



Subordinate Certificate Server

The Subordinate Certificate Server feature allows you to configure a subordinate certificate server to grant all or certain Simple Certificate Enrollment Protocol (SCEP) or manual (PKCS10) certificate requests.

Feature History for Subordinate Certificate Server

| Release | Modification |
|-----------|------------------------------|
| 12.3(14)T | This feature was introduced. |

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- [Prerequisites for Subordinate Certificate Server, page 2](#)
- [Restrictions for Subordinate Certificate Server, page 2](#)
- [Information About Subordinate Certificate Server, page 2](#)
- [How to Configure Subordinate Certificate Server, page 3](#)
- [Configuration Examples for Subordinate Certificate Server, page 10](#)
- [Additional References, page 12](#)
- [Command Reference, page 13](#)



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

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

Prerequisites for Subordinate Certificate Server

- The certificate server supports SCEP over HTTP. The HTTP server must be enabled on the router for the certificate server to use SCEP. (To enable the HTTP server, use the **ip http server** command.) The certificate server will automatically enable or disable SCEP services after the HTTP server is enabled or disabled. If the HTTP server is not enabled, only manual PKCS10 enrollment is supported.
- Time services must be running on the router because the certificate server requires reliable time “knowledge.” If a hardware clock is unavailable, the certificate server will depend on manually configured clock settings, such as Network Time Protocol (NTP). If there is not a hardware clock or the clock is invalid, a message will be displayed at bootup stating that the time has not been set and that the certificate server cannot start:

```
% Time has not been set. Cannot start the Certificate server.
```

For information on manually configuring clock settings, see the section “Setting Time and Calendar Services” in the chapter “Performing Basic System Management” of the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*, Release 12.3.

If the certificate server is enabled, the **show crypto pki server** command will display the enabled state (see “[Show Output for a Subordinate Certificate Server: Example.](#)”)

After the time has been set, the certificate server will automatically switch to running status.

Restrictions for Subordinate Certificate Server

- The root certificate server should be a Cisco IOS certificate server.
- The root certificate server has to run Cisco IOS software Release 12.3(14)T or later.

Information About Subordinate Certificate Server

To configure the Subordinate Certificate Server feature, you should understand the following concept:

- [Subordinate Certificate Authorities, page 2](#)

Subordinate Certificate Authorities

Because the root Rivest, Shamir, and Adelman (RSA) key pairs are extremely important in a public key infrastructure (PKI) hierarchy, it is often advantageous to keep them offline or archived. To support this requirement, PKI hierarchies allow for subordinate certificate authorities (CAs) that have been signed by the root authority. In this way, the root authority can be kept offline (except to issue occasional certificate revocation list [CRL] updates), and the subordinate CA can be used during normal operation.

The Subordinate Certificate Server feature allows you to configure a subordinate certificate server to grant all or certain SCEP or manual certificate requests.

The subordinate certificate server provides all the same features as a root certificate server (see the “[Related Documents](#)” section— *Cisco IOS Certificate Server*).



Note

Enrollment requests that come from a subordinate certificate server must always be manually granted.

How to Configure Subordinate Certificate Server

This section contains the following procedures:

- [Configuring a Subordinate Certificate Server, page 3](#) (required))
- [Verifying the Subordinate Certificate Server, page 4](#) (optional)
- [Troubleshooting the Subordinate Certificate Server Configuration, page 5](#) (optional)

