



Certification Authority Interoperability Commands

This chapter describes certification authority (CA) interoperability commands. 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.

To find complete descriptions of other commands used in this chapter, refer to the *Cisco IOS Command Reference Master Index* or search online.

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

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.

ca trust-point

To identify the trustpoints that will be used to validate a certificate during Internet Key Exchange (IKE) authentication, use the **ca trust-point** command in isakmp profile configuration mode. To remove the trustpoint, use the **no** form of this command.

ca trust-point *trustpoint-name*

no ca trust-point *trustpoint-name*

Syntax Description

<i>trustpoint-name</i>	The trustpoint name as defined in the global configuration.
------------------------	---

Defaults

If there is no trustpoint defined in the Internet Security Association and Key Management Protocol (ISAKMP) profile configuration, the default is to validate the certificate using all the trustpoints that are defined in the global configuration.

Command Modes

Isakmp profile configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The **ca trust-point** command can be used multiple times to define more than one trustpoint.

This command is useful when you want to restrict validation of certificates to a list of trustpoints. For example, the router global configuration has two trustpoints, A and B, which are trusted by VPN1 and VPN2, respectively. Each Virtual Private Network (VPN) wants to restrict validation only to its trustpoint.

Before you can use this command, you must enter the **crypto isakmp profile** command.

Examples

The following example specifies two trustpoints, A and B. The ISAKMP profile configuration restricts each VPN to one trustpoint.

```
crypto ca trustpoint A
enrollment url http://kahului:80
crypto ca trustpoint B
enrollment url http://arjun:80
!
crypto isakmp profile vpn1
  trustpoint A
!
crypto isakmp profile vpn2
  ca trust-point B
```

Related Commands	Command	Description
	crypto isakmp profile	Defines an ISAKMP profile.

certificate

To manually add certificates, use the **certificate** command in certificate chain configuration mode. To delete your router's certificate or any registration authority certificates stored on your router, use the **no** form of this command.

```
certificate certificate-serial-number
```

```
no certificate certificate-serial-number
```

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Certificate chain configuration

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 used only to add or 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.example.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 best-effort



Note

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

To download the certificate revocation list (CRL) but accept certificates if the CRL is not available, use the **crl best-effort** 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.

Syntax Description

This command has no arguments or keywords.

Defaults

If this command is not configured, CRL checking is mandatory before your router can accept a certificate. That is, if CRL downloading is attempted and it fails, the certificate will be considered invalid and will be rejected.

Command Modes

Ca-identity configuration

Command History

Release	Modification
12.2(8)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 appropriate CRL is in the router memory, the 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.)

When a CA system uses multiple CRLs, the certificate of the peer will indicate which CRL applies in its CDP extension and should be downloaded by your router.

If your router does not have the applicable CRL in memory and is unable to obtain one, your router will reject the certificate of the peer—unless you include the **crl best-effort** command in your configuration. When the **crl best-effort** command is configured, your router will try to obtain a CRL, but if it cannot obtain a CRL, it will treat the certificate of the peer as not revoked.

When your router receives additional certificates from peers, the router will continue to attempt to download the appropriate CRL if it was previously unsuccessful. The **crl best-effort** command specifies only that when the router cannot obtain the CRL, the router will not be forced to reject the certificate of a peer.

Examples

The following configuration example declares a CA and permits your router to accept certificates when CRLs are not obtainable:

```
crypto ca identity myid
enrollment url http://mycaserver
crl best-effort
```

Related Commands

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

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
```

■ **crl optional**

```
enrollment retry-period 20
enrollment retry-count 100
crl optional
```

Related Commands

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

crl query

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 **crl query** 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.

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

```
no crl query 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

Not enabled. If **crl query 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
12.1(1)T	This command was introduced.
12.2(8)T	This command replaced the query url 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
  crl query 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.

crypto ca authenticate

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

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

Defaults

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").



