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* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series RoutersSystem Security Configuration Guide for Cisco 8000 Series Routers*.

auto-enroll

To specify the duration after which the router request for automatic renewal of a PKI certificate from the CA, , use the **auto-enroll** command in trustpoint configuration mode. To disable the automatic renewal of the certificate after the said period, use the **no** form of this command.

auto-enroll *percentage*

Syntax Description

percentage	Percentage of the certificate validity after which the router will request for a new certificate from the CA. The range is from 1 to 99.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.5.3	This command was introduced.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure auto renewal of PKI certificate in the router:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#auto-enroll 30
Router(config-trustp)#commit
```

ca-keypair

To create the key pair for the root certificate on the router, use the **ca-keypair** command in trustpoint configuration mode. To remove this configuration, use the **no** form of this command.

ca-keypair { **dsa** | **ecdsanistp256** | **ecdsanistp384** | **ecdsanistp521** | **ed25519** | **rsa** } *key-pair-label*

Syntax Description

key-pair-label	Specifies the key pair label for the respective key signature algorithm (DSA, ECDSA, Ed25519 or RSA).

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.
Release 7.3.1	The command was modified to include the **ed25519** option.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to create the key pair for the root certificate on the router:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#ca-keypair rsa system-root-key
Router(config-trustp)#commit
```

Related Commands

Command	Description
keypair, on page 48	Creates the key pair for the leaf certificate on the router.

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 modeXR EXEC mode.

clear crypto ca certificates *trustpoint*

Syntax Description

trustpoint	Trustpoint name.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/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 modeXR EXEC mode.

clear crypto ca crl

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/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/RP0RSP0/CPU0:router# clear crypto ca crl
RP/0/RP0RSP0/CPU0:router# show crypto ca crls
RP/0/RP0RSP0/CPU0: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 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0RSP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RP0RSP0/CPU0:router(config-trustp)# enrollment retry period 20
RP/0/RP0RSP0/CPU0:router(config-trustp)# enrollment retry count 100
RP/0/RP0RSP0/CPU0:router(config-trustp)# crl optional
```

crypto ca authenticate

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

crypto ca authenticate {*ca-name* | **system-trustpoint**}

Syntax Description

ca-name	Name of the CA Server.
system-trustpoint	Generates self-signed root certificate.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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:

```
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


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

This example shows how to generate a self-signed root certificate:

```
Router#crypto ca authenticate system-trustpoint
```

crypto ca cancel-enroll

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

crypto ca cancel-enroll *ca-name*

Syntax Description

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

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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 55 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.

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/RP0RSP0/CPU0:router# crypto ca cancel-enroll myca
```

crypto ca enroll

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

crypto ca enroll {*ca-name* | **system-trustpoint**}

Syntax Description

ca-name	Name of the CA Server.
system-trustpoint	Generates the leaf certificate.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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 55 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.) 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.

Note The root certificate signs the leaf certificate.

Task ID

Task ID	Operations
crypto	execute

Examples

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

```
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/RPO/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
```

This example shows how to generate a leaf certificate:

```
Router#crypto ca enroll system-trustpoint
```

crypto ca fqdn-check ip-address allow

To avoid server certificate (leaf certificate) failure in the router, resulting from the IP addresses in the Subject Alternate Name (SAN) field of the certificates instead of Fully Qualified Domain Names (FQDNs) when the certificate extension type doesn’t specifies the IP address, use the **crypto ca fqdn-check ip-address allow** command in Global Configuration mode.

crypto ca fqdn-check ip-address allow

Syntax Description

This command has no keywords or arguments.

Command Default

When the certificate extension type doesn’t specifies the IP address, the certificates with IP addresses in the SAN field don’t function properly.

Command Modes

Global Configuration

Command History

Release	Modification
Release 7.4.2	This command was introduced.

Usage Guidelines

In Cisco IOS XR Routers, to use an IP address in the SAN field in server certificates, the certificate extension type is IP addresses. The router rejects certificates that don’t meet this criterion. To prevent such failures when an IP address is present in the SAN field, configure the **crypto ca fqdn-check ip-address allow** command. This command enables the router to validate and accept server certificates with IP addresses in the SAN field without the IP addresses certificate extension type.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to run the command for the router to accept server certificates with ip-address in the SAN field:

```
Router# config
Router(config)# crypto ca fqdn-check ip-address allow
```

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 in EXEC modeXR EXEC mode.

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 17 command.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

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/RP0RSP0/CPU0:router# crypto ca import myca certificate
```

crypto ca http-proxy

To fetch the Certificate Revocation List (CRL) through the http proxy server, use the **crypto ca http-proxy** command in the Global Configuration modeXR Config mode. Use the **no** form of this command to disable the proxy server.

crypto ca http-proxy *proxy-server-IP-address* **port** *port-number*
no crypto ca http-proxy *proxy-server-IP-address* **port** *port-number*

Syntax Description

http-proxy *proxy-server-IP-address*	Specifies the proxy server IP address.
port *port-number*	Specifies the proxy server port number. The range is from 1-65535.

