



Configuring Security and SSL

This chapter provides an overview of BBSM security, the procedure to install an SSL certificate when it is required, and the procedure to configure secured sockets layer (SSL). It also provides the procedure for changing the MSDE username and password and creating or changing the BBSD and Web API account username and password.

Refer to these sections:

- [Security Overview, page 16-1](#)
- [Installing an SSL Certificate, page 16-2](#)
- [Configuring Security, page 16-16](#)

Security Overview

Although BBSM is not a security product, you can increase the security of your system by using the security components described in this section.

BBSM can be made secure in the following ways:

- Microsoft server security—BBSM operates on the Windows 2000 server operating system and includes the basic Microsoft server security. The default BBSM configuration ships with settings configured to enhance its security. Microsoft Networking (File and Print Sharing and Local NetBIOS) is disabled on both the internal and external interfaces of the BBSM server, which means that from the client to the server, only a few ports on BBSM are open to a client connection.
- Password protected with permission levels—The BBSM management interface is password protected with three different user privilege levels.
- For security reasons, the BBSM internal interface does TCP filtering by port. Only the following ports are open on the internal interface:
 - 23: Telnet
 - 80: HTTP
 - 443: HTTPS (SSL traffic)
 - 9488: Used internally by BBSM
 - 8000, 8080, 8888: Common ports for nonstandard proxy

- Anti-virus protection—BBSM can also be protected by installing McAfee NetShield anti-virus software. For information on installing and configuring McAfee NetShield on BBSM, refer to this website:
<http://www.cisco.com/warp/public/135/bbsm-netshield.html>
- Firewalls—Cisco recommends that you configure the firewall features available on the router by using access control lists. For added security, you can protect BBSM by using Cisco PIX firewalls.
- Additional security features—BBSM can also be configured with additional static routing filters to provide security for broadcasts, and you can implement a secure encrypted remote control application for remote management. The router that is installed on the property should also be configured with broadcast thresholds.

The security of the inside LAN must be provided by configuring the in-building LAN infrastructure. This configuration prevents one room from seeing another room's packets, which eliminates attacks between clients and prevents malicious users from stealing authentication information when a session is being initiated. This configuration consists of horizontal protection that prevents clients from seeing other client traffic and vertical protection that prevents clients from seeing client traffic on another switch.

The configuration uses these features to provide protection:

- Port-to-port security (the *protected port* feature)— This feature prevents clients on two different ports from seeing each other without a Layer 3 device to intervene. It is supported on various Cisco Catalyst switches, such as the Catalyst 2900 XL, 2950, and 3550 switches. Because Cisco frequently adds new switches, this feature may also be supported on them.
- Private VLANs—On Cisco Catalyst 4000 and 6500 series switches, this feature provides Layer 2 isolation between ports within the same private VLAN.
- Publicly secure packet forwarding (PSPF)—On Cisco Aironet access points, this feature prevents client devices associated with the access point from communicating with other client devices on the wireless network and inadvertently sharing files. It provides Internet access to client devices without providing the other capabilities of a LAN.

The user's session is also made secure by configuring the page set for SSL, which provides RADIUS or credit card security from the end user's client to BBSM. When SSL is implemented, the end user's authentication is secure from end to end. Refer to the following section on installing an SSL certificate.

Installing an SSL Certificate

This section describes how to install an SSL certificate on the BBSM server. The certificate is needed when end users will be entering sensitive data on the Connect page, such as credit card numbers or RADIUS account information. (When SSL encryption is used, the end user connects to the Internet using *https* instead of *http*.)

If you are using SSL encryption, you must use page sets that provide the SSL encryption protocol. The other default BBSM page sets transmit data in clear text.

Before You Start

Before you install the SSL certificate, read the following:

- 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>

Go to the company's website and follow its instructions for 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, choose the *Clear* version of the RADIUS or credit card page set and then change your page set to the SSL page set. For example, choose RADIUSClear until the certificate is installed and then change the page set to RADIUS after installing the certificate. If you do not install the certificate first, the Start page will not display.
- BBSM requires the use of 128-bit SSL encryption.



