Search

How to install and configure a Virtual Private Network server in Windows Server 2003

This article was previously published under Q323441

Article ID : 323441
Last Review : December 3, 2007
Revision : 8.6

On This Page

SUMMARY

This step-by-step article describes how to install virtual private networking (VPN) and how to create a new VPN connection in servers that are running Windows Server 2003.

With a virtual private network, you can connect network components through another network, such as the Internet. You can make your Windows Server 2003-based computer a remote-access server so that other users can connect to it by using VPN, and then they can log on to the network and access shared resources. VPNs do this by "tunneling" through the Internet or through another public network in a manner that provides the same security and features as a private network. Data is sent across the public network by using its routing infrastructure, but to the user, it appears as if the data is sent over a dedicated private link.

Overview of VPN

A virtual private network is a means of connecting to a private network (such as your office network) by way of a public network (such as the Internet). A VPN combines the virtues of a dial-up connection to a dial-up server with the ease and flexibility of an Internet connection. By using an Internet connection, you can travel worldwide and still, in most places, connect to your office with a local call to the nearest Internet-access phone number. If you have a high-speed Internet connection (such as cable or DSL) at your computer and at your office, you can communicate with your office at full Internet speed, which is much faster than any dial-up connection that uses an analog modem. This technology allows an enterprise to connect to its branch offices or to other companies over a public network while maintaining secure communications. The VPN connection across the Internet logically operates as a dedicated wide area network (WAN) link.

Virtual private networks use authenticated links to make sure that only authorized users can connect to your network. To make sure data is secure as it travels over the public network, a VPN connection uses Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol (L2TP) to encrypt data.

Components of a VPN

A VPN in servers running Windows Server 2003 is made up of a VPN server, a VPN client, a VPN connection (that portion of the connection in which the data is encrypted), and the tunnel (that portion of the connection in which the data is encapsulated). The tunneling is completed through one of the tunneling protocols included with servers running Windows Server 2003, both of which are installed with Routing and Remote Access. The Routing and Remote Access service is installed automatically during the installation of Windows Server 2003. By default, however, the Routing and Remote Access service is turned off.
The two tunneling protocols included with Windows are:

- **Point-to-Point Tunneling Protocol (PPTP)**: Provides data encryption using Microsoft Point-to-Point Encryption.
- **Layer Two Tunneling Protocol (L2TP)**: Provides data encryption, authentication, and integrity using IPSec.

Your connection to the Internet must use a dedicated line such as T1, Fractional T1, or Frame Relay. The WAN adapter must be configured with the IP address and subnet mask assigned for your domain or supplied by an Internet service provider (ISP). The WAN adapter must also be configured as the default gateway of the ISP router.

NOTE: To turn on VPN, you must be logged on using an account that has administrative rights.

How to install and Turn on a VPN Server

To install and turn on a VPN server, follow these steps:

1. Click **Start**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. Click the server icon that matches the local server name in the left pane of the console. If the icon has a red circle in the lower-left corner, the Routing and Remote Access service has not been turned on. If the icon has a green arrow pointing up in the lower-left corner, the Routing and Remote Access service has been turned on. If the Routing and Remote Access service was previously turn on, you may want to reconfigure the server. To reconfigure the server:
   a. Right-click the server object, and then click **Disable Routing and Remote Access**. Click **Yes** to continue when you are prompted with an informational message.
   b. Right-click the server icon, and then click **Configure and Enable Routing and Remote Access** to start the Routing and Remote Access Server Setup Wizard. Click **Next** to continue.
   c. Click **Remote access (dial-up or VPN)** to turn on remote computers to dial in or connect to this network through the Internet. Click **Next** to continue.
3. Click to select **VPN** or **Dial-up** depending on the role that you intend to assign to this server.
4. In the VPN Connection window, click the network interface which is connected to the Internet, and then click **Next**.
5. In the **IP Address Assignment** window, click **Automatically** if a DHCP server will be used to assign addresses to remote clients, or click **From a specified range of addresses** if remote clients must only be given an address from a pre-defined pool. In most cases, the DHCP option is simpler to administer. However, if DHCP is not available, you must specify a range of static addresses. Click **Next** to continue.
6. If you clicked **From a specified range of addresses**, the **Address Range Assignment** dialog box opens. Click **New**. Type the first IP address in the range of addresses that you want to use in the **Start IP address** box. Type the last IP address in the range in the **End IP address** box. Windows calculates the number of addresses automatically. Click **OK** to return to the **Address Range Assignment** window. Click **Next** to continue.
7. Accept the default setting of **No, use Routing and Remote Access to authenticate connection requests**, and then click **Next** to continue. Click **Finish** to turn on the Routing and Remote Access service and to configure the server as a Remote Access server.