Command Default

None

Command Modes

Global Configuration modeXR Config mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	execute

Example

This example shows how to configure the proxy server to enable communication with the certification authority to retrieve the Certificate Revocation List (CRL).

```
Router#configure
Router(config)#crypto ca http-proxy 10.10.10.1 port 1
```

crypto ca crl request

To fetch the latest CRL from a specific CDP (CRL Distribution point), use the **crypto ca crl request** command in the EXEC modeXR EXEC mode.

crypto ca crl request *cdp-url* [**http-proxy** *ip-address* **port** *port-number*]

Syntax Description

cdp-url	Specifies the CDP URL.
http-proxy *proxy-server-IP-address*	Specifies the proxy server IP address.
port *port-number*	Specifies the proxy server port number. The range is from 1-65535.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.3.1	This command was modified.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	execute

Example

This example shows how to fetch the latest CRL from a specific CDP.

```
Router#crypto ca crl request http://zxy-w2k.cisco.com/CertEnroll/zxy-w2k-root.crl
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: /C=US/ST=NC/L=RTP/O=Cisco/OU=GCT/CN=ca-root
        Last Update: Jan 29 11:43:50 2019 GMT
        Next Update: Jan 26 11:43:50 2029 GMT
        CRL extensions:
            xyz321v3 CRL Number:
                292
Revoked Certificates:
    Serial Number: 0138
        Revocation Date: Feb 17 01:01:55 2017 GMT
    Serial Number: 0139
        Revocation Date: Feb 17 01:22:28 2017 GMT
    Serial Number: 013A
        Revocation Date: Feb 17 03:04:32 2017 GMT
    Serial Number: 013B
```

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 in Global Configuration modeXR Config mode.

crypto ca trustpoint {*ca-name* | **system-trustpoint**}

Syntax Description

ca-name	Name of the CA.
system-trustpoint	Specifies the default system trustpoint.

Command Default

None

Command Modes

Global Configuration modeXR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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 a set of commands. See the Related Commands section for details.

Task ID

Task ID	Operations
crypto	execute

Examples

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

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

This example shows how to create a default system trustpoint:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#commit
```

Command	Description
ca-keypair, on page 4	Creates the key pair for the root certificate on the router.
crl optional (trustpoint), on page 7	Allows the certificates of other peers to be accepted without trying to obtain the appropriate CRL.
enrollment retry count, on page 40	Specifies how many times a router resends a certificate request.
enrollment retry period, on page 41	Specifies the wait period between certificate request retries.
enrollment terminal, on page 42	Specifies manual cut-and-paste certificate enrollment.
enrollment url, on page 43	Specifies the URL of the CA.
ip-address (trustpoint), on page 45	Specifies a dotted IP address that is included as an unstructured address in the certificate request.
key-usage, on page 46	Specifies the key usage field for the self-enrollment certificate.
keypair, on page 48	Creates the key pair for the leaf certificate on the router.
lifetime (trustpoint), on page 51	Configures the lifetime for self-enrollment of certificates.
message-digest, on page 52	Configures the message digest hashing algorithm for the certificates.
query url, on page 53	Specifies the LDAP URL of the CRL distribution point. Required only if your CA supports Lightweight Directory Access Protocol (LDAP).
rsakeypair, on page 55	Specifies a named RSA key pair for this trustpoint.
serial-number (trustpoint), on page 56	Specifies a router serial number in the certificate request.
sftp-password (trustpoint), on page 57	Secures the FTP password.
sftp-username (trustpoint), on page 58	Secures the FTP username.
subject-name (trustpoint), on page 72	Specifies a subject name in the certificate request.

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 in EXEC modeXR EXEC mode.

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. This parameter can either be the URL of an external server or the local folder path (**/tmp**) in the router where the certificate is available.

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 modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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** command to manually update certificates in the trust pool if they are not current, are corrupt, or if certain certificates need to be updated.

You can also specify a local folder path (**/tmp**) in the router as the *URL* parameter for **crypto ca trustpool import url** command. This is useful in scenarios where the router does not have connectivity to an external server to download the certificate. In such cases, you can download the certificate from an external server to elsewhere, and then copy it to the **/tmp** folder in the router.

Note The local folder path in the router has to be **/tmp** itself; no other folder paths are allowed.

The format of the certificate can .pem, .der, or .p7b(bundle).

For example,

crypto ca trustpool import url /tmp/certificate.pem

crypto ca trustpool import url /tmp/certificate.der

crypto ca trustpool import url /tmp/pki_bundle_tmp.p7b

Task ID

Task ID	Operation
crypto	execute

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. The certificate is directly downloaded from an external server, in this case.

```
Router#crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
```

This example shows how to import a certificate that resides in the local **/tmp** folder in the router:

```
Router#crypto ca trustpool import url /tmp/certificate.der
```

Related Commands

Command	Description
show crypto ca trustpool policy, on page 63	Displays the CA trust pool certificates of the router in a verbose format.

crypto key generate authentication-ssh

To generate the cryptographic key pair for public key-based authentication of logged-in users on Cisco IOS XR routers that are configured as SSH clients, use the **crypto key generate authentication-ssh** command in EXEC modeXR EXEC mode.

crypto key generate authentication-ssh rsa

Syntax Description

rsa	Generates RSA key pairs for signing and encryption of packets for SSH public key-based authentication.

Command Default

None

Command Modes

EXECXR EXEC

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

Remote AAA servers such as RADIUS and TACACS+ servers do not support public key-based authentication. Hence this functionality is available only for users who are configured locally on the router and not for users who are configured remotely.

To delete the RSA key of a user, use the **crypto key zeroize authentication-ssh rsa username** command in EXEC modeXR EXEC mode.

A user with root privileges has permission to create and delete keys for other users.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to generate an RSA key pair for public key-based authentication of SSH clients on Cisco IOS XR routers:

```
Router#crypto key generate authentication-ssh rsa
Wed Dec 21 10:02:57.684 UTC
The name for the keys will be: cisco
  Choose the size of the key modulus in the range of 512 to 4096. Choosing a key modulus
greater than 512 may take a few minutes.

