



Installing an SSL Certificate

This appendix describes how to install a secured sockets layer (SSL) certificate. When you install an SSL certificate on a BBSM server, it enables visitors to verify the site's authenticity and communicate with it securely through SSL encryption, which protects confidential information, such as credit card numbers, online forms, and financial data. When SSL is being used, the end user connects to the Internet using “https” instead of “http.”

Before You Start

Before you install the SSL certificate, read the following notes and cautions:

- You must purchase a fully qualified domain name (FQDN) for the BBSM server before you can purchase a Secure Server Digital ID (certificate). You cannot use a name purchased for another server. The name can be purchased from any domain name vendor; for example, you can purchase a name from VeriSign by going their website:

<http://www.verisign.com>

Follow the company's website and follow their instructions purchasing the name.

- If you are using RADIUS or credit card page sets, you must install an SSL certificate and configure the page sets for SSL to prevent the unauthorized interception of confidential data.
- Until you install your SSL certificate, select the “Clear” version of the RADIUS or credit card page set and then change your page set to the SSL page set. For example, select RADIUSClear until the certificate is installed, then after installing the certificate, change the page set to RADIUS. If you do not install the certificate first, the Start page will not display.
- BBSM requires the use of 128-bit SSL encryption.

Generating a Certificate Signing Request

Follow this procedure to generate a Certificate Signing Request for your web server certificate. The BBSM administrator should perform this procedure.



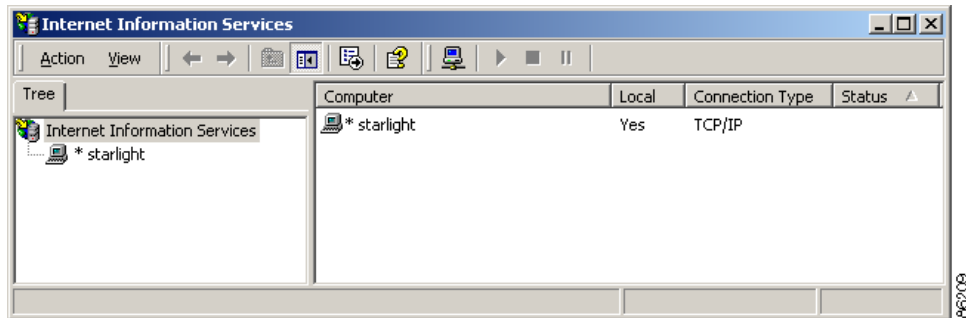
Note

BBSM servers use Microsoft IIS 5.0.

Step 1

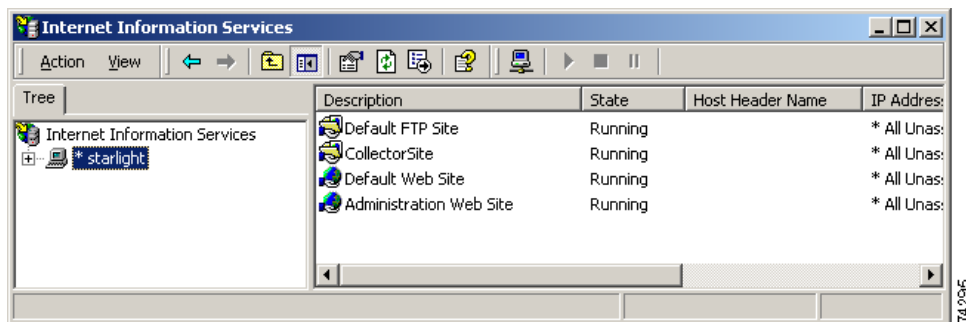
From the BBSM desktop, choose **Start > Programs > Administrative Tools > Internet Services Manager**. The Internet Information Services window appears. (See [Figure A-1](#).)

Figure A-1 Internet Information Services Window



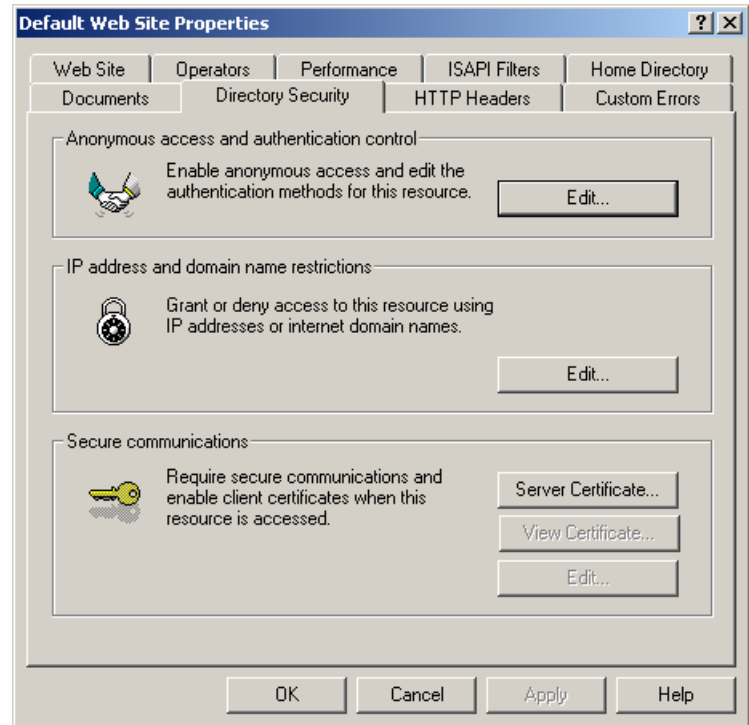
- Step 2 In the left pane, click the server name. (The example server name is “starlight” in Figure A-2.) The server folders appear in the right pane.

