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

percent	(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 *percent* argument was added to support key rollover.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 Rivest, Shamir, and Adelman (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
```

Note If you are using a Secure Shell service, you should set up specific RSA keypairs (different private keys) for the trustpoint and the SSH service. (If the Public Key Infrastructure [PKI] and the SSH infrastructure share the same default RSA keypair, a temporary disruption of SSH service could occur. The RSA keypair could become invalid or change because of the CA system, in which case you would not be able to log in using SSH. You could receive the following error message: "key changed, possible security problem.")

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.