



Trustpoint CLI

Feature History

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

This document describes the Trustpoint CLI feature in Cisco IOS Release 12.2(8)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Configuration Tasks, page 4](#)
- [Monitoring and Maintaining Trustpoint CAs, page 5](#)
- [Configuration Examples, page 5](#)
- [Command Reference, page 6](#)
- [Glossary, page 21](#)

Feature Overview

The Trustpoint CLI feature introduces the **crypto ca trustpoint** command, which combines and replaces the functionality of the existing **crypto ca identity** command and the **crypto ca trusted-root** command.

Although both of these existing commands allow you to declare the certification authority (CA) that your router should use, only the **crypto ca identity** command supports enrollment (the requesting of a router certificate from a CA). Using the **crypto ca trustpoint** command, you can declare the CA and also specify any characteristics for the CA that the existing commands supported.



Note

When an existing configuration is loaded by an image that supports the **crypto ca trustpoint** command, all references to the **crypto ca identity** and **crypto ca trusted-root** commands are written back as **ca-trustpoint**. (Please see “[Identity and Trusted-Root Configuration Command Output Example](#)” for an example.)

Benefits

The **crypto ca trustpoint** command unifies the existing **crypto ca identity** command and **crypto ca trusted-root** command, thereby providing combined functionality under a single command.

Related Documents

- *Certificate Autoenrollment*, Cisco IOS Release 12.2(8)T feature module
- *Certificate Enrollment Enhancements*, Cisco IOS Release 12.2(8)T feature module
- The chapter “Configuring Certification Authority Interoperability” in the *Cisco IOS Security Configuration Guide*, Release 12.2
- The chapter “Certification Authority Interoperability Commands” in the *Cisco IOS Security Command Reference*, Release 12.2

Supported Platforms

This feature runs on all platforms that support IP Security (IPSec) and public key infrastructure (PKI).

- Cisco 800 series
- Cisco 805
- Cisco 806
- Cisco 828
- Cisco 1600 series
- Cisco 1600-R series
- Cisco 1710
- Cisco 1720
- Cisco 1721
- Cisco 1750
- Cisco 2420
- Cisco 2600 series
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series
- Cisco ICS 7700

- Cisco MC3810 series
- Cisco uBR7200 series
- Route Processor Module (RPM)
- Universal Route Module (URM)

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Supported Standards, MIBs, and RFCs

Standards

None

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

None

Configuration Tasks

See the following sections for configuration tasks for the Trustpoint CLI feature. Each task in the list is identified as either required or optional.

- [Configuring a Trustpoint CA](#) (required)
- [Getting the Certificate of a CA](#) (required)
- [Managing NVRAM Memory Usage](#) (optional)
- [Verifying a Trustpoint CA](#) (optional)

Configuring a Trustpoint CA

To declare the CA that your router should use and specify characteristics for the trustpoint CA, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# crypto ca trustpoint <i>name</i>	Declares the CA that your router should use. Enabling this command puts you in ca-trustpoint configuration mode.
Step 2	Router(ca-trustpoint)# enrollment [[mode ra] [retry period <i>minutes</i>] [retry count <i>number</i>] [url <i>url</i>]] or Router(ca-trustpoint)# root tftp <i>server-hostname filename</i>	Specifies enrollment parameters for your CA. Obtains the CA via TFTP.
Step 3	Router(ca-trustpoint)# enrollment http-proxy <i>host-name port-num</i>	Obtains the CA via HTTP through the proxy server. Note This command can be used in conjunction only with the enrollment command.
Step 4	Router(ca-trustpoint)# primary <i>name</i>	(Optional) Assigns a specified trustpoint as the primary trustpoint of the router.
Step 5	Router(ca-trustpoint)# crl { query <i>url</i> optional }	(Optional) Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked. Use query url to specify the Lightweight Directory Access Protocol (LDAP) URL published by the certification authority (CA) server to query the CRL; for example, <code>ldap://another_server</code> . Note If the query url option is not enabled, the router will check the CRL distribution point (CDP) that is embedded in the certificate.
Step 6	Router(ca-trustpoint)# default <i>command-name</i>	(Optional) Sets the value of ca-trustpoint configuration mode subcommand to its default.
Step 7	Router(ca-trustpoint)# exit	Exits ca-trustpoint configuration mode.