Figure A-2 Internet Information Services Description Window



- Step 3 In the right pane, right-click **Default Web Site**, and select **Properties**. The Default Web Site Properties dialog box appears. (See Figure A-3.)

Figure A-3 Default Web Site Properties Dialog Box



Step 4 Click the **Directory Security** tab.

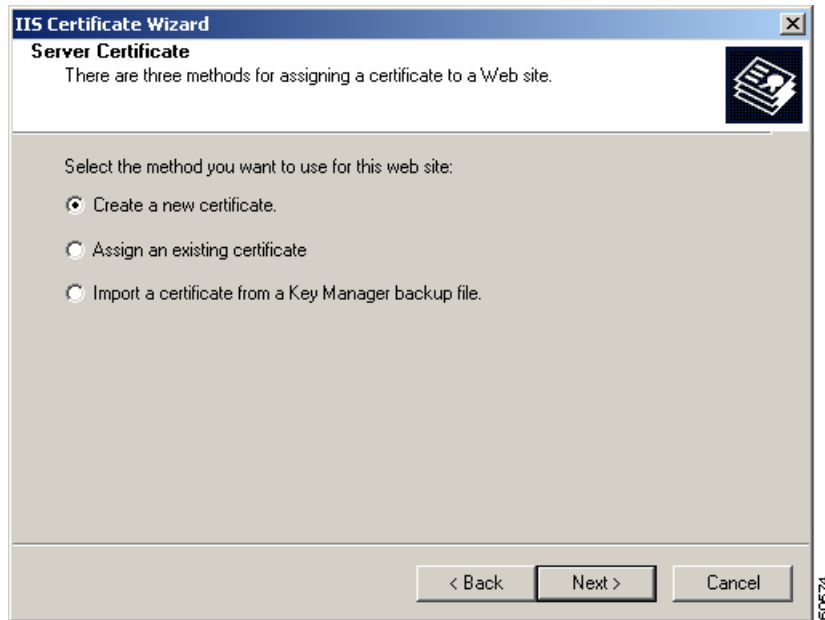
Step 5 In the Secure communications section, click **Server Certificate**. The Welcome to the Web Server Certificate Wizard dialog box appears. (See Figure A-4.)

Figure A-4 Welcome to the Web Server Certificate Wizard Dialog Box



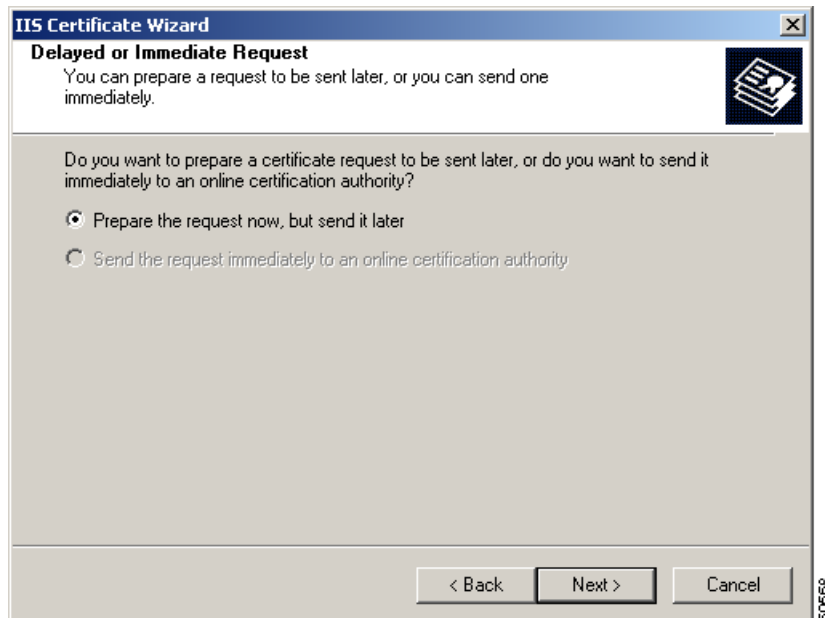
Step 6 Click **Next**. The Server Certificate dialog box appears. (See [Figure A-5](#).)

