Public Key Infrastructure Commands

This module describes the 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 the Cisco ASR 9000 Series Router* module in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

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.

clear crypto ca certificates *trustpoint*

Syntax Description

trustpoint	Trustpoint name.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.

The **clear crypto ca certificates** command deletes both certification authority (CA) and router certificates from the system.

Task ID

Task ID	Operations
crypto	execute

Examples

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

```
RP/0/RSP0/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.

clear crypto ca crl

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.

Task ID

Task ID	Operations
crypto	execute

Examples

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

```
RP/0/RSP0/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/RSP0/CPU0:router# clear crypto ca crl
RP/0/RSP0/CPU0:router# show crypto ca crls
RP/0/RSP0/CPU0:router#
```

Related Commands

Command	Description
show crypto ca crls, on page 48	Displays the information about CRLs on the router.

crl optional (trustpoint)

To allow the certificates of other peers to be accepted without trying to obtain the appropriate CRL, use the **crl optional** command in trustpoint 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 keywords or arguments.

Command Default

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

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When your router receives a certificate from a peer, it searches its memory for the appropriate CRL. If the router finds the appropriate CRL, that CRL is used. Otherwise, the router downloads 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 cannot 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.

Task ID

Task ID	Operations
crypto	read, write

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.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry period 20
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry count 100
RP/0/RSP0/CPU0:router(config-trustp)# crl optional
```

Related Commands

Command	Description
crypto ca trustpoint, on page 13	Configures a trusted point with a selected name.
enrollment retry count, on page 27	Specifies how many times a router resends a certificate request.
enrollment retry period, on page 29	Specifies the wait period between certificate request retries.
enrollment url, on page 32	Specifies the URL of the CA.

crypto ca authenticate

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

crypto ca authenticate *ca-name*

Syntax Description

ca-name	Name of the CA Server.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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. The certificate fingerprint matching is done out-of-band (for example, phone call, and so forth).

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

After the **crypto ca authenticate** command is issued and the CA does not respond by the specified timeout period, you must obtain terminal control again to re-enter the command.

Task ID

Task ID	Operations
crypto	execute

Examples

The CA sends the 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.

The following example shows that the router requests the CA certificate:

```
RP/0/RSP0/CPU0:router# crypto ca authenticate msiox
Retrieve Certificate from SFTP server? [yes/no]: yes
Read 860 bytes as CA certificate
  Serial Number  : 06:A5:1B:E6:4F:5D:F7:83:41:11:D5:F9:22:7F:95:23
```

```
  Subject:
    Name: CA2
    CN= CA2
  Issued By      :
        cn=CA2
  Validity Start : 07:51:51 UTC Wed Jul 06 2005
  Validity End   : 08:00:43 UTC Tue Jul 06 2010
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Certificate has the following attributes:
   Fingerprint: D0 44 36 48 CE 08 9D 29 04 C4 2D 69 80 55 53 A3

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


RP/0/RSP0/CPU0:router#:Apr 10 00:28:52.324 : cepki[335]: %SECURITY-CEPKI-6-INFO : certificate
 database updated
Do you accept this certificate? [yes/no] yes
```

Related Commands

Command	Description
crypto ca trustpoint, on page 13	Configures a trusted point with a selected name.
show crypto ca certificates, on page 46	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.

crypto ca cancel-enroll *ca-name*

Syntax Description

ca-name	Name of the certification authority (CA).

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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, on page 38 command in trustpoint configuration mode. If no rsakeypair, on page 38 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.

Task ID

Task ID	Operations
crypto	execute

Examples

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

```
RP/0/RSP0/CPU0:router# crypto ca cancel-enroll myca
```

Related Commands

Command	Description
crypto ca enroll, on page 10	Obtains a router certificate from the CA.
rsakeypair, on page 38	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.

crypto ca enroll *ca-name*

Syntax Description

ca-name	Name of the CA Server.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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, on page 38 command in trustpoint configuration mode. If no rsakeypair, on page 38 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.) When using manual enrollment, these two operations occur separately.

The 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.