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 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.

```
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 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** command in global configuration mode. (You need to be in certificate chain configuration mode to delete certificates.)

crypto ca certificate chain *name*

Syntax Description

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

Defaults

No default behavior or values.

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.example.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 map

To define certificate-based access control lists (ACLs), use the **crypto ca certificate map** command in ca-certificate-map configuration mode. To remove the certificate-based ACLs, use the **no** form of this command.

crypto ca certificate map *label sequence-number*

no crypto ca certificate map *label sequence-number*

Syntax Description

<i>label</i>	A user-specified label that is referenced within the crypto ca trustpoint command.
<i>sequence-number</i>	A number that orders the ACLs with the same label. ACLs with the same label are processed from lowest to highest sequence number. When an ACL is matched, processing stops with a successful result.

Defaults

No default behavior or value.

Command Modes

Ca-certificate-map configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Issuing this command places the router in CA certificate map configuration mode where you can specify several certificate fields together with their matching criteria. The general form of these fields is as follows:

field-name match-criteria match-value

The *field-name* in the above example is one of the certificate fields. Field names are similar to the names used in the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) X.509 standard. The **name** field is a special field that matches any subject name or related name field in the certificate, such as the **alt-subject-name**, **subject-name**, and **unstructured-subject-name** fields.

- **alt-subject-name**—Case-insensitive string.
- **expires-on**—Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.
- **issuer-name**—Case-insensitive string.
- **name**—Case-insensitive string.
- **subject-name**—Case-insensitive string.
- **unstructured-subject-name**—Case-insensitive string.
- **valid-start**—Date field in the format dd mm yyyy hh:mm:ss or mmm dd yyyy hh:mm:ss.

**Note**

The time portion is optional in both the **expires-on** date and **valid-start** field and defaults to 00:00:00 if not specified. The time is interpreted according to the time zone offset configured for the router. The string **utc** can be appended to the date and time when they are configured as Universal Time, Coordinated (UTC) rather than local time.

The *match-criteria* in the example is one of the following logical operators:

- **eq**—equal (valid for name and date fields)
- **ne**—not equal (valid for name and date fields)
- **co**—contains (valid only for name fields)
- **nc**—does not contain (valid only for name fields)
- **lt**—less than (valid only for date fields)
- **ge**—greater than or equal to (valid only for date fields)

The *match-value* is a case-insensitive string or a date.

Examples

The following example shows how to configure a certificate-based ACL that will allow any certificate issued by Cisco Systems to an entity within the cisco.com domain. The label is Cisco, and the sequence is 10.

```
crypto ca certificate map Cisco 10
 issuer-name co Cisco Systems
 unstructured-subject-name co cisco.com
```

The following example accepts any certificate issued by Cisco Systems for an entity with DIAL or organizationUnit component ou=WAN. This certificate-based ACL consists of two separate ACLs tied together with the common label Group. Because the check for DIAL has a lower sequence number, it is performed first. Note that the string “DIAL” can occur anywhere in the subjectName field of the certificate, but the string WAN must be in the organizationUnit component.