Caution

Because page sets whose names end in *Clear* do not use SSL security, Cisco does not recommend using them in production to transmit data to the BBSM server. (See [Table 18-1](#).) The end user's browser transmits RADIUS and credit card information to BBSM in clear text. BBSM provides them for demonstration and testing situations in which installing a server certificate is not feasible.

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. (BBSM servers use Microsoft IIS 5.0.)

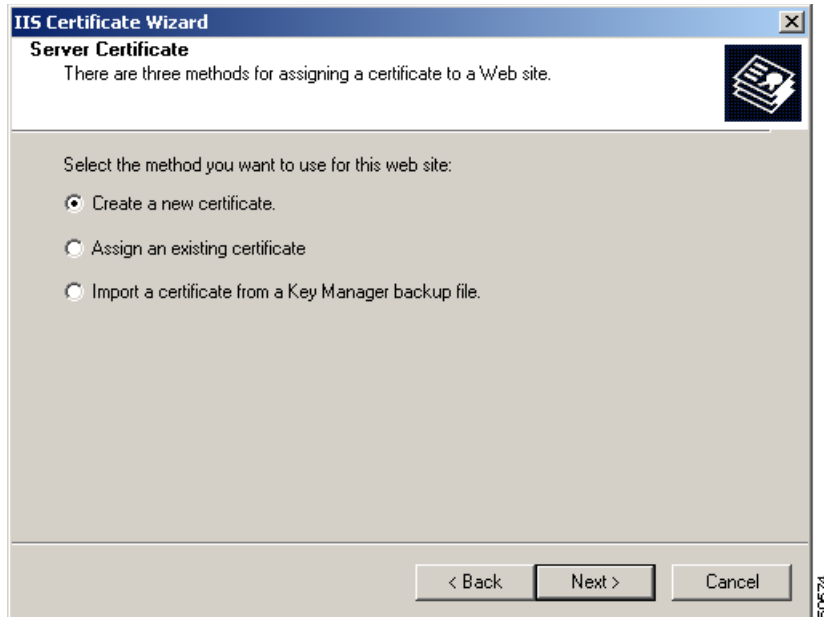
- Step 1** From the BBSM desktop, choose **Start > Programs > Administrative Tools > Internet Services Manager**. The Internet Information Services window appears.
- Step 2** In the left pane, click the server name. The server folders appear in the right pane.
- Step 3** In the right pane, right-click **Default Web Site** and select **Properties**. The Default Web Site Properties dialog box appears.
- Step 4** Click the **Directory Security** tab.
- Step 5** In the Secure communications section, click **Server Certificate**. The Welcome to the Web Server Certificate Wizard dialog box appears. (See [Figure 16-1](#).)

Figure 16-1 Welcome to the Web Server Certificate Wizard Dialog Box



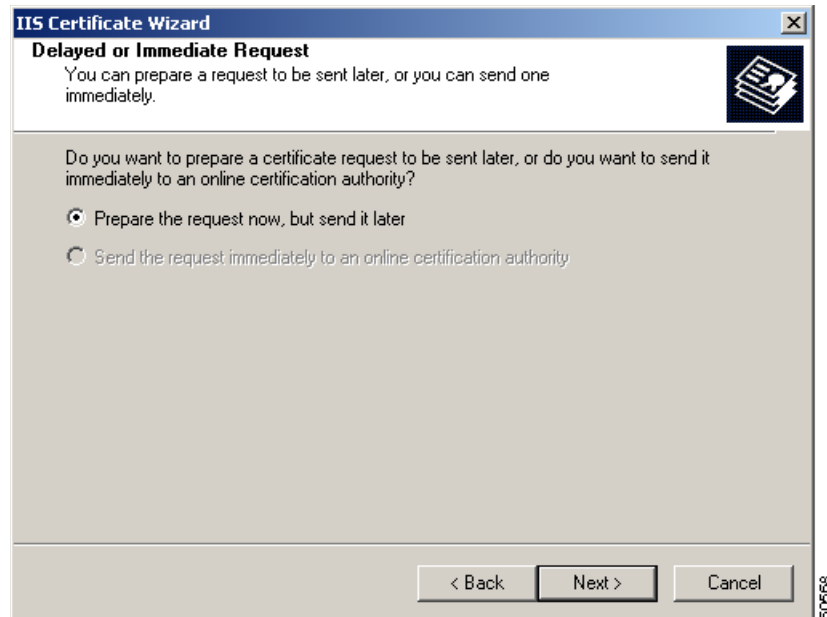
Step 6 Click **Next**. The Server Certificate dialog box appears. (See [Figure 16-2](#).)

