



Publishing a Windows SharePoint Services Site on Windows Small Business Server 2003

Microsoft Corporation

Published: June 2006

Version: 2

Abstract

Your organization may require an efficient way for teams to share files, folders, and resources and to easily work together on documents with people who are not using the local computer network. By using Microsoft Windows SharePoint Services, which is included in Windows Small Business Server, teams can easily work together with external users. This document shows you how.

For the most up-to-date product documentation, see the [Microsoft Web site](http://go.microsoft.com/fwlink/?LinkId=3326) (<http://go.microsoft.com/fwlink/?LinkId=3326>).

Microsoft

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, SharePoint, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Contents

Publishing a Windows SharePoint Services Site on Windows Small Business Server 2003	7
Before You Begin.....	8
Prerequisites	8
Terms and Definitions	8
Process Steps.....	9
Step 1: Plan the Web Site	9
Step 2: Configure Your Network Adapter	14
Step 3: Create the Web Site	16
Step 4: Enable Encrypted Communication Between the Web Server and the Client Computer.....	17
Use a Web server certificate	17
Option 1: Assign a Web server certificate for the entire domain	18
Option 2: Assign a Web server certificate for a single Web server	19
Enable SSL on the Web site	24
Step 5: Convert Your Web Site to an Extranet, and Apply a Template.....	25
Step 6: Set Up User Accounts for External Users.....	26
Step 7: Enable Users to Access the Extranet.....	31
Step 8: Configure the Site to be Accessible from the Intranet.....	34
Related Links	36

Publishing a Windows SharePoint Services Site on Windows Small Business Server 2003

Note

This is Version 2 of this document. To download the latest updated version, visit the [Microsoft Web site](http://go.microsoft.com/fwlink/?LinkId=49932) (<http://go.microsoft.com/fwlink/?LinkId=49932>). The update might contain critical information that was not available when this document was published.

Note

The information in this document applies to the Microsoft® Windows® Small Business Server 2003 server software with Service Pack 1 or to Windows Small Business Server 2003 R2 (Windows SBS). This document does not include information about publishing a Windows SharePoint® Services site that external users can access by using Microsoft Internet Security and Acceleration (ISA) Server.

Note

The intended audience for this document is administrators of Windows SBS. The skill level required to complete the steps in this document assumes general knowledge of how to install, configure, and update Microsoft Office applications and Windows operating systems, and a basic understanding of the concepts of user accounts, groups, and shared folders in a client/server environment.

Your organization may require an efficient way for teams to share files, folders, and resources and to easily work together on documents with people who are not using the local computer network. By using Windows SharePoint Services, which is included in Windows SBS, teams can easily work together, sharing information with external users.

What is Windows SharePoint Services? It is a way for teams to work together. By using Windows SharePoint Services, teams can upload, save, and work together on documents over the Internet. They can communicate ideas and share information more easily. And they can create, author, and administer team Web sites to help organize their projects.

Before You Begin

Prerequisites

Before you begin the steps in this document, you must do the following:

- Complete Setup for Windows SBS, including the **Connect to the Internet** task in the To Do List.
- Register a domain name with an accredited registrar.

Terms and Definitions

The following key terms are associated with hosting a Windows SharePoint Services Web site:

A resource record A domain name system (DNS) resource record that maps server names with IP addresses.

Anonymous authentication An authentication mechanism that does not require user accounts and passwords. Anonymous authentication is used on the Internet to grant visitors restricted access to predefined public resources.

Anonymous user A user who accesses content on a Web site without providing a user login and password.

Authenticated user A user who has a user account on the server and who must provide a user name and password to access network resources.

CNAME resource record Canonical name resource record, also called a domain alias. A CNAME resource record points a new name to an already established A resource record.

External users Users who have access only to the Windows SharePoint Services Web site.

Fully qualified domain name (FQDN) A DNS name that uniquely identifies the computer on the network.

Host header names A server that is running Internet Information Services (IIS) can host multiple Web sites using a single IP address. Host header names identify the individual Web sites that are sharing a single IP address. For example, if you register two domains, wingtip toys.com and contoso.com, they each run on separate virtual servers and appear to be separate Web sites, but they share the same IP address.

Internal users Users who are on the local computer network.

Secure Sockets Layer (SSL) A protocol that supplies secure data communication through data encryption and decryption. It can be used for Web applications that require an encrypted link, such as e-commerce applications, or for controlling access to Web-based subscription services.

Web site A virtual server that resides on a Web server but that appears to the user as a separate Web server. Several Web sites can reside on one computer, each capable of running its own programs. Each Web site has its own fully qualified domain name, and each appears to the user as an individual Web site. Also called a virtual server.

Process Steps

To deploy a Windows SharePoint Services site (also called an extranet) that external users can access, complete the following steps:

1. Plan the Web site.
2. Configure your network adapter.
3. Create the Web site.
4. Enable encrypted communication between the Web server and the client computer.
5. Convert your Web site to an extranet, and apply a template.
6. Set up user accounts for external users.
7. Enable users to access the extranet.
8. Configure the site to be accessible from the intranet.

If you plan to publish multiple extranets on your server, you must complete all of these steps for each site.

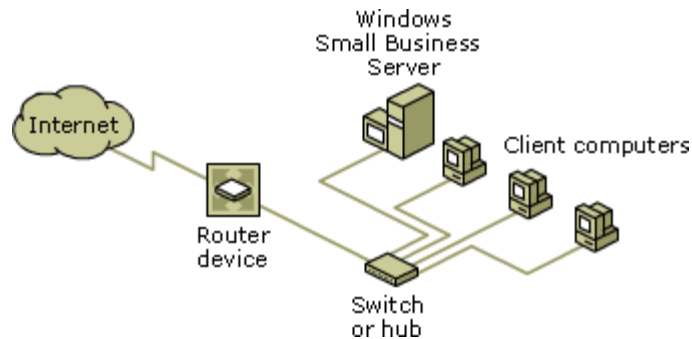
Step 1: Plan the Web Site

The first step is to plan the Web site. In this step, you gather information about your network, and you decide what to name your Web site, who is responsible for administering it, and who will have access to it. Table 1 at the end of this list can help you organize this information. You will use the information that you record in Table 1 to complete the steps in this document.