```
crypto ca certificate map Group 10
 issuer-name co Cisco Systems
 subject-name co DIAL
crypto ca certificate map Group 20
 issuer-name co Cisco Systems
 subject-name co ou=WAN
```

Case is ignored in string comparisons; therefore, DIAL in the previous example will match dial, DIAL, Dial, and so on. Also note that the component identifiers (o=, ou=, cn=, and so on) are not required unless it is desirable that the string to be matched occurs in a specific component of the name. (Refer to the ITU-T security standards for more information about certificate fields and components such as ou=.)

If a component identifier is specified in the match string, the exact string, including the component identifier, must appear in the certificate. This requirement can present a problem if more than one component identifier is included in the match string. For example, “ou=WAN,o=Cisco Systems” will not match a certificate with the string “ou=WAN,ou=Engineering,o=Cisco Systems” because the “ou=Engineering” string separates the two desired component identifiers.

To match both “ou=WAN” and “o=Cisco Systems” in a certificate while ignoring other component identifiers, you could use this certificate map:

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

Any space character proceeding or following the equal sign (=) character in component identifiers is ignored. Therefore “o=Cisco” in the proceeding example will match “o = Cisco,” “o= Cisco,” “o=Cisco,” and so on.

Related Commands

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

crypto ca certificate query (global)

The **crypto ca certificate query** command in global configuration mode is replaced by the **crypto ca certificate query (ca-trustpoint)** command. See the **crypto ca certificate query (ca-trustpoint)** command for more information.

crypto ca certificate query (ca-trustpoint)

To specify that certificates should not be stored locally but retrieved from a certification authority (CA) trustpoint, use the **crypto ca certificate query** command in ca-trustpoint configuration mode. To cause certificates to be stored locally per trustpoint, use the **no** form of this command.

crypto ca certificate query

no crypto ca certificate query

Syntax Description

This command has no arguments or keywords.

Defaults

CA trustpoints are stored locally in the router's NVRAM.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

Normally, certain certificates are stored locally in the router's NVRAM, and each certificate uses a moderate amount of memory. To save NVRAM space, you can use this command to put the router into query mode, preventing certificates from being stored locally; instead, they are retrieved from a specified CA trustpoint when needed. This will save NVRAM space but could result in a slight performance impact.

The **crypto ca certificate query** command is a subcommand for each trustpoint; thus, this command can be disabled on a per-trustpoint basis.

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which puts you in ca-trustpoint configuration mode.



Note

This command deprecates the **crypto ca certificate query** command in global configuration mode. Although you can still enter the global configuration command, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to prevent certificates and certificate revocation lists (CRLs) from being stored locally on the router; instead, they are retrieved from the "ka" trustpoint when needed.

```
crypto ca trustpoint ka
.
.
.
crypto ca certificate query
```

■ **crypto ca certificate query (ca-trustpoint)**

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

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

<i>name</i>	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 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

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

Defaults

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.

```
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.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 ca certificate' command will also show the fingerprint.

myrouter(config)#
```

Some time later, the router receives the certificate from the CA and displays the following 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.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 ca certificates	Displays information about your certificate, the certificate of the CA, and any RA certificates.

crypto ca identity

The **crypto ca identity** command is replaced by the **crypto ca trustpoint** command. See the **crypto ca trustpoint** command for more information.

crypto ca import

To import a certificate manually via TFTP or as a cut-and-paste at the terminal, use the **crypto ca import** command in global configuration mode.

crypto ca import *name* **certificate**

Syntax Description	<i>name</i> certificate	Name of the certification authority (CA). This name is the same name used when the CA was declared with the crypto ca trustpoint command.
--------------------	--------------------------------	--

Defaults No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines You must enter the **crypto ca import** command twice if usage keys (signature and encryption keys) are used. The first time the command is entered, one of the certificates is pasted into the router; the second time the command is entered, the other certificate is pasted into the router. (It does not matter which certificate is pasted first.)

Examples The following example shows how to import a certificate via cut-and-paste. In this example, the CA trustpoint is "MS."

```
crypto ca trustpoint MS
  enroll terminal
  crypto ca authenticate MS
!
crypto ca enroll MS
crypto ca import MS certificate
```

Related Commands	Command	Description
	crypto ca trustpoint	Declares the CA that your router should use.
	enrollment	Specifies the enrollment parameters of your CA.
	enrollment terminal	Specifies manual cut-and-paste certificate enrollment.

crypto ca trusted-root

The **crypto ca trusted-root** command is replaced by the **crypto ca trustpoint** command. See the **crypto ca trustpoint** command for more information.

crypto ca trustpoint

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

<i>name</i>	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.)
-------------	--

Defaults

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.

Usage Guidelines

Use the **crypto ca trustpoint** command to declare a CA, which can be a root CA and have a self-signed certificate that contains its own public key. Issuing this command puts you in ca-trustpoint configuration mode.

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

- **crl best-effort**—Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.
- **crypto pki crl request**—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 TFTP protocol 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**

The **crypto ca trustpoint** command unifies 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, the configuration mode and command will be written back as 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 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 best-effort	Queries the CRL to ensure that the certificate of the peer has not been revoked.
crypto pki crl request	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.
root	Obtains the CA certificate via TFTP.

crypto key zeroize rsa

To delete all RSA keys from your router, use the **crypto key zeroize rsa** command in global configuration mode.

