



Key Rollover for Certificate Renewal

Automatic certificate enrollment was introduced to allow the router to automatically request a certificate from the certification authority (CA) server. By default, the automatic enrollment feature requests a new certificate when the old certificate expires. Connectivity can be lost while the request is being serviced because the existing certificate and key pairs are deleted immediately after the new key is generated. The new key does not have a certificate to match it until the process is complete, and incoming Internet Key Exchange (IKE) connections cannot be established until the new certificate is issued. The Key Rollover for Certificate Renewal 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.

Feature History for the Key Rollover for Certificate Renewal Feature

Release	Modification
12.3(7)T	This feature was introduced.
12.2(18)SXE	This feature was integrated into Cisco IOS Release 12.2(18)SXE.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Key Rollover for Certificate Renewal, page 2](#)
- [Restrictions for Key Rollover for Certificate Renewal, page 2](#)
- [Information About Key Rollover for Certificate Renewal, page 2](#)
- [How to Configure Key Rollover for Certificate Renewal, page 3](#)
- [Configuration Examples for Key Rollover for Certificate Renewal, page 9](#)
- [Additional References, page 10](#)



Corporate Headquarters:

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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 11](#)
- [Glossary, page 16](#)

Prerequisites for Key Rollover for Certificate Renewal

Before implementing the key rollover feature, ensure that your CA permits an automated certificate renewal request before the existing certificate expires.

Restrictions for Key Rollover for Certificate Renewal

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 mismatch.

Information About Key Rollover for Certificate Renewal

To configure key rollover for certificate renewal, you should understand the following concepts:

- [Certificate Autoenrollment with Key Rollover, page 2](#)
- [Manual Certificate Enrollment with Key Rollover, page 3](#)

Certificate Autoenrollment with Key Rollover

Certificate autoenrollment 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 intervention is no longer required at the time the enrollment request is sent to the CA server.

Automatic enrollment is 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.

When the key rollover feature is used, a new certificate is requested before the old certificate expires if the CA allows such a request automatically. A new optional renewal percentage parameter is introduced to allow a new certificate to be requested when a specified percentage of the life 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.

The **regenerate** keyword of the **auto-enroll** command provides seamless key rollover by creating a new key pair with a temporary name and retaining the old certificate and key pair until a new certificate is received from the CA. When the new certificate is received, the old certificate and key pair are discarded and the new key pair is renamed with the name of the original key pair.

Manual Certificate Enrollment with Key Rollover

Key rollover can be used with a manual certificate enrollment request. Using the same method as key rollover with certificate autoenrollment, the **regenerate** command in `ca-trustpoint` configuration mode has been introduced to provide seamless key rollover for manual certificate enrollment. A new key pair is created with a temporary name, and the old certificate and key pair are retained until a new certificate is received from the CA. When the new certificate is received, the old certificate and key pair are discarded and the new key pair is renamed with the name of the original key pair. Do not regenerate the keys manually; key rollover will occur when the **crypto ca enroll** command is issued.

How to Configure Key Rollover for Certificate Renewal

This section contains the following tasks:

- [Configuring Certificate Autoenrollment with Key Rollover, page 3](#) (required)
- [Configuring Manual Certificate Enrollment with Key Rollover, page 6](#) (optional)

Configuring Certificate Autoenrollment with Key Rollover

Perform this task to configure key rollover with automatic certificate enrollment.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ca trustpoint** *name*
4. **enrollment url** *url*
5. **subject-name** [*x.500-name*]
6. **ip-address** {*interface-type interface-number* | **none**}
7. **serial-number** [**none**]
8. **auto-enroll** [*percent*] [**regenerate**]
9. **password** *string*
10. **rsa**keypair *key-label* [*key-size* [*encryption-key-size*]]
11. **exit**
12. **crypto ca authenticate** *name*
13. **exit**
14. **copy system:running-config nvram:startup-config**