Configuring a Subordinate Certificate Server

To configure a subordinate certificate server, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **exit**
6. **crypto pki server** *cs-label*
7. **issuer-name** *DN-string*
8. **mode sub-cs**
9. **no shutdown**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | crypto pki trustpoint <i>name</i> Example: Router (config)# crypto pki trustpoint sub | Declares the trustpoint that your subordinate certificate server should use and enters ca-trustpoint configuration mode. |
| Step 4 | enrollment url <i>url</i> Example: Router (ca-trustpoint)# enrollment url http://10.3.0.6 | Specifies the enrollment URL of the root certificate server. |

| | Command or Action | Purpose |
|--------|--|---|
| Step 5 | <code>exit</code> Example: Router (ca-trustpoint)# exit | Exits ca-trustpoint configuration mode. |
| Step 6 | <code>crypto pki server cs-label</code> Example: Router (config)# crypto pki server sub | Enables a Cisco IOS certificate server and enters cs-server configuration mode. Note The subordinate server must have the same name as the trustpoint created in Step 3 above. |
| Step 7 | <code>issuer-name DN-string</code> Example: Router (cs-server)# issuer-name CN=sub CA, O=Cisco, C=us | (Optional) Specifies the distinguished name (DN) as the CA issuer name for the certificate server. |
| Step 8 | <code>mode sub-cs</code> Example: Router (cs-server)# mode sub-cs | Places the PKI server into sub-certificate server mode. |
| Step 9 | <code>no shutdown</code> Example: Router (cs-server)# no shutdown | Enables or reenables the certificate server. <ul style="list-style-type: none"> If this is the first time that a subordinate certificate server is enabled, the certificate server will generate the key and obtain its signing certificate from the root certificate server. |

Verifying the Subordinate Certificate Server

To verify your configuration of the subordinate certificate server, perform the following steps.

SUMMARY STEPS

1. `enable`
2. `show crypto pki server`

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | show crypto pki server Example: Router# show crypto pki server | Displays the current state and configuration of the certificate server. |

Troubleshooting the Subordinate Certificate Server Configuration

- If the certificate server fails to enable or if the certificate server has trouble handling the request that has been configured, you can use the **debug crypto pki server** command to troubleshoot your configuration as shown in the following examples (Clock Not Set and Trustpoint Not Configured):

Clock Not Set

```
Router (config)# crypto pki server sub
Router (cs-server)# mode sub-cs
Router (cs-server)# no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key % or type Return to exit
Password:
*Jan 6 20:57:37.667: CRYPTO_CS: enter FSM: input state initial, input signal no shut

Re-enter password:
% Generating 1024 bit RSA keys ...
*Jan 6 20:57:45.303: CRYPTO_CS: starting enabling checks
*Jan 6 20:57:45.303: CRYPTO_CS: key 'sub' does not exist; generated automatically[OK]
% Time has not been set. Cannot start the Certificate server
```

Trustpoint Not Configured

```
Router (config)# crypto pki server sub
Router (cs-server)# mode sub-cs
Router (cs-server)# no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key or type Return to exit
Password:
*Jan 6 21:00:15.961: CRYPTO_CS: enter FSM: input state initial, input signal no shut.
Jan 6 21:03:34.309: CRYPTO_CS: enter FSM: input state initial, input signal time set.
Jan 6 21:03:34.313: CRYPTO_CS: exit FSM: new state initial.
Jan 6 21:03:34.313: CRYPTO_CS: cs config has been unlocked Re-enter password:
% Generating 1024 bit RSA keys ...
Jan 6 21:03:44.413: CRYPTO_CS: starting enabling checks
Jan 6 21:03:44.413: CRYPTO_CS: associated trust point 'sub' does not exist; generated
automatically
Jan 6 21:03:44.417: CRYPTO_CS: key 'sub' does not exist; generated automatically[OK]

Jan 6 21:04:03.993: CRYPTO_CS: nvram filesystem
Jan 6 21:04:04.077: CRYPTO_CS: serial number 0x1 written.
You must specify an enrollment URL for this CA before you can authenticate it.
% Failed to authenticate the Certificate Authority
```