Figure A-5 Server Certificate Dialog Box



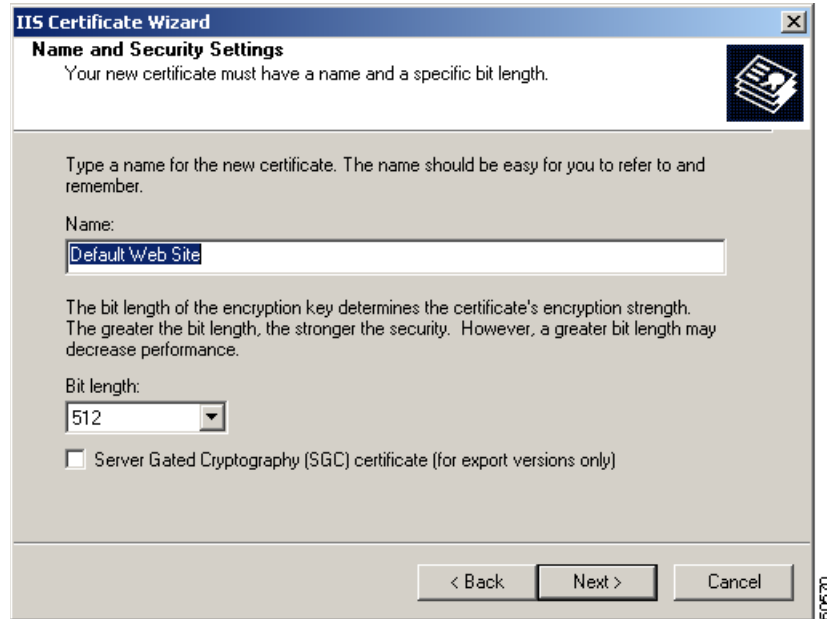
Step 7 Verify that the **Create a new certificate** radio button is selected. If it is not, select it. Then click **Next**. The Delayed or Immediate Request dialog box appears. (See [Figure A-6](#).)

Figure A-6 Delayed or Immediate Request Dialog Box



- Step 8** Verify that the **Prepare the request now, but send it later** radio button is selected. If it is not, select it, and then click **Next**. The Name and Security Settings dialog box appears. (See [Figure A-7](#).)

Figure A-7 Name and Security Settings Dialog Box



- Step 9** Type a descriptive name for the new certificate, such as “SDPacificPlazaBBSM.”
- Step 10** In the Bit length drop-down menu, keep the default setting, and then click **Next**. The Organization Information dialog box appears. (See [Figure A-8](#).)

Figure A-8 Organization Information Dialog Box

IIS Certificate Wizard

Organization Information
Your certificate must include information about your organization that distinguishes it from other organizations.

Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

Organization:
Your Organization Name

Organizational unit:
Your Organizational Unit Name

< Back Next > Cancel

60671

- Step 11** In the Organization and Organizational unit fields, enter your organization and organizational unit names. (You cannot use commas in these fields.)
- Step 12** Click **Next**. The Your Site's Common Name dialog box appears. (See [Figure A-9](#).)

Figure A-9 Your Site's Common Name Dialog Box

IIS Certificate Wizard

Your Site's Common Name
Your Web site's common name is its fully qualified domain name.

Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.

If the common name changes, you will need to obtain a new certificate.

Common name:
Full domain name shown on the Server page in WEBconfig

< Back Next > Cancel

60676

- Step 13** In the Common name field, enter your website's common name, and then click **Next**. The Geographical Information dialog box appears. (See [Figure A-10](#).) This is the name that is entered on the Security/SSL page in WEBconfig. Refer to the “[Configuring Security/SSL](#)” section on page 3-42, Step 3.



Note Do not include “www” when you enter your website's common name. For example, enter **cisco.com**, not www.cisco.com. If the common name changes, you must obtain a new certificate. If you are using SSL page sets, go to the Security/SSL web page in WEBconfig, check the **Enable Domain Name for SSL Page Sets** check box, enter the same common name in the Full Domain Name field, and click **Save**.

Figure A-10 Geographical Information Dialog Box

IIS Certificate Wizard

Geographical Information

The certification authority requires the following geographical information.

Country/Region:
US (United States)

State/province:
Your State/Province

City/locality:
Your City/locality

State/province and City/locality must be complete, official names and may not contain abbreviations.