Getting the Certificate of a CA

To get the certificate of the CA, use the following global configuration command:

Command	Purpose
Router(config)# crypto ca authenticate	Takes the name of the CA as the argument.

Managing NVRAM Memory Usage

To specify that certificates should not be stored locally but retrieved from a CA trustpoint, use the following ca-trustpoint configuration command:

Command	Purpose
Router(ca-trustpoint)# crypto ca certificate query	Turns on query mode per specified trustpoint, causing certificates not to be stored locally.

Verifying a Trustpoint CA

To verify information about your certificate, the certificate of the CA, and registration authority (RA) certificates, use the **show crypto ca certificates** EXEC command.

Monitoring and Maintaining Trustpoint CAs

To monitor and maintain trustpoint CAs, use the following EXEC command:

Command	Purpose
Router# show crypto ca trustpoints	Displays the trustpoints that are configured in the router.

Configuration Examples

This section provides the following configuration examples:

- [Trustpoint CA Configuration Example](#)
- [Identity and Trusted-Root Configuration Command Output Example](#)

Trustpoint CA Configuration Example

The following example shows how to declare the CA named “kahului” and specify characteristics for the trustpoint CA:

```
crypto ca trustpoint kahului
  enrollment url http://kahului
  crl query ldap://kahului
```

Identity and Trusted-Root Configuration Command Output Example

The following example shows two existing configurations—the first configuration uses the **crypto ca identity** command, and the second configuration uses the **crypto ca trusted-root** command—whose new configuration changes to reflect the **crypto ca trustpoint** functionality:

```
! The existing configurations are as follows:
crypto ca identity bar
  enrollment url http://bar.cisco.com
  query url ldap://car.cisco.com
!
crypto ca trusted-root foo
  enrollment url http://foo.cisco.com

! The new configurations are as follows:
crypto ca trustpoint foo
  enrollment url http://bar.cisco.com
  crl query ldap://car.cisco.com
!
crypto ca trustpoint foo
  enrollment url http://foo.cisco.com
```

Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [crl](#)
- [crypto ca certificate query](#)
- [crypto ca trustpoint](#)
- [default \(ca-trustpoint\)](#)
- [enrollment](#)
- [enrollment http-proxy](#)
- [primary](#)
- [root](#)
- [show crypto ca trustpoints](#)

crl

To query the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked, use the **crl** command in ca-trustpoint configuration mode. To return to the default behavior in which the router will check the URL that is embedded in the certificate, use the **no** form of this command.

```
crl { query url | optional | best-effort }
```

```
no crl { query url | optional | best-effort }
```

Syntax Description

query <i>url</i>	The Lightweight Directory Access Protocol (LDAP) URL published by the certification authority (CA) server is specified to query the CRL; for example, ldap://another_server.
optional	CRL verification is optional.
best-effort	CRL verification will be attempted, but if the CRL is unavailable, the certificate will be accepted.

Defaults

If the **query** *url* option is not enabled, the router will check the CRL distribution point (CDP) that is embedded in the certificate. The **query** *url* option does not need to be configured if the CDP that is in the certificate is formatted as a URL (for example, http:// url or ldap:// url), including the fully qualified domain name (FQDN) of the host where the CRL is held.

Command Modes

Ca-trustpoint configuration

Command History

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

Usage Guidelines

The query Keyword

Use the **query** *url* option if the CDP is in LDAP form, which means that the CDP location in the certificate will indicate only where the CDP is located in the directory; that is, the CDP will not indicate the actual query location for the directory.

The optional Keyword

If your router does not have the applicable CRL and is unable to obtain one, your router will reject the peer's certificate—unless you include the **optional** keyword in your configuration. If you use the **optional** keyword, your router will check the CRL if it is cached in the router memory, but it will not download the CRL from the CDP. If the **optional** keyword is configured and a CRL is not available, the certificate will always be accepted. If the **crl optional** command is configured, you cannot manually download the CRL via the **crypto ca crl request** command because the manually downloaded CRL may not be deleted after it expires. The expired CRL may cause all certificate verifications to be denied.