How many bits in the modulus [2048]:
Generating RSA keys ...
Done w/ crypto generate keypair
[OK]

Router#
```

crypto key generate dsa

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

crypto key generate dsa [{**system-enroll-key** | **system-root-key**}]

Syntax Description

system-enroll-key	Specifies key pair generation for the leaf certificate. Note: Crypto key generation in XR Config Mode does not support this option.
system-root-key	Specifies key pair generation for the root certificate. Note: Crypto key generation in XR Config Mode does not support this option.

Command Default

None

Command Modes

XR EXEC mode and XR Config mode

Command History

Release	Modification
Release 7.3.2	This command was introduced in XR Config mode
Release 7.0.12	This command was introduced in XR EXEC mode

Usage Guidelines

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 in XR Config mode, use **no** form of this command in XR Config mode.

To remove the DSA key generated in XR EXEC mode, 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:

```
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]
```

This example shows how to generate a DSA key pair for the root certificate:

```
Router#crypto key generate dsa system-root-key
```

This example shows how to generate a DSA key pair for the leaf certificate:

```
Router#crypto key generate dsa system-enroll-key
```

The following example shows how to generate a 512-bit DSA key-pair in XR Config mode:

```
Router#conf t
Router(config)#crypto key generate dsa 512
Router(config)#commit
```

This example shows how to delete a DSA key-pair in XR Config mode:

```
Router# conf t
Router(config)#no crypto key generate dsa 512
Router(config)#commit
```

crypto key generate ecdsa

To generate an Elliptic Curve Digital Signature Algorithm (ECDSA) key pair, use the **crypto key generate ecdsa** command in XR EXEC mode and XR Config mode.

crypto key generate ecdsa [{**nistp256** | **nistp384** | **nistp521**}] [{**system-enroll-key** | **system-root-key**}]

Syntax Description

nistp256	Generates an ECDSA key of curve type nistp256, with key size 256 bits.
nistp384	Generates an ECDSA key of curve type nistp384, with key size 384 bits.
nistp521	Generates an ECDSA key of curve type nistp521, with key size 521 bits.
system-enroll-key	Specifies key pair generation for the leaf certificate. Note: Crypto key generation in XR Config Mode does not support this option.
system-root-key	Specifies key pair generation for the root certificate. Note: Crypto key generation in XR Config Mode does not support this option.

Command Default

None

Command Modes

XR EXEC mode and XR Config mode

Command History

Release	Modification
Release 7.3.2	This command was introduced in XR Config mode
Release 7.0.12	This command was introduced in XR EXEC mode

Usage Guidelines

To remove the ECDSA key generated in XR Config mode, use **no** form of this command in XR Config mode.

To remove an ECDSA key generated in XR EXEC mode, use the **crypto key zeroize ecdsa** command.

Task ID

Task ID	Operation
crypto	execute

Examples

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

```
Router# crypto key generate ecdsa nistp384
Wed Mar 28 12:53:57.355 UTC
% You already have keys defined for the_default
Do you really want to replace them? [yes/no]: yes
Generating ECDSA keys ...
Done w/ crypto generate ECDSA keypair
[OK]
```

This example shows how to generate a ECDSA key pair for the root certificate:

```
Router#crypto key generate ecdsa system-root-key
```

This example shows how to generate a ECDSA key pair for the leaf certificate:

```
Router#crypto key generate dsa system-enroll-key
```

The following example shows how to generate an ECDSA key-pair in XR Config mode:

```
Router#conf t
Router(config)#crypto key generate ecdsa nistp256
Router(config)#commit
```

This example shows how to delete en ECDSA key-pair in XR Config mode:

```
Router# conf t
Router(config)#no crypto key generate ecdsa nistp256
Router(config)#commit
```

crypto key generate ed25519

To generate Ed25519 crypto key pairs as part of supporting the Ed25519 public-key signature system, use the **crypto key generate ed25519** command in XR EXEC mode and XR Config mode.

crypto key generate ed25519 [{ **system-enroll-key** | **system-root-key** }]

Syntax Description

system-enroll-key	Specifies key pair generation for the leaf certificate. Note: Crypto key generation in XR Config Mode does not support this option.
system-root-key	Specifies key pair generation for the root certificate. Note: Crypto key generation in XR Config Mode does not support this option.

Command Default

None

Command Modes

XR EXEC mode and XR Config mode

Command History

Release	Modification
Release 7.3.2	This command was introduced in XR Config mode
Release 7.3.1	This command was introduced in XR EXEC mode.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit platforms.

To remove the Ed25519 key generated in XR Config mode, use **no** form of this command in XR Config mode.

To remove the Ed25519 key generated in XR EXEC mode, use the **crypto key zeroize ed25519** command.

You can generate the crypto keys either with an empty label or with two predefined labels (**system-root-key** and **system-enroll-key**). In case of empty label, the system generates the key pair against the default label. The key pairs with the predefined labels are used to integrate Cisco IOS XR with Cisco Crosswork Trust Insights.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to generate a Ed25519 crypto key pair:

```
Router# crypto key generate ed25519

Mon Nov 30 07:03:17.058 UTC
The name for the keys will be: the_default
Generating ED25519 keys ...
Done w/ crypto generate keypair
```

```
[OK]
```

This example shows how to generate a Ed25519 crypto key pair for the root certificate:

```
Router#crypto key generate ed25519 system-root-key
```

This example shows how to generate a Ed25519 crypto key pair for the leaf certificate:

