crypto ca authenticate through crypto ca trustpoint

crypto ca authenticate

> **Note** This command was replaced by the **crypto pki authenticate** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To authenticate the certification authority (by getting the certificate of the CA), use the **crypto ca authenticate** command in global configuration mode.

crypto ca authenticate *name*

Syntax Description

name	Specifies the name of the CA. This is the same name used when the CA was declared with the **crypto ca identity** command .

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command is required when you initially configure CA support at your router.

This command authenticates the CA to your router by obtaining the self-signed certificate of the CA that contains the public key of the CA. Because the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator when you perform this command.

If you are using RA mode (using the **enrollment mode ra** command) when you issue the **crypto ca authenticate** command, then registration authority signing and encryption certificates will be returned from the CA as well as the CA certificate.

This command is not saved to the router configuration. However. the public keys embedded in the received CA (and RA) certificates are saved to the configuration as part of the RSA public key record (called the “RSA public key chain”).

If the CA does not respond by a timeout period after this command is issued, the terminal control will be returned so it will not be tied up. If this happens, you must re-enter the command. Cisco IOS software will not recognize CA certificate expiration dates set for beyond the year 2049. If the validity period of the CA certificate is set to expire after the year 2049, the following error message will be displayed when authentication with the CA server is attempted:

error retrieving certificate :incomplete chain

If you receive an error message similar to this one, check the expiration date of your CA certificate. If the expiration date of your CA certificate is set after the year 2049, you must reduce the expiration date by a year or more.

Examples

In the following example, the router requests the certificate of the CA. The CA sends its certificate and the router prompts the administrator to verify the certificate of the CA by checking the CA certificate's fingerprint. The CA administrator can also view the CA certificate's fingerprint, so you should compare what the CA administrator sees to what the router displays on the screen. If the fingerprint on the router's screen matches the fingerprint viewed by the CA administrator, you should accept the certificate as valid.

```
Router(config)#
crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y
#
```

Related Commands

Command	Description
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
show crypto pki certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto ca enroll

Note This command was replaced by the **crypto pki enroll** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXE.

To obtain the certificate(s) of your router from the certification authority, use the **crypto ca enroll** command in global configuration mode. To delete a current enrollment request, use the **no** form of this command.

crypto ca enroll *name*

no crypto ca enroll *name*

Syntax Description

name	Specifies the name of the CA. Use the same name as when you declared the CA using the **crypto pki trustpoint**command.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command requests certificates from the CA for all of your router's RSA key pairs. This task is also known as enrolling with the CA. (Technically, enrolling and obtaining certificates are two separate events, but they both occur when this command is issued.)

Your router needs a signed certificate from the CA for each RSA key pairs of your router; if you previously generated general purpose keys, this command will obtain the one certificate corresponding to the one general purpose RSA key pair. If you previously generated special usage keys, this command will obtain two certificates corresponding to each of the special usage RSA key pairs.

If you already have a certificate for your keys you will be unable to complete this command; instead, you will be prompted to remove the existing certificate first. (You can remove existing certificates with the **no certificate** command.)

The **crypto ca enroll** command is not saved in the router configuration.

Note If your router reboots after you issue the **crypto ca enroll** command but before you receive the certificate(s), you must reissue the command.

Responding to Prompts

When you issue the **crypto ca enroll** command, you are prompted a number of times.

First, you are prompted to create a challenge password. This password can be up to 80 characters in length. This password is necessary in the event that you ever need to revoke your router's certificate(s). When you ask the CA administrator to revoke your certificate, you must supply this challenge password as a protection against fraudulent or mistaken revocation requests.

Note This password is not stored anywhere, so you need to remember this password.

If you lose the password, the CA administrator may still be able to revoke the router's certificate but will require further manual authentication of the router administrator identity.

You are also prompted to indicate whether or not your router's serial number should be included in the obtained certificate. The serial number is not used by IP Security or Internet Key Exchange but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular router. (Note that the serial number stored is the serial number of the internal board, not the one on the enclosure.) Ask your CA administrator if serial numbers should be included. If you are in doubt, include the serial number.

Normally, you would not include the IP address because the IP address binds the certificate more tightly to a specific entity. Also, if the router is moved, you would need to issue a new certificate. Finally, a router has multiple IP addresses, any of which might be used with IPSec.

If you indicate that the IP address should be included, you will then be prompted to specify the interface of the IP address. This interface should correspond to the interface that you apply your crypto map set to. If you apply crypto map sets to more than one interface, specify the interface that you name in the **crypto map local-address** command.