Figure 16-2 Server Certificate Dialog Box



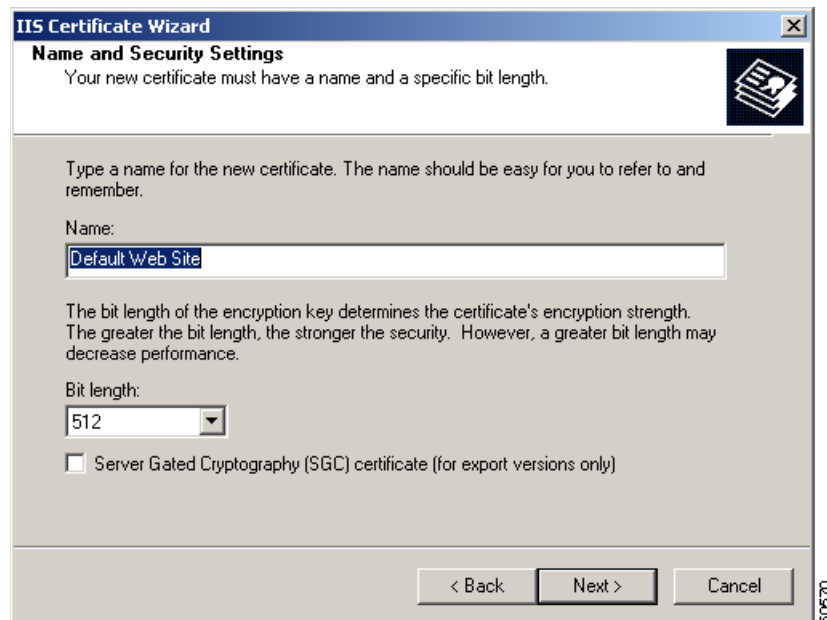
Step 7 Verify that the **Create a new certificate** radio button is selected. If it is not, click it and then **Next**. The Delayed or Immediate Request dialog box appears. (See [Figure 16-3](#).)

Figure 16-3 Delayed or Immediate Request Dialog Box

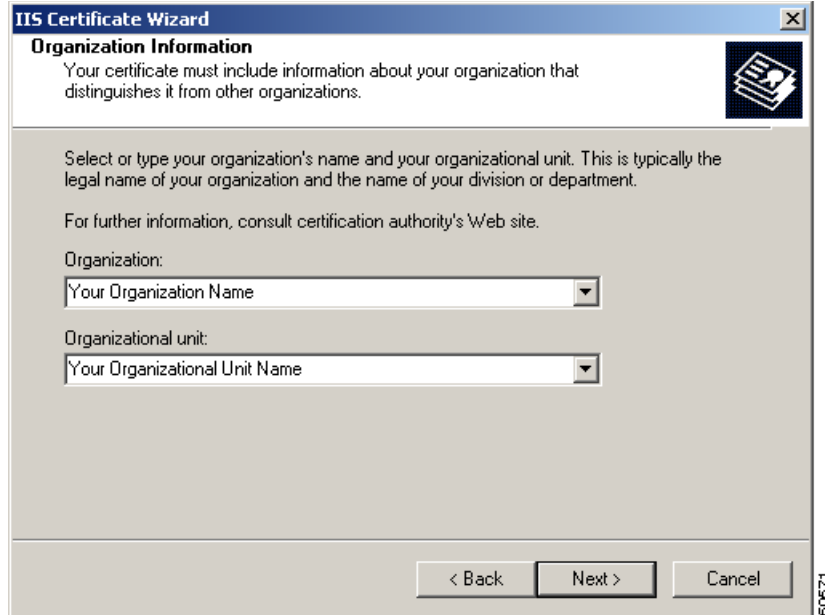


- Step 8** Verify that the **Prepare the request now, but send it later** radio button is selected. If it is not, click it, and then click **Next**. The Name and Security Settings dialog box appears. (See Figure 16-4.)

