



Certification Authority Interoperability Commands

This chapter describes Certification Authority (CA) interoperability commands.

Certification Authority (CA) interoperability is provided in support of the IP Security (IPSec) standard. CA interoperability permits Cisco IOS devices and CAs to communicate so that your Cisco IOS device can obtain and use digital certificates from the CA. Although IPSec can be implemented in your network without the use of a CA, using a CA provides manageability and scalability for IPSec.

Without CA interoperability, Cisco IOS devices could not use CAs when deploying IPSec. CAs provide a manageable, scalable solution for IPSec networks.

Refer to the *Command Reference Master Index* or search online to find complete descriptions of other commands used when configuring CA interoperability.

For configuration information, refer to the chapter “Configuring Certification Authority Interoperability” in the *Security Configuration Guide*.

certificate

To manually add certificates, use the **certificate** chain configuration command. Use the **no** form of this command to delete your router's certificate or any RA certificates stored on your router.

certificate *certificate-serial-number*

no certificate *certificate-serial-number*

Syntax Description

certificate-serial-number Specify the serial number of the certificate to add or delete.

Defaults

There are no defaults for this command.

Command Modes

Certificate chain configuration (config-cert-chain)

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

You could use this command to manually specify a certificate. However, this command is rarely used in this manner. Instead, this command is usually only used to delete certificates.

Examples

The following example deletes the router's certificate. In this example, the router had a general purpose RSA key pair with one corresponding certificate. The **show** command is used in this example to determine the serial number of the certificate to be deleted.

```
myrouter# show crypto ca certificates

Certificate
  Subject Name
    Name: myrouter.companyx.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set

myrouter# configure terminal
myrouter(config)# crypto ca certificate chain myca
myrouter(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
myrouter(config-cert-chain)# exit
myrouter(config)#
```

Related Commands**Command****Description****crypto ca certificate chain** Enters the certificate chain configuration mode.

crl optional



Note

Effective with Cisco IOS Release 12.3(2)T, this command was replaced by the **revocation-check** command.

To allow the certificates of other peers to be accepted without trying to obtain the appropriate CRL, use the **crl optional** command in ca-identity configuration mode. To return to the default behavior in which CRL checking is mandatory before your router can accept a certificate, use the **no** form of this command.

crl optional

no crl optional

Syntax Description

This command has no arguments or keywords.

Defaults

The router must have and check the appropriate CRL before accepting the certificate of another IP Security peer.

Command Modes

Ca-identity configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(2)T	This command was replaced by the revocation-check command.

Usage Guidelines

When your router receives a certificate from a peer, it will search its memory for the appropriate CRL. If the router finds the appropriate CRL, that CRL will be used. Otherwise, the router will download the CRL from either the certificate authority (CA) or from a CRL distribution point (CDP) as designated in the certificate of the peer. Your router will then check the CRL to ensure that the certificate that the peer sent has not been revoked. (If the certificate appears on the CRL, your router will not accept the certificate and will not authenticate the peer.) To instruct the router not to download the CRL and treat the certificate as not revoked, use the **crl optional** command.



Note

If the CRL already exists in the memory (for example, by using the **crypto ca crl request** command to manually download the CRL), the CRL will still be checked even if the **crl optional** command is configured.

Examples

The following example declares a CA and permits your router to accept certificates without trying to obtain a CRL. This example also specifies a nonstandard retry period and retry count.

```
crypto ca identity myca
```

```
enrollment url http://ca_server
enrollment retry-period 20
enrollment retry-count 100
crl optional
```

Related Commands

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

crypto ca authenticate

To authenticate the CA (by getting the CA's certificate), use the **crypto ca authenticate** global configuration command.

crypto ca authenticate *name*

Syntax Description

<i>name</i>	Specify the name of the CA. This is the same name used when the CA was declared with the crypto ca identity command.
-------------	---

Defaults

There are no defaults for this command.

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 CA's self-signed certificate which contains the CA's public key. Because the CA signs its own certificate, you should manually authenticate the CA's public key 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 RA 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").



Note

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 this example, the router requests the CA's certificate. The CA sends its certificate and the router prompts the administrator to verify the CA's certificate 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.

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

Related Commands

Command	Description
crypto ca identity	Declares the CA your router should use.
show crypto ca certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto ca certificate chain

To enter the certificate chain configuration mode, use the **crypto ca certificate chain** global configuration command. (You need to be in certificate chain configuration mode to delete certificates.)

crypto ca certificate chain *name*

Syntax Description

<i>name</i>	Specify the name of the CA. Use the same name as when you declared the CA using the crypto ca identity command.
-------------	--

Defaults

There are no defaults for this command.