How to Configure the VPN Server

To continue to configure the VPN server as required, follow these steps.

How to Configure the Remote Access Server as a Router

For the remote access server to forward traffic properly inside your network, you must configure it as a router with either static routes or routing protocols, so that all of the locations in the intranet are reachable from the remote access server.

To configure the server as a router:

1. Click **Start**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. Right-click the server name, and then click **Properties**.
3. Click the **General** tab, and then click to select **Router** under **Enable this computer as a**.
4. Click **LAN and demand-dial routing**, and then click **OK** to close the **Properties** dialog box.

How to Modify the Number of Simultaneous Connections

The number of dial-up modem connections is dependent on the number of modems that are installed on the server. For example, if you have only one modem installed on the server, you can have only one modem connection at a time.

The number of dial-up VPN connections is dependent on the number of simultaneous users whom you want to permit. By default, when you run the procedure described in this article, you permit 128 connections. To change the number of simultaneous connections, follow these steps:

1. Click **Start**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
2. Double-click the server object, right-click **Ports**, and then click **Properties**.
3. In the **Ports Properties** dialog box, click **WAN Miniport (PPTP)**, and then click **Configure**.
4. In the **Maximum ports** box, type the number of VPN connections that you want to permit.
5. Click **OK**, click **OK** again, and then close Routing and Remote Access.

How to Manage Addresses and Name Servers

The VPN server must have IP addresses available to assign them to the VPN server's virtual interface and to VPN clients during the IP Control Protocol (IPCP) negotiation phase of the connection process. The IP address assigned to the VPN client is assigned to the virtual interface of the VPN client.

For Windows Server 2003-based VPN servers, the IP addresses assigned to VPN clients are obtained through DHCP by default. You can also configure a static IP address pool. The VPN server must also be configured with name resolution servers, typically DNS and WINS server addresses, to assign to the VPN client during IPCP negotiation.

How to Manage Access

Configure the dial-in properties on user accounts and remote access policies to manage access for dial-up networking and VPN connections.

NOTE: By default, users are denied access to dial-up networking.

Access by User Account

To grant dial-in access to a user account if you are managing remote access on a user basis, follow these steps:

1. Click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. Right-click the user account, and then click **Properties**.
3. Click the **Dial-in** tab.
4. Click **Allow access** to grant the user permission to dial in. Click **OK**.

Access by Group Membership

If you manage remote access on a group basis, follow these steps:

1. Create a group with members who are permitted to create VPN connections.
2. Click **Start**, point to **Administrative Tools**, and then click **Routing and Remote Access**.
3. In the console tree, expand **Routing and Remote Access**, expand the server name, and then click **Remote Access Policies**.
4. Right-click anywhere in the right pane, point to **New**, and then click **Remote Access Policy**.
5. Click **Next**, type the policy name, and then click **Next**.
6. Click **VPN** for Virtual Private Access access method, or click **Dial-up** for dial-up access, and then click **Next**.
7. Click **Add**, type the name of the group that you created in step 1, and then click **Next**.
8. Follow the on-screen instructions to complete the wizard.

If the VPN server already permits dial-up networking remote access services, do not delete the default policy. Instead, move it so that it is the last policy to be evaluated.

How to Configure a VPN Connection from a Client Computer

To set up a connection to a VPN, follow these steps. To set up a client for virtual private network access, follow these steps on the client workstation:

NOTE: You must be logged on as a member of the Administrators group to follow these steps.

NOTE: Because there are several versions of Microsoft Windows, the following steps may be different on your computer. If they are, see your product documentation to complete these steps.