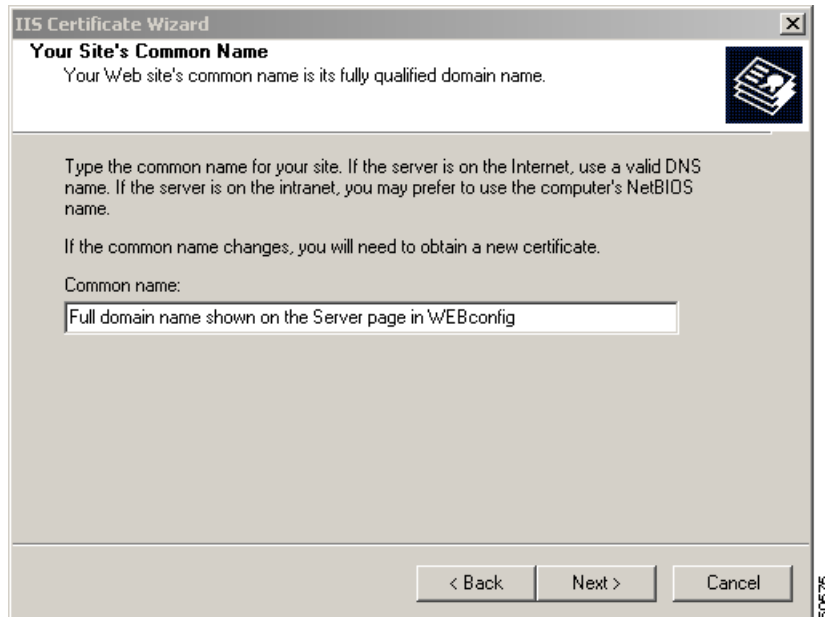
Figure 16-4 Name and Security Settings Dialog Box



- 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 click **Next**. The Organization Information dialog box appears. (See Figure 16-5.)

Figure 16-5 Organization Information Dialog Box

- 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 16-6](#).)

Figure 16-6 Your Site's Common Name Dialog Box

- Step 13** In the Common name field, enter your website's common name and click **Next**. The Geographical Information dialog box appears. (See [Figure 16-7](#).) This is the name that is entered on the Security/SSL page in WEBconfig. Refer to [Step 3](#) of the “Configuring Security” section on page 16-16.



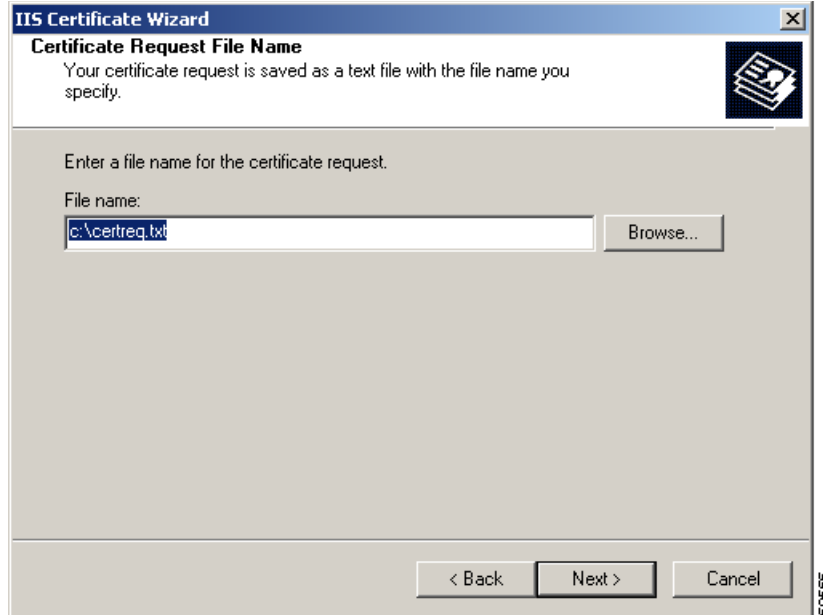
Note When you enter your website's common name, enter **cisco.com**, not www.cisco.com. If the common name changes, you must obtain a new certificate. If you are using SSL page sets, go to the Security/SSL web page in WEBconfig, check the **Enable Domain Name for SSL Page Sets** check box, enter the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