< Back Next > Cancel

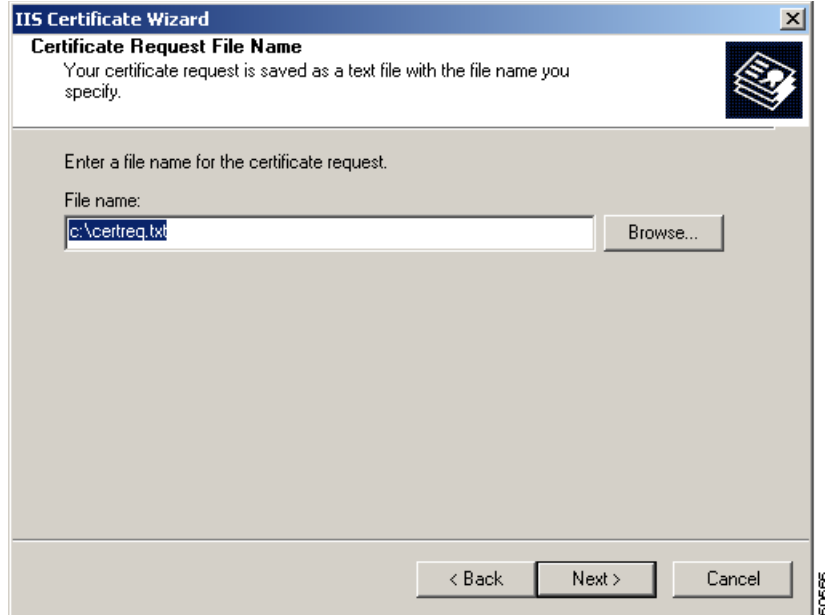
60669

- Step 14** Enter the requested information in the geographical fields, and click **Next**. The Certificate Request File Name dialog box appears. (See [Figure A-11](#).)



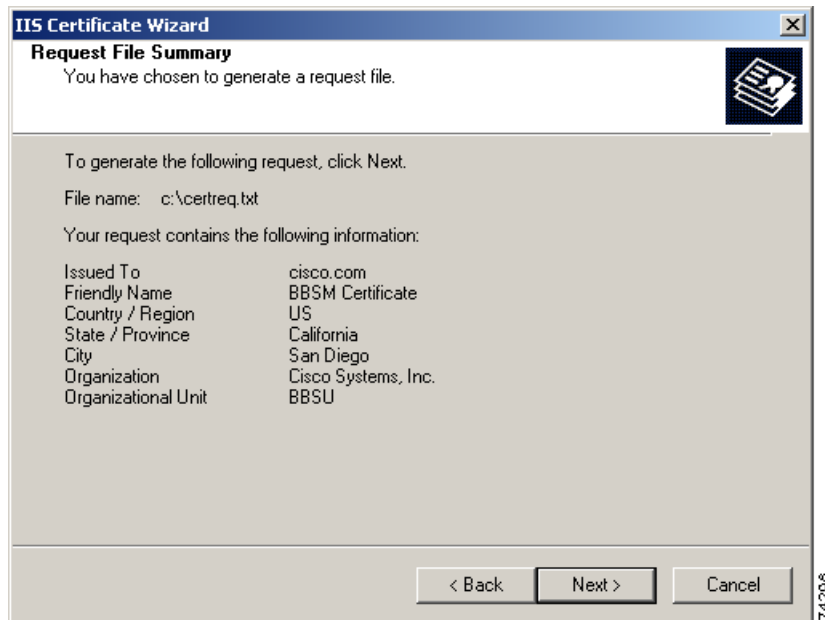
Note In the State/province field, you must use the full name, not the two-letter abbreviation; for example, California, not CA. You cannot use commas in any of these fields.

Figure A-11 Certificate Request File Name Dialog Box



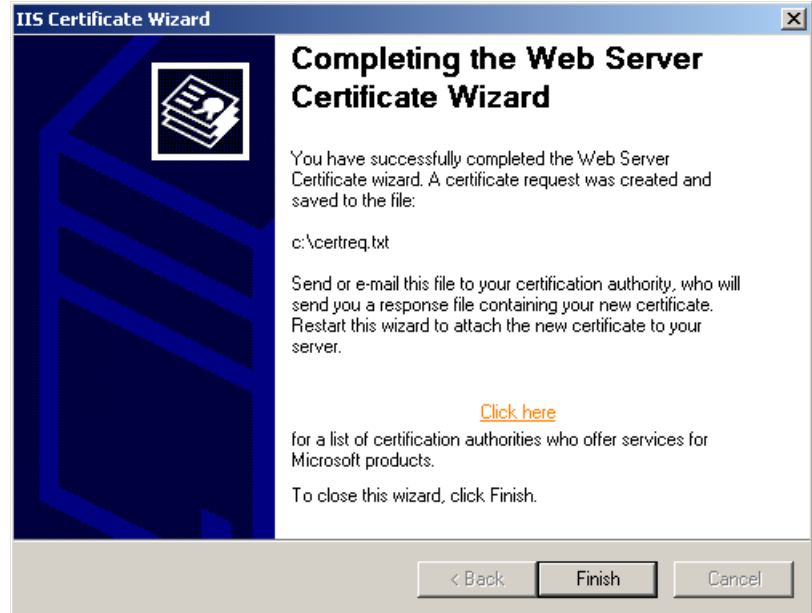
- Step 15** Use the default file name, or enter a new name for the certificate request. (Your certificate request is saved as a text file with the file name that you specify. We recommend that you make a backup copy of this file and store it in a secure location.)
- Step 16** Click **Next**. The Request File Summary dialog box appears. (See [Figure A-12](#).)

