



Public Key Infrastructure Commands on Cisco IOS XR Software

This chapter describes the Cisco IOS XR software commands used to configure Public Key Infrastructure (PKI).

For detailed information about PKI concepts, configuration tasks, and examples, see the *Implementing Certification Authority Interoperability on Cisco IOS XR Software* configuration module.

clear crypto ca certificates

To clear certificates associated with trustpoints that no longer exist in the configuration file, use the **clear crypto ca certificates** command in EXEC mode.

clear crypto ca certificates *trustpoint*

Syntax Description	<i>trustpoint</i> Trustpoint name.
---------------------------	------------------------------------

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

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

If the router is loaded with a new configuration file and certificates in the new configuration file do not have their corresponding trustpoint configuration, use the **clear crypto ca certificates** command to clear the certificates associated with trustpoints that no longer exist in the configuration file.

This command deletes both certification authority (CA) and router certificates from the system.

Examples

The following example shows how to clear the certificates associated with trustpoints that no longer exist in the configuration file:

```
RP/0/RP0/CPU0:router# clear crypto ca certificates tp_1
```

clear crypto ca crl

To clear all the Certificate Revocation Lists (CRLs) stored on the router, use the **clear crypto ca crl** command in EXEC mode.

clear crypto ca crl

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **clear crypto ca crl** command to clear all CRLs stored on the router. As a result, the router goes through the certification authorities (CAs) to download new CRLs for incoming certificate validation requests.

Examples The following example shows how to clear all CRLs stored on the router:

```
RP/0/RP0/CPU0:router# show crypto ca crls

CRL Entry
=====
Issuer : cn=Certificate Manager,ou=HFR,o=Cisco Systems,l=San Jose,st=CA,c=US
Last Update : [UTC] Wed Jun  5 02:40:04 2002
Next Update : [UTC] Wed Jun  5 03:00:04 2002
CRL Distribution Point :
      ldap://manager.cisco.com/CN=Certificate Manager,O=Cisco Systems

RP/0/RP0/CPU0:router# clear crypto ca crl
RP/0/RP0/CPU0:router# show crypto ca crls
```

Related Commands	Command	Description
	show crypto ca crls	Displays the information about CRLs on the router.

crypto ca authenticate

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

crypto ca authenticate *ca-name*

Syntax Description	<i>ca-name</i>	Name of the CA.
--------------------	----------------	-----------------

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

The **crypto ca authenticate** command is required when you initially configure CA support at your router.

This command authenticates the CA to your router by obtaining the CA certificate, which contains the public key for the CA. For self-signed root CA, because the CA signs its own certificate, you should manually authenticate the CA public key by contacting the CA administrator when you use this command.

Authenticating a second-level CA requires prior authentication of the root CA.

After this command is issued and the CA does not respond by the specified timeout period, you will obtain terminal control again in order to reenter the command.

Examples

In the following example, the router requests the CA certificate. The CA sends its certificate and the router prompts the administrator to verify the certificate by checking the certificate fingerprint (a unique identifier). The CA administrator can also display the CA certificate fingerprint, so you should compare what the CA administrator sees to what the router displays on the screen. If the fingerprint on the display matches the fingerprint displayed by the CA administrator, you should accept the certificate as valid.

```
RP/0/RP0/CPU0:router# crypto ca authenticate myca
```

```
Certificate has the following attributes:
```

```
Fingerprint: 0123 4567 89AB CDEF 0123
```

```
Do you accept this certificate? [yes/no] yes
```

Related Commands

Command	Description
crypto ca trustpoint	Configures a trusted point with a selected name.
show crypto ca certificates	Displays information about your certificate and the certificate of the CA.

crypto ca cancel-enroll

To cancel a current enrollment request, use the **crypto ca cancel-enroll** command in EXEC mode.

crypto ca cancel-enroll *ca-name*

Syntax Description	<i>ca-name</i>	Name of the certification authority (CA).
--------------------	----------------	---

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

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **crypto ca enroll** command to request certificates from the CA for the Rivest, Shamir, and Adelman (RSA) key pairs for the router defined by the **rsakeypair** command in trustpoint configuration mode. If no **rsakeypair** command is configured for the current trustpoint, the default RSA key pair is used for enrollment. This task is also known as enrolling with the CA. Use the **crypto ca cancel-enroll** command to cancel a current enrollment request.