```
crypto key zeroize rsa [key-pair-label]
```

Syntax Description	<i>key-pair-label</i> (Optional) Specifies the name of the key pair that router will delete.
---------------------------	--

Defaults	No default behavior or values.
-----------------	--------------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.3 T	This command was introduced.
	12.2(8)T	The <i>key-pair-label</i> argument was added.

Usage Guidelines	<p>This command deletes all Rivest, Shamir, and Adelman (RSA) keys that were previously generated by your router unless you include the <i>key-pair-label</i> argument, which will delete only the specified RSA key pair. If you issue this command, you must also perform two additional tasks for each trustpoint that is associated with the key pair that was deleted:</p>
-------------------------	---

- Ask the certification authority (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 using the **crypto ca enroll** command.
- Manually remove the router's certificates from the configuration by removing the configured trustpoint (using the **no crypto ca trustpoint name** command.)



Note	<p>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 IP Security (IPSec) peers unless you reconfigure CA interoperability by regenerating RSA keys, getting the CA's certificate, and requesting your own certificate again.</p>
-------------	--

This command is not saved to the configuration.

Examples

The following 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 certificate of the router be revoked. The administrator then deletes the certificate of the router from the configuration.

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

Related Commands

Command	Description
certificate	Adds certificates manually.
crypto ca certificate chain	Enters the certificate chain configuration mode.
crypto ca trustpoint	Declares the CA that your router should use.
show crypto ca timers	Specifies which key pair to associate with the certificate.

crypto pki crl request

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

crypto pki crl request *name*

Syntax Description

<i>name</i>	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	The crypto ca crl request command was introduced.
12.3(7)T	This command replaced the crypto ca 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 pki 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 pki crl request
```

default (ca-trustpoint)

To reset the value of a ca-trustpoint configuration subcommand to its default, use the **default** command in ca-trustpoint configuration mode.

default *command-name*

Syntax Description

<i>command-name</i>	Ca-trustpoint configuration subcommand.
---------------------	---

Defaults

No default behavior or values.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which enters ca-trustpoint configuration mode.

Use this command to reset the value of a ca-trustpoint configuration mode subcommand to its default.

Examples

The following example shows how to remove the **crl optional** command from your configuration; the default of **crl optional** is off.

```
default crl optional
```

Related Commands

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

enrollment

To specify the enrollment parameters of a certification authority (CA), use the **enrollment** command in ca-trustpoint configuration mode. To remove any of the configured parameters, use the **no** form of this command.

enrollment [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url*

no enrollment [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url*

Syntax Description

mode	(Optional) Registration authority (RA) mode, if your CA system provides an RA.
retry period <i>minutes</i>	(Optional) Specifies the wait period between certificate request retries. The default is 1 minute between retries. (Specify between 1 to 60 minutes.)
retry count <i>number</i>	(Optional) Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. The default is 10 retries. (Specify from 1 to 100 retries.)
url <i>url</i>	URL of the CA where your router should send certificate requests. If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, <i>url</i> must be in the form <code>http://CA_name</code> , where <i>CA_name</i> is the host Domain Name System (DNS) name or IP address of the CA. If you are using TFTP for enrollment, <i>url</i> must be in the form <code>tftp://certserver/file_specification</code> . (The <i>file_specification</i> is optional. See the “Usage Guidelines” for additional information.)

Defaults

RA mode is turned off until you enable the **mode** keyword.

The router will send the CA another certificate request every 1 minute unless otherwise specified via the **retry period** *minutes* option.

The router will resend a certificate request 10 times unless otherwise specified via the via the **retry count** *number* option.

