CHAPTER 18

Certificate Authority Server

You can configure a Cisco IOS router to serve as a Certificate Authority (CA) server. A CA server handles certificate enrollment requests from clients, and can issue and revoke digital certificates.

To create, back up, restore, or edit a CA server, go to **Configure > VPN > Public Key Infrastructure > Certificate Authority > Create CA Server**.

To manage certificates on an existing CA server, go to **Configure > VPN > Public Key Infrastructure > Certificate Authority > Manage CA Server**.

To monitor a CA server, go to **Monitor > VPN Status > CA Server**.

Create CA Server

This window allows you to launch a wizard for creating a Certificate Authority (CA) server, or a wizard for restoring a CA server. Only one CA server can be set up on a Cisco IOS router.

The CA server should be used to issue certificates to hosts on the private network so that they can use the certificates to authenticate themselves to other

Prerequisite Tasks

If Cisco SDM finds that there are configuration tasks that should be performed before you begin configuring the CA server, it alerts you to them in this box. A link is provided next to the alert text so that you can go to that part of Cisco SDM

and complete the configuration. If Cisco SDM does not discover missing configurations, this box does not appear. Possible prerequisite tasks are described in Prerequisite Tasks for PKI Configurations.

Create Certificate Authority (CA) Server

Click this button to create a CA server on the router. Because only one CA server can be configured on the router, this button is disabled if a CA server is already configured.

Note The CA server you configure using SDM allows you to grant and revoke certificates. Although the router does store the serial numbers and other identifying information about the certificates that it grants, it does not store the certificates themselves. The CA server should be configured with a URL to a Registration Authority (RA) server that can store certificates that the CA server grants.

Restore Certificate Authority (CA) Server

If a CA server already operates on the router, you can restore the CA server configuration, and the information. If no CA server is configured on the router, this option is disabled.

Prerequisite Tasks for PKI Configurations

Before you begin a certificate enrollment or CA server configuration, it may be necessary for you to complete supporting configuration tasks first. SDM reviews the running configuration before allowing you to begin, alerts you to configurations you must complete, and provides links that take you to the areas of SDM that allow you to complete these configurations.

SDM may generate alerts about the following configuration tasks:

- SSH credentials not verified—Cisco SDM requires you to provide your SSH credentials before beginning.
- NTP not configured—The router must have accurate time for certificate enrollment to work. Identifying a Network Time Protocol server from which your router can obtain accurate time provides a time source that is not

affected if the router needs to be rebooted. If your organization does not have an NTP server, you may want to use a publicly available server, such as the server described at the following URL:

http://www.eecis.udel.edu/~mills/ntp/clock2a.html

- DNS not configured—Specifying DNS servers helps ensure that the router is able to contact the certificate server. DNS configuration is required to contact the CA server and any other server related to certificate enrollment such as OCSP servers or CRL repositories if those servers are entered as names and not as IP addresses.
- Domain and/or Hostname not configured—It is recommended that you configure a domain and hostname before beginning enrollment.

CA Server Wizard: Welcome

The Certificate Authority (CA) server wizard guides you through the configuration of a CA server. Be sure to have the following information before you begin:

- General information about the CA server—The name that you intend to give the server, the certificate issuer name that you want to use, and the username and password that enrollees will be required to enter when sending an enrollment request to the server.
- More detailed information about the server—Whether the server will operate in Registration Authority (RA) mode or Certificate Authority (CA) mode, the level of information about each certificate that the server will store, whether the server should grant certificates automatically, and the lifetimes of the certificates granted, and open enrollment requests.
- Supporting information—Links to the RA server that will store the certificates and to the Certificate Revocation List Distribution Point (CDP) server.

CA Server Wizard: Certificate Authority Information

Enter basic information about the CA server that you are configuring in this window.

CA Server Name

Provide a name to identify the server in the CA Server Name field. This could be the host name of the router, or another name that you enter.

Grant

Choose **Manual** if you want to grant certificates manually. Choose **Auto** if you want the server to grant certificates automatically. Auto, used mostly for debug purposes, is not recommended since it will issue certificates to any requester without requiring enrollment information.