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 ca trustpoint name Example: Router(config)# crypto ca trustpoint trustserver	Declares the CA that your router should use and enters ca-trustpoint configuration mode.
Step 4	enrollment url url Example: Router(ca-trustpoint)# enrollment url http://trustserver.company.com	Specifies the URL of the CA on which your router should send certificate requests. <ul style="list-style-type: none"> The <i>url</i> argument 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 (DNS) or its IP address.
Step 5	subject-name [x.500-name] Example: Router(ca-trustpoint)# subject-name	(Optional) Specifies the requested subject name that will be used in the certificate request. <ul style="list-style-type: none"> 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 6	ip-address {interface-type interface-number none} Example: Router(ca-trustpoint)# ip-address ethernet0	Includes the IP address of the specified interface in the certificate request. 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>
Step 7	serial-number [none] Example: Router(ca-trustpoint)# serial-number none	Specifies the router serial number in the certificate request, unless the none keyword is issued.

	Command or Action	Purpose
Step 8	<p>auto-enroll [<i>percent</i>] [regenerate]</p> <p>Example: Router(ca-trustpoint)# auto-enroll 90 regenerate</p>	<p>Enables autoenrollment.</p> <ul style="list-style-type: none"> 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. Use the <i>percent</i> argument to specify that a new certificate will be requested after the percent 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>
Step 9	<p>password <i>string</i></p> <p>Example: Router(ca-trustpoint)# password trustme</p>	<p>(Optional) Specifies the revocation password for the certificate.</p> <p>Note If this command is enabled, you will not be prompted for a password during enrollment for this trustpoint.</p>
Step 10	<p>rsakeypair <i>key-label</i> [<i>key-size</i> [<i>encryption-key-size</i>]]</p> <p>Example: Router(ca-trustpoint)# rsakeypair examplekeys 1024 1024</p>	<p>Specifies which key pair to associate with the certificate.</p> <ul style="list-style-type: none"> <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. <p>Note If this command is not enabled, the FQDN key pair is used.</p>
Step 11	<p>exit</p> <p>Example: Router(ca-trustpoint)# exit</p>	<p>Exits ca-trustpoint configuration mode and returns to global configuration mode.</p>
Step 12	<p>crypto ca authenticate <i>name</i></p> <p>Example: Router(config)# crypto ca authenticate trustserver</p>	<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>

	Command or Action	Purpose
Step 13	<code>exit</code> Example: Router(config)# <code>exit</code>	Exits global configuration mode and returns to privileged EXEC mode.
Step 14	<code>copy system:running-config nvram:startup-config</code> Example: Router# <code>copy system:running-config nvram:startup-config</code>	(Optional) Copies the running configuration to the NVRAM startup configuration. <ul style="list-style-type: none"> Autoenroll will not update NVRAM if the running configuration has been modified but not written to NVRAM.

Configuring Manual Certificate Enrollment with Key Rollover

Perform this task to configure key rollover with manual certificate enrollment.

Restrictions

Do not regenerate the keys manually using the `crypto key generate` command; key rollover will occur when the `crypto ca enroll` command is issued.