Task ID

Task ID	Operations
crypto	execute

Examples

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

```
RP/0/RSP0/CPU0:router# crypto ca enroll msiox
% 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/RSP0/CPU0:May 29 18:49:15.572 : pki_cmd: %PKI-6-LOG_INFO : certificate request pending
RP/0/RSP0/CPU0:May 29 18:52:17.705 : pki_get_cert: %PKI-6-LOG_INFO : certificate is granted
```

Related Commands

Command	Description
crypto ca trustpoint, on page 13	Configures a trusted point with a selected name.
rsakeypair, on page 38	Specifies a named RSA key pair for a trustpoint.

crypto ca import

To import a certification authority (CA) certificate manually through TFTP, SFTP, or cut and paste it at the terminal, use the **crypto ca import** command.

crypto ca import *name* **certificate**

Syntax Description

name **certificate**	Name of the certification authority (CA). This name is the same name used when the CA was declared with the crypto ca trustpoint, on page 13 command.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to import a CA certificate through cut-and-paste. In this example, the certificate is myca.

```
RP/0/RSP0/CPU0:router# crypto ca import myca certificate
```

Related Commands

Command	Description
crypto ca trustpoint, on page 13	Configures a trusted point with a selected name.
show crypto ca certificates, on page 46	Displays information about your certificate and the certification authority (CA) certificate.

crypto ca trustpoint

To configure a trusted point with a selected name, use the **crypto ca trustpoint** command. 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

ca-name	Name of the CA.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.

The **crypto ca trustpoint** command enters trustpoint configuration mode, in which you can specify characteristics for the CA with the following commands:

- crl optional (trustpoint), on page 5 command—The certificates of other peers are accepted without trying to obtain the appropriate CRL.
- enrollment retry count, on page 27 command—The number of certificate request retries your router sends before giving up. Optional.
- enrollment retry period, on page 29 command—(Optional)—The time the router waits between sending certificate request retries.
- enrollment terminal, on page 31 command—When you do not have a network connection between the router and certification authority (CA), manually cut-and-paste certificate requests and certificates.
- enrollment url, on page 32 command—(Optional)—The URL of the CA.
- ip-address (trustpoint), on page 34command—A dotted IP address that is included as an unstructured address in the certificate request.
- query url, on page 36command—The directory server URL in which the Certificate Revocation List (CRL) is published. Only a string that begins with “ldap://” is accepted.

  Required only if your CA supports Lightweight Directory Access Protocol (LDAP).
- rsakeypair, on page 38command—The named Rivest, Shamir, and Adelman (RSA) key pair for this trustpoint.
- serial-number (trustpoint), on page 39command—Router serial number in the certificate request.

- sftp-password (trustpoint), on page 41command—FTP secure password.
- sftp-username (trustpoint), on page 43command—FTP secure username.
- subject-name (trustpoint), on page 44command—Subject name in the certificate request.

Task ID

Task ID	Operations
crypto	execute

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RSP0/CPU0:router(config-trustp)# sftp-password xxxxxx
RP/0/RSP0/CPU0:router(config-trustp)# sftp-username tmordeko
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url
sftp://192.168..254.254/tftpboot/tmordeko/CAcert
RP/0/RSP0/CPU0:router(config-trustp)# rsakeypair label-2
```

Related Commands

Command	Description
crl optional (trustpoint), on page 5	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.
enrollment retry count, on page 27	Specifies how many times a router resends a certificate request.
enrollment retry period, on page 29	Specifies the wait period between certificate request retries.
enrollment terminal, on page 31	Specifies manual cut-and-paste certificate enrollment.
enrollment url, on page 32	Specifies the URL of the CA.
query url, on page 36	Specifies the LDAP URL of the CRL distribution point.
rsakeypair, on page 38	Specifies a named RSA key pair for this trustpoint.
sftp-password (trustpoint), on page 41	Secures the FTP password.
sftp-username (trustpoint), on page 43	Secures the FTP username.

crypto ca trustpool import url

To manually update certificates in the trust pool if they are not current, are corrupt, or if certain certificates need to be updated, use the **crypto ca trustpool import url**command.

crypto ca trustpool import url {**clean***URL*}

Syntax Description

clean	(Optional) Manually remove all downloaded certificate authority (CA) certificates.
URL	Specify the URL from which the CA trust pool certificate bundle must be downloaded. This manually imports (downloads) the CA certificate bundle into the CA trust pool to update or replace the existing CA certificate bundle.

Command Default

The CA trust pool feature is enabled. The router uses the built-in CA certificate bundle in the CA trust pool which is updated automatically from Cisco.

Command Modes

EXEC

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The CA trust pool feature is enabled by default and uses the built-in CA certificate bundle in the trust pool, which receives automatic updates from Cisco. Use the **crypto ca trustpool import url**to manually update certificates in the trust pool if they are not current, are corrupt, or if certain certificates need to be updated.

Task ID

Task ID	Operation
crypto	execute

Example

This example shows how to run the command to manually update certificates in the trust pool if they are not current, are corrupt, or if certain certificates need to be updated.