Figure A-12 Request File Summary Dialog Box



- Step 17** Verify that the information is correct, and click **Next**. The Completing the Web Server Certificate Wizard dialog box appears. (See [Figure A-13](#).)

Figure A-13 Completing the Web Server Certificate Wizard Dialog Box



- Step 18** To close the dialog box, click **Finish**.
- Step 19** To close the Default Web Site Properties dialog box, click **OK**.
- Step 20** Close the Internet Information Services window.

You have now generated a Certificate Signing Request. Continue with the following sections to purchase a certificate and install it on the BBSM server.

Purchasing a Secure Server ID from a Certificate Authority

After generating the Certificate Signing Request on BBSM, you must purchase a Secure Server Digital ID (certificate) from a certificate authority (CA). This authenticates your website and enables the SSL encryption.

- Step 1** Purchase a certificate from a CA; for example, you can purchase the certificate from VeriSign on their website:
- <http://www.verisign.com>
- Follow the company's instructions for purchasing the certificate. (BBSM requires 128-bit encryption.)
- Step 2** To verify that your organization's legitimacy and registration with the proper government authorities, you must provide the CA with your company's Dun & Bradstreet DUNS number. If you do not have a DUNS number, contact Dun & Bradstreet.
- Step 3** At some point during enrollment, you will be asked to use a text editor, such as Windows notepad, to open the CSR text file (c:\certreq.txt) that you created in the previous section.
- Step 4** When asked, copy and paste the CSR into the appropriate text area of the CA's online enrollment form. A CSR looks like this:

```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBCTCBtAIBADBPMQswCQYDVQQGEwJVUzEQMA4GA1UECBMRmxvcmlkYTEYMBYG
A1UEChMPRXllcyBvbiBUaGUgV2ViMRQwEgYDVQQDFAt3d3cuZXR3Lm5ldDBcMA0G
CSqGSIB3DQEBAQUAA0sAMEgCQQCeojtjnHqg0GTxp+XZ56RaSe1iZWpumXjU6Sx7
v1FdXzsY1oLOQa090Jtnu1WsQRHh0yDS+45oncjKm1zCG/IZAgMBAAGgADANBgkq
hkiG9w0BAQQFAANBAFBj9g+NiUh8YWPPrFGntgf4miUd/wqUshptjJy4PjdsD3ugy
5avvuh3G//PpGh2aYXIjHpJXTUBQyzxSEIINYtc=
-----END NEW CERTIFICATE REQUEST-----

```

- Step 5** Complete the rest of the online application, making sure that the information you enter is correct.
-

Installing the Granted Certificate

After submitting your completed application, your domain's Technical and Organizational Contacts will receive an e-mail message confirming enrollment within a few hours of submitting the order. It usually takes at least 3 to 5 working days to issue your certificate.

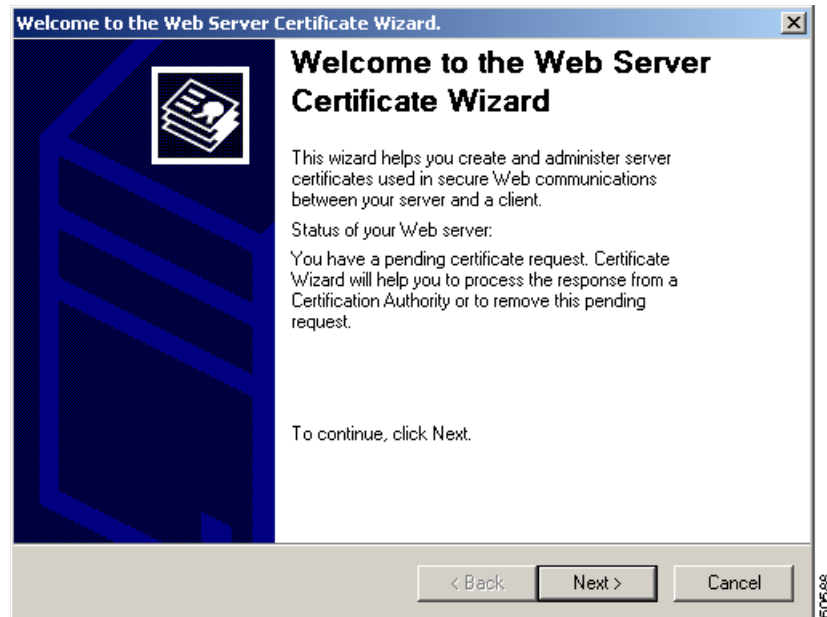


Note You cannot perform this procedure until you have received your certificate from the certificate authority and copied it onto your BBSM server.

Follow this procedure to install the granted certificate onto your BBSM server.