Examples

The following example shows how to cancel a current enrollment request from a CA named myca:

```
RP/0/RP0/CPU0:router# crypto ca cancel-enroll myca
```

Related Commands	Command	Description
	crypto ca enroll	Obtains a router certificate from the CA.
	rsakeypair	Specifies a named RSA key pair for a trustpoint.

crypto ca enroll

To obtain a router certificate from the certification authority (CA), use the **crypto ca enroll** command in EXEC mode.

crypto ca enroll *ca-name*

Syntax Description

<i>ca-name</i>	Name of the CA.
----------------	-----------------

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **crypto ca enroll** command to request certificates from the CA for the Rivest, Shamir, and Adelman (RSA) key pairs for the router defined by the **rsakeypair** command in trustpoint configuration mode. If no **rsakeypair** command is configured for the current trustpoint, the default RSA key pair is used for enrollment. This task is also known as enrolling with the CA. (Enrolling and obtaining certificates are two separate events, but they both occur when the **crypto ca enroll** command is issued.)

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

If you already have a certificate for your keys, you are unable to configure this command; instead, you are prompted to remove the existing certificate first. (You can remove existing certificates by removing the trustpoint configuration with the **no crypto ca trustpoint** command.)

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

Examples

The following sample output is from the **crypto ca enroll** command:

```
RP/0/RP0/CPU0:router# 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 you password will not be saved in the configuration.
% Please make a note of it.
%Password
re-enter Password:
  Fingerprint: 4F35ADC9 2791997A CE211437 AFC66CF7
RP/0/RP0/CPU0:May 29 18:49:15.572 : pki_cmd: %PKI-6-LOG_INFO : certificate request pending
RP/0/RP0/CPU0:May 29 18:52:17.705 : pki_get_cert: %PKI-6-LOG_INFO : certificate is granted
```

Related Commands

Command	Description
crypto ca trustpoint	Configures a trusted point with a selected name.
rsa keypair	Specifies a named RSA key pair for a trustpoint.

crypto ca trustpoint

To configure a trusted point with a selected name, use the **crypto ca trustpoint** command in global configuration mode. To unconfigure a trusted point, use the **no** form of this command.

crypto ca trustpoint *ca-name*

no crypto ca trustpoint *ca-name*

Syntax Description

<i>ca-name</i>	Name of the certification authority (CA).
----------------	---

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **crypto ca trustpoint** command to declare a CA.

This command allows you to configure a trusted point with a selected name so that your router can verify certificates issued to peers. Your router need not enroll with the CA that issued the certificates to the peers.

This command enters trustpoint configuration mode, where you can specify characteristics for the CA with the following commands:

- **enrollment retry count**—The number of certificate request retries your router sends before giving up. Optional.
- **enrollment retry period**—The time the router waits between sending certificate request retries. Optional.
- **enrollment url**—The URL of the CA. Required.
- **query url**—The directory server URL where the Certificate Revocation List (CRL) is published. Only a string that begins with “ldap://” is accepted.
Required only if your CA supports the Lightweight Directory Access Protocol (LDAP) protocol.
- **rsa keypair**—The named Rivest, Shamir, and Adelman (RSA) key pair for this trustpoint.

Examples

The following example shows how to use the **crypto ca trustpoint** command to create a trustpoint:

```
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)# enrollment url http://myca.mydomain.com
```

Related Commands

Command	Description
enrollment retry count	Specifies how many times a router will resend a certificate request.
enrollment retry period	Specifies the wait period between certificate request retries.
enrollment url	Specifies the URL of the CA.
query url	Specifies the LDAP URL of the CRL distribution point.
rsakeypair	Specifies a named RSA key pair for this trustpoint.

crypto key generate dsa

To generate Digital Signature Algorithm (DSA) key pairs, use the **crypto key generate dsa** command in EXEC mode.

crypto key generate dsa

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **crypto key generate dsa** command to generate DSA key pairs for your router.

