



Certificate Autoenrollment

Feature History

Release	Modification
12.2(8)T	This feature was introduced.

This feature module describes the Certificate Autoenrollment feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Configuration Tasks, page 4](#)
- [Monitoring and Maintaining Autoenrollment, page 6](#)
- [Configuration Examples, page 6](#)
- [Command Reference, page 7](#)
- [Glossary, page 11](#)

Feature Overview

The Certificate Autoenrollment feature allows you to configure your router to automatically request a certificate from the certification authority (CA) that is using the parameters in the configuration. Thus, operator convention is no longer required at the time the enrollment request is sent to the CA server.

Automatic enrollment will be performed on startup for any trustpoint CA that is configured and does not have a valid certificate. When the certificate—which is issued by a trustpoint CA that has been configured for autoenrollment—expires, a new certificate is requested. Although this feature does not provide seamless certificate renewal, it does provide unattended recovery from expiration.



Note

Trustpoint CAs combine and replace the functionality of identity and trusted-root CAs. Thus, the **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands. For more information, refer to the *Trustpoint CLI*, Cisco IOS Release 12.2(8)T feature module.

Benefits

Before the Certificate Autoenrollment feature, certificate enrollment required complicated, interactive commands that had to be executed on every router. This feature allows you to preload all of the necessary information into the configuration and cause each router to obtain certificates automatically when it is booted. Autoenrollment also checks for expired router certificates.

Related Documents

- *Enrollment Enhancements*, Cisco IOS Release 12.2(8)T feature module
- *Trustpoint CLI*, Cisco IOS Release 12.2(8)T feature module
- The chapter “Certification Authority Interoperability Commands” in *Cisco IOS Security Command Reference*, Release 12.2
- The chapter “Configuring Certification Authority Interoperability” in *Cisco IOS Security Configuration Guide*, Release 12.2

Supported Platforms

This feature runs on all platforms that support IPSec and public key infrastructure (PKI).

- Cisco 800 series
- Cisco 805
- Cisco 806
- Cisco 828
- Cisco 1600 series
- Cisco 1600-R series
- Cisco 1710
- Cisco 1720
- Cisco 1750
- Cisco 2400 series
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7400 series

- Cisco 7500 series
- Cisco ICS 7700
- Cisco CVA120 series
- Cisco MC3810 series
- Cisco uBR7200 series
- Route Processor Module (RPM)

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

None

Configuration Tasks

See the following sections for configuration tasks for the Certificate Autoenrollment feature. Each task in the list is identified as either required or optional.

- [Configuring Autoenrollment](#) (required)
- [Preloading Root CAs](#) (required)
- [Verifying CA Information](#) (optional)

Configuring Autoenrollment



Note

Before submitting an automatic enrollment request, all necessary enrollment information must be configured.

To configure autoenrollment with a CA on startup, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# crypto ca trustpoint <i>name</i>	Declares the CA that your router should use and enters ca-trustpoint configuration mode.
Step 2	Router(ca-trustpoint)# enrollment url <i>url</i>	Specifies the URL of the CA on which your router should send certificate requests; for example, <code>http://ca_server</code> . <i>url</i> must be in the form of <code>http://CA_name</code> , where <i>CA_name</i> is the name of the CA's host Domain Name System or the IP address.
Step 3	Router(ca-trustpoint)# subject-name [<i>x.500-name</i>]	(Optional) Specifies the requested subject name that will be used in the certificate request. If the <i>x-500-name</i> argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.
Step 4	Router(ca-trustpoint)# ip-address { <i>interface</i> none }	Includes the IP address of the specified interface in the certificate request. Issue the none keyword if no IP address should be included. Note If this command is enabled, you will not be prompted for an IP address during enrollment for this trustpoint.
Step 5	Router(ca-trustpoint)# serial-number [none]	Specifies the router serial number in the certificate request, unless the none keyword is issued.
Step 6	Router(ca-trustpoint)# auto-enroll [regenerate]	Enables autoenrollment. This command allows you to automatically request a router certificate from the CA. By default, only the DNS name of the router is included in the certificate. Issue the regenerate keyword to generate a new key for the certificate even if a named key already exists.

	Command	Purpose
Step 7	Router(ca-trustpoint)# password <i>string</i>	(Optional) Specifies the revocation password for the certificate. Note If this command is enabled, you will not be prompted for a password during enrollment for this trustpoint.
Step 8	Router(ca-trustpoint)# rsa keypair <i>key-label</i> [<i>key-size</i> [<i>encryption-key-size</i>]]	Specifies which key pair to associate with the certificate. <i>key-label</i> 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> for generating the key and specify the <i>encryption-key-size</i> to request separate encryption, signature keys, and certificates. Note If this command is not enabled, the FQDN key pair is used.

Preloading Root CAs

After enabling automatic enrollment, you must authenticate the CA to establish a chain of trust. This can be done by implementing one of the following methods:

- [Getting the Certificate of the CA](#)
- [Adding the Certificate of the CA](#)

Getting the Certificate of the CA

To get the certificate of the CA, use the following command in global configuration mode:

Command	Purpose
Router (config)# crypto ca authenticate <i>name</i>	Authenticates the CA.

Adding the Certificate of the CA

To add the certificate of the CA, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router (config)# crypto ca certificate chain <i>name</i>	Enters certificate chain configuration mode, which allows you to add or delete specified certificates.
Step 2	Router (config-cert-chain)# certificate ca <i>certificate-serial-number</i>	Manually adds or deletes certificates.

Verifying CA Information

To verify CA information, use the following EXEC command:

Command	Purpose
Router# show crypto ca certificates	Displays information about your certificates, the certificates of the CA, and registration authority (RA) certificates.
Router# show crypto ca trustpoints	Displays the trustpoints configured in the routers.