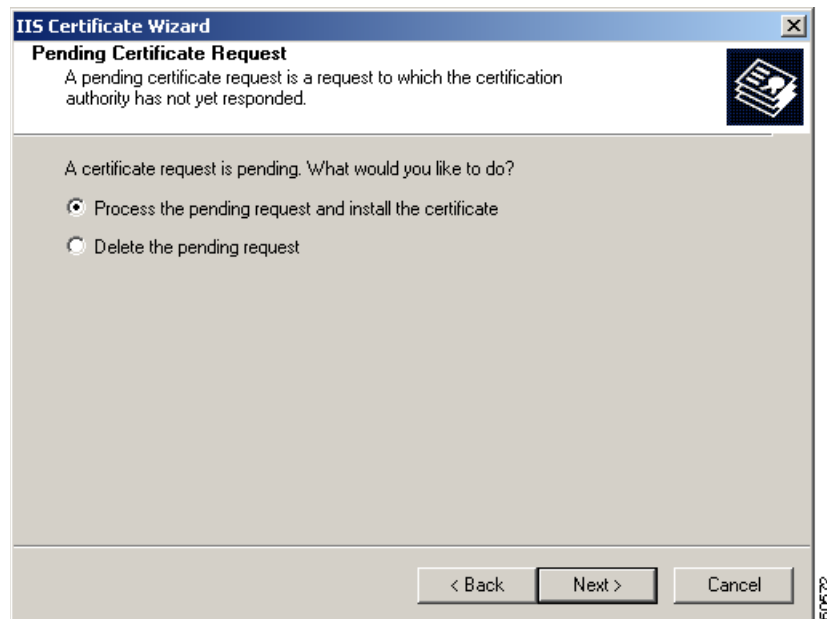
- Step 1** Choose **Start > Programs > Administrative Tools > Internet Services Manager**. The Internet Information Services (IIS) window appears.
- Step 2** In the tree in the left pane, click the server name.
- Step 3** In the right pane, right-click **Default Web Site**, and select **Properties**. The Default Web Site Properties dialog box appears.
- Step 4** Click the **Directory Security** tab. The Directory Security window appears.
- Step 5** In the Secure Communications pane, click **Server Certificate**. The Welcome to the Web Server Certificate Wizard window appears. (See [Figure A-14](#).)

Figure A-14 Welcome to the Web Server Certificate Wizard Dialog Box



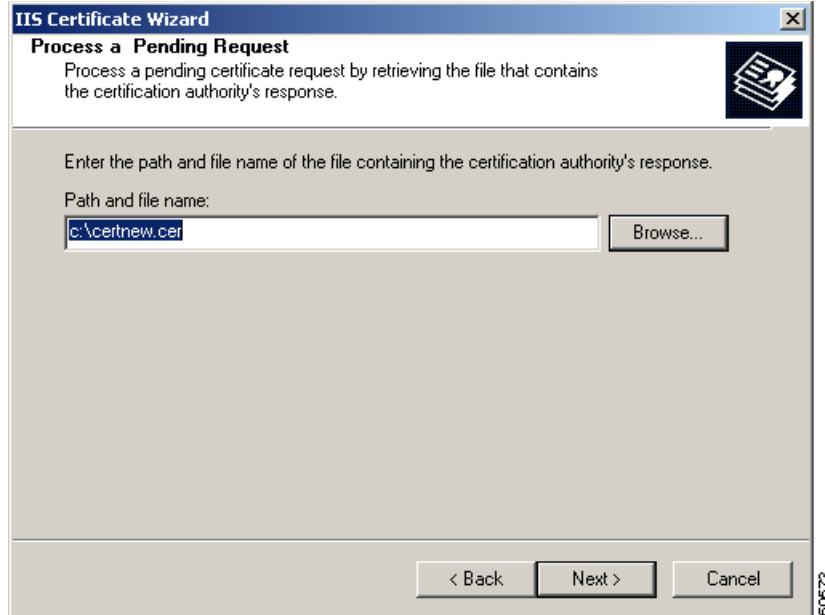
Step 6 Click **Next**. The Pending Certificate Request dialog box appears. (See [Figure A-15](#).)

Figure A-15 Pending Certificate Request Dialog Box



Step 7 Verify that the **Process the pending request and install the certificate** radio button is selected. If it is not, select it, and then click **Next**. The Process a Pending Request dialog box appears. (See [Figure A-16](#).)

