



Query Mode Definition Per Trustpoint

Certificates contain public key information and are signed by Certificate Authority (CA) as proof of identity. Normally, all certificates are stored locally in the router's NVRAM, and each certificate uses a moderate amount of memory. The Query Mode Definition Per Trustpoint feature allows you to define a query for a specific trustpoint so that the certificates associated with that specific trustpoint can be stored on a remote server.

Feature History for Query Mode Definition Per Trustpoint

Release	Modification
12.3(7)T	This feature was introduced.
12.2(18)SXE	This feature migrated to 12.2(18)SXE.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Query Mode Definition per Trustpoint, page 2](#)
- [Information About Query Mode Definition Per Trustpoint, page 2](#)
- [How to Configure a Query Mode Definition per Trustpoint, page 2](#)
- [Configuration Examples for Query Mode Definition per Trustpoint, page 4](#)
- [Where to Go Next, page 5](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2004, 2005 Cisco Systems, Inc. All rights reserved.

Prerequisites for Query Mode Definition per Trustpoint

To initiate the query mode you must first configure CA trustpoints using the **crypto ca trustpoint** command.

Certificate Authority might support Query Mode through either Cisco's Simple Certificate Enrollment Protocol (SCEP) or Lightweight Directory Access Protocol (LDAP). Contact your CA administrator about this information.

Information About Query Mode Definition Per Trustpoint

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 prevent certificates from being stored locally; instead, they are retrieved from a remote server, such as a CA or LDAP server, during startup. This will save NVRAM space but could result in a slight performance impact.

Certificates associated with a specified trustpoint will not be written into NVRAM and the certificate query will be attempted during the next reload of the router.

Backward Compatibility with the **crypto ca certificate query** Command

When the global command **crypto ca certificate query** command is used, the query certificate will be added to all trustpoints on the router. When the **no crypto ca certificate query** command is used, any previous query certificate configuration will be removed from all trustpoints and any query in progress will be halted and the feature disabled.

Benefits of the Query Mode Definition Per Trustpoint

Especially useful for environments where multiple trustpoints are configured on a router, this feature allows you more control over use of the trustpoint. Query mode can be activated on specific trustpoints rather than on all of the trustpoints on a router.

How to Configure a Query Mode Definition per Trustpoint

This section contains instructions for configuring query mode definitions. It contains the following tasks:

- [Configuring a Trustpoint CA and Initiating Query Mode for Trustpoints, page 2](#)

Configuring a Trustpoint CA and Initiating Query Mode for Trustpoints

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:

Summary Steps

1. **enable**

2. **config t**
3. **crypto ca trustpoint *name***
4. **enrollment** [[**mode ra**]|[**retry period *minutes***]|[**retry count *number***]| [**url *url***]]
5. **enrollment http-proxy *host-name port-num***
6. **crl query *url***
7. **default *command-name***
8. **query certificate**
9. **exit**

	Command	Purpose
Step 1	Router(config)# crypto ca trustpoint <i>name</i> Example:	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>]] Example:	Specifies enrollment parameters for your CA.
Step 3	Router(ca-trustpoint)# enrollment http-proxy <i>host-name port-num</i> Example:	(Optional) 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)# crl query <i>url</i> Example: crl query http://ca-server1	(Optional) Specifies the URL for the CA server. If the CA server supports Query Mode through LDAP, configure the LDAP server information in this command "crl query ldap://ldap-server[:ldap-port]"
Step 5	Router(ca-trustpoint)# default <i>command-name</i> Example: Router(ca-trustpoint)# default query certificate	(Optional) Sets the value of ca-trustpoint configuration mode subcommand to its default. Default is off.
Step 6	Router(ca-trustpoint)# query certificate Example: Router(ca-trustpoint)# query certificate	Turns on query mode per specified trustpoint, causing certificates not to be stored locally and to be retrieved from a remote server.
Step 7	Router(ca-trustpoint)# exit Example: Router(ca-trustpoint)# exit	Exits ca-trustpoint configuration mode.

	Command	Purpose
Step 8	Router(config)# crypto ca authenticate <i>trustpoint-name</i>	Obtains CA certificate.
	Example: Router(config)# crypto ca authenticate trustpoint1	
Step 9	Router(config)# crypto key generate rsa	(Optional) Generates RSA key pairs.
	Example: Router(config)# crypto key generate rsa	
Step 10	Router(config)# crypto ca enroll <i>trustpoint-name</i>	(Optional) Obtains router certificate.
	Example: Router(config)# crypto ca enroll trustpoint1	

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.

For Query Mode to operate correctly during the next reload, the certificates need to be associated with the trustpoint. Use the **show crypto ca certificates command** to verify that each of the trustpoints has the needed certificates before storing the configuration and reloading the router.

Configuration Examples for Query Mode Definition per Trustpoint

The following example shows how to configure a trustpoint and initiate query mode.