Figure 16-7 Geographical Information Dialog Box

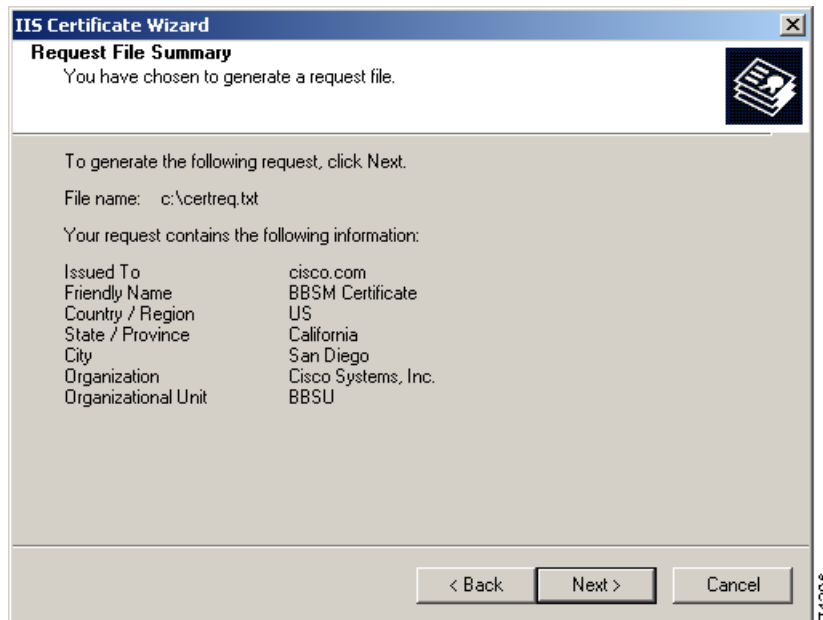
- Step 14** Enter the requested information in the geographical fields and click **Next**. The Certificate Request File Name dialog box appears. (See [Figure 16-8](#).)



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.

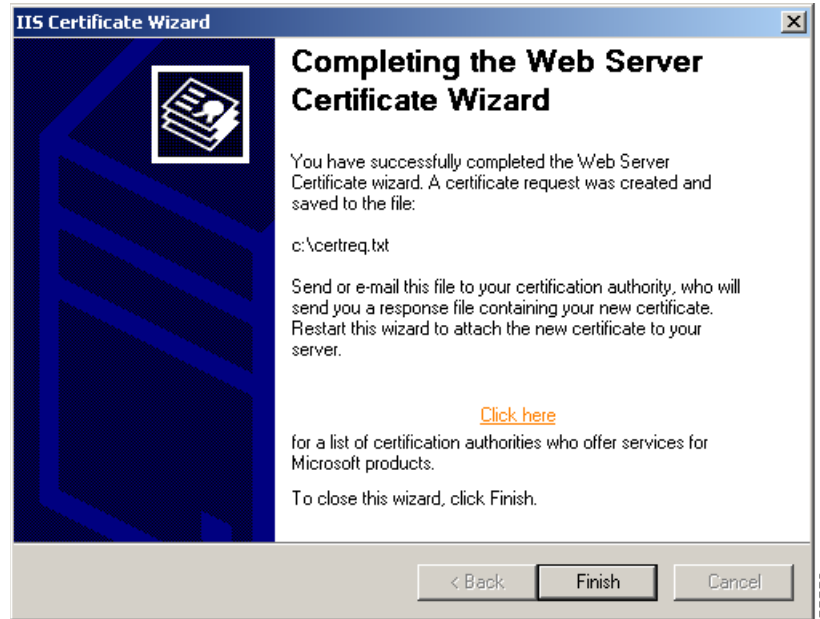
Figure 16-8 Certificate Request File Name Dialog Box

- 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. Cisco recommends 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 16-9](#).)