1. **Determine the type of Internet connection.** You may have one of the following types of Internet connections:

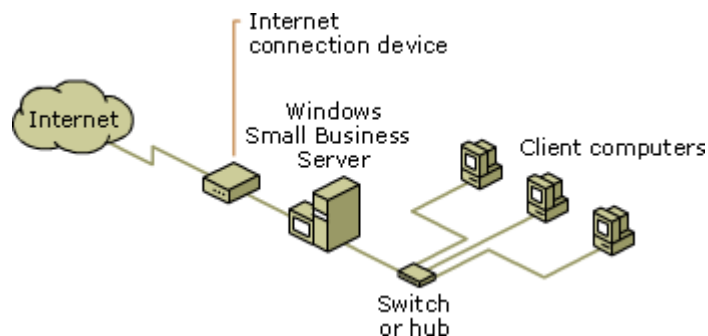
- **Router connection and one network adapter.** This is a broadband connection that requires a router, such as a dial-on-demand router or an ISDN router. Your Internet service provider (ISP) supplies an IP address for the router interface that connects to the Internet. In this configuration, the local router is the gateway and firewall to the Internet, as shown in Figure 1.

Figure 1. Router connection with one network adapter



- **Direct broadband connection.** This is a broadband connection type that requires an Internet connectivity device, such as a cable modem or a DSL modem. An IP address is not assigned to the network device. Your server must have two network adapters, as shown in Figure 2. One network adapter connects your server to the Internet, and the other one connects your server to the local network. In this configuration, your server is the gateway and firewall to the Internet.

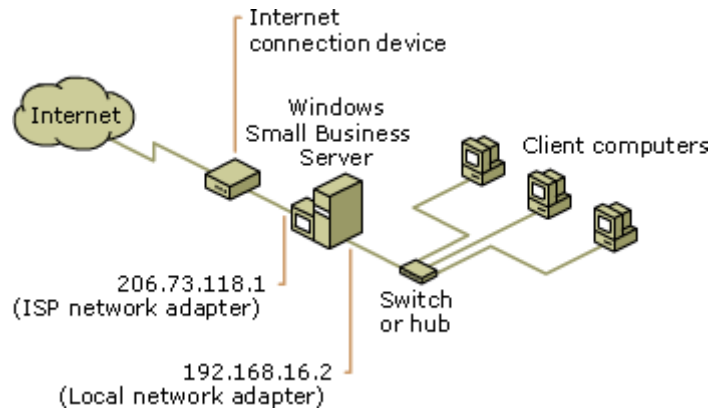
Figure 2. Direct broadband connection with two network adapters



2. **Determine security requirements.** Decide whether you want to help secure your Web site by using SSL to encrypt confidential information that is sent to and from the Web server. It is highly recommended that you use SSL.

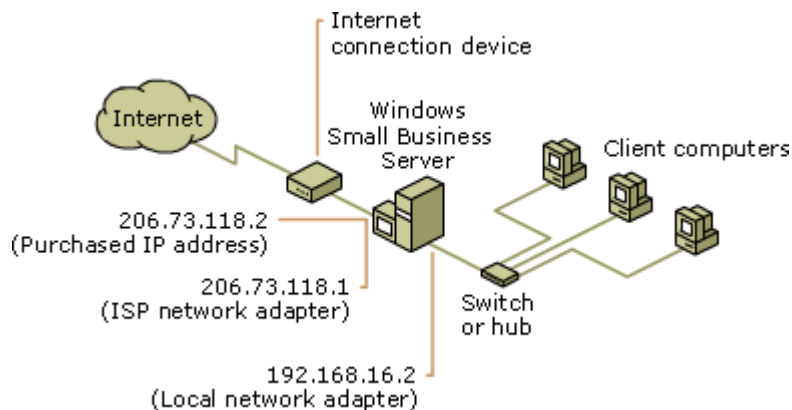
3. **Determine internal and external IP addresses.** Select one of the following four network configurations that represents the internet connection type and how you want your network set up to support your extranet. Use the drawing and description of your network setup to help you determine how many internal and external IP addresses you need to set up a Windows SharePoint Services site for external users.

- **Figure 3. Direct broadband connection, two network adapters, without SSL**



If you do not plan to use SSL and your server has two network adapters, you need one external IP address and one internal IP address. If your broadband connection type requires a static IP address and you do not have one, you must purchase one from an ISP, and you must ask the ISP to create an A resource record that points to that IP address.

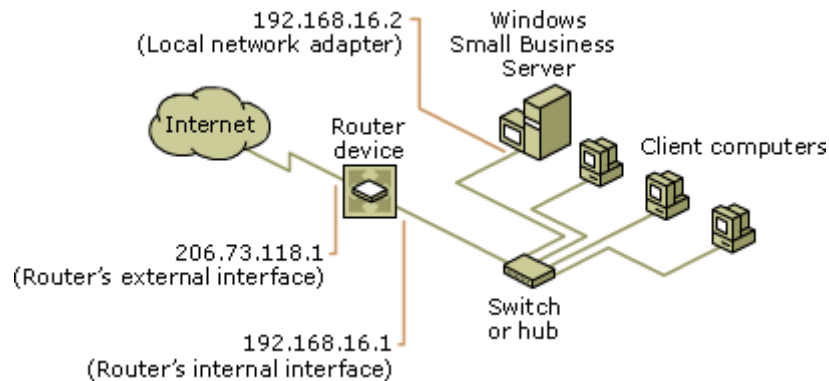
- **Figure 4. Direct broadband connection, two network adapters, with SSL**



If you plan to use SSL and your server has two network adapters, you need two external IP addresses and one internal IP address. If your broadband connection type requires static IP addresses and you do not have them, you must purchase

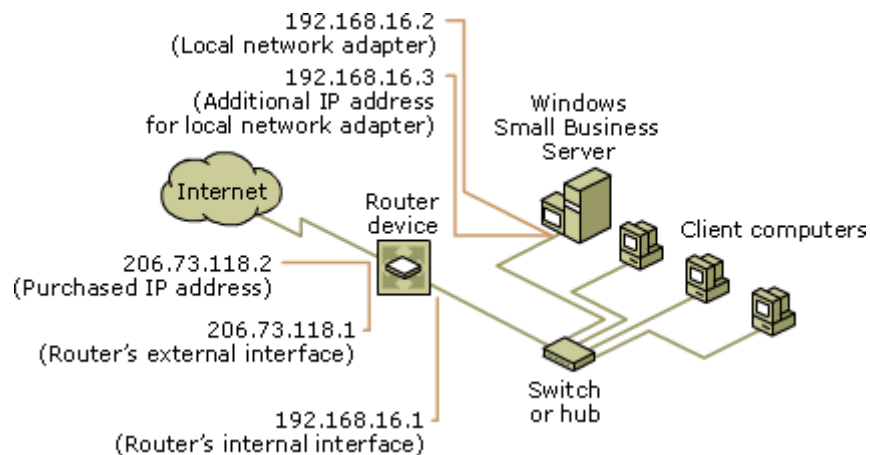
them from an ISP, and you must ask the ISP to create A resource records that point to the IP addresses.

