

Network Configuration Settings

Many small businesses already have an existing firewall device for their local network when they purchase Microsoft® Windows® Small Business Server 2003. Often, these devices also assign IP addresses to the client computers. If you are using a firewall device other than the one provided with Windows Small Business Server 2003, and the device does not support Universal Plug and Play (UPnP), you must manually configure the necessary settings.

Configuration Settings for an Existing Firewall Device

A firewall protects your local network from unauthorized Internet access. If you are not using the firewall service provided with Windows Small Business Server 2003, you must use a firewall device on the local network. Additionally, the firewall device must be configured with the necessary settings for your local network. If the device supports UPnP, it is possible for the Configure E-mail and Internet Connection Wizard to configure the device automatically. Otherwise, you must manually configure the device with the necessary settings.

If the firewall device also serves as a router to connect to the Internet and your server uses two network adapters (one to connect to the Internet and one to connect to the local network), you can use the firewall service provided by the router, the one provided with Windows Small Business Server 2003, or both.

Services to be Accessible Through the Firewall Device

If you are running any of the following services on your server, you must forward the port numbers for these services to pass through the firewall. The protocol type for each of the services listed in the following table is Transmission Control Protocol (TCP). Configure the appropriate settings on the firewall as defined in the following table.

Service	TCP port number	Purpose
E-mail	25	Allows incoming and outgoing Simple Mail Transfer Protocol (SMTP) traffic so Exchange can send and receive Internet e-mail.
Web server	80 (for http://) and 443 (for https://)	Allows users on the Internet to access the default Web site or specific Web site services. Port 80 is required for HTTP requests for your site, and port 443 is required for HTTPS requests using Secure Sockets Layer (SSL), which secures communications from your server and a Web browser.
		Web site services that use ports 80 and/or port 443 include the following: <ul style="list-style-type: none">• Outlook® Web Access, which allows users to access their e-mail from the Internet using a Web browser. This service

requires that users type **https://** to connect securely from a Web browser to the Web server.

- Server performance and usage reports, which contain detailed information about the overall health and use of your server. Users can connect to this service typing either an **http://** or **https://** connection.
- Outlook Mobile Access, which allows users to access their e-mail from a mobile device.

Web site services that use port 80 include the following:

- Business Web site (wwwroot), which allows users to access the company's Internet Web site from the Internet.
- Outlook via the Internet, which allows users to remotely access their e-mail from a client computer on the Internet using Microsoft® Office Outlook® 2003, without needing to create a virtual private network (VPN) connection. Outlook connects to an Exchange server through the Internet using remote procedure call (RPC) over HTTP.

This Web service requires that the client computers meet the necessary requirements. For more information about configuring the client computers, click **Information and Answers** at the Remote Web Workplace. For more information about accessing the Remote Web Workplace, see "Connect remotely to the server" in Help and Support Center.

Note

- In addition to forwarding the ports for Web server access, you must allow access to Web sites on the **Web Services Configuration** page of the Configure E-mail and Internet Connection Wizard.

Allows users to access the intranet Web site created by Microsoft® Windows® SharePoint™ Services. Port 444 is required to secure communications from your server and a Web browser.

Windows
SharePoint
Services
intranet site

444

To securely connect to the intranet Web site from the Internet, users must type **https://**. If users are on the local network, users can type **http://**.

If you create sites below the `http://companyweb/` site in Windows SharePoint Services, the sites will also be accessible to the Internet

when you allow access to the intranet Web site.

Note

- In addition to opening the ports for Web server access, you must select to allow access to Web sites on the **Web Services Configuration** page of the Configure E-mail and Internet Connection Wizard.

Allows designated users to:

- Connect to the local network from Outlook Web Access.
- Create a direct Remote Desktop Web Connection to client computers on the local network.
- Use the Windows SharePoint Services intranet site.
- Download Connection Manager to configure the remote client computer for remote access.

Remote Web Workplace	4125 and 443	This service requires that users type https:// to connect securely form a Web browser to the Web server.
----------------------	--------------	---

Note

- In addition to opening the ports for Web server access, you must allow access to this Web site on the **Web Services Configuration** page of the Configure E-mail and Internet Connection Wizard.