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

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

To remove the DSA key generated, use the **crypto key zeroize dsa** command.

Examples The following example shows how to generate a 512-bit DSA key:

```
RP/0/RP0/CPU0:router# crypto key generate dsa
```

```
The name for the keys will be: the_default
```

```
Choose the size of your DSA key modulus. Modulus size can be 512, 768, or 1024 bits.
```

```
Choosing a key modulus
```

```
How many bits in the modulus [1024]: 512
```

```
Generating DSA keys...
```

```
Done w/ crypto generate keypair
```

```
[OK]
```

crypto key generate dsa

Related Commands	Command	Description
	crypto key zeroize dsa	Deletes a DSA key pair from your router.
	show crypto key mypubkey dsa	Displays the DSA public keys for your router.

crypto key generate rsa

To generate a Rivest, Shamir, and Adelman (RSA) key pair, use the **crypto key generate rsa** command in EXEC mode.

```
crypto key generate rsa [usage-keys | general-keys] [keypair-label]
```

Syntax Description

usage-keys	(Optional) Generates separate RSA key pairs for signing and encryption.
general-keys	(Optional) Generates a general-purpose RSA key pair for signing and encryption.
<i>keypair-label</i>	(Optional) RSA key pair label that names the RSA key pairs.

Defaults

RSA key pairs do not exist. If the **usage-keys** keyword is not used, general-purpose keys are generated. If no RSA label is specified, the key is generated as the default RSA key.

Command Modes

EXEC

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **crypto key generate rsa** command to generate RSA key pairs for your router.

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

If your router already has RSA keys when you issue this command, you are warned and prompted to replace the existing keys with new keys. The keys generated by this command are saved in the secure NVRAM (which is not displayed to the user or backed up to another device).

To remove an RSA key, use the **crypto key zeroize rsa** command.

Examples

The following example shows how to generate an RSA key pair:

```
RP/0/RP0/CPU0:router# crypto key generate rsa
```

```
The name for the keys will be: the_default
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```
How many bits in the modulus[1024]: <return>
```

crypto key generate rsa**Related Commands**

Command	Description
crypto key zeroize rsa	Deletes the RSA key pair for your router.
show crypto key mypubkey rsa	Displays the RSA public keys for your router.

crypto key zeroize dsa

To delete the Digital Signature Algorithm (DSA) key pair from your router, use the **crypto key zeroize dsa** command in EXEC mode.

crypto key zeroize dsa

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **crypto key zeroize dsa** command to delete the DSA key pair that was previously generated by your router.

Examples The following example shows how to delete DSA keys from your router:

```
RP/0/RP0/CPU0:router# crypto key zeroize dsa

% Keys to be removed are named the_default
Do you really want to remove these keys? [yes/no]: yes
```

Related Commands	Command	Description
	crypto key generate dsa	Generates DSA key pairs.
	show crypto key mypubkey dsa	Displays the DSA public keys for your router.

crypto key zeroize rsa

To delete all Rivest, Shamir, and Adelman (RSA) keys from the router, use the **crypto key zeroize rsa** command in EXEC mode.

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

Syntax Description	<i>keypair-label</i> (Optional) Names the RSA key pair to be removed.
---------------------------	---

Defaults	If the key pair label is not specified, the default RSA key pair is removed.
-----------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
-------------------------	--

Use the **crypto key zeroize rsa** command to delete all RSA keys that were previously generated by the router. After issuing this command, you must perform two additional tasks:

- Ask the certification authority (CA) administrator to revoke the certificates for the router at the CA; you must supply the challenge password you created when you originally obtained the router certificates with the **crypto ca enroll** command CA.
- Manually remove the certificates from the configuration using the **clear crypto ca certificates** command.