2. If the certificate server fails to obtain its signing certificate from the root certificate server, you can use the **debug crypto pki transactions** command to troubleshoot your configuration as shown in the following example:

```
Router# debug crypto pki transactions

Jan  6 21:07:00.311: CRYPTO_CS: enter FSM: input state initial, input signal time set
Jan  6 21:07:00.311: CRYPTO_CS: exit FSM: new state initial
Jan  6 21:07:00.311: CRYPTO_CS: cs config has been unlockedno sh
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key % or type Return to exit
Password:
Jan  6 21:07:03.535: CRYPTO_CS: enter FSM: input state initial, input signal no shut

Re-enter password:
% Generating 1024 bit RSA keys ...
Jan  6 21:07:10.619: CRYPTO_CS: starting enabling checks
Jan  6 21:07:10.619: CRYPTO_CS: key 'sub' does not exist; generated automatically[OK]

Jan  6 21:07:20.535: %SSH-5-ENABLED: SSH 1.99 has been enabled
Jan  6 21:07:25.883: CRYPTO_CS: nvram filesystem
Jan  6 21:07:25.991: CRYPTO_CS: serial number 0x1 written.
Jan  6 21:07:27.863: CRYPTO_CS: created a new serial file.
Jan  6 21:07:27.863: CRYPTO_CS: authenticating the CA 'sub'
Jan  6 21:07:27.867: CRYPTO_PKI: Sending CA Certificate Request:
GET /cgi-bin/pkiclient.exe?operation=GetCACert&message=sub HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)

Jan  6 21:07:27.867: CRYPTO_PKI: can not resolve server name/IP address
Jan  6 21:07:27.871: CRYPTO_PKI: Using unresolved IP Address 10.3.0.6 Certificate has
the following attributes:
    Fingerprint MD5: 328ACC02 52B25DB8 22F8F104 B6055B5B
    Fingerprint SHA1: 02FD799D DD40C7A8 61DC53AB 1E89A3EA 2A729EE2

% Do you accept this certificate? [yes/no]:
Jan  6 21:07:30.879: CRYPTO_PKI: http connection opened
Jan  6 21:07:30.903: CRYPTO_PKI: HTTP response header:
    HTTP/1.1 200 OK
    Date: Thu, 06 Jan 2005 21:07:30 GMT
    Server: cisco-IOS
    Content-Type: application/x-x509-ca-cert
    Expires: Thu, 06 Jan 2005 21:07:30 GMT
    Last-Modified: Thu, 06 Jan 2005 21:07:30 GMT
    Cache-Control: no-store, no-cache, must-revalidate
    Pragma: no-cache
    Accept-Ranges: none

Content-Type indicates we have received a CA certificate.

Jan  6 21:07:30.903: Received 507 bytes from server as CA certificate:
Jan  6 21:07:30.907: CRYPTO_PKI: transaction GetCACert completed
Jan  6 21:07:30.907: CRYPTO_PKI: CA certificate received.
Jan  6 21:07:30.907: CRYPTO_PKI: CA certificate received.
Jan  6 21:07:30.927: CRYPTO_PKI: crypto_pki_authenticate_tp_cert()

Jan  6 21:07:30.927: CRYPTO_PKI: trustpoint sub authentication status = 0 y Trustpoint
CA certificate accepted.%

% Certificate request sent to Certificate Authority

% Enrollment in progress...