Figure 16-9 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 16-10](#).)

Figure 16-10 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 prompted, 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
A1UEChMPRXl1lcyBvb3V2ViMRQwEgYDVQQDFAt3d3cuZXR3Lm5ldDBcMA0G
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 you submit your completed application, your domain's Technical and Organizational Contacts will receive an email 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.

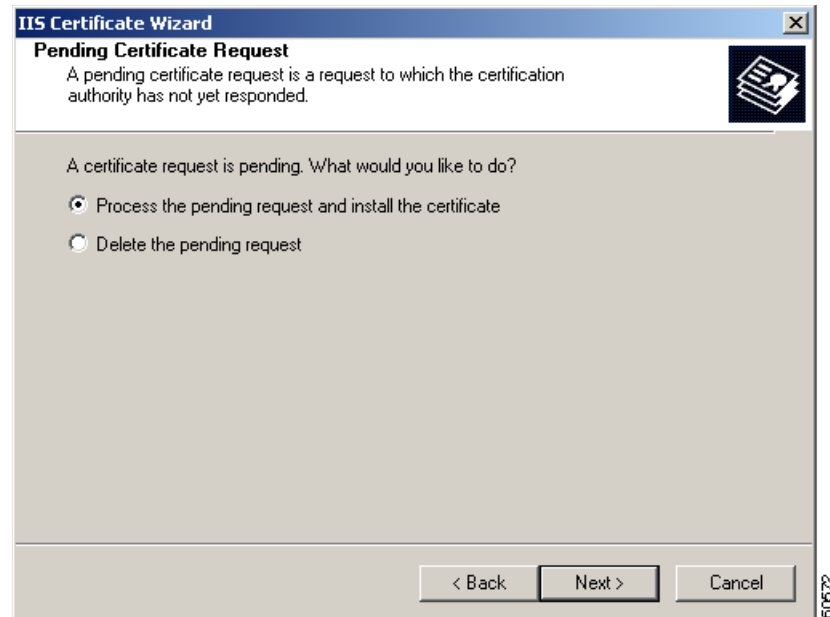


Note

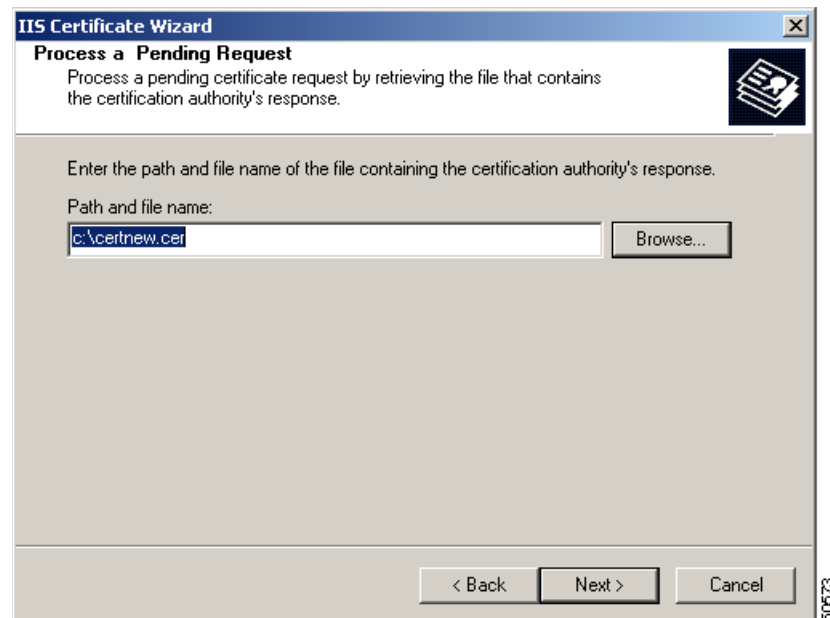
You cannot perform this procedure until you have received your certificate from the certificate authority and copied it onto your BBSM server.

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 16-1](#).)
- Step 6** Click **Next**. The Pending Certificate Request dialog box appears. (See [Figure 16-11](#).)