Monitoring and Maintaining Autoenrollment

To monitor and maintain autoenrollment, use the following EXEC command.

Command	Purpose
Router# show crypto ca timers	Displays the status of the managed timers that are maintained by Cisco IOS for PKI.

Configuration Examples

This section provides the following configuration example:

- [Autoenrollment Sample Configuration Example](#)

Autoenrollment Sample Configuration Example

The following example shows how to configure the router to autoenroll with a CA on start-up:

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 auto-enroll regenerate
 password revokeme
 rsa-key frog 2048
!
crypto ca certificate chain frog
certificate ca 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
```

Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [auto-enroll](#)
- [rsakeypair](#)
- [show crypto ca timers](#)

auto-enroll

To enable autoenrollment, use the **auto-enroll** command in ca-trustpoint configuration mode. To disable the autoenrollment feature, use the **no** form of this command.

auto-enroll [regenerate]

no auto-enroll [regenerate]

Syntax Description

regenerate	(Optional) A new key is generated for the certificate even if the named key already exists.
-------------------	---

Defaults

Autoenrollment is not enabled

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **auto-enroll** command to automatically request a router certificate from the certification authority (CA) that is using the parameters in the configuration. This command will generate a new RSA key only if a new key does not exist with the requested label.

A trustpoint that is configured for autoenroll will attempt to reenroll when the router certificate expires.

If the **regenerate** keyword is configured, a new key will be generated. Some CAs require a new key for reenrollment to work.

Examples

The following example shows how to configure the router to autoenroll with the CA “frog” on startup. In this example, regenerate is issued, so a new key will be generated for the certificate.

```
crypto ca trustpoint frog
  enrollment url http://frog.phoobin.com/
  subject-name OU=Spiral Dept., O=tiedye.com
  ip-address ethernet-0
  auto-enroll regenerate
  password revokeme
  rsa-key frog 2048
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

rsakeypair

To specify which key pair to associate with the certificate, use the **rsakeypair** command in ca-trustpoint configuration mode.

```
rsakeypair key-label [key-size [encryption-key-size]]
```

Syntax Description

<i>key-label</i>	The name of the key pair, which is generated during enrollment if it does not already exist or if the auto-enroll regenerate command is configured.
<i>key-size</i>	(Optional) The size of the desired RSA key. If not specified, the existing keysize is used. (The specified size must be the same as the <i>encryption-key-size</i> .)
<i>encryption-key-size</i>	(Optional) The size of the second key, which is used to request separate encryption, signature keys, and certificates. (The specified size must be the same as the <i>key-size</i> .)

Defaults

The fully-qualified domain name (FQDN) key is used.

Command Modes

Ca-identity Configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

When you regenerate a key pair, you are responsible for reenrolling the identities associated with the key pair. Use the **rsakeypair** command to refer back to the named key pair.

Examples

The following example is a sample trustpoint configuration that specifies the rsa keypair “exampleCAkeys”:

```
crypto ca trustpoint exampleCA
enroll url http://exampleCA/certsrv/mscep/mscep.dll
rsakeypair exampleCAkeys 1024 1024
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crypto ca trustpoint	Declares the CA that your router should use.
crypto key generate rsa (CA)	Generates RSA key pairs.

show crypto ca timers

To display the status of the managed timers that are maintained by Cisco IOS for public key infrastructure (PKI), use the **show crypto ca timers** command in EXEC mode.

show crypto timers

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.2(8)T	This command was introduced.

Usage Guidelines For each timer, this command displays the time remaining before the timer expires. It also associates trustpoint certification authorities (CAs), except for certificate revocation list (CRL) timers, by displaying the CRL distribution point.

Examples The following example is sample output for the **show crypto ca timers** command:

```
Router# show crypto ca timers

PKI Timers
| 4d15:13:33.144
| 4d15:13:33.144 CRL http://msca-root.cisco.com/CertEnroll/msca-root.crl
| 328d11:56:48.372 RENEW msroot
| 6:43.201 POLL verisign
```

Related Commands	Command	Description
	auto-enroll	Enables autoenrollment.
	crypto ca trustpoint	Declares the CA that your router should use.

Glossary

certification authority (CA)—A service responsible for managing certificate requests and issuing certificates to participating IPsec network devices. This service provides centralized key management for the participating devices and is explicitly entrusted by the receiver to validate identities and to create digital certificates.

enrollment—The process of obtaining a new certificate from a CA.

identity CA—A CA that issues a certificate verifying the identity of a router. An identity CA can be a root CA (and have a self-signed certificate), or it can have a chain of certificates that validate each CA between itself and the root CA. An identity CA uses its own certificate to sign the certificate of a router, thereby validating the identity of the router.

Internet Key Exchange (IKE)—A hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the ISAKMP framework. Although IKE can be used with other protocols, its initial implementation is with IPsec. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates IPsec security associations.

IP Security (IPsec)—A framework of open standards developed by the Internet Engineering Task Force (IETF). IPsec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (“peers”), such as Cisco routers.

peer certificate—The certificate presented by a peer, which contains the peer’s public key and is signed by the peer’s identity CA.

public key infrastructure (PKI)—Provides trusted and efficient key and certificate management to support security protocols such as IPsec.

registration authority (RA)—A server that acts as a proxy for the CA so that CA functions can continue when the CA is offline.

root CA—A top level CA. A root CA has a self-signed certificate that contains its own public key. The router obtains this certificate via a user interface command, thereby enabling the root CA to sign other certificates.

RSA keys—RSA keys come in pairs—one public key and one private key—and are used to sign and encrypt IKE key management messages and are required before you can obtain a certificate for your router.

