificate Enrollment with Key Regeneration Example

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

```

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

```

Creating and Verifying a Persistent Self-Signed Certificate Example

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

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



Note

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

- [Enabling the HTTPS Server Example, page 37](#)
- [Verifying the Self-Signed Certificate Configuration Example, page 38](#)

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 095E4865 F8C95A2B
 BFD1C2B7 E64A3804 9BBB7326 207BD456 19BAB78B D075E78E 00D2560C B09289AE
 6DECB8B0 6672FB3A 5CDAEE92 9D4C4F71 F3BCB269 214F6293 4BA8FABF 9486BCFC
 2B941BCA 550999A7 2EFE12A5 6B7B669A 2D88AB77 39B38E0E AA23CB8C B7020301 0001
% Key pair was generated at: 19:14:13 GMT Dec 21 2004
Key name: TP-self-signed-3326000105.server
Usage: Encryption Key
Key is not exportable.
Key Data:
 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00C5680E 89777B42
 463E5783 FE96EA9E F446DC7B 70499AF3 EA266651 56EE29F4 5B003D93 2FC9F81D
 8A46E12F 3FBAC2F3 046ED9DD C5F27C20 1BBA6B9B 08F16E45 C34D6337 F863D605
 34E30F0E B4921BC5 DAC9EBBA 50C54AA0 BF551BDD 88453F50 61020301 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

Related Topic	Document Title
USB token RSA operations: Benefits of using USB tokens	“Storing PKI Credentials” module in the Cisco IOS Security Configuration Guide: Secure Connectivity
USB token RSA operations: Certificate server configuration	“Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment” chapter in the Cisco IOS Security Configuration Guide: Secure Connectivity See the “Generating a Certificate Server RSA Key Pair” section, the “Configuring a Certificate Server Trustpoint” section, and related examples.
Overview of PKI, including RSA keys, certificate enrollment, and CAs	“ Cisco IOS PKI Overview: Understanding and Planning a PKI ” module in the Cisco IOS Security Configuration Guide: Secure Connectivity
Secure Device Provisioning: functionality overview and configuration tasks	“ Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI ” module in the Cisco IOS Security Configuration Guide: Secure Connectivity
RSA key generation and deployment	“ Deploying RSA Keys Within a PKI ” module in the Cisco IOS Security Configuration Guide: Secure Connectivity
Cisco IOS certificate server overview information and configuration tasks	“ Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment ” module in the Cisco IOS Security Configuration Guide: Secure Connectivity

Related Topic	Document Title
Setting up and using a USB token	“ Storing PKI Credentials ” module in the Cisco IOS Security Configuration Guide: Secure Connectivity
Cisco IOS security commands	<i>Cisco IOS Security Command Reference</i>
Suite-B ESP transforms	Configuring Security for VPNs with IPsec feature module.
Suite-B SHA-2 family (HMAC variant) and Elliptic Curve (EC) key pair configuration.	Configuring Internet Key Exchange for IPsec VPNs feature module.
Suite-B Integrity algorithm type transform configuration.	Configuring Internet Key Exchange Version 2 (IKEv2) feature module.
Suite-B Elliptic Curve Digital Signature Algorithm (ECDSA) signature (ECDSA-sig) authentication method configuration for IKEv2.	Configuring Internet Key Exchange Version 2 (IKEv2) feature module.
Suite-B Elliptic curve Diffie-Hellman (ECDH) support for IPsec SA negotiation	Configuring Internet Key Exchange for IPsec VPNs and Configuring Internet Key Exchange Version 2 (IKEv2) feature modules.
Recommended cryptographic algorithms	<i>Next Generation Encryption</i>

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for PKI Certificate Enrollment

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

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

Table 1 Feature Information for PKI Certificate Enrollment

Feature Name	Releases	Feature Information
Cisco IOS USB Token PKI Enhancements--Phase 2	12.4(11)T	<p>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.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none">• Configuring Certificate Enrollment or Autoenrollment, page 6 <p>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 “Feature Information for PKI Certificate Enrollment, page 41” section.</p>

Feature Name	Releases	Feature Information
Certificate Authority Key Rollover	12.4(2)T	<p>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.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Automatic Certificate Enrollment, page 4 • Configuring Certificate Enrollment or Autoenrollment, page 6 <p>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.</p>
Certificate Autoenrollment	12.2(8)T	<p>This feature introduces certificate autoenrollment, which allows the router to automatically request a certificate from the CA that is using the parameters in the configuration.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Automatic Certificate Enrollment, page 4 • Configuring Certificate Enrollment or Autoenrollment, page 6 <p>The following commands were introduced by this feature: auto-enroll, rsakeypair, show crypto ca timers.</p>