Virtual Private Network (VPN)	1723	Allows remote clients to connect securely to the network and then use resources as if the client were connected locally.
-------------------------------	------	--

Terminal Services	3389	Allows remote clients to connect to the server using Terminal Services. Allows file transfer protocol (FTP) connections to the server.
-------------------	------	---

Note

File Transfer Protocol (FTP)	21	<ul style="list-style-type: none">• To use your server as an FTP server, you must first install and configure the FTP service. For more information, click Start, and then click Help and Support.
------------------------------	----	--

Configuring Settings for an Existing DHCP Server Service on Your Network

Internet Protocol (IP) addresses for client computers can either be assigned dynamically or you can use static IP addresses.

Using Dynamic Host Configuration Protocol (DHCP) to assign IP address settings to client computers simplifies the administration of your local network addresses. If you have an existing device on the local network that assigns IP addresses to client computers using DHCP, it must be configured with the necessary settings for your local network. If the device supports Universal Plug and Play (UPnP), you will be prompted during Setup to configure the device automatically. If the device does not support UPnP or the standard used by the UPnP device is not supported by Setup, you must manually configure the DHCP settings as specified in the section "Settings to configure for an existing DHCP Server service."

Optionally, you can use the DHCP Server service provided with Windows Small Business Server 2003. If you use this service, do not disable the existing DHCP server device until you are prompted by Setup. This allows Setup to determine the range of IP addresses already in use on the network.

Important

- Using the DHCP Server service provided with Windows Small Business Server 2003 ensures your DHCP settings are properly configured for your server. However, do not disable the existing DHCP server until after Setup prompts you to do so. Otherwise, Setup will not be able to determine the IP address range currently used by your local network.

If you elect to assign static IP addresses for client computers, you will need to manually configure an IP address for each client computer based on the guidelines given for configuring DHCP. For more information about how to statically assign an IP address, click **Start**, click **Help and Support**, and then search for "Setting up TCP/IP."

Settings to Configure for an Existing DHCP Server Service

To ensure that the DHCP Server service is properly configured for your local network, you must configure the settings as follows:

1. Create a DHCP scope using the options specified in the section "DHCP Scope Options for an Existing DHCP Device." The scope needs to include enough IP addresses to accommodate each client computer, additional services, and network devices that require an IP address in your local network. Add an additional IP address to this range for each remote user you plan to allow to remotely connect to your local network, plus one for the remote access server.

2. Exclude the IP address of the network adapter used to connect to the local network. This ensures that this address will not be given out by the DHCP server to a client computer. If you have additional devices on your network that use a static IP address, these should also be excluded from the scope. It is also recommended that you create an exclusion of 5 to 10 IP addresses in case you need to assign a static IP address to another device at a later time.

Note

- o It is not necessary to exclude the IP address of the local network adapter if the range of IP addresses used in the DHCP scope does not include the IP address used for the local network adapter.

DHCP Scope Options for an Existing DHCP Device

If the DHCP Server service has any of the following DHCP options, configure the options as defined in the following table.

Option	Description	Record value here
Router (default gateway)	<p>Defines the default gateway used by client computers.</p> <ul style="list-style-type: none"> • If the computer running Windows Small Business Server 2003 has two network adapters, specify the IP address of the server's local network adapter. • If the computer running Windows Small Business Server 2003 has only one network adapter and you are using a router device to connect to the Internet, specify the IP address of the router's internal interface. 	_____
Domain Name System (DNS) server	<p>Provides client computers with name resolution services for the local network.</p> <p>Specify the IP address of the local network adapter of the computer running Windows Small Business Server 2003.</p>	_____
DNS domain name	<p>Provides client computers with the fully qualified domain name (FQDN) for the local network.</p> <p>Specify the full DNS name for the internal domain of the local network. For example, if you used the default full DNS for internal domain, it is your organization's name with the label .local, such as,</p>	_____

wingtiptoys.local.

Provides local network name resolution for computers running to Microsoft® Windows NT® Server 4.0 and earlier and Windows® 98 and earlier.

Windows
Internet Name
Service (WINS)
server

If the DHCP server has the option to set a WINS server option, specify the IP address of the computer running Windows Small Business Server.

Prevents unnecessary broadcast traffic.

WINS node
type

If the DHCP server has the option to set a WINS server, specify the WINS node type as hybrid or h-node (0x8).