Warning **Do not set Grant to Auto if your router is connected to the Internet. Grant should be set to Auto only for internal purposes such as when executing debugging procedures.**

CDP URL

Enter the URL to a Certificate Revocation List Distribution Point (CDP) server in the CDP URL field. The URL must be an HTTP URL. A sample URL follows:

```
http://172.18.108.26/cisco1cdp.cisco1.crl
```

The Certificate Revocation List (CRL) is the list of revoked certificates. Devices needing to check the validity of another device's certificate will fetch the CRL from the CA server. Since many devices may attempt to fetch the CRL, offloading it to a remote device, preferably an HTTP server, will reduce the performance impact on the Cisco IOS router hosting the CA server. If the checking device cannot connect to the CDP, as a backup it will use SCEP to fetch the CRL from the CA server.

Issuer Name Attributes

Common Name (cn)

Enter the common name that you want to use for the certificate. This might be the CA server name, the router hostname or another name you choose.

Organizational Unit (ou)

Enter the Organizational Unit, or department name to use for this certificate. For example, IT support, or Engineering might be organizational units.

Organization (o)

Enter the organization or company name.

State (st)

Enter the state or province in which the organization is located.

Country (c)

Enter the country in which the organization is located.

Email (e)

Enter the email address to be included in the router certificate.

Advanced Options

Click this button to enter advanced options for the CA server.

Advanced Options

The Advanced Options screen allows you to change default values for server settings and to specify the URL for the database that is to contain the certificate information.

Database

Configure the database level, the database URL, and database format in this section of the dialog.

Database Level

Choose the type of data that will be stored in the certificate enrollment database:

- **minimal—**Enough information is stored to continue issuing new certificates without conflict. This is the default.
- **names—**In addition to the information given by the minimal option, this includes the serial number and subject name of each certificate.

- **complete—**In addition to the information given by the minimal and names options, each issued certificate is written to the database.

Database URL

Enter the location to which the CA server will write certificate enrollment data. If no location is given, certificate enrollment data will be written to flash memory by default.

For example, to write certificate enrollment data to a tftp server, enter tftp://mytftp. To reset the database URL to flash memory, enter nvram.

Database Archive

Choose **pem** to create the archive in pem format, or **pkcs12** to create the archive in pkcs12 format.

Database Username

Enter a username for the database archive in the Database Username field. The username and password will be used to authenticate the server to the database.

Database Password and Confirm Password

Enter a password in the Database Password field, and reenter it in the Confirm Password field.

Lifetimes

Set the lifetime, or time before expiration, of items associated with the CA server. To set the lifetime for a specific item, choose it from the Lifetime drop-down list and enter a value in the Lifetime field.

You can set lifetimes for the following items:

- **Certificate**—Certificates issued by the CA server. Lifetime is entered in days, in the range 1–1825. If no value is entered, a certificate expires after one year. If a new value is entered, it affects certificates created only after that value is in effect.
- **CRL**—The Certificate Revocation List for certificates issued by the CA server. Lifetime is entered in hours, in the range 1–336. If no value is entered, a CRL expires after 168 hours (one week).

- **Enrollment-Request**—Open certificate requests existing in the enrollment database, but not including requests received through SCEP. Lifetime is entered in hours, in the range 1–1000. If no value is entered, an open enrollment request expires after 168 hours (one week).

CA Server Wizard: RSA Keys

The CA server uses public and private RSA keys to encrypt data and to sign certificates. SDM automatically generates a new key pair and gives it the name of the CA server. You can change the key modulus and type, and you can make the key exportable. You must enter a passphrase to use when restoring the CA server.

Label

This field is read-only. SDM uses the name of the CA server as the name of the key pair.

Modulus

Enter the key modulus value. If you want a modulus value between 512 and 1024 enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer.

The modulus determines the size of the key. The larger the modulus, the more secure the key, but keys with large modulus take longer to generate, and encryption/decryption operations take longer with larger keys.

Type

By default, Cisco SDM creates a general purpose key pair that is used for both encryption and signature. If you want Cisco SDM to generate separate key pairs for encrypting and signing documents, choose **Usage Keys**. Cisco SDM will generate usage keys for encryption and signature.

Key is exportable

Check **Key is exportable** if you want the CA server key to be exportable.

Passphrase and Confirm Passphrase

In the Passphrase field, enter a passphrase to use when restoring the CA server from backup. Reenter the same passphrase in the Confirm Passphrase field.

Open Firewall

The Open Firewall window appears when a firewall configuration must be modified in order to allow communication between the CDP server and the CA server. Select the interface, and check the **Modify** box to allow SDM to modify the firewall to allow this traffic. Click **Details** to view the ACE that would be added to the firewall.