```
Router#crypto key generate ed25519 system-enroll-key
```

The following example shows how to generate an Ed25519 key-pair in XR Config mode:

```
Router#conf t
Router(config)#crypto key generate ed25519
Router(config)#commit
```

This example shows how to delete en Ed25519 key-pair in XR Config mode:

```
Router# conf t
Router(config)#no crypto key generate ed25519
Router(config)#commit
```

Related Commands

Command	Description
crypto key zeroize ed25519, on page 37	Deletes Ed25519 crypto key pairs from the router.
show crypto key mypubkey ed25519, on page 68	Displays the Ed25519 public keys of the router.

crypto key generate rsa

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

crypto key generate rsa [{**usage-keys** | **general-keys** | **system-enroll-key** | **system-root-key**}] [*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.
system-enroll-key	Specifies key pair generation for the leaf certificate. Note: Crypto key generation in XR Config Mode does not support this option.
system-root-key	Specifies key pair generation for the root certificate. Note: Crypto key generation in XR Config Mode does not support this option.

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

XR EXEC mode and XR Config mode

Command History

Release	Modification
Release 7.3.2	This command was introduced in XR Config mode
Release 7.0.12	This command was introduced in XR EXEC mode.

Usage Guidelines

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 generated in XR Config mode, use **no** form of this command in XR Config mode.

To remove an RSA key generated in XR EXEC mode, 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:

```
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>
Router#
```

This example shows how to generate an RSA key pair for the root certificate:

```
Router#crypto key generate rsa system-root-key
```

This example shows how to generate an RSA key pair for the leaf certificate:

```
Router#crypto key generate rsa system-enroll-key
```

The following example shows how to generate an RSA key-pair in XR Config mode:

```
Router#conf t
Router(config)#crypto key generate rsa user1 general-keys 2048
Router(config)#commit
```

This example shows how to delete en RSA key-pair in XR Config mode:

```
Router# conf t
Router(config)#no crypto key generate rsa user1 general-keys 2048
Router(config)#commit
```

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 in EXEC modeXR EXEC mode.

crypto key import authentication rsa [**username** *name*] [**WORD** | **second** | **third** | **fourth**]

Syntax Description

rsa	Imports the RSA public key on the router.
username	(Optional) Imports the RSA public key for the user *name*.
name	Specifies the name of the user for which the RSA public key is imported. If you do not specify a *name*, the RSA public key for the currently logged-in user is imported.
WORD	(Optional) Specifies the path (`harddisk:/` or `disk0:/` or `tftp`) to the RSA public key file.
second	(Optional) Imports the second RSA public key for a user.
third	(Optional) Imports the third RSA public key for a user.
fourth	(Optional) Imports the fourth RSA public key for a user.

Command Default

- The **crypto key import authentication rsa** command imports the first RSA public key for the currently logged-in user if you do not specify the **WORD**, **second**, **third**, or **fourth** option.
- The **crypto key import authentication rsa username** *name* command imports the first RSA public key for the user *name* if you do not specify the **second**,**third**, or **fourth** option.

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.11.1	This command was modified to include the **second**,**third**,and **fourth** options.
Release 3.9.0	This command was introduced.

Usage Guidelines

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

This example shows how to import the second RSA public key for the currently logged-in user.

```
RP/0/RP0/CPU0:OC_router1#crypto key import authentication rsa harddisk:/id_rsa_key2.pub
Thu Nov  9 20:43:19.568 IST
RP/0/RP0/CPU0:Nov  9 20:43:19.740 IST: cepki[129]: %SECURITY-CEPKI-6-KEY_INFO : crypto key
 RSA(public key authentication) generated, label:cafyauto, modBits:4096
RP/0/RP0/CPU0:OC_router1#RP/0/RP0/CPU0:Nov  9 20:43:20.964 IST: cepki[129]:
%SECURITY-CEPKI-6-INFO : key database updated successfully
RP/0/RP0/CPU0:OC_router1#
```

This example shows how to import the third RSA public key for the currently logged-in user by manually copy-pasting the key.

```
RP/0/RP0/CPU0:OC_router1#crypto key import authentication rsa third
Thu Nov  9 20:51:52.599 IST
Enter the public key
ssh-rsa
[illegible]

RP/0/RP0/CPU0:Nov  9 20:52:38.122 IST: cepki[129]: %SECURITY-CEPKI-6-KEY_INFO : crypto key
 RSA(public key authentication) generated, label:cafyauto, modBits:4096
RP/0/RP0/CPU0:OC_router1#
```

This example shows how to import the fourth RSA public key for user *test*.

```
RP/0/RP0/CPU0:OC_router1#crypto key import authentication rsa username test fourth
harddisk:/id_rsa_key4.pub
Thu Nov  9 20:55:02.586 IST
RP/0/RP0/CPU0:Nov  9 20:55:02.757 IST: cepki[129]: %SECURITY-CEPKI-6-KEY_INFO : crypto key
 RSA(public key authentication) generated, label:test, modBits:4096
RP/0/RP0/CPU0:OC_router1
```

crypto key zeroize authentication-ssh

To delete the cryptographic key pair on the router that was generated for public key-based authentication of SSH clients, use the **crypto key zeroize authentication-ssh** command in EXEC modeXR EXEC mode.

crypto key zeroize authentication-ssh rsa [**username** *name*]

Syntax Description

rsa	Deletes the RSA key pair on the router.
username *name*	Specifies the name of the user whose RSA key pairs are to be deleted from the router.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

If the **username** is not specified, then the command deletes the key for the user who is currently logged in.

A user with root privileges has permission to create and delete keys for other users.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to delete the RSA key pair that was generated for public key-based authentication of SSH clients.