```
RP/0/RSP0/CPU0:IMC0#crypto ca trustpool import url
http://www.cisco.com/security/pki/trs/ios.p7b
```

Related Commands

Command	Description
show crypto ca trustpool policy, on page 49	Display the CA trust pool certificates of the router in a verbose format.

Command	Description
crypto ca trustpool policy, on page 17	Configure CA trust pool policy parameters.

crypto ca trustpool policy

To configure certificate authority (CA) trust pool policy, use the **crypto ca trustpool policy** command.

crypto ca trustpool policy {**cabundle url** *url* | **crl optional** | **description** *line*}

Syntax Description

cabundle url *URL*	Configures the URL from which the CA trust pool bundle is downloaded.
crl optional	To specify the certificate revocation list (CRL) query for the CA trust pool, use the crl command in ca-trustpool configuration mode. By default, the router enforces a check of the revocation status of the certificate by querying the certificate revocation list (CRL). Setting this to optional disables revocation checking when the trust pool policy is in use.
description *line*	Indicates the description for the trust pool policy.

Command Default

The default CA trust pool policy is used.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **crypto ca trustpool policy** command enters ca-trustpool configuration mode, where commands can be accessed to configure certificate authority (CA) trustpool policy parameters.

Task ID

Task ID	Operation
crypto	READ, WRITE

Example

This example shows you how to disable certificate revocation checks when the trust pool policy is in use.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:IMC0(config)#crypto ca trustpool policy
RP/0/RSP0/CPU0:IMC0(config-trustpool)#RP/0/RSP0/CPU0:IMC0(config-trustpool)#crl optional
```

Related Commands

Command	Description
crypto ca trustpool import url, on page 15	Allows you to manually update certificates in the trust pool.
show crypto ca trustpool policy, on page 49	Displays the CA trust pool certificates of the router in a verbose format.

crypto key generate dsa

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

crypto key generate dsa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.

Task ID

Task ID	Operations
crypto	execute

Examples

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

```
RP/0/RSP0/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]
```

Related Commands

Command	Description
crypto key zeroize dsa, on page 23	Deletes a DSA key pair from your router.
show crypto key mypubkey dsa, on page 50	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.

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.
keypair-label	(Optional) RSA key pair label that names the RSA key pairs.

Command Default

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 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.

Task ID

Task ID	Operations
crypto	execute

Examples

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

```
RP/0/RSP0/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>
RP/0/RSP0/CPU0:router#
```

Related Commands

Command	Description
crypto key zeroize rsa, on page 24	Deletes the RSA key pair for your router.
show crypto key mypubkey rsa, on page 51	Displays the RSA public keys for your router.

crypto key import authentication rsa

To import a public key using the Rivest, Shamir, and Adelman (RSA) method, use the **crypto key import authentication rsa** command.

crypto key import authentication rsa *path*

Syntax Description

path	(Optional) This denotes the path to the RSA public key file.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.9.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

1. Use shh-keygen generation mechanism to generate keys using either a LINUX or UNIX client. This creates two keys: one public and one private.
2. Remove the comment and other header tag from the keys, except the base64encoded text.
3. Decode the base64encoded text, and use the for authentication.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example displays how to import a public key:

```
RP/0/RSP0/CPU0:k2#crypto key import authentication rsa
```

crypto key zeroize dsa

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

crypto key zeroize dsa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

Task ID

Task ID	Operations
crypto	execute

Examples

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

```
RP/0/RSP0/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, on page 19	Generates DSA key pairs.
show crypto key mypubkey dsa, on page 50	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.

crypto key zeroize rsa [*keypair-label*]

Syntax Description

keypair-label	(Optional) Names the RSA key pair to be removed.

Command Default

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

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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, on page 10 command CA.
- Manually remove the certificates from the configuration using the **clear crypto ca certificates** command.

Task ID

Task ID	Operations
crypto	execute

Examples

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

```
RP/0/RSP0/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, on page 3	Clears certificates associated with trustpoints that no longer exist in the configuration file.
crypto ca enroll, on page 10	Obtains a router certificate from the CA.