- **Figure 5. Router connection, one network adapter, without SSL**



If you do not plan to use SSL and your network configuration includes one network adapter on the server plus a router, you need one external IP address and one internal IP address for the router, plus one internal IP address for the server. If your broadband connection type requires a static IP address and you do not have one, you must purchase one from an ISP, and you must ask the ISP to create an A resource record that points to the IP address.

- **Figure 6. Router connection, one network adapter with router, with SSL**



If you plan to use SSL and your network configuration includes one network adapter on the server plus a router, you need two external IP addresses and one internal IP address for the router, plus two internal IP addresses for the server. Ensure that the router supports multiple IP addresses on a single network

interface. If your broadband connection type requires static IP addresses and you do not have them, you must purchase two external IP addresses for the router from an ISP, and you must ask the ISP to create A resource records that point to the IP addresses.

Collect and record the IP addresses for the internal and external network cards on your server. You can use the **ipconfig** command to get the addresses that you currently have on your network.

If you plan to use SSL, ensure that the second IP address that you configure on a network adapter is in the same range as the first IP address (for example, 192.168.16.2 and 192.168.16.3). If the second IP address is on the local area network, ensure that it is excluded from the scope of IP addresses that are distributed by the DHCP server.

4. **Choose the host header names.** Choose the host header names that users will use to access the extranet either from the Internet (<http://www.wingtiptoys.com>) or from the intranet (<http://companyweb>).
5. **Choose the site owner.** The site owner is responsible for maintaining and managing the site. The site owner must be a member of either the Domain Admins group or the Domain Power Users group.
6. **Decide whether to allow anonymous access to the site.** Decide whether anonymous users can access the site, or whether only authenticated users can access it.
7. **Create a security group and decide how many user accounts to create.** Create a new security group. All external user accounts are members of this security group and can access the extranet, but they do not have privileges to access other resources on your network.

In addition, determine what external user accounts you need to set up. You can create a separate user account for each external person working on a project. Or you can set up one user account for several people to use to access the extranet. For example, if you are working on a project with another organization, instead of setting up separate user accounts for each member of the organization, you can create one user account for all of them to use to access the extranet.

Record the information that you collect in this step in Table 1. You will need this information when you complete the procedures later in this document.

Table 1. Information for Planning

Description	Information
IP address for external router interface provided by ISP (if needed)	(1) _____ . _____ . _____ . _____ (2) _____ . _____ . _____ . _____ (for SSL only)
IP address for internal router interface (if needed)	_____ . _____ . _____ . _____
IP address for external server adapter (if needed)	(1) _____ . _____ . _____ . _____ (2) _____ . _____ . _____ . _____ (for SSL only)
IP address for internal server adapter	1) _____ . _____ . _____ . _____ (2) _____ . _____ . _____ . _____ (for SSL plus router only)
Subnet mask provided by ISP	_____ . _____ . _____ . _____
Default gateway provided by ISP	_____ . _____ . _____ . _____
Host header name for the Web site when it is accessed from the Internet	_____
Host header name for the Web site when it is accessed from the intranet	_____
Use SSL? (strongly recommended)	Yes/No
Site owner	_____
Allow anonymous users to access the site?	Yes/No
Use an existing Web server certificate?	Yes/No

The network configuration that you selected in this step determines which steps you need to complete to publish your extranet for internal and external users.

Step 2: Configure Your Network Adapter

In this step, you configure your network adapter with static IP addresses. Use the information you collected in Table 1 to completed the following procedures.

▶ **To configure a network adapter with a static IP address**

1. Click **Start**, click **Server Management**, and then click **Internet and E-mail**.
2. In the details pane, click **Configure Network Connections**.
3. Under **LAN or High Speed Internet**, right-click the network adapter that you want to configure with a static IP address, and then click **Properties**.
4. In the **Network Connection Properties** dialog box, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
5. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Use the following IP Address**, and then type the IP address, subnet mask, and default gateway that are provided by your ISP.
6. Click **Advanced**. The **Advanced TCP/IP Settings** dialog box appears.
7. On the **IP Settings** tab, in the **IP address** field, click **Add**.
8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.
9. Click **OK** to save your new settings.

▶ **To configure a network adapter with a second static IP address**

1. Click **Start**, click **Server Management**, and then click **Internet and E-mail**.
2. In the details pane, click **Configure Network Connections**.
3. Under **LAN or High Speed Internet**, right-click the network adapter that you want to configure with a second static IP address, and then click **Properties**.
4. In the **Network Connection Properties** dialog box, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
5. Click **Advanced**. The **Advanced TCP/IP Settings** dialog box appears.
6. On the **IP Settings** tab, in the **IP address** field, click **Add**.
7. In the **TCP/IP Address** dialog box, type the second IP address and subnet mask that are provided by your ISP, and then click **OK**.

 **Note**

The subnet mask for both of the static IP addresses that are provided by your ISP must be the same.

8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** dialog box.
9. Click **OK** to save your new settings.

Configure your router to allow access to the new IP address

If you are using a router, ensure that the router supports multiple IP addresses and port forwarding. Configure the router to allow access to the Internet using the purchased IP address. For more information about how to configure your router, see the documentation that is included with the router.

Step 3: Create the Web Site

In this step, you create the Web site by using the Web Site Creation Wizard. The information about your IP address and port settings varies, depending on your network configuration.