Your router does not know the CA URL until you specify it via **url** *url*.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(13)T	The url <i>url</i> option was enhanced to support TFTP enrollment.

Usage Guidelines

Use the **mode** keyword to specify the mode supported by the CA. This keyword is required if your CA system provides an RA.

Use the **retry period** *minutes* option to change the retry period from the default of 1 minute between retries. 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. By default, the router will send a maximum of 10 requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries (specified via the **retry count** *number* option) is exceeded.

Use the **url** *url* option to specify or change the URL of the CA. You can specify enrollment via SCEP (an HTTP URL) or TFTP (a TFTP URL).

TFTP enrollment is used to send the enrollment request and retrieve the certificate of the CA and the certificate of the router. If the *file_specification* is included in the URL, the router will append an extension onto the file specification. When the **crypto ca authenticate** command is entered, the router will retrieve the certificate of the CA from the specified TFTP server. As appropriate, the router will append the extension “.ca” to the filename or the fully qualified domain name (FQDN). (If the **url** *url* option does not include a file specification, the FQDN of the router will be used.)

**Note**

The **crypto ca trustpoint** command deprecates 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 declare a CA named “ka” and specify the URL of the CA as “http://kahului:80”:

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

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto ca trustpoint	Declares the CA that your router should use.

enrollment http-proxy

To access the certification authority (CA) by HTTP through the proxy server, use the **enrollment http-proxy** command in ca-trustpoint configuration mode.

enrollment http-proxy *host-name* *port-num*

Syntax Description

<i>host-name</i>	Defines the proxy server used to get the CA.
<i>port-num</i>	Specifies the port number used to access the CA.

Defaults

If this command is not enabled, the CA will not be accessed via HTTP.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

The **enrollment http-proxy** command must be used in conjunction with the **enrollment** command, which specifies the enrollment parameters for the CA.

Examples

The following example shows how to access the CA named “ka” by HTTP through the bomborra proxy server:

```
crypto ca trustpoint ka
enrollment url http://kahului
enrollment http-proxy bomborra 8080
crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of your CA.

enrollment mode ra

The **enrollment mode ra** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment retry count

The **enrollment retry count** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment retry period

The **enrollment retry period** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

enrollment terminal

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal** command in ca-trustpoint configuration mode. To delete a current enrollment request, use the **no** form of this command.

enrollment terminal

no enrollment terminal

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Ca-trustpoint configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines A user may wish to manually cut-and-paste certificate requests and certificates when he or she does not have a network connection between the router and certification authority (CA). When this command is enabled, the certificate request is printed on the console terminal so that it can be manually copied (cut) by the user.

Examples The following example shows how to specify manually certificate enrollment via cut-and-paste. In this example, the CA trustpoint is “MS.”

```
crypto ca trustpoint MS
 enrollment terminal
 crypto ca authenticate MS
!
crypto ca enroll MS
crypto ca import MS certificate
```

Related Commands	Command	Description
	crypto ca import	Imports a certificate manually via TFTP or cut-and-paste at the terminal.
	crypto ca trustpoint	Declares the CA that your router should use.

enrollment url

The **enrollment url** command is replaced by the **enrollment** command. See the **enrollment** command for more information.

ip-address (ca-trustpoint)

To specify a dotted IP address or an interface that will be included in the certificate request, use the **ip-address** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

```
ip-address {ip-address | interface}
```

```
no ip-address
```

Syntax Description

<i>ip-address</i>	Specifies a dotted IP address that will be included in the certificate request.
<i>interface</i>	Specifies an interface, from which the router can get an IP address, that will be included in the certificate request.

Defaults

You are prompted for the IP address during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

Before you can issue this command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode. The **ip address** command is a subcommand that allows you to specify a certificate enrollment parameter.

Use the **ip-address** command to include the IP address of the specified interface in the certificate request or to specify that an IP address should not be included in the certificate request.

If this command is enabled, you will not be prompted for an IP address during certificate enrollment.

Examples

The following example shows how to include the IP address of the Ethernet-0 interface in the certificate request for the trustpoint “frog”:

```
crypto ca trustpoint frog
  enrollment url http://frog.phoobin.com/
  subject-name OU=Spiral Dept., O=tiedye.com
  ip-address ethernet-0
```

Related Commands

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

match certificate

To associate a certificate-based access control list (ACL) defined with the **crypto ca certificate map** command, use the **match certificate** subcommand in ca-trustpoint configuration mode. To remove the association, use the **no** form of this subcommand.

match certificate *certificate-map-label*

no match certificate *certificate-map-label*

Syntax Description	<i>certificate-map-label</i> Matches the <i>label</i> argument specified in a previously defined crypto ca certificate map command.
---------------------------	--

Defaults	No default match certificate is configured.
-----------------	---

Command Modes	Ca-trustpoint configuration
----------------------	-----------------------------

Command History	Release	Modification
	12.2(15)T	This subcommand was introduced.

Usage Guidelines

The **match certificate** subcommand associates the certificate-based ACL defined with the **crypto ca certificate map** command to the trustpoint. The *certificate-map-label* argument in the **match certificate** subcommand must match the *label* argument specified in a previously defined **crypto ca certificate map** command.

The certificate map with the label *certificate-map-label* must be defined before it can be used with the **match certificate** subcommand.

A certificate referenced in a **match certificate** subcommand may not be deleted until all references to the certificate map are removed from configured trustpoints (that is, no **match certificate** subcommands can reference the certificate map being deleted).

When the certificate of a peer has been verified, the certificate-based ACL as specified by the certificate map is checked. If the certificate of the peer matches the certificate ACL, or a certificate map is not associated with the trustpoint used to verify the certificate of the peer, the certificate of the peer is considered valid.

If the certificate map does not have any attributes defined, the certificate is rejected.

Examples

The following example shows a certificate-based ACL with the label “Group” defined in a **crypto ca certificate map** command and included in the **match certificate** subcommand of the **crypto ca 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
crypto ca certificate map	Defines certificate-based ACLs.
crypto ca trustpoint	Declares the CA that your router should use.

password (ca-trustpoint)

To specify the revocation password for the certificate, use the **password** command in ca-trustpoint configuration mode. To erase any stored passwords, use the **no** form of this command.

password *string*

no password

Syntax Description

<i>string</i>	Name of the password.
---------------	-----------------------

Defaults

You are prompted for the password during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

Before you can issue the **password** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

This command allows you to specify the revocation password for the certificate before actual certificate enrollment begins. The specified password is encrypted when the updated configuration is written to NVRAM by the router.

If this command is enabled, you will not be prompted for a password during certificate enrollment.

Examples

The following example shows how to specify the password “revokme” for the certificate request:

```
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 revokme
```

Related Commands

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

primary

To assign a specified trustpoint as the primary trustpoint of the router, use the **primary** command in ca-trustpoint configuration mode.

primary *name*

Syntax Description

<i>name</i>	Name of the primary trustpoint of the router.
-------------	---

Defaults

No default behavior or values.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

Use the **primary** command to specify a given trustpoint as primary.

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which defines the trustpoint and enters ca-trustpoint configuration mode.

Examples

The following example shows how to configure the trustpoint “ka” as the primary trustpoint:

```
crypto ca trustpoint ka
  enrollment url http://xxx
  primary
  crl optional
```

Related Commands

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

query url



Note

Effective with Cisco IOS Release 12.2(8)T, this command was replaced by the **cr1 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 cr1 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.

root

To obtain the certification authority (CA) certificate via TFTP, use the **root** command in ca-trustpoint configuration mode. To deconfigure the CA, use the **no** form of this command.