Command	Description
crypto key generate rsa, on page 20	Generates RSA key pairs.
show crypto key mypubkey rsa, on page 51	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

string	Character string describing the trustpoint.

Command Default

The default description is blank.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **description** command in the trustpoint configuration mode to create a description for a trustpoint.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to create a trustpoint description:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/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

number	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 1 to 100.

Command Default

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

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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).

Task ID

Task ID	Operations
crypto	read, write

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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry period 10
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry count 60
```

Related Commands

Command	Description
crl optional (trustpoint), on page 5	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.
crypto ca trustpoint, on page 13	Configures a trusted point with a selected name.
enrollment retry period, on page 29	Specifies the wait period between certificate request retries.
enrollment url, on page 32	Specifies the certification authority (CA) location by naming the CA URL.

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.

Command Default

minutes: *1*

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.)

Task ID

Task ID	Operations
crypto	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry period 5
```

Related Commands

Command	Description
crl optional (trustpoint), on page 5	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.
crypto ca trustpoint, on page 13	Configures a trusted point with a selected name.
enrollment retry count, on page 27	Specifies the number of times a router resends a certificate request.

enrollment terminal

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal** command in 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 keywords or arguments.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can manually cut and paste certificate requests and certificates when you do not have a network connection between the router and certification authority (CA). When the **enrollment terminal** command is enabled, the router displays the certificate request on the console terminal, which allows you to enter the issued certificate on the terminal.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to manually specify certificate enrollment through cut-and-paste. In this example, the CA trustpoint is myca.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment terminal
```

Related Commands

Command	Description
crypto ca trustpoint, on page 13	Configures a trusted point with a selected name.

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/pkiclient.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.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.

This table lists the available enrollment methods.

Table 1: Certificate Enrollment Methods

Enrollment Method	Description
SFTP	Enroll through SFTP: file system
TFTP[1]	Enroll through TFTP: file system

[1] If you are using TFTP for enrollment, the URL must be in the form tftp://certserver/file_specification. (The file specification is optional.)

TFTP enrollment sends the enrollment request and retrieves the certificate of the CA and the certificate of the router. If the file specification is included in the URL, the router appends an extension to the file specification.

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

Task ID

Task ID	Operations
crypto	read, write

Examples

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

```
 RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#
               crypto ca trustpoint myca
 RP/0/RSP0/CPU0:router(config-trustp)#
               enrollment url http://ca.domain.com/certsrv/mscep/mscep.dll
```

Related Commands

Command	Description
crl optional (trustpoint), on page 5	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.
crypto ca trustpoint, on page 13	Configures a trusted point with a selected name.
ip-address (trustpoint), on page 34	Specifies a dotted IP address that is included as an unstructured address in the certificate request.

ip-address (trustpoint)

To specify a dotted IP address that is included as an unstructured address in the certificate request, use the **ip-address** command in trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

ip-address {*ip-address* | **none**}
no ip-address {*ip-address* | **none**}

Syntax Description

ip-address	Dotted IP address that is included in the certificate request.
none	Specifies that an IP address is not included in the certificate request.

Command Default

You are prompted for the IP address during certificate enrollment.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.

Task ID

Task ID	Operations
crypto	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint frog
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://frog.phoobin.com
RP/0/RSP0/CPU0:router(config-trustp)# subject-name OU=Spiral Dept., O=tiedye.com
RP/0/RSP0/CPU0:router(config-trustp)# ip-address 172.19.72.120
```

The following example shows that an IP address is not to be included in the certificate request:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://10.3.0.7:80
RP/0/RSP0/CPU0:router(config-trustp)# subject-name CN=subject1, OU=PKI, O=Cisco Systems,
```

```
C=US
RP/0/RSP0/CPU0:router(config-trustp)# ip-address none
```

Related Commands

Command	Description
crl optional (trustpoint), on page 5	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.
crypto ca trustpoint, on page 13	Configures a trusted point with a selected name.
enrollment url, on page 32	Specifies the certification authority (CA) location by naming the CA URL.
serial-number (trustpoint), on page 39	Specifies whether the router serial number should be included in the certificate request.
subject-name (trustpoint), on page 44	Specifies the subject name in the certificate request.

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

LDAP-URL	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.

Command Default

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

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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.

Task ID

Task ID	Operations
crypto	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# query url ldap://my-ldap.domain.com
```

Related Commands

Command	Description
crypto ca trustpoint, on page 13	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

keypair-label	RSA key pair label that names the RSA key pairs.