```
Router#crypto key zeroize authentication-ssh rsa username user1
```

crypto key zeroize authentication rsa

To delete a public key imported on the router using the Rivest, Shamir, and Adelman (RSA) method, use the **crypto key zeroize authentication rsa** command in EXEC modeXR EXEC mode.

crypto key zeroize authentication rsa [**username** *name*] [**all** | **second** | **third** | **fourth**]

Syntax Description

rsa	Deletes the RSA public key on the router.
username	Deletes the RSA public key for the user specified in the *name*.
name	(Optional) Specifies the name of the user for which the RSA public key is deleted. If you do not specify a *name*, the RSA public key for the currently logged-in user is deleted.
all	Deletes all imported RSA public keys.
second	Deletes second imported RSA public key.
third	Deletes third imported RSA public key.
fourth	Deletes fourth imported RSA public key.

Command Default

- The **crypto key zeroize authentication rsa** command deletes the first imported RSA public key if you do not specify the **all**, **second**, **third**, or **fourth** option.
- The **crypto key zeroize authentication rsa username** *name* command deletes the first imported RSA public key for the user *name* if you do not specify the **second**,**third**, or **fourth** option.

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.11.1	This command was modified to include the **second**,**third**, and **fourth** options.
Release 7.2.1	This command was introduced.

Usage Guidelines

If the **username** is not specified, then the command deletes the first imported RSA public key for the currently logged-in user.

A user with root privileges can create and delete keys for other users.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to delete the first imported RSA public key for the currently logged-in user *test1*.

```
RP/0/RP0/CPU0:OC_router1#crypto key zeroize authentication rsa

Wed Oct 25 18:32:30.421 IST
% Keys to be removed are named test1
Do you really want to remove these keys ?? [yes/no]: yes

RP/0/RP0/CPU0:OC_router1#
```

This example shows how to delete the fourth imported RSA public key for the currently logged-in user *test1*.

```
RP/0/RP0/CPU0:OC_router1#crypto key zeroize authentication rsa fourth

Wed Oct 25 21:18:04.336 IST
% Keys to be removed are named test1
Do you really want to remove these keys ?? [yes/no]: yes

RP/0/RP0/CPU0:OC_router1#
```

This example shows how to delete the first imported RSA public key for user *test2*.

```
RP/0/RP0/CPU0:OC_router1#crypto key zeroize authentication rsa username test2

Wed Oct 25 18:54:34.153 IST
% Keys to be removed are named test2
Do you really want to remove these keys ?? [yes/no]: yes

RP/0/RP0/CPU0:OC_router1#
```

This example shows how to delete the second imported RSA public key for user *test3*.

```
RP/0/RP0/CPU0:OC_router1#crypto key zeroize authentication rsa username test3 second

Wed Oct 25 18:54:34.153 IST
% Keys to be removed are named test3
Do you really want to remove these keys ?? [yes/no]: yes

RP/0/RP0/CPU0:OC_router1#
```

This example shows how to delete all imported RSA public keys on the router in EXEC mode.

```
RP/0/RP0/CPU0:OC_router1#crypto key zeroize authentication rsa all

Wed Oct 25 18:32:58.007 IST
Do you really want to remove all these keys ?? [yes/no]: yes

RP/0/RP0/CPU0:OC_router1#
```

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 modeXR EXEC mode.

crypto key zeroize dsa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/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
```

crypto key zeroize ecdsa

To delete the Elliptic Curve Digital Signature Algorithm (ECDSA) key pair from your router, use the **crypto key zeroize ecdsa** command.

crypto key zeroize ecdsa [**nistp256** | **nistp384** | **nistp521**]

Syntax Description

nistp256	Deletes an ECDSA key of curve type nistp256, with key size 256 bits.
nistp384	Deletes an ECDSA key of curve type nistp384, with key size 384 bits.
nistp521	Deletes an ECDSA key of curve type nistp521, with key size 521 bits.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

None

Task ID

Task ID	Operation
crypto	execute

Example

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

```
RP/0/RP0/CPU0:router# crypto key zeroize ecdsa nistp384

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

crypto key zeroize ed25519

To delete the Ed25519 crypto key pair from the router, use the **crypto key zeroize ed25519** command in EXEC modeXR EXEC mode.

crypto key zeroize ed25519

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to delete Ed25519 crypto key pairs from your router:

```
Router# crypto key zeroize ed25519
% 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 ed25519, on page 26	Generates Ed25519 crypto key pairs.
show crypto key mypubkey ed25519, on page 68	Displays the Ed25519 public keys of 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 modeXR EXEC mode.

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 modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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 11 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/RP0RSP0/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
```

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 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0RSP0/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 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0RSP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RP0RSP0/CPU0:router(config-trustp)# enrollment retry period 10
RP/0/RP0RSP0/CPU0:router(config-trustp)# enrollment retry count 60
```

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 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0RSP0/CPU0:router(config-trustp)# enrollment retry period 5
```

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 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0RSP0/CPU0:router(config-trustp)# enrollment terminal
```