Router (cs-server)#
Jan  6 21:07:51.772: CRYPTO_CA: certificate not found
Jan  6 21:07:51.772: CRYPTO_CA: certificate not found
```

```
Jan 6 21:07:52.460: CRYPTO_CS: Publishing 213 bytes to crl file nvram:sub.crl
Jan 6 21:07:54.348: CRYPTO_CS: enrolling the server's trustpoint 'sub'
Jan 6 21:07:54.352: CRYPTO_CS: exit FSM: new state check failed
Jan 6 21:07:54.352: CRYPTO_CS: cs config has been locked
Jan 6 21:07:54.356: CRYPTO_PKI: transaction PKCSReq completed
Jan 6 21:07:54.356: CRYPTO_PKI: status:
Jan 6 21:07:55.016: CRYPTO_PKI: Certificate Request Fingerprint MD5: 1BA027DB
1C7860C7 EC188F65 64356C80
Jan 6 21:07:55.016: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 840DB52C
E17614CB 0C7BE187 0DFC884D D32CAA75
Jan 6 21:07:56.508: CRYPTO_PKI: can not resolve server name/IP address
Jan 6 21:07:56.508: CRYPTO_PKI: Using unresolved IP Address 10.3.0.6
Jan 6 21:07:56.516: CRYPTO_PKI: http connection opened
Jan 6 21:07:59.136: CRYPTO_PKI: received msg of 776 bytes
Jan 6 21:07:59.136: CRYPTO_PKI: HTTP response header:
  HTTP/1.1 200 OK
  Date: Thu, 06 Jan 2005 21:07:57 GMT
  Server: cisco-IOS
  Content-Type: application/x-pki-message
  Expires: Thu, 06 Jan 2005 21:07:57 GMT
  Last-Modified: Thu, 06 Jan 2005 21:07:57 GMT
  Cache-Control: no-store, no-cache, must-revalidate
  Pragma: no-cache
  Accept-Ranges: none

Jan 6 21:07:59.324: The PKCS #7 message has 1 verified signers.
Jan 6 21:07:59.324: signing cert: issuer=cn=root1
Jan 6 21:07:59.324: Signed Attributes:

Jan 6 21:07:59.328: CRYPTO_PKI: status = 102: certificate request pending
Jan 6 21:08:00.788: CRYPTO_PKI: can not resolve server name/IP address
Jan 6 21:08:00.788: CRYPTO_PKI: Using unresolved IP Address 10.3.0.6
Jan 6 21:08:00.796: CRYPTO_PKI: http connection opened
Jan 6 21:08:11.804: CRYPTO_PKI: received msg of 776 bytes
Jan 6 21:08:11.804: CRYPTO_PKI: HTTP response header: HTTP/1.1 200 OK
  Date: Thu, 06 Jan 2005 21:08:01 GMT
  Server: cisco-IOS
  Content-Type: application/x-pki-message
  Expires: Thu, 06 Jan 2005 21:08:01 GMT
  Last-Modified: Thu, 06 Jan 2005 21:08:01 GMT
  Cache-Control: no-store, no-cache, must-revalidate
  Pragma: no-cache
  Accept-Ranges: none

Jan 6 21:08:11.992: The PKCS #7 message has 1 verified signers.
Jan 6 21:08:11.992: signing cert: issuer=cn=root1
Jan 6 21:08:11.996: Signed Attributes:

Jan 6 21:08:11.996: CRYPTO_PKI: status = 102: certificate request pending
Jan 6 21:08:21.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:08:31.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:08:41.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:08:51.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:09:01.996: CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:09:11.996: CRYPTO_PKI: resend GetCertInitial, 1 Jan 6 21:09:11.996:
CRYPTO_PKI: All sockets are closed for trustpoint sub.
Jan 6 21:09:11.996: CRYPTO_PKI: resend GetCertInitial for session: 0
Jan 6 21:09:11.996: CRYPTO_PKI: can not resolve server name/IP address
Jan 6 21:09:11.996: CRYPTO_PKI: Using unresolved IP Address 10.3.0.6
Jan 6 21:09:12.024: CRYPTO_PKI: http connection opened% Exporting Certificate Server
signing certificate and keys...
```

```

Jan  6 21:09:14.784: CRYPTO_PKI: received msg of 1611 bytes
Jan  6 21:09:14.784: CRYPTO_PKI: HTTP response header:
HTTP/1.1 200 OK
Date: Thu, 06 Jan 2005 21:09:13 GMT
Server: cisco-IOS
Content-Type: application/x-pki-message
Expires: Thu, 06 Jan 2005 21:09:13 GMT
Last-Modified: Thu, 06 Jan 2005 21:09:13 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Accept-Ranges: none

Jan  6 21:09:14.972: The PKCS #7 message has 1 verified signers.
Jan  6 21:09:14.972: signing cert: issuer=cn=root1
Jan  6 21:09:14.972: Signed Attributes:

Jan  6 21:09:14.976: CRYPTO_PKI: status = 100: certificate is granted
Jan  6 21:09:15.668: The PKCS #7 message contains 1 certs and 0 crls.
Jan  6 21:09:15.688: Newly-issued Router Cert: issuer=cn=root serial=2
Jan  6 21:09:15.688: start date: 21:08:03 GMT Jan 6 2005
Jan  6 21:09:15.688: end date: 21:08:03 GMT Jan 6 2006
Jan  6 21:09:15.688: Router date: 21:09:15 GMT Jan 6 2005
Jan  6 21:09:15.692: Received router cert from CA
Jan  6 21:09:15.740: CRYPTO_CA: certificate not found
Jan  6 21:09:15.744: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.
Jan  6 21:09:15.744: %PKI-6-CERTRET: Certificate received from Certificate Authority
Jan  6 21:09:15.744: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.
Jan  6 21:09:15.744: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.
Jan  6 21:09:15.748: CRYPTO_CS: enter FSM: input state check failed, input signal cert
configured
Jan  6 21:09:15.748: CRYPTO_CS: starting enabling checks
Jan  6 21:09:15.748: CRYPTO_CS: nvram filesystem
Jan  6 21:09:15.796: CRYPTO_CS: found existing serial file.
Jan  6 21:09:15.820: CRYPTO_CS: old router cert flag 0x4
Jan  6 21:09:15.820: CRYPTO_CS: new router cert flag 0x44
Jan  6 21:09:18.432: CRYPTO_CS: DB version 1
Jan  6 21:09:18.432: CRYPTO_CS: last issued serial number is 0x1
Jan  6 21:09:18.480: CRYPTO_CS: CRL file sub.crl exists.
Jan  6 21:09:18.480: CRYPTO_CS: Read 213 bytes from crl file sub.crl.
Jan  6 21:09:18.532: CRYPTO_CS: SCEP server started
Jan  6 21:09:18.532: CRYPTO_CS: exit FSM: new state enabled
Jan  6 21:09:18.536: CRYPTO_CS: cs config has been locked
Jan  6 21:09:18.536: CRYPTO_PKI: All enrollment requests completed for trustpoint sub.