The best-effort Keyword

If you prefer to have the CRL checked and accept certificates if the CRL is not available, use the **best-effort** keyword. This keyword allows the router to attempt to retrieve the CRL from the CDP that is contained in the certificate (or from a different location that is specified via the **crl query url** command). However, if the CRL is not available, the router will accept the certificate if it is presented within its validity period and if the certificate was issued by a trusted CA.

**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 your router to query the CRL with the LDAP URL that is published by the CA named “bar”:

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

Related Commands

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

crypto ca certificate query

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 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
```

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

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 know about any CAs until you declare one using this command.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command 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. Performing this command puts you in ca-trustpoint configuration mode.

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

- **crl**—Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.
- **default (ca-trustpoint)**—Resets the value of ca-trustpoint configuration mode subcommands to their defaults.
- **enrollment**—Specifies enrollment parameters (optional).
- **enrollment http-proxy**—Accesses the CA by HTTP through the proxy server.
- **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 deprecating 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 declare the CA named “ka” and specify enrollment and CRL parameters:

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

Related Commands

Command	Description
crl	Queries the CRL to ensure that the certificate of the peer has not been revoked.
crypto ca certificate query	Specifies that certificates and CRLs should not be stored locally but retrieved from a CA trustpoint.
default (ca-trustpoint)	Resets the value of a ca-trustpoint configuration subcommand to its default.
enrollment	Specifies the enrollment parameters of your CA.
enrollment http-proxy	Accesses the CA by HTTP through the proxy server.
primary	Assigns a specified trustpoint as the primary trustpoint of the router.
root	Obtains the CA certificate via TFTP.

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	<p>Before you can configure this command, you must enable the crypto ca trustpoint command, which puts you in ca-trustpoint configuration mode.</p> <p>Use this command to reset the value of a ca-trustpoint configuration mode subcommand to its default.</p>
-------------------------	--

Examples	<p>The following example shows how to remove crl optional from your configuration; the default of crl optional is off.</p> <pre>default crl optional</pre>
-----------------	--

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

enrollment

To specify the enrollment parameters of your 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 ra**] | [**retry period** *minutes*] | [**retry count** *number*] | [**url** *url*]]

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

Syntax Description

mode ra	(Optional) Specifies registration authority (RA) mode if your CA system provides a 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>	(Optional) Specifies the URL of the CA where your router should send certificate requests; for example, http://ca_server. <i>url</i> must be in the form http://CA_name, where CA_name is the CA's host Domain Name System (DNS) name or IP address.

Defaults

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

Usage Guidelines

Use the **mode ra** 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 (via the **retry count** *number* option) is exceeded.

Use **url** *url* to specify or change the URL of the CA.

**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 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 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.

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 puts you in 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.

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 the 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
crl optional
```

Related Commands

Command	Description
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.

Glossary

certification authority (CA)—A service responsible for managing certificate requests and issuing certificates to participating IPsec network devices. This service provides centralized key management for the participating devices and is explicitly entrusted by the receiver to validate identities and to create digital certificates.

enrollment—The process of obtaining a new certificate from a CA.

identity CA—A CA that issues a certificate verifying the identity of a router. An identity CA can be a root CA (and have a self-signed certificate), or it can have a chain of certificates that validate each CA between itself and the root CA. An identity CA uses its own certificate to sign the certificate of a router, thereby validating the identity of the router.

IP Security (IPsec)—A framework of open standards developed by the Internet Engineering Task Force (IETF). IPsec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (“peers”), such as Cisco routers.

peer certificate—The certificate presented by a peer, which contains the peer’s public key and is signed by the peer’s identity CA.

public key infrastructure (PKI)—Provides trusted and efficient key and certificate management to support security protocols such as IPsec.

registration authority (RA)—A server that acts as a proxy for the CA so that CA functions can continue when the CA is offline.