Figure 16-11 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 click **Next**. The Process a Pending Request dialog box appears. (See [Figure 16-12](#).)

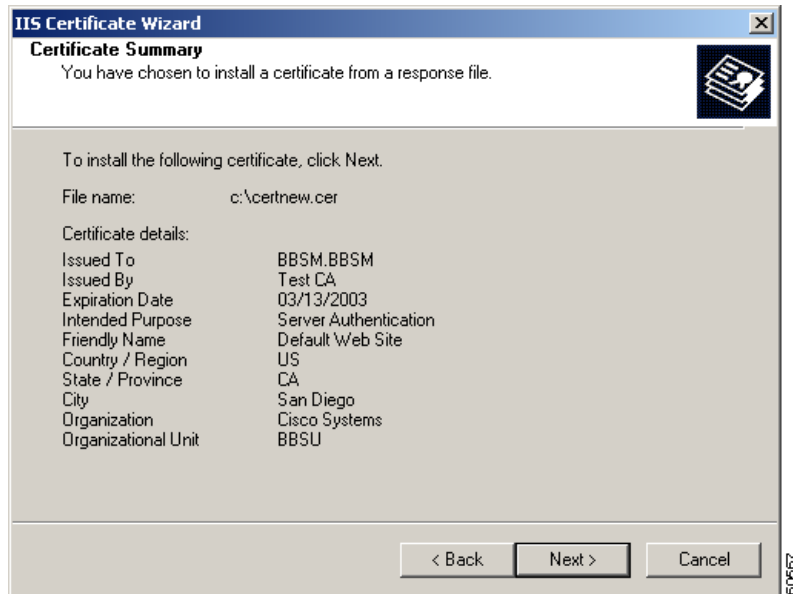
Figure 16-12 Process a Pending Request Dialog Box

- 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, and then click **Next**. The Certificate Summary dialog box appears. (See [Figure 16-13](#).)



Note You cannot reinstall this certificate on a different machine.

Figure 16-13 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 16-14](#).)

Figure 16-14 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** twice to close the Default Web Site Properties dialog box and the Internet Information Services window.
-

You now have a server certificate installed. You may want to test the website 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 (snap-ins). Their primary purpose is to perform management tasks and enable 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. Adding the snap-in enables you to work with any certificates in your computer's certificate store. 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** Choose **Certificates** and click **Add**. The Certificates snap-in window appears.
- Step 7** Click the **Computer account** radio button and then **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. Click **Close**.
- Step 9** From the Add/Remove Snap-in window, click **OK**. The Console1 and Console Root windows appear.
- Step 10** 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 later on a damaged or rebuilt BBSM server. Now that you have added the Certificates snap-in, follow the procedure below to export the key pair that your web server is using.

- 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 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 choose *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 creates a PFX file.
- Step 6** Choose a password to protect the PFX file and click **Next**.
- Step 7** Choose a file name for saving the file. Do not include an extension in your file name. The wizard adds the suffix automatically. Click **Next**.
- Step 8** Read the summary. Pay special attention to the location where the file is being saved. 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. Move this file to a floppy disk and store it in a secure location.

Importing a Server Certificate in IIS 5.0

This section describes how to reinstall a copy of the server certificate onto a BBSM server. To complete the process, 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.

To create an MMC snap-in to manage certificates, use the same procedure that is described in the “[Creating an MMC Snap-in for Managing Certificates](#)” section on page 16-13. After you create a new MMC and add the Certificates snap-in with this procedure, you can import the server certificate into your computer’s certificate store using the procedure below.

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



Note No certificates are listed when no certificates 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 window showing what the wizard is about to do. If this information is correct, click **Finish**.
-

The server certificate for your web server is now located in the list of Personal Certificates. 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 and click **Next**.

- Step 8** A summary window showing the certificate details appears. Verify that this information is correct, click **Next**, and then 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.

Configuring Security

You must enable the SSL security and specify the associated domain name by using the Security/SSL web page in WEBconfig. From this web page, you can also access these web pages:

- MSDE *sa* Account - Change Password Form
- BBSD Account - Change User Form
- Web API Account - Change User Form

Follow this procedure to configure SSL, change the MSDE password, and create (or later change) the BBSD and Web API usernames and passwords.