Command Default

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 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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

Task ID

Task ID	Operations
crypto	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# rsakeypair key1
```

Related Commands

Command	Description
crypto key generate rsa, on page 20	Generates RSA key pairs.

serial-number (trustpoint)

To specify whether the router serial number should be included in the certificate request, use the **serial-number** command in 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 is not included in the certificate request.

Command Default

You are prompted for the serial number during certificate enrollment.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Before you can use 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 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.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to omit a serial number from the root certificate request:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint root
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://10.3.0.7:80
RP/0/RSP0/CPU0:router(config-trustp)# ip-address none
RP/0/RSP0/CPU0:router(config-trustp)# serial-number none
RP/0/RSP0/CPU0:router(config-trustp)# subject-name ON=Jack, OU=PKI, O=Cisco Systems, C=US
```

Related Commands

Command	Description
crl optional (trustpoint), on page 5	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.

Command	Description
crypto ca trustpoint, on page 13	Configures a trusted point with a selected name.
enrollment url, on page 32	Specifies the certification authority (CA) location by naming the CA URL.
ip-address (trustpoint), on page 34	Specifies a dotted IP address that is included as an unstructured address in the certificate request.
subject-name (trustpoint), on page 44	Specifies the subject name in the certificate request.

sftp-password (trustpoint)

To secure the FTP password, use the **sftp-password** command in trustpoint configuration mode. To disable this feature, use the **no** form of this command.

sftp-password {*clear text* | **clear** *text* | **password** *encrypted string*}
no sftp-password {*clear text* | **clear** *text* | **password** *encrypted string*}

Syntax Description

clear text	Clear text password and is encrypted only for display purposes.
password *encrypted string*	Enters the password in an encrypted form.

Command Default

The *clear text* argument is the default behavior.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Passwords are stored in encrypted form and not as plain text. The command-line interface (CLI) contains the provisioning (for example, clear and encrypted) to specify the password input.

The username and password are required as part of the SFTP protocol. If you specify the URL that begins with the prefix (sftp://), you must configure the parameters for the **sftp-password** command under the trustpoint. Otherwise, the certificate from the SFTP server, which is used for manual certificate enrollment, cannot be retrieved.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to secure the FTP password in an encrypted form:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RSP0/CPU0:router(config-trustp)# sftp-password password xxxxxx
```

Related Commands

Command	Description
crypto ca trustpoint, on page 13	Configures a trusted point with a selected name.

Command	Description
sftp-username (trustpoint), on page 43	Secures the FTP username.

sftp-username (trustpoint)

To secure the FTP username, use the **sftp-username** command in trustpoint configuration mode. To disable this feature, use the **no** form of this command.

sftp-username *username*
no sftp-username *username*

Syntax Description

username	Name of the user.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **sftp-username** command is used only if the URL has (sftp://) in the prefix. If (sftp://) is not specified in the prefix, the manual certificate enrollment using SFTP fails.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to secure the FTP username:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RSP0/CPU0:router(config-trustp)# sftp-username tmordeko
```

Related Commands

Command	Description
crypto ca trustpoint, on page 13	Configures a trusted point with a selected name.
sftp-password (trustpoint), on page 41	Secures the FTP password.

subject-name (trustpoint)

To specify the subject name in the certificate request, use the **subject-name** command in 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

x.500-name	(Optional) Specifies the subject name used in the certificate request.

Command Default

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

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Before you can use 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 trustpoint configuration mode.