SUMMARY STEPS

- `enable`
- `configure terminal`
- `crypto ca trustpoint name`
- `enrollment url url`
- `subject-name [x.500-name]`
- `ip-address {interface-type interface-number | none}`
- `serial-number [none]`
- `regenerate`
- `password string`
- `rsakeypair key-label [key-size [encryption-key-size]]`
- `exit`
- `crypto ca authenticate name`
- `crypto ca enroll name`
- `exit`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<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: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>crypto ca trustpoint name</p> <p>Example: Router(config)# crypto ca trustpoint trustserver</p>	<p>Declares the CA that your router should use and enters ca-trustpoint configuration mode.</p>
Step 4	<p>enrollment url url</p> <p>Example: Router(ca-trustpoint)# enrollment url http://trustserver.company.com</p>	<p>Specifies the URL of the CA on which your router should send certificate requests.</p> <ul style="list-style-type: none"> The <i>url</i> argument 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 (DNS) or its IP address.
Step 5	<p>subject-name [x.500-name]</p> <p>Example: Router(ca-trustpoint)# subject-name</p>	<p>(Optional) Specifies the requested subject name that will be used in the certificate request.</p> <ul style="list-style-type: none"> 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 6	<p>ip-address {interface-type interface-number none}</p> <p>Example: Router(ca-trustpoint)# ip-address ethernet0</p>	<p>Includes the IP address of the specified interface in the certificate request. Issue the none keyword if no IP address should be included.</p> <p>Note If this command is enabled, you will not be prompted for an IP address during enrollment for this trustpoint.</p>
Step 7	<p>serial-number [none]</p> <p>Example: Router(ca-trustpoint)# serial-number</p>	<p>Specifies the router serial number in the certificate request, unless the none keyword is issued.</p>

	Command or Action	Purpose
Step 8	<p>regenerate</p> <p>Example: Router(ca-trustpoint)# regenerate</p>	<p>Enables key rollover with certificate enrollment when the crypto ca enroll command is issued.</p> <ul style="list-style-type: none"> This command generates a new key for the certificate even if a named key already exists. <p>Note Do not use the crypto key generate command with the key rollover feature.</p> <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 keypair associated with trustpoint is exportable.</p>
Step 9	<p>password <i>string</i></p> <p>Example: Router(ca-trustpoint)# password trustme</p>	<p>(Optional) Specifies the revocation password for the certificate.</p> <p>Note If this command is enabled, you will not be prompted for a password during enrollment for this trustpoint.</p>
Step 10	<p>rsakeypair <i>key-label</i> [<i>key-size</i> [<i>encryption-key-size</i>]]</p> <p>Example: Router(ca-trustpoint)# rsa keypair examplekeys 1024 1024</p>	<p>Specifies which key pair to associate with the certificate.</p> <ul style="list-style-type: none"> <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. <p>Note If this command is not enabled, the FQDN key pair is used.</p>
Step 11	<p>exit</p> <p>Example: Router(ca-trustpoint)# exit</p>	<p>Exits ca-trustpoint configuration mode and returns to global configuration mode.</p>
Step 12	<p>crypto ca authenticate <i>name</i></p> <p>Example: Router(config)# crypto ca authenticate trustserver</p>	<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>

	Command or Action	Purpose
Step 13	<pre>crypto ca enroll name</pre> <p>Example: Router(config)# crypto ca enroll trustserver</p>	<p>Requests certificates for all of your RSA key pairs.</p> <ul style="list-style-type: none"> This command causes your router to request as many certificates as there are RSA key pairs, so you need perform this command only once, even if you have special-usage RSA key pairs. When the regenerate ca-trustpoint configuration command is configured, this command will perform key rollover. <p>Note This command requires you to create a challenge password that is not saved with the configuration. This password is required if your certificate needs to be revoked, so you must remember this password.</p>
Step 14	<pre>exit</pre> <p>Example: Router(config)# exit</p>	<p>Exits global configuration mode and returns to privileged EXEC mode.</p>

Configuration Examples for Key Rollover for Certificate Renewal

This section contains the following examples:

- [Configuring Certificate Autoenrollment with Key Rollover: Example, page 9](#)
- [Configuring Manual Certificate Enrollment with Key Rollover: Example, page 10](#)

