CHAPTER 16

Using Digital Certificates

Certificates are special encrypted text files that are generated by a trusted Certificate Authority (CA) that encrypt and decrypt the data. A CA can generate public and private keys and put them into signed certificates, revoke certificates, and renew certificates. If you are only using certificates on the server, and do not have a CA, you can use the VPN 5000 concentrator as a certificate generator (CG). The CG can generate signed certificates, but it cannot revoke them or renew them.

Certificates Configuration Dialog Box

The Cisco VPN 5000 concentrator can be configured to be a CG. This section explains how to configure the VPN 5000 concentrator series to be a CG and to set the enroll protocol.

To access the Certificates Configuration dialog box (Figure 16-1), select Global/Certificate Configuration from the Device view. Table 16-1 describes the entry fields in this dialog box.

Figure 16-1 Certificates Configuration Dialog Box

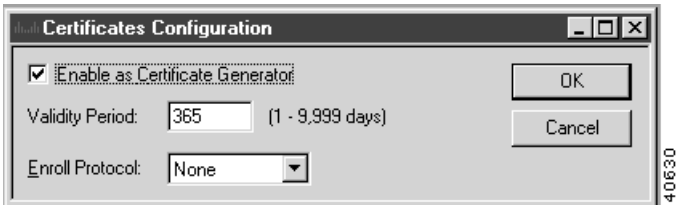


Table 16-1 Certificates Configuration Parameters

Parameter	Action
Enable as Certificate Generator	This checkbox sets the server as a CG.
Validity Period	This sets the validity period for all certificates generated. The default is 365.
Enroll Protocol	None. This is currently a read-only field.

Save Certificate Configuration

After you enable the concentrator as a CG, you must save the configuration to the device. Use the Save to - Device option from the File menu, or click the Save Config to Device icon on the Device toolbar.

Note Before the concentrator can generate a server or root certificate, you must set the system clock. You can do this either by selecting Device Properties from the Database menu, and set the date on the System Clock tab, or by selecting Global/Time Server from the device view. If you choose the time server option this is done automatically.

For more information on system clock settings, see the "System Clock Tab" section on page 1-10, or the "Time Server Dialog Box" section on page 14-13.

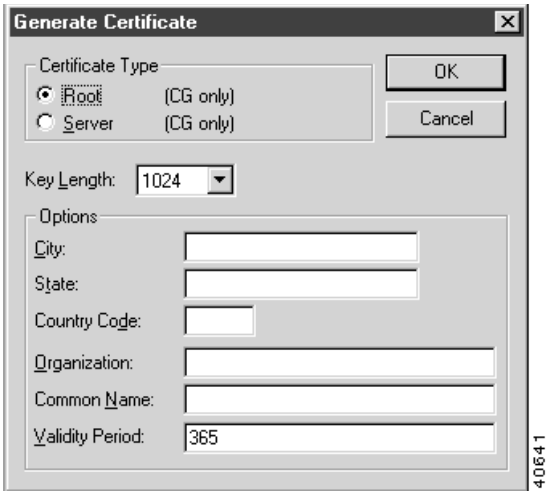
Generate Certificate Dialog Box

The VPN 5000 concentrator supports server-side authentication, where the concentrator has a private certificate, called a server certificate, and clients have a root certificate to authenticate the server.

For a CG, this section describes how to generate a root or server certificate.

To access the Generate Certificate dialog box (Figure 16-2), select Certificates/Generate Root/Server Certificate from the File menu.

Figure 16-2 Generate Certificate Dialog Box



To view the root or server certificate, select a Certificates/Show option from the Statistics menu. For more information on the Statistics menu, refer to "The Statistics Menu" section on page 1-14.

Table 16-2 describes the parameters in the Generate Certificate dialog box.

Table 16-2 Generate Certificate Parameters

Parameter	Description
Root (CG only)	Generates a root certificate on the CG. The root certificate is generated in PEM format.
Server (CG only)	Generates a server certificate for the CG. A root certificate must be generated first, or the server certificate will not be signed properly.