```

3. If the certificate server fails to enable or if the certificate server has trouble handling the request that has been configured, you can use the **debug crypto pki server** command to troubleshoot the progress of an enrollment. This command can also be used to debug the root CA (turn it on at the root CA).

Examples

```

Router# debug crypto pki server

Jan  6 21:07:57.529: CRYPTO_CS: received a SCEP request
Jan  6 21:07:57.533: CRYPTO_CS: read SCEP: registered and bound service
SCEP_READ_DB_1
Jan  6 21:07:57.649: CRYPTO_CS: scep msg type - 19
Jan  6 21:07:57.649: CRYPTO_CS: trans id -
3AE00CCCCE6F0F6AE7F163A277906964
Jan  6 21:07:58.345: CRYPTO_CS: read SCEP: unregistered and unbound service
SCEP_READ_DB_1

```

```

Jan 6 21:07:58.345: CRYPTO_CS: received an enrollment request
Jan 6 21:07:58.353: CRYPTO_CS: found basic_constraints in enrollment request
Jan 6 21:07:58.353: CRYPTO_CS: received a sub-CS cert enrollment request
Jan 6 21:07:58.357: CRYPTO_CS: reqID = 1
Jan 6 21:07:58.357: CRYPTO_CS: write SCEP: registered and bound service
SCEP_WRTE_DB_1
Jan 6 21:07:59.109: CRYPTO_CS: write SCEP: unregistered and unbound service
SCEP_WRTE_DB_1
Jan 6 21:07:59.117: CRYPTO_CS: sent SCEP pending reply
Router#
Router#
Router# crypto pki server grant 1
Router#
Jan 6 21:08:01.805: CRYPTO_CS: received a SCEP request
Jan 6 21:08:01.809: CRYPTO_CS: read SCEP: registered and bound service SCEP_READ_DB_2
Jan 6 21:08:01.929: CRYPTO_CS: scep msg type - 20
Jan 6 21:08:01.929: CRYPTO_CS: trans id - 3AE00CCCCE6F0F6AE7F163A277906964
Jan 6 21:08:02.617: CRYPTO_CS: read SCEP: unregistered and unbound service
SCEP_READ_DB_2
Jan 6 21:08:02.621: CRYPTO_CS: received an enrollment request
Jan 6 21:08:02.621: CRYPTO_CS: reqID = 1
Jan 6 21:08:02.621: CRYPTO_CS: write SCEP: registered and bound service
SCEP_WRTE_DB_2
Jan 6 21:08:03.377: CRYPTO_CS: write SCEP: unregistered and unbound service
SCEP_WRTE_DB_2
Jan 6 21:08:03.381: CRYPTO_CS: sent SCEP pending reply
Jan 6 21:08:03.385: CRYPTO_CS: Granting enrollment request 1
Jan 6 21:08:03.389: CRYPTO_CS: generating a CA cert
Jan 6 21:08:03.393: CRYPTO_CS: added key usage extension
Jan 6 21:08:04.109: CRYPTO_CS: serial number 0x2 written.
Jan 6 21:08:06.253: CRYPTO_CS: reqID=1 granted,
fingerprint=1BA027DB1C7860C7EC188F6564356C80
Router#
Router#
Router# crypto pki server root info request
Enrollment Request Database:

Subordinate CA certificate requests:
ReqID      State      Fingerprint                               SubjectName
-----
1          granted   1BA027DB1C7860C7EC188F6564356C80      cn=sub
RA certificate requests:
ReqID      State      Fingerprint                               SubjectName
-----

Router certificates requests:
ReqID      State      Fingerprint                               SubjectName
> -----

Router#
Jan 6 21:09:13.032: CRYPTO_CS: received a SCEP request
Jan 6 21:09:13.036: CRYPTO_CS: read SCEP: registered and bound service SCEP_READ_DB_3
Jan 6 21:09:13.148: CRYPTO_CS: scep msg type - 20
Jan 6 21:09:13.152: CRYPTO_CS: trans id - 3AE00CCCCE6F0F6AE7F163A277906964
Jan 6 21:09:13.848: CRYPTO_CS: read SCEP: unregistered and unbound service
SCEP_READ_DB_3
Jan 6 21:09:13.848: CRYPTO_CS: received an enrollment request
Jan 6 21:09:13.852: CRYPTO_CS: write SCEP: registered and bound service
SCEP_WRTE_DB_3
Jan 6 21:09:14.760: CRYPTO_CS: write SCEP: unregistered and unbound service
SCEP_WRTE_DB_3
Jan 6 21:09:14.768: CRYPTO_CS: Certificate sent to requestor Router

```

Configuration Examples for Subordinate Certificate Server

This section provides the following output examples:

- [Subordinate Certificate Server: Example, page 10](#)
- [Root Certificate Server Differentiation: Example, page 11](#)
- [Show Output for a Subordinate Certificate Server: Example, page 11](#)