▶ To create a Web site

1. Click **Start**, and then click **Server Management**.
2. In the console tree, double-click **Advanced Management**, double-click **Internet Information Services**, double-click the server name, and then click **Web Sites**.
3. Right-click **Web sites**, select **New**, and then click **Web Site**. The Web Site Creation Wizard appears.
4. On the **Welcome to the Web Site Creation Wizard** page, click **Next**.
5. On the **Web Site Description** page, type the name of the extranet that you want to host (for example, SharePoint extranet).
6. On the **IP Address and Port Settings** page, do the following:
 - a. In **Enter IP address to use for this Web site**, choose the IP address of the internal network adapter from the drop-down list (for example, 192.168.16.2, as shown in Figure 6).
 - b. In **TCP port this Web site should use (Default 80)**, type **80**.
 - c. In **Host header for this Web site (Default none)**, type a host header for the Web site (for example, extranet.wingtiptoys.com).
7. On the **Web Site Home Directory** page, create a folder for your Web site home directory. To create a folder for the Web site home directory, do the following:
 - a. Click **Browse**, and then navigate to the **Inetpub** folder (%SystemDrive%\Inetpub).
 - b. Click **Make New Folder**, type the name of the new folder (for example, **SharePoint Extranet**), and then click **OK**.

- c. Click **Next**.
8. On the **Web Site Access Permissions** page, select **Read** and **Run Scripts (such as ASP)**, and then click **Next**.
9. Click **Finish** to close the wizard.

You have now created the Web site. If you plan to use SSL, continue to Step 4. If you do not plan to use SSL, skip Step 4 and go to Step 5.

Step 4: Enable Encrypted Communication Between the Web Server and the Client Computer

You can help make your Web site more secure by using SSL to encrypt communication between the server that is hosting the Web site and the Web browser. Host headers do not function when you use SSL because IIS does not support the use of host headers with SSL.

Note

It is recommended that you enable SSL to help secure communications with the Web server if you intend to use your Web site to share business-critical information with your external users. However, you must complete additional setup steps to use SSL.

Note

To publish a Web site that does not use SSL, contact the registrar for your Internet domain name and ask the registrar to create a new name record that points to the external IP address of your server.

Complete this step only if you want to enable SSL on your server that is hosting the Web site. If you do not want to enable SSL, go to Step 5.

To help secure communications with the Web server, do the following:

1. Use a Web server certificate.
2. Enable SSL on the Web site.

Use a Web server certificate

To allow access to the Web site from the Internet, you must use a Web server certificate. The certificate is used to configure SSL to help secure communications between a Web

browser and your Web server. You can use either a Web server certificate that is automatically created when you run the Configure E-mail and Internet Connection Wizard (CEICW) or a certificate that is signed by a commercial certification authority (CA). You can purchase a certificate for the entire domain (for example, www.wingtiptoys.com) or for a single Web server.

Before you proceed with this step, make sure that you have run the CEICW at least once to set up the type of Internet connection and the firewall.

If you have a certificate for the entire domain, continue to "Option 1: Assign a Web server certificate for the entire domain." If you have a certificate for a single Web server, skip "Option 1" and go to "Option 2: Assign a Web server certificate to a single Web server."

Option 1: Assign a Web server certificate for the entire domain

Complete this step only if you have a certificate for your entire domain. Otherwise, go to "Option 2: Assign a Web server certificate to a single Web server."

If you have a certificate for your entire domain (for example www.wingtiptoys.com), assign this certificate to your Web site.

▶ To assign a Web server certificate for the entire domain to the Web site

1. Click **Start**, and then click **Server Management**.
2. In the console tree, double-click **Advanced Management**, double-click **Internet Information Services**, double-click the server name, and then double-click **Web Sites**.
3. Right-click the virtual server name (for example, SharePoint Extranet) that you want to add the Web server certificate to, and then click **Properties**.
4. On the **Directory Security** tab, under **Secure communications**, click **Server Certificate**.
5. In the Web Server Certificate Wizard, complete the following:
 - a. On the **Server Certificate** page, select **Assign an existing certificate**.
 - b. On the **Available Certificates** page, select the certificate (for example, www.wingtiptoys.com) for your entire domain.
6. Follow the instructions to complete the wizard.

Skip "Option 2" and go to the section "Enable SSL on the Web site," later in this document.

Option 2: Assign a Web server certificate for a single Web server

If you also use your existing certificate for the extranet, every time a user logs on to the Web site, the user receives a warning that the name of the certificate is invalid or does not match the name of the site.

To eliminate this message and improve the user's logon experience, you need to do the following:

- Export the certificate from the Default Web site.
- Create a new certificate with the name of the extranet.
- Add the new certificate to the extranet Web site.
- Import the original certificate to the Default Web site.
- Import the original certificate to the http://companyweb Web site.

Export the certificate from the Default Web site

In this procedure, you save the certificate that is currently assigned to the Default Web site by exporting it and saving it as a .pfx file, so that you can retrieve it later.

To export a certificate from the Default Web site

1. Click **Start**, and then click **Server Management**.
2. In the console tree, double-click **Advanced Management**, double-click **Internet Information Services**, double-click the server name, and then double-click **Web Sites**.
3. Right-click **Default Web Site**, and then click **Properties**.
4. On the **Directory Security** tab, under **Secure communications**, click **Server Certificate**.
5. In the Web Server Certificate Wizard, complete the following:
 - a. On the **Modify the Current Certificate Assignment** page, select **Export the current certificate to a .pfx file**.
 - b. On the **Export Certificate** page, type the path and the file name of the file that you want to use to export the certificate.
 - c. On the **Certificate Password** page, type and confirm the password for encrypting the exported .pfx file.

Obtain a new Web server certificate

Next, you obtain a new Web server certificate for the extranet. You can obtain a new certificate by using either of the following two methods:

- Rerun the Configure E-mail and Internet Connection Wizard (CEICW).
- Obtain a new certificate from a trusted certification authority.

Rerun the CEICW only if you want to create a self-signed Web server certificate for your site. Otherwise, follow the procedure to obtain a certificate from a trusted authority.

▶ To rerun the Configure E-mail and Internet Connection Wizard (CEICW)

1. Click **Start**, and then click **Server Management**.
2. In the console tree, click **Internet and E-mail**. In the details pane, click **Connect to the Internet**.
3. On the **Connection Type** page, click **Do not change connection type**.
4. On the **Firewall** page, click **Do not change firewall configuration**.
5. On the **Web Server Certificate** page, click **Create a new Web server certificate**, and then type the full Internet name (or FQDN name) of the extranet site.
6. On the **Internet E-mail** page, click **Do not change Internet e-mail configuration**.
7. Follow the instructions to complete the wizard.