Examples

The following example shows how to delete the general-purpose RSA key pair that was previously generated:

```
RP/0/RP0/CPU0:router# crypto key zeroize rsa key1

% Keys to be removed are named key1
Do you really want to remove these keys? [yes/no]: yes
```

Related Commands

Command	Description
clear crypto ca certificates	Clears certificates associated with trustpoints that no longer exist in the configuration file.
crypto ca enroll	Obtains a router certificate from the CA.
crypto key generate rsa	Generates RSA key pairs.
show crypto key mypubkey rsa	Displays the RSA public keys for your router.

description (trustpoint)

To create a description of a trustpoint, use the **description** command in trustpoint configuration mode. To delete a trustpoint description, use the **no** form of this command.

description *string*

no description

Syntax Description	<i>string</i>	Character string describing the trustpoint.
--------------------	---------------	---

Defaults	The default description is blank.
----------	-----------------------------------

Command Modes	Trustpoint configuration
---------------	--------------------------

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
------------------	--

Use the **description** command inside the trustpoint configuration submode to create a description for a trustpoint.

Examples	The following example shows how to create a trustpoint description:
----------	---

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)# description this is the primary trustpoint
```

enrollment retry count

To specify the number of times a router resends a certificate request to a certification authority (CA), use the **enrollment retry count** command in trustpoint configuration mode. To reset the retry count to the default, use the **no** form of this command.

enrollment retry count *number*

no enrollment retry count *number*

Syntax Description

<i>number</i>	Number of times the router resends a certificate request when the router does not receive a certificate from the previous request. The range is from 0 to 100, with 0 representing an infinite number of retries.
---------------	---

Defaults

If no retry count is specified, the default value is 10.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a specified time (the retry period), the router sends another certificate request. The router continues to send requests until it receives a valid certificate, the CA returns an enrollment error, or the configured number of retries (the retry count) is exceeded.

To reset the retry count to the default of 10, use the **no** form of this command. Setting the retry count to 0 indicates an infinite number of retries. The router sends the CA certificate requests until a valid certificate is received (there is no limit to the number of retries).

Examples

The following example shows how to declare a CA, change the retry period to 10 minutes, and change the retry count to 60 retries. The router resends the certificate request every 10 minutes until receipt of the certificate or approximately 10 hours pass since the original request was sent, whichever occurs first (10 minutes x 60 tries = 600 minutes = 10 hours).

```
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RP0/CPU0:router(config-trustp)# enrollment retry period 10
RP/0/RP0/CPU0:router(config-trustp)# enrollment retry count 60
```

■ enrollment retry count

Related Commands	Command	Description
	crypto ca trustpoint	Configures a trustpoint with a selected name.
	enrollment retry period	Specifies the wait period between certificate request retries.

enrollment retry period

To specify the wait period between certificate request retries, use the **enrollment retry period** command in trustpoint configuration mode. To reset the retry period to the default of 1 minute, use the **no** form of this command.

enrollment retry period *minutes*

no enrollment retry period *minutes*

Syntax Description

minutes Period (in minutes) between certificate requests issued to a certification authority (CA) from the router. The range is from 1 to 60 minutes.

Defaults

minutes: 1 minute

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a specified time (the retry period), the router sends another certificate request. The router continues to send requests until it receives a valid certificate, the CA returns an enrollment error, or the configured number of retries (the retry count) is exceeded.

The router sends the CA another certificate request every minute until a valid certificate is received. (By default, the router sends ten requests, but you can change the number of permitted retries with the **enrollment retry count** command.)

enrollment retry period**Examples**

The following example shows how to declare a CA and change the retry period to 5 minutes:

```
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca  
RP/0/RP0/CPU0:router(config-trustp)# enrollment retry period 5
```

Related Commands

Command	Description
crypto ca trustpoint	Configures a trustpoint with a selected name.
enrollment retry count	Specifies the number of times a router resends a certificate request.

enrollment url

To specify the certification authority (CA) location by naming the CA URL, use the **enrollment url** command in trustpoint configuration mode. To remove the CA URL from the configuration, use the **no** form of this command.

enrollment url *CA-URL*

no enrollment url *CA-URL*

Syntax Description

CA-URL URL of the CA server. The URL string must start with http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA (for example, http://ca-server).

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

Defaults

No default behavior or values

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **enrollment url** command to specify the CA URL. This command is required when you declare a CA with the **crypto ca trustpoint** command. The URL must include the CA script location if the CA scripts are not loaded into the default cgi-bin script location. The CA administrator should be able to tell you where the CA scripts are located.

To change the CA URL, repeat the **enrollment url** command to overwrite the previous URL.

enrollment url**Examples**

The following example shows the absolute minimum configuration required to declare a CA:

```
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca  
RP/0/RP0/CPU0:router(config-trustp)# enrollment url http://ca.domain.com/certsrv/mscep/  
mscep.d11
```

Related Commands

Command	Description
crypto ca trustpoint	Configures a trusted point with a selected name.

query url

To specify Lightweight Directory Access Protocol (LDAP) protocol support, use the **query url** command in trustpoint configuration mode. To remove the query URL from the configuration, use the **no** form of this command.

query url *LDAP-URL*

no query url *LDAP-URL*

Syntax Description

<i>LDAP-URL</i>	URL of the LDAP server (for example, ldap://another-server). This URL must be in the form of ldap://server-name where server-name is the host Domain Name System (DNS) name or IP address of the LDAP server.
-----------------	--

Defaults

The URL provided in the router certificate's CRLDistributionPoint extension is used.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

LDAP is a query protocol used when the router retrieves the Certificate Revocation List (CRL). The certification authority (CA) administrator should be able to tell you whether the CA supports LDAP; if the CA supports LDAP, the CA administrator can tell you the LDAP location where certificates and certificate revocation lists should be retrieved.

To change the query URL, repeat the **query url** command to overwrite the previous URL.

Examples

The following example shows the configuration required to declare a CA when the CA supports LDAP:

```
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)# query url ldap://my-ldap.domain.com
```

Related Commands

Command	Description
crypto ca trustpoint	Configures a trusted point with a selected name.

rsakeypair

To specify a named Rivest, Shamir, and Adelman (RSA) key pair for this trustpoint, use the **rsakeypair** command in trustpoint configuration mode. To reset the RSA key pair to the default, use the **no** form of this command.

rsakeypair *keypair-label*

no rsakeypair *keypair-label*

Syntax Description

<i>keypair-label</i>	RSA key pair label that names the RSA key pairs.
----------------------	--

Defaults

If the RSA key pair is not specified, the default RSA key is used for this trustpoint.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **rsakeypair** command to specify a named RSA key pair generated using the **crypto key generate rsa** command for this trustpoint.

Examples

The following example shows how to specify the named RSA key pair key1 for the trustpoint myca:

```
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)# rsakeypair key1
```

Related Commands

Command	Description
crypto key generate rsa	Generates RSA key pairs.

show crypto ca certificates

To display information about your certificate and the certification authority (CA) certificate, use the **show crypto ca certificates** command in EXEC mode.

show crypto ca certificates

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Use the **show crypto ca certificates** command to display information about the following certificates:

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

Examples The following sample output is from the **show crypto ca certificates** command. The output is self-explanatory.

```
RP/0/RP0/CPU0:router# show crypto ca certificates

Trustpoint          : myca
=====
CA certificate
  Serial Number    : 01
  Subject Name     :
    cn=Certificate Manager,ou=HFR,o=Cisco Systems,l=San Jose,st=CA,c=US
  Issued By        :
    cn=Certificate Manager,ou=HFR,o=Cisco Systems,l=San Jose,st=CA,c=US
  Validity Start   : [UTC] Thu Mar 28 08:00:00 2002
  Validity End     : [UTC] Sun Mar 28 08:00:00 2010
Router certificate
  Key usage        : General Purpose
  Status           : Available
  Serial Number    : 00:C4
  Subject Name     :
```

show crypto ca certificates

```

unstructuredName=user1.cisco.com,o=Cisco Systems
Issued By      :
  cn=Certificate Manager,ou=HFR,o=Cisco Systems,l=San Jose,st=CA,c=US
Validity Start : [UTC] Wed May 29 18:53:29 2002
Validity End   : [UTC] Wed Jun  5 18:53:29 2002
CRL Distribution Point
  ldap://manager.cisco.com/CN=Certificate Manager,O=Cisco Systems

```

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.
crypto ca trustpoint	Configures a trustpoint with a selected name.

show crypto ca crls

To display information about the local cache Certificate Revocation List (CRL), use the **show crypto ca crls** command in EXEC mode.

show crypto ca crls

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Examples The following sample output is from the **show crypto ca crls** command. The output is self-explanatory.