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

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to specify the subject name for the frog certificate:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint frog
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://frog.phoobin.com
RP/0/RSP0/CPU0:router(config-trustp)# subject-name OU=Spiral Dept., O=tiedye.com
RP/0/RSP0/CPU0:router(config-trustp)# ip-address 172.19.72.120
```

Related Commands

Command	Description
crl optional (trustpoint), on page 5	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.

Command	Description
crypto ca trustpoint, on page 13	Configures a trusted point with a selected name.
enrollment url, on page 32	Specifies the certification authority (CA) location by naming the CA URL.
ip-address (trustpoint), on page 34	Specifies a dotted IP address that is included as an unstructured address in the certificate request.
serial-number (trustpoint), on page 39	Specifies whether the router serial number should be included in the certificate request.

show crypto ca certificates

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

show crypto ca certificates

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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).
- CA certificate, if you have received the certificate (see the **crypto ca authenticate** command).

Task ID

Task ID	Operations
crypto	read

Examples

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

```
RP/0/RSP0/CPU0:router# show crypto ca certificates
Trustpoint       : msiox
==================================================
CAa certificate
  Serial Number  : 06:A5:1B:E6:4F:5D:F7:83:41:11:D5:F9:22:7F:95:23
  Subject:
    Name: CA2
    CN= CA2
  Issued By      :
        cn=CA2
  Validity Start : 07:51:51 UTC Wed Jul 06 2005
  Validity End   : 08:00:43 UTC Tue Jul 06 2010
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Router certificate
  Status         : Available
  Key usage      : Signature
  Serial Number  : 38:6B:C6:B8:00:04:00:00:01:45
  Subject:
```

```
    Name: tdlr533.cisco.com
    IP Address: 3.1.53.3
    Serial Number: 8cd96b64
  Issued By      :
        cn=CA2
  Validity Start : 08:30:03 UTC Mon Apr 10 2006
  Validity End   : 08:40:03 UTC Tue Apr 10 2007
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Associated Trustpoint: MS-IOX
Router certificate
  Status         : Available
  Key usage      : Encryption
  Serial Number  : 38:6D:2B:A7:00:04:00:00:01:46
  Subject:
    Name: tdlr533.cisco.com
    IP Address: 3.1.53.3
    Serial Number: 8cd96b64
  Issued By      :
        cn=CA2
  Validity Start : 08:31:34 UTC Mon Apr 10 2006
  Validity End   : 08:41:34 UTC Tue Apr 10 2007
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Associated Trustpoint: msiox
```

Related Commands

Command	Description
crypto ca authenticate, on page 7	Authenticates the CA by obtaining the certificate of the CA.
crypto ca enroll, on page 10	Obtains the certificates of your router from the CA.
crypto ca import, on page 12	Imports a certification authority (CA) certificate manually through TFTP, SFTP, or cut and paste it at the terminal.
crypto ca trustpoint, on page 13	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.

show crypto ca crls

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

XR EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read

Examples

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

```
RP/0/RSP0/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, on page 4	Clears all the CRLs stored on the router.

show crypto ca trustpool policy

To display the CA trust pool certificates of the router in a verbose format use the **show crypto ca trustpool policy**command.

show crypto ca trustpool policy

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 5.2.0	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the command to display the CA trust pool certificates of the router in a verbose format.

Task ID

Task ID	Operation
crypto	read

Example

This example shows you how to run the command to view details of your CA certificate trust pool policy.

```
RP/0/RSP0/CPU0:IMC0#show crypto ca trustpool policy

Trustpool Policy

   Trustpool CA certificates will expire [UTC] Thu Sep 30 14:01:15 2021
   CA Bundle Location: http://cisco.com/security/pki/trs/ios.p7b
```

Related Commands

Command	Description
crypto ca trustpool import url, on page 15	Allows you to manually update certificates in the trust pool.
crypto ca trustpool policy, on page 17	Configures CA trust pool policy parameters.

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.

show crypto key mypubkey dsa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto key mypubkey dsa** command:

```
RP/0/RSP0/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, on page 19	Generates DSA key pairs.
crypto key zeroize dsa, on page 23	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.

show crypto key mypubkey rsa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID

Task ID	Operations
crypto	read

Examples

The following is sample output from the **show crypto key mypubkey rsa** command:

```
RP/0/RSP0/CPU0:router# show crypto key mypubkey rsa

Key label: mykey
Type : RSA General purpose
Size : 1024
Created  : 07:46:15 UTC Fri Mar 17 2006
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
Created  : 07:46:15 UTC Fri Mar 17 2006
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, on page 20	Generates RSA key pairs.
crypto key zeroize rsa, on page 24	Deletes all RSA keys from the router.