CA Server Wizard: Summary

The Summary window displays the information that you entered in the wizard screens so that you can review the information before sending it to the router. A sample summary display follows:

```
------------------------------------------------------------
CA Server Configuration
------------------------------------------------------------
CA Server Name :CASvr-a
Grant:Manual
CDP URL:http://192.27.108.92/snrs.com
Common Name (cn):CS1841
Organization Unit (ou):IT Support
Organization (o):Acme Enterprises
State (st):CA
Country (c):US

------------------------------------------------------------
Advanced CA Server Configuration
------------------------------------------------------------
Database URL:nvram:
Database Archive:pem
Database Username:bjones
Database Password:*********

------------------------------------------------------------
RSA Keys:
------------------------------------------------------------
```

```
CA Server will automatically generate RSA key pair with following
defaults:-
Modulus:1024
Type of Key:General Purpose
Exportable Key:No
Passphrase configured:******


------------------------------------------------------------
Firewall Pass-through ACEs for Interface(s):
------------------------------------------------------------

FastEthernet0/0
    permit tcp host 192.27.108.92 eq www host 192.27.108.91 gt 1024
```

The summary display contains four sections, the CA Server Configuration section, the CA Server Advanced Configuration section, the RSA Keys section, and the Firewall Pass-through section. The name of this CA server is CAsvr-a. Certificates will be manually granted. Certificate information will be stored in nvram, in PEM format. SDM will generate a general-purpose key pair with the default modulus 1024. The key will not be exportable. an ACE will be configured to allow traffic to between the router and the CDP host with the IP address 192.27.108.92.

Manage CA Server

You can start and stop the CA server from this window, grant and reject certificate requests, and revoke certificates. If you need to change the CA server configuration, you can uninstall the server from this window and return to the Create CA Server window to create the server configuration that you need.

Name

Displays the name of the server. The name of the server was created when the server was created.

Status Icon

If the CA server is running, the word Running and a green icon is displayed. If the CA server is not running, the word Stopped and a red icon is displayed.

Start Server

The Start Server button is displayed if the server is stopped. Click **Start Server** to start the CA server.

Stop Server

The Stop Server button is displayed if the server the server is running, click **Stop Server** if you need to stop the CA server.

Backup Server

Click **Backup Server** to backup the server configuration information onto the PC. Enter the backup location in the displayed dialog.

Uninstall Server

Click to uninstall the CA server from your Cisco IOS router. All of the CA server configuration and data will be removed. If you backed up the CA server before uninstalling it, you can restore its data only after you create a new CA server. See Create CA Server.

Details of CA Server

The Details of CA Server table provides a snapshot of the CA Server configuration. The following table shows sample information.

Item Name	Item Value
CA Certificate Lifetime	1095 days
CDP URL	http://192.168.7.5
CRL Lifetime	168 hours
Certificate Lifetime	365 days
Database Level	minimal
Database URL	nvram:
Enrollment Request Lifetime	168 hours
Grant	manual

Item Name	Item Value
Issuer Name	CN=CertSvr
Mode	Certificate Authority
Name	CertSvr

See CA Server Wizard: Certificate Authority Information and Advanced Options for descriptions of these items.

Backup CA Server

You can back up the files that contain the information for the CA server to your PC. The Backup CA Server window lists the files that will be backed up. The listed files must be present in the router NVRAM for the backup to be successful.

Click **Browse** and specify a folder on the PC to which the CA server files should be backed up.

Manage CA Server Restore Window

If you have backed up and uninstalled a CA server, you can restore the server configuration to the router by clicking the **Restore CA Server** button. You must be able to provide the CA server name, complete database URL, and the backup passphrase that was used during initial configuration. When you restore the CA server, you are given the opportunity to change configuration settings.

Restore CA Server

If you have backed up the configuration for a CA server that was uninstalled, you can restore it by providing the information about it in the Restore CA Server window. You can edit settings for the server by clicking **Edit CA server settings before restoration**. You must provide the name, file format, URL to the database, and passphrase in order to back up the server or edit server settings.

CA Server Name

Enter the name of the CA server that you backed up.

File Format

Choose the file format that was specified in server configuration, either PEM or PKCS12.

Complete URL

Enter the router database URL that was provided when the CA server was configured. This is the location to which the CA server writes certificate enrollment data. Two sample URLs follow:

```
nvram:/mycs_06.p12
tftp://192.168.3.2/mycs_06.pem
```

Passphrase

Enter the passphrase that was entered when the CA server was configured.

Copy CA Server Files from PC

Check the **Copy CA Server Files from PC checkbox** if you want to copy the server information that you backed up to the PC to router nvram.