You have now created a new, self-signed Web server certificate. Skip the following procedure and go to the section “Add the new certificate to the extranet Web site.”

Complete the following procedure to obtain a certificate from a trusted authority. To obtain a certificate from a trusted authority, you must create a certificate request by using the Web Server Certificate Wizard in Internet Information Services (IIS).

▶ To obtain a certificate from a trusted authority

1. Click **Start**, and then click **Server Management**.
2. In the console tree, double-click **Advanced Management**, double-click **Internet Information Services**, double-click the server name, and then double-click **Web Sites**.
3. Right-click the virtual server name (for example, SharePoint Extranet) that you want to add the new certificate to, and then click **Properties**.

4. On the **Directory Security** tab, under **Secure communications**, click **Server Certificate**.
5. On the **Server Certificate** page of the IIS Web Server Certificate Wizard, click **Create a new certificate**.
6. On the **Delayed or Immediate Request** page, prepare a request to be sent later or immediately, as needed.
7. On the **Name and Security Settings** page, in **Name**, type a name for the new certificate. Next, select the appropriate bit length based on your organization's requirement. Before submitting the certificate request, verify with the certification authority that it supports certificates of the corresponding encryption strength.
8. On the **Organization Information** page, in **Organizational Name**, type the legal name of your organization. In **Organizational unit**, type the name of your division or department. If your organization does not have a division, you can type the legal name of your organization.
9. On the **Your Site's Common Name** page, type the common name for your site, such as www.wingtiptoys.com, exactly as it appears to external users.
10. On the **Geographic Information** page, type the required information.
11. On the **Certificate Request File Name** page, type a file name.
12. On the **Request File Summary Page**, click **Next**.
13. Click **Finish**.
14. The certification authority will send you the certificate as well as instructions for installing it.

Add the new Web server certificate to the extranet Web site

In this step, you assign the Web server certificate to the extranet Web site.

▶ To add the new certificate to the extranet Web site

1. Click **Start**, and then click **Server Management**.
2. In the console tree, double-click **Advanced Management**, double-click **Internet Information Services**, double-click the server name, and then double-click **Web Sites**.
3. Right-click the virtual server name (for example, SharePoint Extranet) that you want to add the new certificate to, and then click **Properties**.
4. On the **Directory Security** tab, in **Secure communications**, click **Server**

Certificate.

5. In the Web Server Certificate Wizard, complete the following:
 - a. On the **Server Certificate** page, select the certificate that you created for the Web site.
 - b. On the **Available Certificates** page, select the Web server certificate that you created.
 - c. On the **SSL Port** page, type **443**.
 - d. Follow the instructions to complete the wizard.

Import the original certificate to the Default Web site

When you created a new certificate for the extranet, the certificate, like all new Web server certificates, was assigned to the Default Web site and the http://companyweb Web site. Therefore, you need to reassign the original certificate back to the Default Web site.

You can reassign the original certificate back to the Default Web site by completing the following two procedures.

▶ To remove the new certificate from the Default Web site

1. Click **Start**, and then click **Server Management**.
2. In the console tree, double-click **Advanced Management**, double-click **Internet Information Services**, double-click the server name, and then double-click **Web Sites**.
3. Right-click **Default Web Site**, and then click **Properties**.
4. On the **Directory Security** tab, in **Secure communications**, click **Server Certificate**.
5. In the Web Server Certificate Wizard, complete the following:
 - a. On the **Modify Current Certificate Assignment** page, select **Remove the current certificate**.
 - b. Follow the instructions to complete the wizard.

▶ To reassign the original certificate to the Default Web site

1. Click **Start**, and then click **Server Management**.
2. In the console tree, double-click **Advanced Management**, double-click **Internet Information Services**, double-click the server name, and then double-click **Web**

Sites.

3. Right-click **Default Web Site**, and then click **Properties**.
4. On the **Directory Security** tab, under **Secure communications**, click **Server Certificate**.
5. In the Web Server Certificate Wizard, complete the following:
 - a. On the **Server Certificate** page, click **Assign an existing certificate**.
 - b. On the **Available Certificates** page, click **Import a certificate from a .pfx file**.
 - c. On the **Import Certificate** page, type the path of the saved .pfx file.
 - d. On the **Import Certificate Password** page, type the password.
 - e. On the **SSL Port** page, type **443**.
 - f. Follow the instructions to complete the wizard.

Import the original certificate to the http://companyweb Web Site

When you created a new certificate for the Windows SharePoint Services site, the certificate also was assigned to the http://companyweb Web site. Therefore, you need to reassign the original certificate back to the company Web Site.

You can reassign the original certificate back to the http://companyweb Web site by completing the following two procedures.

▶ To remove the new certificate from the http://companyweb Web site

1. Click **Start**, and then click **Server Management**.
2. In the console tree, double-click **Advanced Management**, double-click **Internet Information Services**, double-click the server name, and then double-click **Web Sites**.
3. Right-click **http://companyweb Web Site**, and then click **Properties**.
4. On the **Directory Security** tab, in **Secure communications**, click **Server Certificate**.
5. In the Web Server Certificate Wizard, complete the following:
 - a. On the **Modify Current Certificate Assignment** page, select **Remove the current certificate**.
 - b. Follow the instructions to complete the wizard.

- ▶ **To reassign the original certificate to the http://companyweb Web site**
1. Click **Start**, and then click **Server Management**.
 2. In the console tree, double-click **Advanced Management**, double-click **Internet Information Services**, double-click the server name, and then double-click **Web Sites**.
 3. Right-click **http://companyweb Web Site**, and then click **Properties**.
 4. On the **Directory Security** tab, in **Secure communications**, click **Server Certificate**.
 5. In the **Web Server Certificate Wizard**, complete the following:
 - a. On the **Server Certificate** page, click **Assign an existing certificate**.
 - b. On the **Available Certificates** page, click **Import a certificate from a .pfx file**.
 - c. On the **Import Certificate** page, type the path of the saved .pfx file.
 - d. On the **Import Certificate Password** page, type the password.
 - e. On the **SSL Port** page, type **444**.
 6. Follow the instructions to complete the wizard.