Table 16-2 Generate Certificate Parameters (continued)

Parameter	Description
Key Length	512, 1024, 2048, or 4096 Specifies the number of bits generated for the key. The default is 1024 and is the recommended key length. Larger keys can take the system up to an hour to generate.
Options	
City	A text string with no spaces identifying the city name where the concentrator resides.
State	A text string with no spaces identifying the full state name where the concentrator resides
Country Code	A two-letter country code where the concentrator resides.
Organization	A phrase, with spaces allowed, identifying the company name or other organization name.
Common Name	A phrase, with spaces allowed, identifying the concentrator name, or a description of the certificate. If you do not specify a name, the concentrator uses its device name.
Validity Period	1 to 9999 Specifies the validity period of the certificate. If you do not specify a value, the system uses the value set in the Certificate Configuration Dialog Box. See the "Certificates Configuration Dialog Box" section on page 16-1.

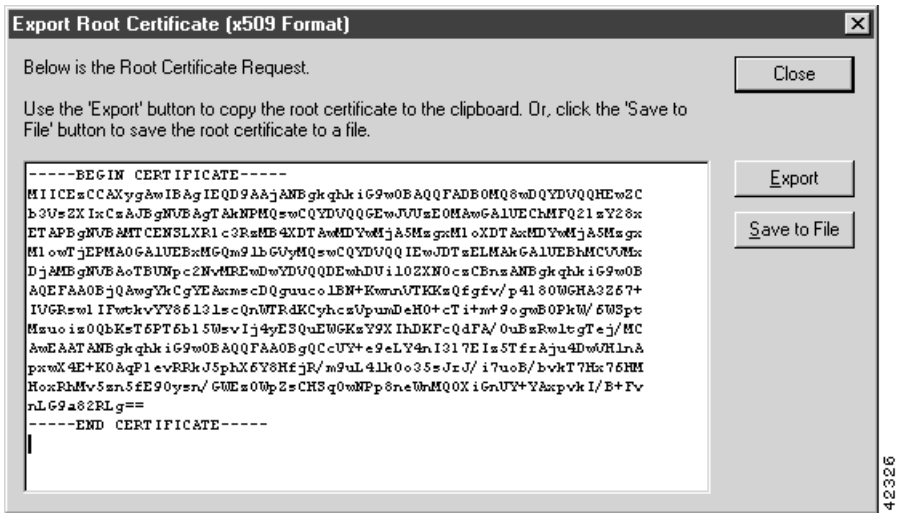
Export Root Certificate

To export a root certificate, select Certificates/Export Root Certificate from the File menu.

You will be asked if you want to export the root certificate in X.509 format. Click **Yes** if you want to export the root certificate in X.509 format. Click **No** to export in PEM format.

The Export Root Certificate window (Figure 16-3) appears with the root certificate shown.

Figure 16-3 Export Root Certificate Window



This window displays the last generated root certificate. To export the root certificate, click the **Export** button. This copies the root certificate to the Windows clipboard, which can be pasted to the application of your choice.

To save the root certificate to a file, click the **Save to File** button to open a file browser window.

Generate Certificate Request Dialog Box

For non-CG servers, this section describes how to request a server certificate.

The non-CG concentrator generates a request certificate to be exported to a CG or Certificate Authority (CA). The CA, or CG then generates a certificate, which must be imported back into the non-CG server.

To access the Generate Certificate Request dialog box (Figure 16-4), select Certificates/Generate Certificate Request from the File menu. Table 16-3 describes the parameters in the Generate Certificate Request Dialog Box.