```
root tftp server-hostname filename
```

```
no root tftp server-hostname filename
```

Syntax Description

tftp	Defines the TFTP protocol to get the root certificate.
<i>server-hostname</i>	Specifies a name for the server and a name for the file that will store the trustpoint CA.
<i>filename</i>	

Defaults

A CA certificate is not configured.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

This command allows you to access the CA via the TFTP protocol, which is used to get the CA. You want to configure a CA certificate so that your router can verify certificates issued to peers. Thus, your router does not have to enroll with the CA that issued the certificates the peers.

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which puts you in ca-trustpoint configuration mode.



Note

The **crypto ca trustpoint** command deprecates 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 the CA certificate named “bar” using TFTP:

```
crypto ca trustpoint bar
root tftp xxx fff
cr1 optional
```

■ root

Related Commands

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

root CEP

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

root PROXY

The **root PROXY** command is replaced by the **enrollment http-proxy** command. See the **enrollment http-proxy** command for more information.

root TFTP

The **root TFTP** command is replaced by the **root** command. See the **root** command for more information.

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>	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) Size of the desired Rivest, Shamir, Adelman (RSA) key. If not specified, the existing key size is used. (The specified size must be the same as the size of the <i>encryption-key-size</i> argument.)
<i>encryption-key-size</i>	(Optional) 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 size of the <i>key-size</i> argument.)

Defaults

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

Command Modes

Ca-trustpoint 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 key pair “exampleCAkeys”:

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

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crl best-effort	Generates RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

serial-number

To specify whether a serial number should be included in the certificate request, use the **serial-number** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

serial-number [none]

no serial-number

Syntax Description

none	(Optional) Specifies that a serial number will not be included in the certificate request.
-------------	--

Defaults

You are prompted for the serial number during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

Before you can issue the **serial-number** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

Use this command to specify the router serial number in the certificate request, or use the **none** keyword to specify that a serial number should not be included in the certificate request.

Examples

The following example shows how to omit a serial number from the “frog” certificate request:

```
crypto ca trustpoint frog
enrollment url http://frog.phoobin.com/
subject-name OU=Spiral Dept., O=tiedye.com
ip-address ethernet-0
serial-number none
auto-enroll regenerate
password revokeme
rsa-key frog 2048
```

Related Commands

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

show crypto ca certificates

To view information about your certificate, the certification authority certificate, and any registration authority certificates, use the **show crypto ca certificates** command in EXEC mode.

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 certificate of the CA, 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.example.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.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 428125BDA34196003F6C78316CD8FA95
  Key Usage: Signature
```

```
Certificate
  Subject Name
    Name: myrouter.example.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 authenticate	Authenticates the CA (by obtaining the certificate of the CA).
crypto ca enroll	Obtains the certificates of your router from the CA.
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the route.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.

show crypto ca crls

To display the current certificate revocation list (CRL) on router, use the **show crypto ca crls** command in EXEC configuration mode.

show crypto ca crls

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	12.1	This command was introduced.

Examples The following is sample output of the **show crypto ca crls** command:

```
Router# show crypto ca crls

CRL Issuer Name:
  OU = sjvpn, O = cisco, C = us
  LastUpdate: 16:17:34 PST Jan 10 2002
  NextUpdate: 17:17:34 PST Jan 11 2002
  Retrieved from CRL Distribution Point:
    LDAP: CN = CRL1, OU = sjvpn, O = cisco, C = us
```

Related Commands	Command	Description
	crypto ca crl request	Requests that a new CRL be obtained immediately from the CA.

show crypto ca roots

The **show crypto ca roots** command is replaced by the [show crypto ca trustpoints](#) command. See the [show crypto ca trustpoints](#) command for more information.

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 ca 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.

show crypto ca trustpoints

To display the trustpoints that are configured in the router, use the **show crypto ca trustpoints** command in EXEC mode.

show crypto ca trustpoints

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

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

Usage Guidelines This command deprecates the **show crypto ca roots** command. If you enter the **show crypto ca roots** command, the output will be written back as the **show crypto ca trustpoints** command.

Examples The following is sample output from the **show crypto ca trustpoints** command:

```
Router# show crypto ca trustpoints

Trustpoint bo:
  Subject Name:
    CN = bomborra Certificate Manager
    O = cisco.com
    C = US
    Serial Number:01
  Certificate configured.
  CEP URL:http://bomborra
  CRL query url:ldap://bomborra
```

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

source interface

To specify the address of an interface to be used as the source address for all outgoing TCP connections associated with a trustpoint, use the **source interface** command in ca-trustpoint configuration mode. To disable the interface that was specified, use the **no** form of this command.

source interface *interface-name*

no source interface *interface-name*

Syntax Description	<i>interface-name</i>	Interface address to be used as the source address for all outgoing TCP connections associated with a trustpoint.
Defaults	If this command is not specified, the address of the outgoing interface is used.	
Command Modes	Ca-trustpoint configuration	
Command History	Release	Modification
	12.2(15)T	This command was introduced.
Usage Guidelines	This command must be used following the crypto ca trustpoint command. If this command is used and the address of the outgoing interface is specified, the router uses the specified address (or address of the specified interface) as the source address for any datagrams that are sent to the certification authority (CA) server or Lightweight Directory Access Protocol (LDAP) server during authentication, enrollment, and if appropriate, when obtaining certificate revocation lists (CRLs).	
Examples	<p>In the following example, the router is located in a branch office. The router uses IP Security (IPSec) to communicate with the main office. Ethernet 1 is the “outside” interface that connects to the Internet Service Provider (ISP). Ethernet 0 is the interface connected to the LAN of the branch office. To access the CA server located in the main office the router needs to send its IP datagrams out interface Ethernet 1 (address 10.2.2.205) using the IPSec tunnel. Address 10.2.2.205 is assigned by the ISP. Address 10.2.2.205 is not a part of the branch office or main office.</p> <p>The CA cannot access any address outside the company because of a firewall. The CA sees a message coming from 10.2.2.205 and cannot respond (that is, it does not know that the router is located in a branch office at address 10.1.1.1, which it is able to reach).</p> <p>Adding the source interface command tells the router to use address 10.1.1.1 as the source address of the IP datagram that it sends to the CA. The CA is able to respond to 10.1.1.1.</p>	

This scenario is configured using the **source interface** command and the interface addresses as described above.

```
crypto ca trustpoint ms-ca
  enrollment url http://yourname:80/certsrv/mscep/mscep.dll
  source interface ethernet0
!
interface ethernet 0
  description inside interface
  ip address 10.1.1.1 255.255.255.0
!
interface ethernet 1
  description outside interface
  ip address 10.2.2.205 255.255.255.0
  crypto map main-office
```

Related Commands

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

subject-name

To specify the subject name in the certificate request, use the **subject-name** command in ca-trustpoint configuration mode. To clear any subject name from the configuration, use the **no** form of this command.

subject-name [*x.500-name*]

no subject-name [*x.500-name*]

Syntax Description

<i>x.500-name</i>	(Optional) Specifies the subject name used in the certificate request.
-------------------	--

Defaults

If the *x-500-name* argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

Before you can issue the **subject-name** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

The **subject-name** command is an attribute that can be set for autoenrollment; thus, issuing this command prevents you from being prompted for a subject name during enrollment.

Examples

The following example shows how to specify the subject name for the “frog” 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 revokme
```

Related Commands

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

usage

To specify the intended use for the certificate, use the **usage** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

```
usage method1 [method2, [method3]]
```

```
no usage method1 [method2, [method3]]
```

Syntax Description

<i>method1</i> [<i>method2</i> [<i>method3</i>]]	Intended use for the certificate; the available options are ike, ssl-client, and ssl-server. You must choose at least one method, and you may choose all three methods.
--	--

Defaults

ike

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

Before you can issue the **usage** command, you must enable the **crypto ca trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

This command may be used as a hint to set or clear key usage or other attributes in the certificate request.

Examples

The following example shows how to specify the certificate named “frog” for Internet Key Exchange (IKE):

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

Related Commands

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