Enable SSL on the Web site

After you assign a Web server certificate to your extranet site, you can help secure communication with the Web server by enabling SSL on the Web site.

Note

It is recommended that you enable SSL to help secure communications with the Web server if you intend to use your Web site to share business-critical information with your external users.

▶ **To enable SSL on the Web site**

1. Click **Start**, and then click **Server Management**.
2. In the console tree, double-click **Advanced Management**, double-click **Internet Information Services**, double-click the server name, and then double-click **Web Sites**.
3. Right-click the virtual server name (for example, SharePoint Extranet) that you want to configure, and then click **Properties**.

4. On the **Directory Security** tab, in **Secure communications**, click **Server Certificate**.
5. In the Web Server Certificate Wizard, complete the following:
 - a. On the **Server Certificate** page, click **Assign an existing certificate**.
 - b. On the **Available Certificates** page, click the Web server certificate that you want to use for your Web server.
6. Follow the instructions to complete the wizard.

Step 5: Convert Your Web Site to an Extranet, and Apply a Template

After you create the Web site, you need to convert it to an extranet. This process is called “extending the server,” and you complete it by using the Windows SharePoint Services Central Administration page.

After you convert your Web site, you need to apply a Windows SharePoint Services template to the site. Several templates are available, and the Team Site template is the best one for teams who want to work together on projects. This template creates a site that teams can use to create, organize, and share information quickly and easily. It includes a document library where the teams can share documents, and it includes basic lists such as Announcements, Events, Contacts, and Quick Links.

▶ To convert the Web site to a Windows SharePoint Services site, and to apply a template

1. Click **Start**, click **Administrative tools**, and then click **SharePoint Central Administration**.
2. On the **Central Administration** page, in **Virtual Server Configuration**, click **Extend or upgrade virtual server**.
3. On the **Virtual Server List** page, in the **Name** column, click the Web site name (for example, SharePoint Extranet) that you want to apply Windows SharePoint Services on.
4. On the **Extend Virtual Server** page, under **Provisioning Options**, click **Extend and create a content database**.
5. On the **Extend Virtual Server** page, do the following:
 - a. In the **Application Pool** section, select **Use an existing application pool**

and select **DefaultAppPool (NT AUTHORITY\NETWORK SERVICE)**.

- b. In the **Site Owner** section, type the **User name** and **E-mail** address of the person who will manage the site. This person must be a member of either the Domain Admins group or the Domain Power Users group.
 - c. Scroll to the end of the page, and then click **OK**.
6. On the **Virtual Server Successfully Extended** page, click the Web site address.
 7. Enter the administrator credentials to access the Web site.
 8. On the **Template Selection** page, in the **Template** list, click **Team Site**.

Step 6: Set Up User Accounts for External Users

External users are users who have access only to the Windows SharePoint Services Web site. In order to enable external users to upload documents, add new documents, or modify existing content on the Web site, you must set up user accounts for them on your local network.

To set up the user accounts, first create a security group, by using the Add a Security Group Wizard. Then use the security group to add users who have permission to access only the extranet and not to access any other resources on the network.

Specifically, to set up user accounts for external users, do the following:

1. Create a security group.
2. Create a new template for external user accounts .
3. Create user accounts that are based on the new template.
4. Set permissions for the external user accounts.
5. Enable the **Deny logon locally** Group Policy setting for the security group.
6. Delete folders of external users.

Use the information that you recorded in Step 1, Table 1, to complete this section.

To create a security group

1. Click **Start**, and then click **Server Management**.
2. In the console tree, click **Security Groups**, and then in the details pane click **Add a Security Group**.

3. From the taskpad in the details pane, click **Add a Security Group**.
4. In the Add a Security Group Wizard, do the following:
 - a. On the **Security Group Information** page, type the name (for example, Extranet Users) and description of the security group.
 - b. On the **Group Membership** page, click **Next**.
 - c. Click **Finish**.

After you create the security group, create a new template that you can use to add user accounts for external users.

▶ **To create a new template for external user accounts**

1. Click **Start**, and then click **Server Management**.
2. In the console tree, click **User Templates**.
3. On the details pane, click **Add a Template**. The **Add Template Wizard** starts.
4. On the **Welcome to the Add Template Wizard** page, click **Next**.
5. On the **Template Account Information** page, do the following:
 - a. Type a name for the new template in the **Template name box** (for example, Extranet Users Template).
 - b. Type a description of the user-account properties in the **Description** box, (for example, "has permission to access only the extranet site").
 - c. Clear the **This template should be the default option in the Add User Wizard** check box, and then click **Next**.
6. On the **Security Groups** page, double-click the security group that you created in the previous procedure, in order to add it to the **Users will be members of** column, and then click **Next**.
7. Do not add users to any distribution groups on the **Distribution Group** page. Click **Next**.
8. Do not choose to assign any roles on the **SharePoint Access** page. Click **Next**.
9. Do not type any information on the **Address Information** page. Click **Next**.
10. On the **Disk Quota** page, accept the default for both **Disk space limits in megabytes** and **Warning level in megabytes**, and then click **Next**.
11. Click **Finish**, and then click **Close** to close the Add Template Wizard.

▶ **To create user accounts that are based on the new template**

1. Click **Start**, and then click **Server Management**.
2. In the console tree, click **Users**.
3. On the details pane, click **Add Multiple Users**. The **Add User Wizard** starts.
4. On the **Welcome to the Add User Wizard** page, click **Next**.
5. On the **Template Selection** page, select the template that you created in the previous procedure, and then click **Next**.
6. On the **User Information** page, click **Add**.
7. On the **Specify the user information** page, do the following:
 - a. Type a user's first and last names in the appropriate text boxes. The **Logon name** and **E-mail alias** boxes are automatically filled in.
 - b. You may change the **Logon name** either by selecting a different naming standard from the drop-down list box or by typing a different logon name. The **E-mail alias** also changes.
 - c. Clear the **E-mail Alias** field.
 - d. Type a password for the user.
 - e. Click **OK**.
 - f. Click **Yes** in the **Add User Wizard** alert box.
8. Repeat steps 6 and 7 of this procedure to add additional external user accounts. When you have added all of the external user accounts, click **Next**.
9. On the **Set Up Client Computers** page, select **Do not set up computers at this time**, and click **Next**.
10. Click **Finish**.
11. Click **Close** after the Add User Wizard finishes processing the new user accounts.