Command Modes

Global configuration.

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command puts you into certificate chain configuration mode. When you are in certificate chain configuration mode, you can delete certificates using the **certificate** command.

Examples

The following example deletes the router's certificate. In this example, the router had a general purpose RSA key pair with one corresponding certificate. The **show** command is used to determine the serial number of the certificate to be deleted.

```
myrouter# show crypto ca certificates

Certificate
  Subject Name
    Name: myrouter.companyx.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 0123456789ABCDEF0123456789ABCDEF
  Key Usage: General Purpose

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set

myrouter# configure terminal
myrouter(config)# crypto ca certificate chain myca
myrouter(config-cert-chain)# no certificate 0123456789ABCDEF0123456789ABCDEF
% Are you sure you want to remove the certificate [yes/no]? yes
% Be sure to ask the CA administrator to revoke this certificate.
myrouter(config-cert-chain)# exit
myrouter(config)#
```

Related Commands

Command	Description
certificate	Adds certificates manually.

crypto ca certificate query

To specify that certificates and Certificate Revocation Lists (CRLs) should not be stored locally but retrieved from the CA when needed, use the **crypto ca certificate query** global configuration command. This command puts the router into query mode. Use the **no** form of this command to cause certificates and CRLs to be stored locally (the default).

crypto ca certificate query

no crypto ca certificate query

Syntax Description This command has no arguments or keywords.

Defaults Certificates and CRLs are stored locally in the router's NVRAM.

Command Modes Global configuration

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines Normally, certain certificates and Certificate Revocation Lists (CRLs) are stored locally in the router's NVRAM, and each certificate and CRL uses a moderate amount of memory.

To save NVRAM space, you can use this command to put the router into query mode, which prevents certificates and CRLs from being stored locally; instead, they are retrieved from the CA when needed. This will save NVRAM space but could result in a slight performance impact.

Examples This example prevents certificates and CRLs from being stored locally on the router; instead, they are retrieved from the CA when needed.

```
crypto ca certificate query
```

crypto ca crl request



Note

Effective with Cisco IOS Release 12.3(7)T, this command was replaced by the **crypto pki crl request** command.

To request that a new certificate revocation list (CRL) be obtained immediately from the certification authority, use the **crypto ca crl request** command in global configuration mode.

crypto ca crl request *name*

Syntax Description

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

Defaults

Normally, the router requests a new CRL when it is verifying a certificate and there is no CRL cached.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(7)T	This command was replaced by the crypto pki crl request command.

Usage Guidelines

A CRL lists all the certificates of the network device that have been revoked. Revoked certificates will not be honored by your router; therefore, any IPsec device with a revoked certificate cannot exchange IP Security traffic with your router.

The first time your router receives a certificate from a peer, it will download a CRL from the CA. Your router then checks the CRL to make sure the certificate of the peer has not been revoked. (If the certificate appears on the CRL, it will not accept the certificate and will not authenticate the peer.)

A CRL can be reused with subsequent certificates until the CRL expires. If your router receives the certificate of a peer after the applicable CRL has expired, it will download the new CRL.

If your router has a CRL which has not yet expired, but you suspect that the contents of the CRL are out of date, use the **crypto ca crl request** command to request that the latest CRL be immediately downloaded to replace the old CRL.

This command is not saved to the configuration.



Note

This command should be used only after the trustpoint is enrolled.

Examples

The following example immediately downloads the latest CRL to your router:

```
crypto ca crl request
```

crypto ca enroll

To obtain your router's certificate(s) from the CA, use the **crypto ca enroll** global configuration command. Use the **no** form of this command to delete a current enrollment request.

crypto ca enroll *name*

no crypto ca enroll *name*

Syntax Description

<i>name</i>	Specify the name of the CA. Use the same name as when you declared the CA using the crypto ca identity command.
-------------	--

Defaults

There are no defaults for this command.