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 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)#
               crypto ca trustpoint myca
 RP/0/RP0RSP0/CPU0:router(config-trustp)#
               enrollment url http://ca.domain.com/certsrv/mscep/mscep.dll
```

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 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# crypto ca trustpoint frog
RP/0/RP0RSP0/CPU0:router(config-trustp)# enrollment url http://frog.phoobin.com
RP/0/RP0RSP0/CPU0:router(config-trustp)# subject-name OU=Spiral Dept., O=tiedye.com
RP/0/RP0RSP0/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/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0RSP0/CPU0:router(config-trustp)# enrollment url http://10.3.0.7:80
RP/0/RP0RSP0/CPU0:router(config-trustp)# subject-name CN=subject1, OU=PKI, O=Cisco Systems,
 C=US
RP/0/RP0RSP0/CPU0:router(config-trustp)# ip-address none
```

key-usage

To specify the key usage field for the self-enrollment certificate, use the **key-usage** command in trustpoint configuration mode. To remove this configuration, use the **no** form of this command.

key-usage {**ca-certificate** {**crlsign** | **digitalsignature** | **keycertsign** | **nonrepudiation**} | **certificate** {**dataencipherment** | **digitalsignature** | **keyagreement** | **keyencipherment** | **nonrepudiation**}}

Syntax Description

ca-certificate	Specifies the key usage field for the CA certificate.
certificate	Specifies the key usage field for the leaf certificate.
crlsign	Asserts **cRLSign** (bit 6) for the key usage field to verify signatures on certificate revocation list (CRL).
digitalsignature	Asserts **digitalSignature** (bit 0) for the key usage field. This is used when the subject public key is used with a digital signature mechanism to support security services other than certificate signing (bit 5), or CRL signing (bit 6).
keycertsign	Asserts **keyCertSign** (bit 5) for the key usage field when the subject public key is used for verifying a signature on public key certificates.
nonrepudiation	Asserts **nonRepudiation** (bit 1) for the key usage field when the subject public key is used to verify digital signatures that is used to provide a non-repudiation service.
dataencipherment	Asserts **dataEncipherment** (bit 3) for the key usage field when the subject public key is used for enciphering user data, other than cryptographic keys.
keyagreement	Asserts **keyAgreement** (bit 4) for the key usage field when the subject public key is used for key agreement.
keyencipherment	Asserts **keyEncipherment** (bit 2) for the key usage field when the subject public key is used for key transport.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to specify the key usage field for the self-enrollment certificate:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#key-usage certificate digitalsignature keyagreement dataencipherment
Router(config-trustp)#commit
```

keypair

To create the key pair for the leaf certificate on the router, use the **keypair** command in trustpoint configuration mode. To remove this configuration, use the **no** form of this command.

keypair { **dsa** | **ecdsanistp256** | **ecdsanistp384** | **ecdsanistp521** | **ed25519** | **rsa** } *key-pair-label*

Syntax Description

key-pair-label	Specifies the key pair label for the respective key signature algorithm (DSA, ECDSA, Ed25519 or RSA).

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.
Release 7.3.1	The command was modified to include the **ed25519** option.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to create the key pair for the leaf certificate on the router:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#keypair rsa system-enroll-key
Router(config-trustp)#commit
```

Related Commands

Command	Description
ca-keypair, on page 4	Creates the key pair for the root certificate on the router.

keystring

To import the RSA public key in SSH format into the router for authenticating a user, use the **keystring** command in the SSH user key configuration mode. To remove the imported public key, use the **no** form of this command.

keystring [**second** | **third** | **fourth**] *key*

Syntax Description

second	(Optional) Imports the second RSA public key.
third	(Optional) Imports the third RSA public key.
fourth	(Optional) Imports the fourth RSA public key.
key	Specifies the key in SSH format.

Command Default

The command imports the first RSA public key into the router if none of the options are specified.

Command Modes

SSH user key configuration mode

Command History

Release	Modification
Release 7.11.1	This command was modified to include the **second**,**third**, and **fourth** options.
Release 7.2.1	This command was introduced.

Usage Guidelines

This command imports the first RSA public key if you do not specify the **second**,**third**, or **fourth** option.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to import the first RSA public key specified in SSH format for user *test*.

```
RP/0/RP0/CPU0:OC_router1#conf t
Tue Nov  7 20:28:58.585 IST
RP/0/RP0/CPU0:OC_router1(config)#ssh server username test
RP/0/RP0/CPU0:OC_router1(config-user-key)#keystring ssh-rsa
[illegible]
RP/0/RP0/CPU0:OC_router1(config-user-key)#commit
Tue Nov  7 20:29:19.109 IST
RP/0/RP0/CPU0:OC_router1(config-user-key)#
```

This example shows how to import the third RSA public key specified in SSH format for user *test*.

```
RP/0/RP0/CPU0:OC_router1#conf t
Tue Nov  7 20:28:58.585 IST
RP/0/RP0/CPU0:OC_router1(config)#ssh server  username test
```

```
RP/0/RP0/CPU0:OC_router1(config-user-key)#keystring third ssh-rsa
[illegible]

RP/0/RP0/CPU0:OC_router1(config-user-key)#commit
Tue Nov  7 20:30:51.892 IST
RP/0/RP0/CPU0:OC_router1(config-user-key)#
```

lifetime (trustpoint)

To configure the lifetime for self-enrollment of certificates, use the **lifetime** command in trustpoint configuration mode. To remove this configuration, use the **no** form of this command.