Figure A-16 Process a Pending Request Dialog Box

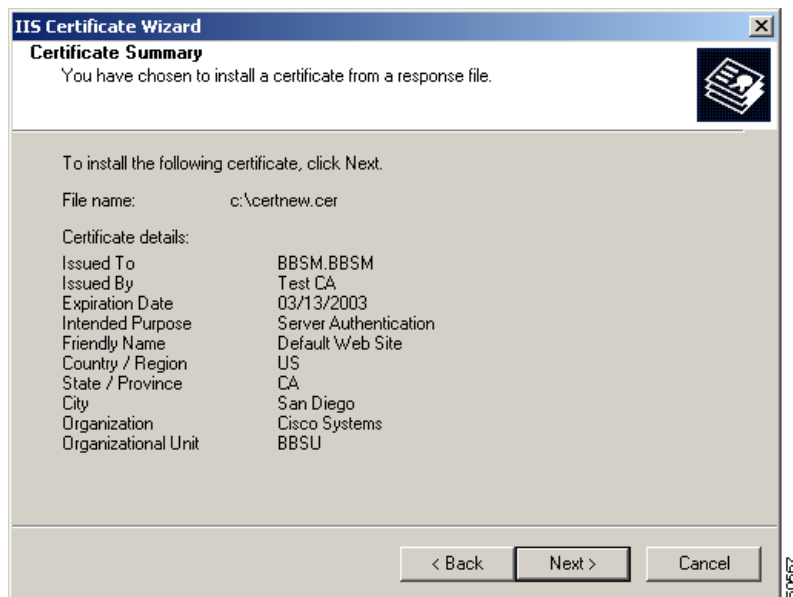


- Step 8** In the Path and file name field, browse to or type the path and file name of the signed certificate that you copied to the BBSM server at the beginning of this procedure. Then click **Next**. The Certificate Summary dialog box appears. (See [Figure A-17](#).)



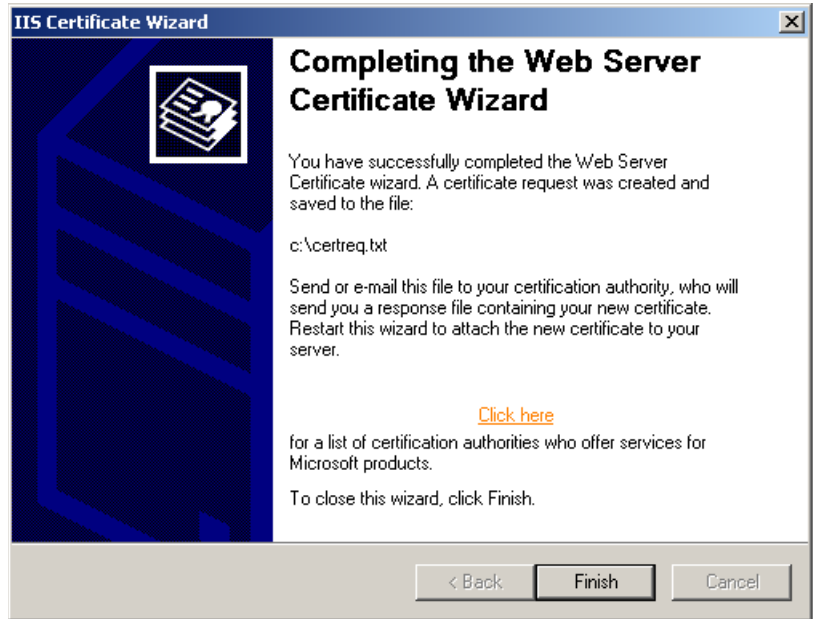
Note You cannot reinstall this certificate on a different machine.

Figure A-17 Certificate Summary Dialog Box



- Step 9** Click **Next**. The Completing the Web Server Certificate Wizard dialog box appears, indicating that the installation is complete. (See [Figure A-18](#).)

Figure A-18 Completing the Web Server Certificate Wizard Dialog Box



- Step 10** Click **Finish** to close the dialog box. You return to the Default Web Site Properties dialog box.
- Step 11** Click **OK** to close the Default Web Site Properties dialog box.
- Step 12** Click **OK** to close the Internet Information Services window.

You now have a server certificate installed. You may want to test the Web site to ensure that everything is working correctly. Be sure to use `https://` when you test connectivity to the site.

Backing Up the Server Certificate in IIS 5.0

If your BBSM server becomes damaged or needs to be rebuilt, you will need to reinstall a backup of your server certificate onto your BBSM server. The following procedures explain how to manage certificates, export them (create backups), and import them (reinstall them) at a later date, if necessary by using the Windows-based Microsoft Management Console (MMC) application *snap-ins*. (MMC is included in the Windows 2000 operating system and also runs in Windows 95, 98, and NT 4.0. It is part of the Microsoft Platform SDK and available for general use.)

MMC provides a GUI and programming framework in which *consoles*, which are collections of administrative tools, can be created, saved, and opened. It also provides an environment for running management applications and administrative tools called *snap-ins* whose primary purpose is to perform management tasks and allow administrators and other users to create custom management tools for later use or for sharing with other administrators and users.

Snap-ins can be created in various development environments such as Microsoft Visual Basic 6.0 and Microsoft Visual C++ 5.0 and 6.0. The MMC GUI allows snap-ins to integrate with the console, which has no management functionality. Snap-ins always reside in a console. They do not run by themselves.

Creating an MMC Snap-in for Managing Certificates

To perform the backup, you must first create a new MMC and add the Certificates snap-in, as follows. You can also add the snap-in to another MMC as long as MMC is opened in Author mode.