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 of your router's RSA key pairs; 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 IPSec or IKE 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 this 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.

```
myrouter(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.companyx.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 ca certificate' command will also show the fingerprint.

myrouter(config)#
```

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

```
myrouter(config)#  Fingerprint: 01234567 89ABCDEF FEDCBA98 75543210

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

myrouter(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.domain.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
show crypto ca certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto ca identity

To declare the CA your router should use, use the **crypto ca identity** global configuration command. Use the **no** form of this command to delete all identity information and certificates associated with the CA.

crypto ca identity *name*

no crypto ca identity *name*

Syntax Description

<i>name</i>	Create a name for the CA. (If you previously declared the CA and just want to update its characteristics, specify the name you previously created.) The CA might require a particular name, such as its domain name.
-------------	--

Defaults

Your router does not know about any CA until you declare one with this command.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command to declare a CA. Performing this command puts you into the ca-identity configuration mode, where you can specify characteristics for the CA with the following commands:

- **enrollment url** (Specify the URL of the CA—always required.)
- **enrollment mode ra** (Specify RA mode, required only if your CA system provides a Registration Authority [RA]).
- **query url** (Specify the URL of the LDAP server, required only if your CA supports an RA and the LDAP protocol.)
- **enrollment retry-period** (Specify a period of time the router should wait between sending certificate request retries—optional.)
- **enrollment retry-count** (Specify how many certificate request retries your router will send before giving up—optional.)
- **crl optional** (Specify that your router can still accept other peers' certificates if the CRL is not accessible—optional.)

Examples

The following example declares a CA and identifies characteristics of the CA. In this example, the name “myca” is created for the CA, which is located at `http://ca_server`.

The CA does not use an RA or LDAP, and the CA's scripts are stored in the default location. This is the minimum possible configuration required to declare a CA.

```
crypto ca identity myca
  enrollment url http://ca_server
```

The following example declares a CA when the CA uses an RA. The CA's scripts are stored in the default location, and the CA uses the certificate enrollment protocol (CEP) instead of LDAP. This is the minimum possible configuration required to declare a CA that uses an RA.

```
crypto ca identity myca_with_ra
  enrollment url http://ca_server
  enrollment mode ra
  query url ldap://serverx
```

The following example declares a CA that uses an RA and a nonstandard cgi-bin script location. This example also specifies a nonstandard retry period and retry count, and permits the router to accept certificates when CRLs are not obtainable.

```
crypto ca identity myca_with_ra
  enrollment url http://companyx_ca/cgi-bin/somewhere/scripts.exe
  enrollment mode ra
  query url ldap://serverx
  enrollment retry-period 20
  enrollment retry-count 100
  crl optional
```

In the previous example, if the router does not receive a certificate back from the CA within 20 minutes of sending a certificate request, the router will resend the certificate request. The router will keep sending a certificate request every 20 minutes until a certificate is received or until 100 requests have been sent.

If the CA cgi-bin script location is not /cgi-bin/pkiclient.exe at the CA (the default CA cgi-bin script location) you need to also include the nonstandard script location in the URL, in the form of http://CA_name/script_location where script_location is the full path to the CA scripts.

Related Commands

Command	Description
enrollment url	Changes the URL of the CA.
enrollment mode ra	Turns on RA mode.
query url	Specifies LDAP protocol support.
enrollment retry-period	Specifies the wait period between certificate request retries.
enrollment retry-count	Specifies how many times a router will resend a certificate request.
crl optional	Allows other peer certificates to still be accepted by your router even if the appropriate CRL is not accessible to your router.

crypto key generate rsa (CA)

To generate RSA key pairs, use the **crypto key generate rsa** global configuration command.