```
RP/0/RP0/CPU0:router# show crypto ca crls

CRL Entry
=====
Issuer : cn=xyz-w2k-root,ou=HFR,o=Cisco System,l=San Jose,st=CA,c=US
Last Update : [UTC] Thu Jan 10 01:01:14 2002
Next Update : [UTC] Thu Jan 17 13:21:14 2002
CRL Distribution Point :
http://xyz-w2k.cisco.com/CertEnroll/xyz-w2k-root.crl
```

Related Commands	Command	Description
	clear crypto ca crl	Clears all the CRLs stored on the router.

show crypto key mypubkey dsa

To display the Directory System Agent (DSA) public keys for your router, use the **show crypto key mypubkey dsa** command in EXEC mode.

```
show crypto key mypubkey dsa
```

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Examples The following sample output is from the **show crypto key mypubkey dsa** command. The output is self-explanatory.

```
RP/0/RP0/CPU0:router# show crypto key mypubkey dsa

Key label: mykey
Type : RSA General purpose
Size : 1024
Created : 17:33:23 UTC Thu Sep 18 2003
Data :
3081F230 81AA0605 2B0E0302 0C3081A0 02020200 024100C8 A36B6179 56B8D620
1F77595C 32EF3004 577A9F79 0A8ABDA4 89FB969D 35C04E7E 5491ED4E 120C657C
610576E5 841696B6 0948846C C92F56E5 B4921458 70FC4902 1500AB61 5C0D63D3
EB082BB9 F16030C5 AA0B5D1A DFE50240 73F661EA 9F579E77 B413DBC4 9047B4F2
10A1CFCB 14D98B57 3E0BBA97 9B5120AD F52BBDC7 15B63454 8CB54885 92B6C9DF
7DC27768 FD296844 42024945 5E86C81A 03430002 4071B49E F80F9E4B AF2B62E7
AA817460 87EFD503 C668AD8C D606050B 225CC277 7C0A0974 8072D7D7 2ADDDE42
329FE896 AB015ED1 3A414254 6935FDCA 0043BA4F 66
```

Related Commands	Command	Description
	crypto key generate dsa	Generates DSA key pairs.
	crypto key zeroize dsa	Deletes all DSA keys from the router.

show crypto key mypubkey rsa

To display the Rivest, Shamir, and Adelman (RSA) public keys for your router, use the **show crypto key mypubkey rsa** command in EXEC mode.

show crypto key mypubkey rsa

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Examples The following sample output is from the **show crypto key mypubkey rsa** command. The output is self-explanatory.

```
RP/0/RP0/CPU0:router# show crypto key mypubkey rsa

Key label: mykey
Type : RSA General purpose
Size : 1024
Data :
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CF8CDF
5BFCA055 DA4D164D F6EDB78B 926B1DDE 0383027F BA71BCC6 9D5592C4 5BA8670E
35CD19B7 1C973A46 62CC5F8C 82BD596C F292410F 8E83B753 4BA71BAC 41AB6B60
F34A2499 EDE11639 F88B4210 B2A0CF5F DD678C36 0D8B7DE1 A2AB5122 9ED947D5
76CF5BCD D9A2039F D02841B0 7F8BFF97 C080B791 10A9ED41 00FB6F40 95020301
0001

Key label: the_default
Type : RSA General purpose
Size : 512
Data :
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C7DE73 7B3EA447
CCE8F3DF DD1327D8 C1C30C45 2EEB4981 B1B48D2B 1AF14665 178058FB 8F6BB6BB
E08C6163 FA0EE356 395C8E5F 2AC59383 0706BDDF EC8E5822 9B020301 0001
```

Related Commands

Command	Description
crypto key generate rsa	Generates RSA key pairs.
crypto key zeroize rsa	Deletes all RSA keys from the router.

■ show crypto key mypubkey rsa