Feature Name	Releases	Feature Information
Certificate Enrollment Enhancements	12.2(8)T	<p>This feature introduces five new crypto ca trustpoint commands that provide new options for certificate requests and allow users to specify fields in the configuration instead of having to go through prompts.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> • Configuring Certificate Enrollment or Autoenrollment, page 6 <p>The following commands were introduced by this feature: ip-address(ca-trustpoint), password(ca-trustpoint), serial-number, subject-name, usage.</p>
Direct HTTP Enrollment with CA Servers	12.3(4)T	<p>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.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Certificate Enrollment Profiles, page 5 • Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment, page 28 <p>The following commands were introduced by this feature: authentication command, authentication terminal, authentication url, crypto ca profile enrollment, enrollment command, enrollment profile, enrollment terminal, enrollment url, parameter.</p>

Feature Name	Releases	Feature Information
Import of RSA Key Pair and Certificates in PEM Format	12.3(4)T	<p>This feature allows customers to issue certificate requests and receive issued certificates in PEM-formatted files.</p> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none">• Configuring Manual Certificate Enrollment, page 12 <p>The following commands were modified by this feature: enrollment, enrollment terminal.</p>
Key Rollover for Certificate Renewal	12.3(7)T	<p>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.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none">• Automatic Certificate Enrollment, page 4• Configuring Certificate Enrollment or Autoenrollment, page 6• Configuring Manual Certificate Enrollment, page 12 <p>The following commands were introduced or modified by this feature: auto-enroll, regenerate.</p>

Feature Name	Releases	Feature Information
Manual Certificate Enrollment (TFTP Cut-and-Paste)	12.2(13)T	<p>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.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none">• Supported Certificate Enrollment Methods, page 3• Configuring Manual Certificate Enrollment, page 12 <p>The following commands were introduced or modified by this feature: crypto ca import, enrollment, enrollment terminal.</p>
Multiple-Tier CA Hierarchy	12.2(15)T	<p>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.</p> <p>The following section provides information about this enhancement:</p> <ul style="list-style-type: none">• Framework for Multiple CAs, page 2 <p>Note This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.</p>

Feature Name	Releases	Feature Information
Persistent Self-Signed Certificates	12.2(33)SXH 12.2(33)SRA 12.3(14)T	<p>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.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> • Supported Certificate Enrollment Methods, page 3 • Configuring a Persistent Self-Signed Certificate for Enrollment via SSL, page 23 <p>The following commands were introduced or modified by this feature: enrollment selfsigned, show crypto pki certificates, show crypto pki trustpoints.</p>
PKI Status	12.3(11)T	<p>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.</p> <p>The following section provides information about this enhancement:</p> <ul style="list-style-type: none"> • How to Configure Certificate Enrollment for a PKI, page 6 <p>Note This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.</p>

Feature Name	Releases	Feature Information
Reenroll Using Existing Certificates	12.3(11)T	<p>This feature allows users to reenroll a router with a Cisco IOS CA via existing certificates from a third-party vendor CA.</p> <p>The following section provides information about this enhancement:</p> <ul style="list-style-type: none">• Configuring a Certificate Enrollment Profile for Enrollment or Reenrollment, page 28 <p>The following commands were introduced by this feature: enrollment credential, grant auto trustpoint.</p>
Trustpoint CLI	12.2(8)T	<p>This feature introduces the crypto pki trustpoint command, which adds support for trustpoint CAs.</p>

Feature Name	Releases	Feature Information
Suite-B support in IOS SW crypto	15.1(2)T	<p>Suite-B adds the following support for certificate enrollment for a PKI:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
Public Key Infrastructure (PKI) IPv6 Support for VPN Solutions	15.2(1)T	<p>The enrollment url (ca-trustpoint) command was modified to allow the specification of an IPv6 address in the URL for the CA.</p> <p>The ip-address (ca-trustpoint) command was modified to allow the specification of an IPv6 address that is included as “unstructuredAddress” in the certificate request.</p>

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)

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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. (1110R)

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

© 2012 Cisco Systems, Inc. All rights reserved.