```
crypto key generate rsa [usage-keys]
```

Syntax Description	usage-keys (Optional) Specifies that two special-usage key pairs should be generated, instead of one general-purpose key pair.				
Defaults	RSA key pairs do not exist. If the usage-keys keyword is not used, general-purpose keys will be generated.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>11.3 T</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	11.3 T	This command was introduced.
Release	Modification				
11.3 T	This command was introduced.				

Usage Guidelines

Use this command to generate RSA key pairs for your Cisco device (such as a router).

RSA keys are generated in pairs—one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys.



Note

Before issuing this command, make sure your router has a hostname and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a host name and IP domain name.

This command is not saved in the router configuration; however, the keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device).

There are two mutually-exclusive styles of RSA key pairs: special usage keys and general purpose keys. When you generate RSA key pairs, you will be prompted to select whether to generate special usage keys or general purpose keys.

Special Usage Keys

If you generate special usage keys, two pairs of RSA keys will be generated. One pair will be used with any IKE policy that specifies RSA signatures as the authentication method, and the other pair used with any IKE policy that specifies RSA encrypted nonces as the authentication method. (You configure RSA signatures or RSA encrypted nonces in your IKE policies as described in the *Security Configuration Guide*.)

A CA is used only with IKE policies specifying RSA signatures, not with IKE policies specifying RSA encrypted nonces. (However, you could specify more than one IKE policy, and have RSA signatures specified in one policy and RSA encrypted nonces in another policy.)

If you plan to have both types of RSA authentication methods in your IKE policies, you might prefer to generate special usage keys. With special usage keys, each key is not unnecessarily exposed. (Without special usage keys, one key is used for both purposes, increasing that key's exposure.)

General Purpose Keys

If you generate general purpose keys, only one pair of RSA keys will be generated. This pair will be used with IKE policies specifying either RSA signatures or RSA encrypted nonces. Therefore, a general purpose key pair might get used more frequently than a special usage key pair.

Modulus Length

When you generate RSA keys, you will be prompted to enter a modulus length. A longer modulus could offer stronger security, but takes longer to generate (see Table 413 for sample times) and takes longer to use. (The Cisco IOS software does not support a modulus greater than 2048 bits.) Below 512 is normally not recommended. (In certain situations, the shorter modulus may not function properly with IKE, so Cisco recommends using a minimum modulus of 1024.)

Table 413 Sample Times Required to Generate RSA Keys

Router	Modulus Length			
	360 bits	512 bits	1024 bits	2048 (maximum)
Cisco 2500	11 seconds	20 seconds	4 minutes, 38 seconds	longer than 1 hour
Cisco 4700	less than 1 second	1 second	4 seconds	50 seconds

Examples

This example generates special usage RSA keys.

```
myrouter(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.companyx.com
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

```
myrouter(config)#
```

This example generates general purpose RSA keys. (Note, you cannot generate both special usage and general purpose keys; you can only generate one or the other.)

```
myrouter(config)# crypto key generate rsa  
The name for the keys will be: myrouter.companyx.com
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose  
Keys. Choosing a key modulus greater than 512 may take a few minutes.  
How many bits in the modulus[512]? <return>  
Generating RSA keys.... [OK].
```

```
myrouter(config)#
```

Related Commands

Command	Description
show crypto key mypubkey rsa	Displays the RSA public key(s) of your router.

crypto key zeroize rsa

To delete all of your router's RSA keys, use the **crypto key zeroize rsa** global configuration command.

crypto key zeroize rsa

Syntax Description

There are no arguments or keywords for this command.

Defaults

There are no defaults for this command.

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command deletes all RSA keys that were previously generated by your router. If you issue this command, you must also perform two additional tasks:

- Ask the CA administrator to revoke your router's certificates at the CA; you must supply the challenge password you created when you originally obtained the router's certificates with the **crypto ca enroll** command.
- Manually remove the router's certificates from the configuration using the **certificate** command.



Note

This command cannot be undone (after you save your configuration), and after RSA keys have been deleted you cannot use certificates or the CA or participate in certificate exchanges with other IPSec peers unless you reconfigure CA interoperability by regenerating RSA keys, getting the CA's certificate, and requesting your own certificate again.

This command is not saved to the configuration.

Examples

This example deletes the general purpose RSA key pair that was previously generated for the router. After deleting the RSA key pair, the administrator contacts the CA administrator and requests that the router's certificate be revoked. The administrator then deletes the router's certificate from the configuration.

```
crypto key zeroize rsa
crypto ca certificate chain
no certificate
```

Related Commands

Command	Description
crypto ca certificate chain	Enters the certificate chain configuration mode.
certificate	Adds certificates manually.

enrollment mode ra

To turn on RA mode, use the **enrollment mode ra** ca-identity configuration command. Use the **no** form of the command to turn off RA mode.

enrollment mode ra

no enrollment mode ra

Syntax Description This command has no arguments or keywords.

Defaults RA mode is turned off.

Command Modes Ca-identity configuration

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines This command is required if your CA system provides a Registration Authority (RA). This command provides compatibility with RA systems.

Examples The following is an example of the minimum configuration required to declare a CA when the CA provides an RA.

```
crypto ca identity myca
enrollment url http://ca_server
enrollment mode ra
query url ldap://serverx
```

Related Commands	Command	Description
	crypto ca identity	Declares the CA your router should use.

enrollment retry-count

To specify how many times a router will resend a certificate request, use the **enrollment retry-count** *ca-identity* configuration command. Use the **no** form of the command to reset the retry count to the default of 0 which indicates an infinite number of retries.

enrollment retry-count *number*

no enrollment retry-count

Syntax Description

<i>number</i>	Specify how many times the router will resend a certificate request when the router does not receive a certificate from the CA from the previous request. Specify from 1 to 100 retries.
---------------	---

Defaults

The router will send the CA another certificate request until a valid certificate is received (no limit to the number of retries).