- [Configuring a Trustpoint and Defining Query Mode Per Trustpoint Example, page 4](#)

Configuring a Trustpoint and Defining Query Mode Per Trustpoint Example

When you use the **query certificate** command, the certificates associated with the specified trustpoint will not be written into NVRAM. The query will be attempted during the next reload of the router.

In this example three trustpoints are configured: trustpoint1, trustpoint2, trustpoint3. The ca-server1 supports query mode through LDAP and stores certificates on ldap-server1. The ca-server2 supports Query Mode through SCEP. The certificates associated with trustpoint3 are stored locally in the NVRAM.

```
crypto ca trustpoint trustpoint1
  enrollment url http://ca-server1
  crl query ldap://ldap-server1
  query certificate
exit
```

```
crypto ca trustpoint trustpoint2
  enrollment url http://ca-server2
  query certificate
  exit
```

```
crypto ca trustpoint trustpoint3
  enrollment url http://ca-server3
  exit
```

If you use the **show startup config** command to look at the startup configuration, you can see that the trustpoint1 and trustpoint2 certificates will not be stored in NVRAM. Instead, they will be retrieved from the CA servers each time the router boots. Compare the displays that follow:

Query Mode Initiated

```
crypto ca certificate chain trustpoint1
  certificate 3869 query
  distinguished-name
    30463112 30100603 55040A13 09636973 636F2E63 6F6D3130 300F0603 55040513
    08313536 31373439 30301D06 092A8648 86F70D01 09021610 73747572 6E732E63
    6973636F 2E636F6D
  quit
  certificate ca 01 query
  fingerprint C21514AC1281594609F635EDFBB6CF31
  distinguished-name
    304E310B 30090603 55040613 02555331 12301006 0355040A 13096369 73636F2E
    636F6D31 0C300A06 0355040B 1303706B 69311D30 1B060355 04031314 6E736361
    2D723120 43657274 204D616E 61676572
  quit
```

```
crypto ca certificate chain trustpoint2
  certificate 5636499F0000000007CB query
  certificate 56363CFD0000000007CA query
  certificate ca 1244325DE0369880465F977A18F61CA8 query
  fingerprint 84E470A238176CB1AA0476B9C0B4F478
```

Certificates Stored in NVRAM

```
crypto ca certificate chain trustpoint3
  certificate 34AD nvram:nsca-r1CertM#33AD.cer
  certificate 34AC nvram:nsca-r1CertM#33AC.cer
  certificate ca 01 nvram:nsca-r1CertM#7201CA.cer
```

Additional References

The following sections provide references related to Query Mode Definition per Trustpoint.

Related Documents

Related Topic	Document Title
Information about certificate authorization	<i>Cisco IOS Security Configuration Guide, Release 12.3</i>
Information about trustpoint (introduced in Cisco IOS Release 12.2(8)T)	<i>Cisco IOS Security Configuration Guide, Release 12.3, Part IV, IP Security and Encryption</i> http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/sec_vcg.htm

Standards

Standards	Title
None.	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No specific RFCs are supported by this feature.	

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents the following new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3(7)T and 12.3 command reference publications.

- [query certificate](#)

query certificate

To configure query certificates on a per-trustpoint basis, use the **query certificate** command in Ca-trustpoint configuration mode. To disable creation of query certificates per trustpoint, use the **no** form of this command.

query certificate

[no] query certificate

Syntax Description

This command has no keywords or arguments.

Defaults

Query certificates are disabled. Certificates are stored in NVRAM.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(18)SXE	This command was incorporated into Release 12.2(18)SXE.

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 prevent certificates from being stored locally; instead, they are retrieved from a remote server, such as a Certificate Authority (CA) or Lightweight Directory Access Protocol (LDAP) server, during startup.

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

Using the query certificate Command with a Specific Trustpoint

When the **query certificate** command is used, certificates associated with the specified trustpoint will not be written into NVRAM and the certificate query will be attempted during the next reload of the router.

Applying the Query Mode Globally

When the global command **crypto ca certificate query** command is used, the query certificate will be added to all trustpoints on the router. When the **no crypto ca certificate query** command is used, any previously query certificate configuration will be removed from all trustpoints and any query in progress will be halted and the feature disabled.

Turning of Query Mode Already In-progress

During router startup, a one-minute timer will be set to trigger certificate query. You can use the **show crypto ca timers** command to display how much time is left before Query Mode starts. If the query attempt fails, the one-minute timer will be reset to trigger the next try. If you want to turn off the next query attempt, enter the **no query certificate** command.

Examples

The following example shows how to configure a trustpoint and initiate LDAP query mode for certificate authority:

```
crypto ca trustpoint trustpoint1
  enrollment url http://trustpoint1
  crl query ldap://trustpoint1
  query certificate
exit
```

Related Commands

Command	Description
crypto ca certificate query	Specifies that certificates should not be stored locally but retrieved from a CA trustpoint
crypto ca trustpoint	Declares the CA that your router should use.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)