Configuring Certificate Autoenrollment with Key Rollover: Example

The following example shows how to configure the router to autoenroll with the CA named trustm1 on startup. In this example, the **regenerate** keyword is issued, so a new key will be generated for the certificate. 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 ca trustpoint trustm1
  enrollment url http://trustm1.company.com/
  subject-name OU=Spiral Dept., O=tiedye.com
  ip-address ethernet0
  serial-number none
  auto-enroll 90 regenerate
  password revokeme
  rsakeypair trustm1 2048
  exit
crypto ca authenticate trustm1
copy system:running-config nvram:startup-config
```

Configuring Manual Certificate Enrollment with Key Rollover: Example

The following example shows how to configure key rollover to regenerate new keys with a manual certificate enrollment from the CA named trustme2.

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

Additional References

The following sections provide references related to key rollover.

Related Documents

Related Topic	Document Title
Certificate autoenrollment	<i>Certificate Autoenrollment</i> feature document, Release 12.2(8)T
Enhancements to certificate enrollment	<i>Certificate Enrollment Enhancements</i> feature document, Release 12.2(8)T
Trustpoint commands	<i>Trustpoint CLI</i> feature document, Release 12.2(8)T
Certification authority commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i> , Release 12.3 T
Certification configuration	The chapter “Configuring Certification Authority Interoperability” in the <i>Cisco IOS Security Configuration Guide</i>

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands only.

- [auto-enroll](#)
- [regenerate](#)

auto-enroll

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

auto-enroll [*percent*] [**regenerate**]

no auto-enroll [*percent*] [**regenerate**]

Syntax Description

<i>percent</i>	(Optional) The renewal percentage parameter causes the router to request a new certificate after the specified percent lifetime of the current certificate is reached. If not specified, the request for a new certificate is made when the old certificate expires. The specified percent value must not be less than 10.
regenerate	(Optional) Generates a new key for the certificate even if the named key already exists.

Defaults

Certificate autoenrollment is not enabled.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.3(7)T	The <i>percent</i> argument was added to support key rollover.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.

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 certificate autoenrollment will attempt to reenroll when the router certificate expires.

Use the **regenerate** keyword to provide seamless key rollover for manual certificate enrollment. A new key pair is created with a temporary name, and the old certificate and key pair are retained until a new certificate is received from the CA. When the new certificate is received, the old certificate and key pair are discarded and the new key pair is renamed with the name of the original key pair. Some CAs require a new key for reenrollment to work.

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 keypair associated with trustpoint is exportable
```

Examples

The following example shows how to configure the router to autoenroll with the CA named trustme1 on startup. In this example, the **regenerate** keyword is issued, so a new key will be generated for the certificate. 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.

```
crypto ca trustpoint trustme1
  enrollment url http://trustme1.company.com/
  subject-name OU=Spiral Dept., O=tiedye.com
  ip-address ethernet0
  serial-number none
  auto-enroll 90 regenerate
  password revokeme
  rsakeypair trustme1 2048
  exit
crypto ca authenticate trustme1
```

Related Commands

Command	Description
crypto ca authenticate	Retrieves the CA certificate and authenticates it.
crypto ca trustpoint	Declares the CA that your router should use.

regenerate

To enable key rollover with manual certificate enrollment, use the **regenerate** command in ca-trustpoint configuration mode. To disable key rollover, use the **no** form of this command.

regenerate

no regenerate

Syntax Description This command has no arguments or keywords.

Defaults Key rollover is not enabled.

Command Modes Ca-trustpoint configuration

Command History	Release	Modification
	12.3(7)T	This command was introduced.
	12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.

Usage Guidelines Use the **regenerate** command to provide seamless key rollover for manual certificate enrollment. A new key pair is created with a temporary name, and the old certificate and key pair are retained until a new certificate is received from the CA. When the new certificate is received, the old certificate and key pair are discarded and the new key pair is renamed with the name of the original key pair.

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 keypair associated with trustpoint is exportable
```

Do not regenerate the keys manually; key rollover will occur when the **crypto ca enroll** command is issued.

Examples The following example shows how to configure key rollover to regenerate new keys with a manual certificate enrollment from the CA named trustme2.

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

Related Commands

Command	Description
crypto ca authenticate	Retrieves the CA certificate and authenticates it.
crypto ca enroll	Requests certificates from the CA for all of your router's RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

Glossary

CA—certification authority. 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.

IKE—Internet Key Exchange. 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.

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.

**Note**

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.