lifetime {**ca-certificate** | **certificate**} *validity*

Syntax Description

ca-certificate	Configures the lifetime for self-enrollment of CA certificate.
validity	Specifies the validity for the certificates, in days. The range is from 30 to 5474 days.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to configure the lifetime for self-enrollment of CA certificate:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#lifetime ca-certificate 30
Router(config-trustp)#commit
```

message-digest

To configure the message digest hashing algorithm for the certificates, use the **message-digest** command in trustpoint configuration mode. To remove this configuration, use the **no** form of this command.

message-digest {**md5** | **sha1** | **sha256** | **sha384** | **sha512**}

Syntax Description

md5	Specifies MD5 as the message digest hashing algorithm for the certificate.
sha1	Specifies SHA1 as the message digest hashing algorithm for the certificate.
sha256	Specifies SHA256 as the message digest hashing algorithm for the certificate.
sha384	Specifies SHA384 as the message digest hashing algorithm for the certificate.
sha512	Specifies SHA512 as the message digest hashing algorithm for the certificate.

Command Default

None

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to specify SHA256 as the message digest hashing algorithm for the certificate:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#message-digest sha256
Router(config-trustp)#commit
```

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 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0RSP0/CPU0:router(config-trustp)# query url ldap://my-ldap.domain.com
```

renewal-message-type

Allows you to configure the request type from the router to the CA for automatic PKI certificate renewal.

renewal-message-type { **pkcsreq** | **renewalreq** }

Syntax Description

pkcsreq	The router uses Public Key Cryptography Standards (PKCS) requests for automatic PKI certificate renewal.
renewalreq	The router uses Renew requests for automatic PKI certificate renewal.

Command Default

By default, the PKCS request is available in the router.

Command Modes

Trustpoint configuration

Command History

Release	Modification
Release 7.5.3	This command was introduced.

Usage Guidelines

This command is applicable only for Cisco IOS XR 64-bit Software.

Task ID

Task ID	Operations
crypto	read, write

Examples

This example shows how to use this command in the router:

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)# renewal-message-type renewalreq
Router(config-trustp)# keypair rsa system-enroll-key
Router(config-trustp)# commit
```

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 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0RSP0/CPU0:router(config-trustp)# rsakeypair key1
```

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 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# crypto ca trustpoint root
RP/0/RP0RSP0/CPU0:router(config-trustp)# enrollment url http://10.3.0.7:80
RP/0/RP0RSP0/CPU0:router(config-trustp)# ip-address none
RP/0/RP0RSP0/CPU0:router(config-trustp)# serial-number none
RP/0/RP0RSP0/CPU0:router(config-trustp)# subject-name ON=Jack, OU=PKI, O=Cisco Systems,
C=US
```

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 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RP0RSP0/CPU0:router(config-trustp)# sftp-password password xxxxxx
```

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 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RP0RSP0/CPU0:router(config-trustp)# sftp-username tmordeko
```

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 modeXR EXEC mode.

show crypto ca certificates

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was modified to include the **Trusted Certificate Chain** field in the output as part of supporting multi-tier CA for trustpoint authentication.
Release 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/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
```

The following is a sample output with multi-tier CA. The command output displays the **Trusted Certificate Chain** field if there is one or more subordinate CAs involved in the hierarchy.

```
Router#show crypto ca certificates test-ca
Mon Feb  6 09:03:53.019 UTC

Trustpoint       : test-ca
==================================================
CA certificate
  Serial Number  : 10:01
  Subject:
            CN=SUB_CA_CERT,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Issued By      :
            CN=TWO-LEVEL-CA,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Validity Start : 12:31:40 UTC Sun Jun 14 2020
  Validity End   : 12:31:40 UTC Wed Jun 12 2030

  CRL Distribution Point
            http://10.105.236.78/crl_akshath_two_level_ca/crl.der
  SHA1 Fingerprint:
             D8E0C11ECED96F67FDBC800DB6A126676A76BD62
Trusted Certificate Chain
  Serial Number  : 0F:A0:06:7A:C9:5E:A9:E7:61:A2:B9:2B:27:D1:D6:8F:3D:51:43:3B
  Subject:
            CN=TWO-LEVEL-CA,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Issued By      :
            CN=TWO-LEVEL-CA,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Validity Start : 13:12:32 UTC Sun Jun 07 2020
  Validity End   : 13:12:32 UTC Sat Jun 02 2040

  CRL Distribution Point
            http://10.105.236.78/crl_akshath_two_level_ca/crl.der
  SHA1 Fingerprint:
             08E71248FB7578614442E713AC87C461D173952F
```

```
Router certificate
  Key usage      : General Purpose
  Status         : Available
  Serial Number  : 28:E5
  Subject:
            CN=test
  Issued By      :
            CN=SUB_CA_CERT,OU=SPBU,O=CSCO,L=BGL,ST=KA,C=IN
  Validity Start : 08:49:54 UTC Mon Feb 06 2023
  Validity End   : 08:49:54 UTC Wed Mar 08 2023
  SHA1 Fingerprint:
             6C8644FA67D9CEBC7C5665C35838265F578835AB
Associated Trustpoint: test-ca
```

show crypto ca crls

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

show crypto ca crls

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read

Examples

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

```
RP/0/RP0RSP0/CPU0:router: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
```

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 in EXEC modeXR EXEC mode.

show crypto ca trustpool policy

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

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/RP0RSP0/CPU0:router# 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
```

show crypto key mypubkey authentication-ssh

To display the cryptographic keys that are used for the public key-based authentication of SSH clients on the router, use the **show crypto key mypubkey authentication-ssh** command in EXEC modeXR EXEC mode.

show crypto key mypubkey authentication-ssh rsa [{ **all** | **username** *name* }]

Syntax Description

rsa	Displays the RSA key of the user.
username *name*	Specifies the name of the user whose RSA key is to be displayed.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.10.1	This command was introduced.

Usage Guidelines

If the **username** is not specified, then the command displays the key for the currently logged-in user.