Command Modes

Ca-identity configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a period of time (the retry period) the router will send another certificate request. The router will continue to send requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries (the retry count) is exceeded. By default, the router will keep sending requests forever, but you can change this to a finite number with this command.

A retry count of 0 indicates that there is no limit to the number of times the router should resend the certificate request. By default, the retry count is 0.

Examples

This example declares a CA, changes the retry period to 10 minutes, and changes the retry count to 60 retries. The router will resend the certificate request every 10 minutes until the router receives the certificate or until approximately 10 hours pass since the original request was sent, whichever occurs first. (10 minutes x 60 tries = 600 minutes = 10 hours.)

```
crypto ca identity myca
enrollment url http://ca_server
enrollment retry-period 10
enrollment retry-count 60
```

■ enrollment retry-count

Related Commands

Command	Description
crypto ca identity	Declares the CA your router should use.
enrollment retry-period	Specifies the wait period between certificate request retries.

enrollment retry-period

To specify the wait period between certificate request retries, use the **enrollment retry-period** *ca-identity* configuration command. Use the **no** form of the command to reset the retry period to the default of 1 minute.

enrollment retry-period *minutes*

no enrollment retry-period

Syntax Description

minutes Specify the number of minutes the router waits before resending a certificate request to the CA, when the router does not receive a certificate from the CA by the previous request.

Specify from 1 to 60 minutes. By default, the router retries every 1 minute.

Defaults

The router will send the CA another certificate request every 1 minute until a valid certificate is received.

Command Modes

Ca-identity configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a period of time (the retry period) the router will send another certificate request. The router will continue to send requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries is exceeded. (By default, the router will keep sending requests forever, but you can change this to a finite number of permitted retries with the **enrollment retry-count** command.)

Use the **enrollment retry-period** command to change the retry period from the default of 1 minute between retries.

Examples

This example declares a CA and changes the retry period to 5 minutes.

```
crypto ca identity myca
  enrollment url http://ca_server
  enrollment retry-period 5
```

■ enrollment retry-period

Related Commands	Command	Description
	crypto ca identity	Declares the CA your router should use.
	enrollment retry-count	Specifies how many times a router will resend a certificate request.

enrollment url

To specify the CA location by naming the CA's URL, use the **enrollment url** ca-identity configuration command. Use the **no** form of this command to remove the CA's URL from the configuration.

enrollment url *url*

no enrollment url *url*

Syntax Description

url Specify the URL of the CA where your router should send certificate requests, for example, `http://ca_server`.

This URL must be in the form of `http://CA_name` where `CA_name` is the CA's host DNS name or IP address.

If the CA cgi-bin script location is not `/cgi-bin/pkiclient.exe` at the CA (the default CA cgi-bin script location) you need to also include the non-standard script location in the URL, in the form of `http://CA_name/script_location` where `script_location` is the full path to the CA scripts.

Defaults

Your router does not know the CA URL until you specify it with this command.

Command Modes

Ca-identity configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

Use this command to specify the CA's URL. This command is required when you declare a CA with the **crypto ca identity** command.

The URL must include the CA script location if the CA scripts are not loaded into the default cgi-script location. The CA administrator should be able to tell you where the CA scripts are located.

To change a CA's URL, repeat the **enrollment url** command to overwrite the older URL.

Examples

The following is an example of the absolute minimum configuration required to declare a CA.

```
crypto ca identity myca
  enrollment url http://ca_server
```

Related Commands

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

query url



Note

Effective with Cisco IOS Release 12.2(8)T, this command was replaced by the **crl query** command.

If you have to query the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked and you have to provide the Lightweight Directory Access Protocol (LDAP) server information, use the **query url** command in ca-trustpoint configuration mode. To return to the default behavior, assuming that the CRL distribution point (CDP) has a complete (LDAP) URL, use **no** form of this command.

```
query url ldap://hostname:[port]
```

```
query url ldap://hostname:[port]
```

Syntax Description

ldap://hostname	Query is made to the hostname of the LDAP server that serves the CRL for the certification authority (CA) server (for example, ldap://myldap.cisco.com).
:port	(Optional) Port number of the LDAP server (for example, ldap://myldap.cisco.com:3899).