Figure 16-4 Generate Certificate Request Dialog Box

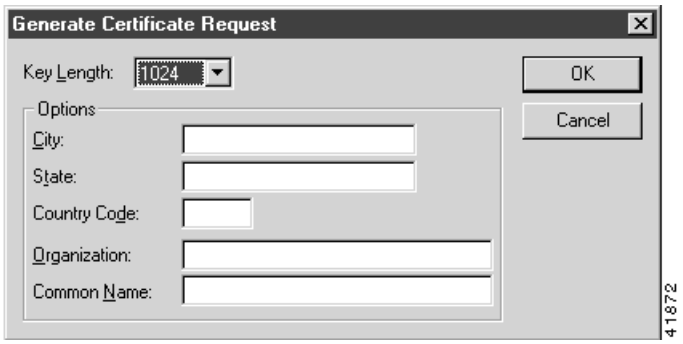


Table 16-3 Generate Certificate Request Parameters

Parameter	Description
Key Length	512, 1024, 2048, or 4096 Specifies the number of bits generated for the key. The default is 1024 and is the recommended key length. Larger keys can take the system up to an hour to generate.
Options	
City	A text string with no spaces identifying the city name where the concentrator resides.
State	A text string with no spaces identifying the full state name where the concentrator resides
Country Code	A two letter country code where the concentrator resides.
Organization	A phrase, with spaces allowed, identifying the company name or other organization name.
Common Name	A phrase, with spaces allowed, identifying the concentrator name, or a description of the certificate. If you do not specify a name, the concentrator uses its device name.

Export Certificate Request Window

This window is for non-CG certificate requests. After the concentrator generates a certificate request, you must export it to a CA or CG. The CA takes the certificate request and creates a server certificate.

If your concentrator is non-CG, and you need to import a server certificate from a CA or CG, you must use the command line interface. The Cisco VPN 5000 Manager does not support importing of certificates at this time. See the *Cisco VPN 5000 Concentrator Series Command Reference Guide* for more information about importing certificates.

To export a certificate request, select Certificates/Export Request from the File menu.

This window displays the last generated certificate request in the Export Certificate Request window (Figure 16-5).

Figure 16-5 Export Certificate Request Window

To export the certificate request, click the **Export** button. This copies the certificate request in PEM format to the Windows clipboard, which can be pasted to the application of your choice.

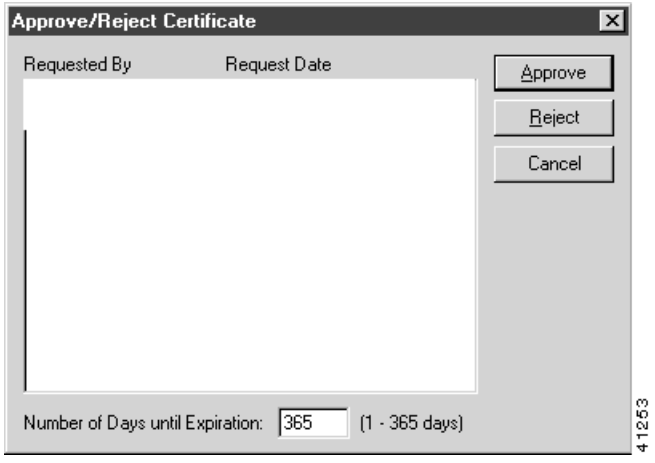
To save the certificate request to a file, click the **Save to File** button to open a file browser window.

Approve/Reject Certificate Window

This window is for CGs only. If you have imported a server certificate using the command line interface, you need to approve or reject the request. The certificate request stays in the server until it has been approved or rejected by an administrator.

To approve or reject certificate requests, select Certificates/Approve (or Reject) from the File menu. This opens a window that displays a list of pending certificate requests (Figure 16-6).

Figure 16-6 Approve/Reject Certificate Window



To approve a certificate request, highlight the appropriate certificate from the list and click the **Approve** button. The CG generates a certificate for the server that requested it. After completion, the server certificate will be displayed and the request is removed from the pending list.

To reject a certificate request, highlight the appropriate certificate from the list and click the **Reject** button. This removes the certificate request from the pending list. This option is only valid for servers that have been configured as certificate generators.

The **Number of Days until Expiration** value corresponds to the selected certificate request. The default value is 365 days.