Task ID

Task ID	Operations
crypto	read

Examples

This example shows how to display the RSA key used for public key-based authentication of SSH clients on Cisco IOS XR routers:

```
Router#show crypto key mypubkey authentication-ssh rsa
Wed Dec 21 10:24:34.226 UTC
Key label: cisco
Type     : RSA Authentication
Size     : 2048
Created  : 10:02:59 UTC Wed Dec 21 2022
Data     :
 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
 00A292B0 E45ACBB9 47B9EDA8 47E4664E 58FC3EA5 CE0F6B7A 3C6B7A73 537E6CEB
 .
 .
 .
 FF6BAF95 D9617CF6 65C058CC 7C6C22A9 9E48CC43 FDFF0EB7 ABADEB77 55A274DB
 15020301 0001

OpenSSH Format:
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCikrDkWsu5R7ntqEfkZk5Y/.../2uvldlhfPZlwFjMfGwiqZ5IzEP9/w63q63rd1WidNsV

Router#
```

The key value starts with *ssh-rsa* in the above output.

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 modeXR EXEC mode.

show crypto key mypubkey dsa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read

Examples

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

```
RP/0/RP0RSP0/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
```

show crypto key mypubkey ecdsa

To display the Elliptic Curve Digital Signature Algorithm (ECDSA) public keys for your router, use the **show crypto key mypubkey ecdsa** command.

show crypto key mypubkey ecdsa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Task ID

Task ID	Operation
crypto	read

Example

```
RP/0/RSP0/CPU0:Router# show crypto key mypubkey ecdsa

Key label: the_default
Type     : ECDSA General Curve Nistp256
Degree   : 256
Created  : 19:10:54 IST Mon Aug 21 2017
Data     :
 04255331 89B3CC40 BCD5A5A3 3BCCE7FF 522BF88D F3CC300D CEC9D7FD 98796ABB
 6A69523F E5FBAB66 804A05BF ECCDABC6 63F73AE8 E89827DD 18EB106A 7735C34A
```

show crypto key mypubkey ed25519

To display the Ed25519 crypto public keys of your router, use the **show crypto key mypubkey ed25519** command in EXEC modeXR EXEC mode.

show crypto key mypubkey ed25519

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.3.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read

Examples

This example shows the sample output of the **show crypto key mypubkey ed25519** command:

```
Router# show crypto key mypubkey  ed25519

Mon Nov 30 07:05:06.532 UTC
Key label: the_default
Type : ED25519
Size : 256
Created : 07:03:17 UTC Mon Nov 30 2020
Data :
FF0ED4E7 71531B3D 9ED72C48 3F79EC59 9EFECCC3 46A129B2 FAAA12DD EE9D0351
```

Related Commands

Command	Description
crypto key generate ed25519, on page 26	Generates Ed25519 crypto key pairs.
crypto key zeroize ed25519, on page 37	Deletes all Ed25519 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 modeXR EXEC mode.

show crypto key mypubkey rsa

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	read

Examples

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

```
RP/0/RP0RSP0/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
```

show platform security integrity dossier

To collect the data from various IOS XR applications, use the **show platform security integrity dossier** command in EXEC modeXR EXEC mode.

show platform security integrity dossier [**include** {**packages** | **reboot-history** | **rollback-history** | **running-config** | **system-integrity-snapshot** | **system-inventory**}] [**nonce** *nonce-value*]

Syntax Description

packages	Displays active package(s) installed.
reboot-history	Displays reboot history of the node.
rollback-history	Displays rollback history of the node.
running-config	Displays the currently committed running configuration on the node, as displayed by **show running configuration** command.
system-integrity-snapshot	Displays the system integrity snapshot.
system-inventory	Displays the system inventory.
nonce	Specifies the nonce to generate the signature.
nonce-value	Specifies the nonce value in hexadecimal string format.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The output of this command is displayed in JSON format.

Task ID

Options	Task ID	Operations
packages	pkg-mgmt	read
reboot-history	system	read
rollback-history	config-services	read
running-config	NA (available to all users)	read
system-integrity-snapshot	basic-services	read
system-inventory	sysmgr	read

Examples

This example shows the usage of **show platform security integrity dossier** command with various selectors:

```
Router#show platform security integrity dossier include packages reboot-history
rollback-history system-integrity-snapshot system-inventory nonce 1580 | utility sign nonce
 1580 include-certificate
```

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 [**ca-certificate**] *subject-name*

Syntax Description

ca-certificate	(Optional) Specifies the subject name for the CA certificate for self-enrollment.
subject-name	(Optional) Specifies the subject name used in the certificate request.

Command Default

If the *subject-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 7.0.12	This command was introduced.

Usage Guidelines

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:

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

This example shows how to specify the subject name for the CA certificate for self-enrollment.

```
Router#configure
Router(config)#crypto ca trustpoint system-trustpoint
Router(config-trustp)#subject-name ca-certificate CN=labuser-ca,C=US,ST=CA,L=San Jose,O=cisco
 systems,OU=ASR
Router(config-trustp)#commit
```

utility sign

To sign the command output with the enrollment key to verify its data integrity and authenticity, use the **utility sign** command along with any of the Cisco IOS XR commands.

utility sign [{**include-certificate** | **nonce** *nonce-value*}]

Syntax Description

include-certificate	Includes the certificate of the signer.
nonce	Indicates the nonce to generate the signature.
nonce-value	Specifies the nonce value in hexadecimal string format.

Command Default

None

Command Modes

Any IOS XR command configuration mode.

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
crypto	execute

Examples

This example shows how to add a signature to the command output data to verify its data integrity and authenticity:

```
Router#show version | utility sign nonce 1234 include-certificate
```