Subordinate Certificate Server: Example

The following output is typical of what you might see after configuring a subordinate certificate server:

```
Router (config)# crypto pki trustpoint sub
Router (ca-trustpoint)# enrollment url http://10.3.0.6
Router (ca-trustpoint)# exit

Router (config)# crypto pki server sub
Router (cs-server)# mode sub-cs
Router (ca-server)# no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key % or type Return to exit Password:
Jan 6 22:32:22.698: CRYPTO_CS: enter FSM: input state initial, input signal no shut

Re-enter password:
% Generating 1024 bit RSA keys ...
Jan 6 22:32:30.302: CRYPTO_CS: starting enabling checks
Jan 6 22:32:30.306: CRYPTO_CS: key 'sub' does not exist; generated automatically[OK]

Jan 6 22:32:39.810: %SSH-5-ENABLED: SSH 1.99 has been enabled
Certificate has the following attributes:
    Fingerprint MD5: 328ACC02 52B25DB8 22F8F104 B6055B5B
    Fingerprint SHA1: 02FD799D DD40C7A8 61DC53AB 1E89A3EA 2A729EE2

% Do you accept this certificate? [yes/no]:
Jan 6 22:32:44.830: CRYPTO_CS: nvram filesystem
Jan 6 22:32:44.922: CRYPTO_CS: serial number 0x1 written.
Jan 6 22:32:46.798: CRYPTO_CS: created a new serial file.
Jan 6 22:32:46.798: CRYPTO_CS: authenticating the CA 'sub'y
Trustpoint CA certificate accepted.%

% Certificate request sent to Certificate Authority

% Enrollment in progress...
Router (cs-server)#
Jan 6 22:33:30.562: CRYPTO_CS: Publishing 213 bytes to crl file nvram:sub.crl
Jan 6 22:33:32.450: CRYPTO_CS: enrolling the server's trustpoint 'sub'
Jan 6 22:33:32.454: CRYPTO_CS: exit FSM: new state check failed
Jan 6 22:33:32.454: CRYPTO_CS: cs config has been locked
Jan 6 22:33:33.118: CRYPTO_PKI: Certificate Request Fingerprint MD5: CED89E5F 53B9C60E
> AA123413 CDDAD964
Jan 6 22:33:33.118: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 70787C76 ACD7E67F
7D2C8B23 98CB10E7 718E84B1
% Exporting Certificate Server signing certificate and keys...

Jan 6 22:34:53.839: %PKI-6-CERTRET: Certificate received from Certificate Authority
Jan 6 22:34:53.843: CRYPTO_CS: enter FSM: input state check failed, input signal cert
configured
Jan 6 22:34:53.843: CRYPTO_CS: starting enabling checks
Jan 6 22:34:53.843: CRYPTO_CS: nvram filesystem
```

```

Jan 6 22:34:53.883: CRYPTO_CS: found existing serial file.
Jan 6 22:34:53.907: CRYPTO_CS: old router cert flag 0x4
Jan 6 22:34:53.907: CRYPTO_CS: new router cert flag 0x44
Jan 6 22:34:56.511: CRYPTO_CS: DB version
Jan 6 22:34:56.511: CRYPTO_CS: last issued serial number is 0x1
Jan 6 22:34:56.551: CRYPTO_CS: CRL file sub.crl exists.
Jan 6 22:34:56.551: CRYPTO_CS: Read 213 bytes from crl file sub.crl.
Jan 6 22:34:56.603: CRYPTO_CS: SCEP server started
Jan 6 22:34:56.603: CRYPTO_CS: exit FSM: new state enabled
Jan 6 22:34:56.603: CRYPTO_CS: cs config has been locked
Jan 6 22:35:02.359: CRYPTO_CS: enter FSM: input state enabled, input signal time set
Jan 6 22:35:02.359: CRYPTO_CS: exit FSM: new state enabled
Jan 6 22:35:02.359: CRYPTO_CS: cs config has been locked

```

Root Certificate Server Differentiation: Example

When issuing certificates, the root certificate server (or parent subordinate certificate server) will differentiate the certificate request from “Sub CA,” “RA,” and peer requests, as shown in the following sample output:

```

Router# crypto pki server server1 info req

Enrollment Request Database:
RA certificate requests:
ReqID      State      Fingerprint                               SubjectName
-----
Subordinate CS certificate requests:
ReqID      State      Fingerprint                               SubjectName
-----
1          pending    CB9977AD8A73B146D3221749999B0F66 hostname=bubinga-subcs.cisco.com
RA certificate requests:
ReqID      State      Fingerprint                               SubjectName
-----
Router certificate requests:
ReqID      State      Fingerprint                               SubjectName
-----