◆ **Important**

You must perform the following procedure for each external user account that you created by using the new template.

▶ **To set permissions for the new user accounts**

1. In the details pane, select a new user account, and then click **Change User**

Properties from the task pad. The Properties dialog box for that user opens.

2. On the **Member of** tab, click **Add**.
3. If the security group that you created is not listed in the **Member of** text box, do the following:
 - a. Click **Advanced**, and then click **Find Now**.
 - b. Click the security group that you created for external users.
 - c. Click **OK**, and then click **OK** again.
4. On the **Member of** page, click the security group that you created, and then do the following:
 - a. Click **Set Primary Group**.
 - b. Click the **Domain Users** group, and then click **Remove**.
 - c. In the **Remove user from group** alert box, click **Yes**.
5. On the **Dial-in** tab, in the **Remote Access Permissions (Dial-in or VPN)** section, click **Deny access**.
6. On the **Terminal Services Profile** tab, select the **Deny this user permission to log on to any Terminal Server** check box.
7. If you want to set a date for this account to expire, on the **Account** tab, in the **Account expires** section, click **End of**, and then type a date when the account expires.
8. Click **OK** to apply your changes and to close the **Properties** dialog box.

You should allow the external users to access only the Windows SharePoint Services Web site. However, it is possible for the external users to use their accounts to log on to any computer on your local network. To help prevent this, you must enable the **Deny logon locally** Group Policy setting for the external users security group. This helps ensure that external users can access only the Windows SharePoint Services Web Site and cannot log on to computers on the local network.

 **To enable the Deny logon locally Group Policy setting for the security group**

1. Click **Start**, and then click **Server Management**.
2. In the console tree, double-click **Advanced Management**, double-click **Group Policy Management**, double-click **Forest: ForestName**, double-click **Domains**, double-click the domain name, and then double-click **My Business**.
3. Right-click **Computers**, and then click **Create and Link a GPO Here**.

4. In the **New GPO** dialog box, type a name for this new Group Policy object (for example, **Logon access denial**), and then click **OK**.
5. Double-click **Group Policy Objects** in the console tree (in **My Business**).
6. In the details pane, right-click the newly created Group Policy object (GPO), and then click **Edit**.
7. In Group Policy Object Editor, double-click **Computer Configuration**, double-click **Windows Settings**, double-click **Security Settings**, double-click **Local Policies**, and then double-click **User Rights Assignment**.
8. In the details pane, right-click **Deny logon locally**, and then click **Properties**.
9. In the **Deny logon locally** dialog box, click the check box to select **Define these policy settings**.
10. To add the security group that you created for the external users, do the following:
 - a. Click **Add User or Group**.
 - b. In the **Add User or Group** dialog box, click **Browse**.
 - c. In the **Select User, Computers or Groups** dialog box, click **Advanced**, and then click **Find Now**.
 - d. Select the security group that you created for the external users, click **OK**, and then click **OK** again.
 - e. In the **Add User or Group** dialog box, click **OK**.
11. In the **Deny log on locally** dialog box, click **OK**.
12. Close Group Policy Object Editor.
13. To update Group Policy, open the command prompt, type **gpupdate /force**, and then press ENTER. When you receive the message, "To check for errors in policy processing, review the event log," the update is complete.
14. Type **exit** to close the command prompt.

Shared folders are automatically created for each external user account. But because external users cannot access the shared folders, you can delete folders by using the following procedure.

▶ **To delete shared folders for external user accounts**

1. Open Windows Explorer, and then navigate to **Users Shared Folders**. The default location for Users Shared Folder is %SystemDrive%/Users Shared

Folders (for example C:/Users Shared Folders).

2. Open **Users Shared Folders**, click the shared folder for each external user account, and then delete it.
3. Close the **Users Shared Folders** window.

Step 7: Enable Users to Access the Extranet

The next step is to enable users to access the site. You can choose whether to allow anonymous users to access the site, anonymous and authenticated users, or only authenticated users. Anonymous users are users who do not have accounts on the server, and authenticated users are users who do have accounts on the server. Depending on how you want users to access your site, complete the following procedures as appropriate, using the information that you recorded in Table 1.

Important

Complete the following procedure only if you want to allow anonymous users to access the site.

To enable anonymous users to access to the site

1. Click **Start**, and then click **Server Management**.
2. In the console tree, double-click **Advanced Management**, double-click **Internet Information Services**, double-click the server name, and then double-click **Web Sites**.
3. Right-click the Web site name that you want to configure for anonymous users, and then click **Properties**.
4. On the **Directory Security** tab, in **Authentication and access control**, click **Edit**.
5. Select **Enable anonymous access**, and then click **OK**.
6. Click **OK** to save your changes and close the popup windows.

To enable authenticated users to upload, edit, or delete documents on the site, you must set permissions for them. You can set the permissions by using site groups. Windows SharePoint Services includes the following preconfigured site groups:

- **Reader:** Has read-only access to the Web site.
- **Contributor:** Can add content to the existing document libraries and lists.

- **Web Designer:** Can create lists and document libraries, and can customize pages on the Web site.
- **Administrator:** Has full control over the Web site.

A user can belong to more than one site group. By using site groups, you can assign different permissions to each user or group of users, or you can collectively assign the same permissions to all of the users by making them members of the same site group. For example, users who are members of the Contributor site group can add content to Windows SharePoint Services lists or to document libraries.

 **Note**

If you enable both anonymous and authenticated users to access your Web site, a **Sign In** button appears on the site, which users who have the appropriate permissions can click to contribute to the Web site.

If you enable only authenticated users to access the site, the users are prompted for credentials first.

 **To configure anonymous users to access the site**

1. Open Internet Explorer.
2. In the **Address** text box, type **https://InternalHeaderName** (for example, **https://extranet**), and then click **GO**. Make sure you include the "s" after "http," and verify that you are accessing the encrypted Windows SharePoint Services Web site.
3. Type your Web site administrator name and password to log on to the **Home** page of the Web site.
4. On the **Home** page, click **Site Settings**.
5. On the **Site Settings** page, in the **Administration** section, click **Go to Site Administration**.
6. On the **Top-level Site Administration** page, in the **Users and Permissions** section, click **Manage anonymous access**.
7. On the **Change Anonymous Access Settings: Team Web Site** page, in the **Anonymous Access** section, select **Entire Web site** to allow anonymous users to visit this Web site.
8. Click **OK** to accept the changes.