For additional information about passwords, refer to the “[Entering Security Passwords](#)” section on [page 3-2](#).

Step 1 From the Dashboard, click **WEBconfig**. The BBSM Server Settings web page appears.

Step 2 In the NavBar, click **Security/SSL**. The Security/SSL web page appears. (See [Figure 16-15](#).)

Figure 16-15 Security/SSL Web Page

The screenshot shows the Security/SSL configuration page in the Building Broadband Service Manager WEBconfig interface. The page has a blue sidebar on the left with a navigation menu. The main content area is white with a Cisco Systems logo and a title bar. The title bar includes 'Building Broadband Service Manager', 'WEBconfig', and 'Dashboard | Help | Logout'. The main content area is titled 'Security/SSL' and contains the following sections:

- Secure Sockets Layer (SSL)**: Includes a checkbox for 'Enable Domain Name for SSL Page Sets' (unchecked) and a text input field for 'Full Domain Name'.
- User Accounts and Passwords**: Lists three accounts with 'Change' or 'Create' buttons:
 - MSDE System Administrator (sa) Account: Change
 - BBSD Account: Create
 - Web API Account: Create

A yellow callout box on the right contains the following text:

Enable Domain Name for SSL Page Sets:
Check this box if you want to use SSL-enabled web pages.

SSL is recommended if you are using RADIUS or Credit Card policies, as it will protect sensitive user information.

Note:
You must purchase a fully qualified domain name for the BBSM server to use this option. The domain name **must match** the name on the installed SSL certificate.

See the *Cisco BBSM 5.2 User Guide* for details.

At the bottom of the page, there are 'Requery' and 'Save' buttons. The page number '86280' is visible in the bottom right corner.

Step 3 Enter data based on the information shown in [Table 16-1](#) and click **Save**.

Table 16-1 Security/SSL Web Page Options

Field	Description
Enable Domain Name for SSL Page Sets	<p>Check if you want to use SSL-enabled page sets.</p> <p>Note You must purchase a fully qualified domain name for the BBSM server to use SSL security. Refer to “Installing an SSL Certificate” section on page 16-2.</p>
Full Domain Name	<p>Enter the full domain name for the BBSM server that page sets will use to reach the BBSM server. This domain name must match the name on the SSL certificate that is installed on BBSM, such as <i>cisco.com</i>. This is the name entered in “Installing an SSL Certificate” section on page 16-2 (Step 13).</p>
MSDE System Administrator (sa), Change	<p>Click Change to access the MSDE ‘sa’ Password Form and change the password. (For additional information about BBSM passwords, refer to the “Entering Security Passwords” section on page 3-2.)</p>
BBSD Account, Create (or Change)	<p>Click Create to access the BBSD Account - Create User Form and create a BBSD username and password. Click Submit to enter the data. A confirmation dialog box appears.</p> <p>To ensure that only one BBSD account exists, the new account replaces the previous account so you are given the option to cancel. (These alerts appear only if the username is changed. If only the password is changed, the alert is not displayed.)</p> <p>The <i>Create</i> button on the Security/SSL web page now reads <i>Change</i>. When you click the Change button and the window pops up, the username is now filled in. (The username can be changed.)</p> <p>(For additional information about BBSM passwords, refer to the “Entering Security Passwords” section on page 3-2.)</p>
Web API Account, Create (or Change)	<p>Click Create to access the Web API Account - Create User Form and create a Web API username and password. Click Submit to enter the data. A confirmation dialog box appears.</p> <p>To ensure that only one Web API account exists, the new account replaces the previous account so you are given the option to cancel. (These alerts appear only if the username is changed. If only the password is changed, the alert is not displayed.)</p> <p>The <i>Create</i> button on the Security/SSL web page now reads <i>Change</i>. When you click the Change button and the window pops up, the username is now filled in. (The username can be changed.)</p> <p>(For additional information about BBSM passwords, refer to the “Entering Security Passwords” section on page 3-2.)</p>
Buttons	
Requery	Refreshes the web page (click before saving changes).
Save	Saves the changes made to the web page.