Defaults

No enabled. If **query url ldap://hostname:[port]** is not enabled, the router assumes that the CDP that is embedded in the certificate is a complete URL (for example, ldap://myldap.cisco.com/CN=myCA,O=Cisco) and uses it to download the CRL.

If the port number is not configured, the default LDAP server port 389 will be used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(8)T	This command was replaced by the crl query command.

Usage Guidelines

When Cisco IOS software tries to verify a peer certificate (for example, during Internet Key Exchange [IKE] or Secure Sockets Layer [SSL] handshake), it queries the CRL to ensure that the certificate has not been revoked. To locate the CRL, it first looks for the CDP extension in the certificate. If the extension exists, it is used to download the CRL. Otherwise, the Simple Certificate Enrollment Protocol (SCEP) GetCRL mechanism is used to query the CRL from the CA server directly (some CA servers do not support this method).

Cisco IOS software supports three types of CDP:

- HTTP URL (Example 1: http://10.10.10.10:81/myca.crl)
- LDAP URL (Example 2: ldap://10.10.10.10:3899/CN=myca, O=cisco or Example 3: ldap:///CN=myca, O=cisco)

- LDAP/X.500 DN (Example 4: CN=myca, O=cisco)

To locate the CRL, a complete URL needs to be formed. As a result, Example 3 and Example 4 still require the hostname and the port number. The **ldap://hostname:[port]** keywords and arguments are used to provide this information.

**Note**

The **crypto ca trustpoint** command replaces the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to configure your router to query the CRL with the LDAP URL that is published by the CA named “bar”:

```
crypto ca trustpoint mytp
  enrollment url http://bar.cisco.com
  query url ldap://bar.cisco.com:3899
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
revocation-check	Checks the revocation status of a certificate.

show crypto ca certificates

To view information about your certificate, the CA's certificate, and any RA certificates, use the **show crypto ca certificates** EXEC command.

show crypto ca certificates

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.3 T	This command was introduced.

Usage Guidelines This command shows information about the following certificates:

- Your certificate, if you have requested one from the CA (see the **crypto ca enroll** command)
- The CA's certificate, if you have received the CA's certificate (see the **crypto ca authenticate** command)
- RA certificates, if you have received RA certificates (see the **crypto ca authenticate** command)

Examples The following is sample output from the **show crypto ca certificates** command after you authenticated the CA by requesting the CA's certificate and public key with the **crypto ca authenticate** command:

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The CA certificate might show Key Usage as "Not Set."

The following is sample output from the **show crypto ca certificates** command, and shows the router's certificate and the CA's certificate. In this example, a single, general purpose RSA key pair was previously generated, and a certificate was requested but not received for that key pair:

```
Certificate
  Subject Name
    Name: myrouter.companyx.com
    IP Address: 10.0.0.1
    Serial Number: 04806682
  Status: Pending
  Key Usage: General Purpose
    Fingerprint: 428125BD A3419600 3F6C7831 6CD8FA95 00000000

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

Note that in the previous sample, the router's certificate Status shows "Pending." After the router receives its certificate from the CA, the Status field changes to "Available" in the **show** output.

The following is sample output from the **show crypto ca certificates** command, and shows two router's certificates and the CA's certificate. In this example, special usage RSA key pairs were previously generated, and a certificate was requested and received for each key pair:

```
Certificate
  Subject Name
    Name: myrouter.companyx.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 428125BDA34196003F6C78316CD8FA95
  Key Usage: Signature

Certificate
  Subject Name
    Name: myrouter.companyx.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: AB352356AFCD0395E333CCFD7CD33897
  Key Usage: Encryption

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The following is sample output from the **show crypto ca certificates** command when the CA supports an RA. In this example, the CA and RA certificates were previously requested with the **crypto ca authenticate** command:

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set

RA Signature Certificate
  Status: Available
  Certificate Serial Number: 34BCF8A0
  Key Usage: Signature

RA KeyEncipher Certificate
  Status: Available
  Certificate Serial Number: 34BCF89F
  Key Usage: Encryption
```

Related Commands

Command	Description
crypto ca enroll	Obtains the certificate(s) of your router from the CA.
crypto ca authenticate	Authenticates the CA (by obtaining the certificate of the CA).

■ show crypto ca certificates