 **Important**

Complete the following procedure only if you want to allow all authenticated users to add content to the document libraries and lists.

 **To assign all authenticated users to the Contributor site group**

1. Open Internet Explorer.
2. In the **Address** text box, type **https://InternalHeaderName** (for example **https://extranet**), and then click **GO**. Make sure you include the "s" after "http," and verify that you are accessing the encrypted Windows SharePoint Services Web site.
3. Type your Web site administrator name and password to log on the **Home** page of the Web site.
4. On the **Home page**, click **Site Settings**.
5. On the **Site Settings** page, in the **Administration** section, click **Go to Site Administration**.
6. On the **Top-level Site Administration** page, in the **Users and Permissions** section, click **Manage anonymous access**.
7. On the **Change Anonymous Access Settings: Team Web Site** page, in the **All Authenticated Users** section, do the following:
 - a. Click **Yes** to allow all users, including anonymous users, to access the site.
 - b. In the **Assign these users to the following site group** list box, select **Contributor**, and then click **OK**.

 **Important**

Complete the following procedure only if you want to assign different permissions to authenticated users.

 **To assign authenticated users to different site groups**

1. Open Internet Explorer.
2. In the **Address** text box, type **https://InternalHeaderName** (for example **https://extranet**), and then click **GO**. Make sure you include the "s" after "http," and verify that you are accessing the encrypted Windows SharePoint Services Web site.
3. Type your Web site administrator name and password to log on the **Home** page

of the Web site.

4. On the **Home** page, click **Site Settings**.
5. On the **Site Settings** page, in the **Administration** section, click **Manage Users**.
6. On the **Manage Users** page, click **Add Users**.
7. On the **Add Users** page, do the following:
 - a. In **Step 1: Choose Users**, type the domain and user name of the users you want to add to the site group. Use the following syntax: *Domain\UserName* (for example **wingtip toys\NewUser**). Use a colon to separate multiple user names.
 - b. In **Step 2: Choose Site Groups**, select the site groups (Reader, Contributor, Web Designer, or Administrator) that you want these users to belong to. Users may belong to more than one site group. Click **Next**.
8. If you have enabled e-mail services on your server, on the **Add Users: Team Web Site** page, do the following:
 - a. In **Step 3: Confirm Users**, type the e-mail address of each external user in the **E-mail address** text box.
 - b. In **Step 4: Send E-Mail**, select the **Send the following e-mail to let the users know that they have been added** check box.
 - c. Type a message in the **Body** section to tell the users that they can now access the extranet and to tell them what their password and access permissions are. Click **Finish**.
9. If you have not enabled e-mail services on your server, on the **Add Users: Team Website** page, verify that the **Send the following e-mail to let the users know that they have been added** check box is cleared, and then click **Finish**.
10. Repeat steps 8-10 of this procedure until you have assigned all external users to one or more site groups.
11. Close Internet Explorer.

Step 8: Configure the Site to be Accessible from the Intranet

At this point, internal users can access the extranet only from the Internet, which creates unnecessary traffic on your router. In this step, you make it possible for internal users to access the site from the intranet, which eliminates the unnecessary traffic.

To configure the site for access from the intranet, do the following, using the information that you recorded in Table 1:

- Create a CNAME resource record.
- Define a host header.

In the following procedure, you create a CNAME resource record on your DNS server. The CNAME resource record points to the A resource record of the computer that is running Windows SBS.

▶ **To create a CNAME resource record**

1. Click **Start**, click **Administrative Tools**, and then click **DNS**.
2. In the DNS console tree, double-click the server name, double-click **Forward Lookup Zones**, right-click the domain name, and then click **New Alias (CNAME)**.
3. In the **New Resource Record** dialog box, under **Alias** name, type the name that you want to use to access the site from the intranet (for example, **http://extranet**).
4. In **Fully qualified domain name (FQDN) for target host**, type the fully qualified domain name of the computer that is running Windows SBS (for example, **server1.wingtiptoys.com**).

In the following procedure, you define the host header name (for example, **http://extranet**) that internal users can use to access the site from the intranet.

▶ **To define a host header name**

1. Click **Start**, and then click **Server Management**.
2. In the console tree, double-click **Advanced Management**, double-click **Internet Information Services**, double-click the server name, and then double-click **Web Sites**.
3. Right-click the Web site name (for example, SharePoint Extranet), and then click **Properties**.
4. On the **Web site** tab, do the following:
 - a. Click **Advanced** next to the **IP address** box.
 - b. In the **Advanced Web Site Identification** dialog box, click **Add**.
 - c. In the **Add/Edit Web Site Identification** dialog box, for **IP address**, select

the internal IP address of the local network adapter. If your configuration has one network adapter, with SSL enabled, select the additional IP address of the local network adapter. For **Port**, type **80**, and for **Host Header** value, type the name you want to use to access the extranet from the intranet (for example, http://extranet). This host header name must be identical to the Alias name that you used in the previous procedure.

Related Links

For more information, see the following resources:

- For more information about Windows SharePoint Services, see "Microsoft SharePoint Products and Technologies: Technical Overview" at the [Microsoft Web site](http://go.microsoft.com/fwlink/?LinkId=19723) (http://go.microsoft.com/fwlink/?LinkId=19723).
- For more information about DNS, see "DNS Technical Reference" at the [Microsoft Web site](http://go.microsoft.com/fwlink/?LinkId=19725) (http://go.microsoft.com/fwlink/?LinkId=19725).
- For an overview of IIS 6.0, see "Technical Overview of Internet Information Services (IIS) 6.0" at the [Microsoft Web site](http://go.microsoft.com/fwlink/?LinkId=19726) (http://go.microsoft.com/fwlink/?LinkId=19726).
- For the latest information about Windows SBS, see the [Windows SBS 2003 Web site](http://go.microsoft.com/fwlink/?LinkId=17117) (http://go.microsoft.com/fwlink/?LinkId=17117).