Edit CA Server settings before restoration

Click **Edit CA Server settings before restoration** if you want to change CA server configuration settings before restoring the server. See CA Server Wizard: Certificate Authority Information and CA Server Wizard: RSA Keys for information about the settings that you can change.

Edit CA Server Settings: General Tab

Edit general CA server configuration settings in this window. You cannot change the name of the CA server. For information on the settings that you can change, see CA Server Wizard: Certificate Authority Information.

Edit CA Server Settings: Advanced Tab

You can change any of the advanced CA server settings in this window. For information on these settings, see Advanced Options.

Manage CA Server: CA Server Not Configured

This window appears when you click **Manage CA Server** but no CA server is configured. Click **Create CA Server** and complete the wizard to configure a CA server on your router.

Manage Certificates

Clicking VPN > Public Key Infrastructure > Certificate Authoring > Manage Certificates displays the Pending Requests tab and the Revoked Certificates tab. To go to the help topics for these tabs, click the following links:

- Pending Requests
- Revoked Certificates

Pending Requests

This window displays a list of certificate enrollment requests received by the CA server from clients. The upper part of the window contains CA server information and controls. For information on stopping, starting, and uninstalling the CA server, see Manage CA Server.

You can choose a certificate enrollment request in the list, then choose to issue (accept), reject, or delete it. The actions available depend on the status of the chosen certificate enrollment request.

Select All

Click **Select All** to select all outstanding certificate requests. When all certificate requests are selected, clicking **Grant** grants all requests. Clicking **Reject** when all certificate requests are selected rejects all the requests..

Grant

Click **Grant** to issue the certificate to the requesting client.

Note The CA server windows do not show the IDs of the certificates that are granted. In case it is ever necessary to revoke a certificate, you should obtain the certificate ID from the administrator of the client that the certificate was issued for. The client administrator can determine the certificate ID by entering the Cisco IOS command sh crypto pki cert.

Delete

Click **Delete** to remove the certificate enrollment request from the database.

Reject

Click **Reject** to deny the certificate enrollment request.

Refresh

Click **Refresh** to update the certificate enrollment requests list with the latest changes.

Certificate Enrollment Requests Area

The certificate enrollment requests area has the following columns:

Request ID—A unique number assigned to the certificate enrollment request.

Status—The current status of the certificate enrollment request. The status can be Pending (no decision), Granted (issued certificate), Rejected (denied request).

Fingerprint—A unique digital client identifier.

Subject Name—The subject name in the enrollment request.

A sample enrollment request follows:

Request ID	State	Fingerprint	Subject Name
1	pending	serialNumber=FTX0850Z0GT+ hostname=c1841.snrsprp.com	B398385E6BB6604E9E98B8FDBBB5E8BA

Revoke Certificate

Click **Revoke Certificate** to display a dialog that allows you to enter the ID of the certificate that you want to revoke.

Note The certificate ID does not always match the request ID shown in the CA server windows. It may be necessary to obtain the ID of the certificate to be revoked from the administrator of the client for which the certificate was granted. See Pending Requests for information on how the client administrator can determine the certificate ID.

Revoked Certificates

This window displays a list of issued and revoked certificates. Only issued certificates can be revoked. The upper part of the window contains CA server information and controls. For information on stopping, starting, and uninstalling the CA server, see Manage CA Server.

The list of certificates has the following columns:

- **Certificate Serial Number**—A unique number assigned to the certificate. This number is displayed in hexadecimal format. For example, the decimal serial number 1 is displayed as 0x01.
- **Revocation Date**—The time and date that the certificate was revoked. If a certificate was revoked at 41 minutes and 20 seconds after midnight on February 6, 2007, the revocation date is displayed as 00:41:20 UTC Feb 6 2007.

Revoke Certificate

Click **Revoke Certificate** to display a dialog that allows you to enter the ID of the certificate that you want to revoke.

Note The certificate ID does not always match the request ID shown in the CA server windows. It may be necessary to obtain the ID of the certificate to be revoked from the administrator of the client for which the certificate was granted. See Pending Requests for information on how the client administrator can determine the certificate ID.

Revoke Certificate

You can revoke certificates that have been granted by this CA server in this window.

Certificate ID

Enter the ID of the certificate that you are revoking.

Note The certificate ID does not always match the request ID shown in the CA server windows. It may be necessary to obtain the ID of the certificate to be revoked from the administrator of the client for which the certificate was granted. See Pending Requests for information on how the client administrator can determine the certificate ID.