-
- Step 1 From the BBSM desktop, choose **Start > Run**. The Run window appears.
 - Step 2 Enter **mmc.exe**, and click **OK**. The Console1 and Console Root windows appear.
 - Step 3 From the Console1 window, click **Console**.
 - Step 4 Click **Add/Remove Snap-in**. The Add/Remove Snap-in window appears.
 - Step 5 Click **Add**. The Add Standalone window appears.
 - Step 6 Select **Certificates**, and click **Add**. The Certificates snap-in window appears.
 - Step 7 Click the **Computer account** radio button, and click **Next**. The Select Computer window appears.
 - Step 8 Verify that the **Local computer** radio button is selected, and click **Finish**. The Add Standalone Snap-in window appears.
 - Step 9 Click **Close**.
 - Step 10 From the Add/Remove Snap-in window, click **OK**. The Console1 and Console Root windows appear.



Note You have now added the Certificates snap-in, which will allow you to work with any certificates in your computer's certificate store.

- Step 11 Save this MMC for later use.
-

Continue to the next section.

Exporting a Certificate

Exporting a certificate is the same as creating a backup copy of the server certificate in case you need to reinstall it onto a damaged or rebuilt BBSM server at a later time. Now that you have added the Certificates snap-in, you can export the key pair that your Web server is using. To do so, follow this procedure.

-
- Step 1 From the Console Root window, open the Certificates (Local Computer) snap-in that you added in the last section, navigate to **Personal**, and then to **Certificates**.



Note You will see your Web server certificate denoted by the Common Name, which is found in the Subject field of the certificate.

- Step 2 Right-click on the server certificate, select **All Tasks**, and click **Export**.

- Step 3** After the wizard starts, click **Next**.
- Step 4** Choose to export the private key, and click **Next**.



Caution Do not select Require Strong Encryption. This option causes a password prompt every time an application attempts to access the private key and causes IIS to fail.

- Step 5** Choose the file format **Personal Information Exchange**, and click **Next**. This will create a PFX file.
- Step 6** Choose a password to protect the PFX file, and click **Next**.
- Step 7** Choose a file name that you want to save this as. Do not include an extension in your file name; the wizard adds it automatically.
- Step 8** Click **Next**.
- Step 9** Read the summary. Pay special attention to where the file is being saved to. If you are sure the information is correct, click **Finish**.

You now have a PFX file containing your server certificate and its corresponding private key. Be sure to move this file to a floppy disk and store it in a secure location.

Importing a Server Certificate in IIS 5.0

The following procedures explain how to reinstall a copy of the server certificate onto a BBSM server. To complete this operation, you must have the backup copy of the server certificate, which is contained in the PFX file that you created in the previous procedure.



Caution Do not use the following procedures unless you have to reinstall a backup copy of the server certificate onto a new or rebuilt BBSM server at a later time.

Creating MMC Snap-in for Managing Certificates

Use the same procedure that is described in the [“Creating an MMC Snap-in for Managing Certificates” section on page A-14](#). After you complete this procedure, continue to the next section.

Importing the Certificate

After you create a new MMC and add the Certificates snap-in, you can import the server certificate into your computer’s certificate store by using the following procedure.

- Step 1** From the Console Root window, open the Certificates (Local Computer) snap-in, navigate to **Personal**, and then to **Certificates**.



Note If no certificates are listed, it is because none were installed.

- Step 2 Right-click **Certificates**, (or **Personal**, if that option does not exist) and select **All Tasks**.
- Step 3 Click **Import**.
- Step 4 When the wizard starts, click **Next**.
- Step 5 Browse to the PFX file you created containing your server certificate, and click **Next**.
- Step 6 Enter the password you gave the PFX file when you created it.



Note Verify that the **Mark the key as exportable** option is selected if you want to be able to export the key pair again from this computer.

- Step 7 Click **Next**, and then choose the Certificate Store **Personal** to save the certificate to.
 - Step 8 Click **Next**. You should see a summary screen showing what the wizard is about to do. If this information is correct, click **Finish**.
-

You will now see the server certificate for your Web server in the list of Personal Certificates.

Enabling IIS 5.0 to Use the Imported Certificate

Now that you have the certificate backup imported into the certificate store, you can enable IIS 5.0 to use that certificate by following this procedure.

-
- Step 1 Choose **Start > Programs > Administrative Tools > Internet Services Manager**.
 - Step 2 Right-click **Default Web Site** (the website where you want to enable secure communications), and select **Properties**.
 - Step 3 Click the **Directory Security** tab.
 - Step 4 In the **Secure communications** section, click **Server Certificate**.
 - Step 5 When the Web Site Certificate Wizard starts, click **Next**.
 - Step 6 Choose the **Assign an existing certificate** option, and click **Next**.
 - Step 7 A screen showing the contents of your computer's personal certificate store appears. Select your web server certificate. Then click **Next**.
 - Step 8 A summary screen showing you the certificate details appears. Verify that this information is correct. Then click **Next**.
 - Step 9 Click **OK** to exit the wizard.

You now have an SSL-enabled Web server. Be sure to protect your PFX files from any unauthorized personnel.