```

Show Output for a Subordinate Certificate Server: Example

The following **show crypto pki server** command output indicates that a subordinate certificate server has been configured:

```

Router# show crypto pki server

Certificate Server sub:
  Status: enabled
  Server's configuration is locked (enter "shut" to unlock it)
  Issuer name: CN=sub
  CA cert fingerprint: 11B586EE 3B354F33 14A25DDD 7BD39187
  Server configured in subordinate server mode
  Upper CA cert fingerprint: 328ACC02 52B25DB8 22F8F104 B6055B5B
  Granting mode is: manual
  Last certificate issued serial number: 0x1
  CA certificate expiration timer: 22:33:44 GMT Jan 6 2006
  CRL NextUpdate timer: 22:33:29 GMT Jan 13 2005
  Current storage dir: nvram:
  Database Level: Minimum - no cert data written to storage

```

Additional References

The following sections provide references related to Subordinate Certificate Server.

Related Documents

| Related Topic | Document Title |
|---------------------------------|--|
| Configuring certificate servers | <i>Cisco IOS Certificate Server</i> , Release 12.3(4)T |
| Configuring trustpoints | “Configuring Certification Authority Interoperability” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.3 |
| Security commands | <i>Cisco IOS Security Command Reference</i> , Release 12.3T |

Standards

| Standards | Title |
|---|-------|
| No new or modified standards are supported by this feature. | — |

MIBs

| MIBs | MIBs Link |
|--|--|
| No new or modified MIBs are supported by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

RFCs

| RFCs | Title |
|--|-------|
| No new or modified RFCs are supported by this feature. | — |

Technical Assistance

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

Command Reference

This section documents only the following new command:

- [mode sub-cs](#)

mode sub-cs

To place the public key infrastructure (PKI) server into sub-certificate server mode, use the **mode sub-cs** command in certificate server mode. To remove the PKI server from sub-certificate mode, use the **no** form of this command.

mode sub-cs

no mode sub-cs

Syntax Description

This command has no arguments or keywords.

Defaults

The PKI server is not placed into sub-certificate server mode.

Command Modes

Certificate server

Command History

| Release | Modification |
|-----------|------------------------------|
| 12.3(14)T | This command was introduced. |

Usage Guidelines

When this command is configured, ensure that the **crypto pki trustpoint** command has also been configured and that the enrollment URL is pointed to a Cisco IOS root certification authority (CA). If the **mode sub-cs** command is not configured and the certificate server is enabled for the first time, a self-signed CA certification will be generated and the certificate server will operate as a root CA.



Note

The **no mode sub-cs** command will have no effect if the server has been configured already. For example, if you want to make the subordinate CA a root CA, you must delete the server and re-create it.

Examples

The following configuration example shows that a subordinate certificate server named “sub” has been configured:

```
Router (config)# crypto pki trustpoint sub
Router (ca-trustpoint)# enrollment url http://10.3.0.6
Router (ca-trustpoint)# exit

Router (config)# crypto pki server sub
Router (cs-server)# issuer-name CN=sub CA, O=Cisco, C=us
Router (cs-server)# mode sub-cs
Router (cs-server)# no shutdown
```

Related Commands

| Command | Description |
|------------------------------|--|
| crypto pki server | Enables a Cisco IOS certificate server. |
| crypto pki trustpoint | Declares the trustpoint that your router should use. |

| Command | Description |
|-------------------------------|---|
| enrollment | Specifies the enrollment parameters of a CA. |
| issuer-name | Specifies the DN as the CA issuer name for the certificate server. |
| show crypto pki server | Displays the current state and configuration of the certificate server. |

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

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

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