Examples

In the following example, a router with a general-purpose RSA key pair requests a certificate from the CA. When the router displays the certificate fingerprint, the administrator verifies this number by calling the CA administrator, who checks the number. The fingerprint is correct, so the router administrator accepts the certificate.

There can be a delay between when the router administrator sends the request and when the certificate is actually received by the router. The amount of delay depends on the CA method of operation.

```
Router(config)# crypto ca enroll myca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: <mypassword>
Re-enter password: <mypassword>
% The subject name in the certificate will be: myrouter.example.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 03433678
% Include an IP address in the subject name [yes/no]? yes
Interface: ethernet0/0
Request certificate from CA [yes/no]? yes
```

```
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificates' command will also show the fingerprint.
```

Some time later, the router receives the certificate from the CA and displays the following confirmation message:

```
Router(config)#   Fingerprint: 01234567 89ABCDEF FEDCBA98 75543210
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
Router(config)#
```

If necessary, the router administrator can verify the displayed Fingerprint with the CA administrator.

If there is a problem with the certificate request and the certificate is not granted, the following message is displayed on the console instead:

```
%CRYPTO-6-CERTREJ: Certificate enrollment request was rejected by Certificate Authority
```

The subject name in the certificate is automatically assigned to be the same as the RSA key pair's name. In the above example, the RSA key pair was named "myrouter.example.com." (The router assigned this name.)

Requesting certificates for a router with special usage keys would be the same as the previous example, except that two certificates would have been returned by the CA. When the router received the two certificates, the router would have displayed the same confirmation message:

```
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
```

Related Commands

Command	Description
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the router.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.
show crypto pki certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto ca trustpoint

Note Effective with Cisco IOS Release 12.3(8)T, 12.2(18)SXD, and 12.2(18)SXE, the **crypto ca trustpoint** command is replaced with the **crypto pki trustpoint** command. See the **crypto pki trustpoint** command for more information.

To declare the certification authority (CA) that your router should use, use the **crypto ca trustpoint** command in global configuration mode. To delete all identity information and certificates associated with the CA, use the **no** form of this command.

crypto ca trustpoint *name*

no crypto ca trustpoint *name*

Syntax Description

name	Creates a name for the CA. (If you previously declared the CA and just want to update its characteristics, specify the name you previously created.)

Command Default

Your router does not recognize any CAs until you declare a CA using this command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(15)T	The **match certificate** subcommand was introduced.
12.3(7)T	This command was replaced by the **crypto pki trustpoint** command. You can still enter the **crypto ca trusted-root**or **crypto ca trustpoint** command, but the command will be written in the configuration as "crypto pki trustpoint."

Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA, which can be a self-signed root CA or a subordinate CA. Issuing the **crypto ca trustpoint** command puts you in ca-trustpoint configuration mode.

You can specify characteristics for the trustpoint CA using the following subcommands:

- **crl** --Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.

- **default (ca-trustpoint)** --Resets the value of ca-trustpoint configuration mode subcommands to their defaults.
- **enrollment** --Specifies enrollment parameters (optional).
- **enrollment http-proxy** --Accesses the CA by HTTP through the proxy server.
- **match certificate** --Associates a certificate-based access control list (ACL) defined with the **crypto ca certificate map**command.
- **primary** --Assigns a specified trustpoint as the primary trustpoint of the router.
- **root** --Defines the Trivial File Transfer Protocol (TFTP) to get the CA certificate and specifies both a name for the server and a name for the file that will store the CA certificate.

Note Beginning with Cisco IOS Release 12.2(8)T, the **crypto ca trustpoint** command unified the functionality of the **crypto ca identity** and **crypto ca trusted-root** commands, thereby replacing these commands. Although you can still enter the **crypto ca identity** and **crypto ca trusted-root** commands, theconfiguration mode and command will be written in the configuration as **"crypto ca trustpoint**."

Examples

The following example shows how to declare the CA named "ka" and specify enrollment and CRL parameters:

```
crypto ca trustpoint ka
 enrollment url http://kahului:80
```

The following example shows a certificate-based access control list (ACL) with the label "Group" defined in a **crypto ca certificate map** command and included in the **match certificate** subcommand of the **crypto ca | pki trustpoint** command:

```
crypto ca certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto ca trustpoint pki
 match certificate Group
```

Related Commands

Command	Description
crl	Queries the CRL to ensure that the certificate of the peer has not been revoked.
default (ca-trustpoint)	Resets the value of a ca-trustpoint configuration subcommand to its default.
enrollment	Specifies the enrollment parameters of your CA.
enrollment http-proxy	Accesses the CA by HTTP through the proxy server.
primary	Assigns a specified trustpoint as the primary trustpoint of the router.

Command	Description
root	Obtains the CA certificate via TFTP.