1. On the client computer, confirm that the connection to the Internet is correctly configured.
2. Click **Start**, click **Control Panel**, and then click **Network Connections**. Click **Create a new connection** under **Network Tasks**, and then click **Next**.
3. Click **Connect to the network at my workplace** to create the dial-up connection. Click **Next** to continue.
4. Click **Virtual Private Network connection**, and then click **Next**.
5. Type a descriptive name for this connection in the **Company name** dialog box, and then click **Next**.
6. Click **Do not dial the initial connection** if the computer is permanently connected to the Internet. If the computer connects to the Internet through an Internet Service Provider (ISP), click **Automatically dial this initial connection**, and then click the name of the connection to the ISP. Click **Next**.
7. Type the IP address or the host name of the VPN server computer (for example, VPNServer.SampleDomain.com).
8. Click **Anyone's use** if you want to permit any user who logs on to the workstation to have access to this dial-up connection. Click **My use only** if you want this connection to be available only to the currently logged-on user. Click **Next**.
9. Click **Finish** to save the connection.
10. Click **Start**, click **Control Panel**, and then click **Network Connections**.
11. Double-click the new connection.

12. Click **Properties** to continue to configure options for the connection. To continue to configure options for the connection, follow these steps:
    - If you are connecting to a domain, click the **Options** tab, and then click to select the **Include Windows logon domain** check box to specify whether to request Windows Server 2003 logon domain information before trying to connect.
    - If you want the connection to be redialed if the line is dropped, click the **Options** tab, and then click to select the **Redial if line is dropped** check box.

To use the connection, follow these steps:

1. Click **Start**, point to **Connect to**, and then click the new connection.
2. If you do not currently have a connection to the Internet, Windows offers to connect to the Internet.
3. When the connection to the Internet is made, the VPN server prompts you for your user name and password. Type your user name and password, and then click **Connect**.
   Your network resources must be available to you in the same way they are when you connect directly to the network.**NOTE**: To disconnect from the VPN, right-click the connection icon, and then click **Disconnect**.

Troubleshooting

Troubleshooting Remote Access VPNs

Cannot Establish a Remote Access VPN Connection

- **Cause**: The name of the client computer is the same as the name of another computer on the network.

  Solution: Verify that the names of all computers on the network and computers connecting to the network are using unique computer names.
- **Cause**: The Routing and Remote Access service is not started on the VPN server.

  Solution: Verify the state of the Routing and Remote Access service on the VPN server.

  See Windows Server 2003 Help and Support Center for more information about how to monitor the Routing and Remote Access service, and how to start and stop the Routing and Remote Access service. Click **Start** to access the Windows Server 2003 Help and Support Center.
- **Cause**: Remote access is not turned on on the VPN server.

  Solution: Turn on remote access on the VPN server.

  See the Windows Server 2003 Help and Support Center for more information about how to turn on the remote access server. Click **Start** to access the Windows Server 2003 Help and Support Center.
- **Cause**: PPTP or L2TP ports are not turned on for inbound remote access requests.

  Solution: Turn on PPTP or L2TP ports, or both, for inbound remote access requests.

  See the Windows Server 2003 Help and Support Center for more information about how to configure ports for remote access. Click **Start** to access the Windows Server 2003 Help and Support Center.
- **Cause**: The LAN protocols used by the VPN clients are not turned on for remote access on the VPN server.

  Solution: Turn on the LAN protocols used by the VPN clients for remote access on the VPN server.

  See the Windows Server 2003 Help and Support Center for more information about how to view properties of the remote access server. Click **Start** to access the Windows Server 2003 Help and Support Center.
- **Cause**: All of the PPTP or L2TP ports on the VPN server are already being used by currently connected remote access clients or demand-dial routers.

  Solution: Verify that all of the PPTP or L2TP ports on the VPN server are already being used. To do so, click **Ports** in Routing and Remote Access. If the number of PPTP or L2TP ports permitted is not high enough, change the number of PPTP or L2TP ports to permit more concurrent connections.

  See the Windows Server 2003 Help and Support Center for more information about how to add PPTP or L2TP ports. Click **Start** to access the Windows Server 2003 Help and Support Center.
- **Cause**: The VPN server does not support the tunneling protocol of the VPN client.

  By default, Windows Server 2003 remote access VPN clients use the **Automatic** server type option, which means that they try to establish an L2TP over IPSec-based VPN connection first, and then they try to establish a PPTP-based VPN connection. If VPN clients use either the **Point-to-Point Tunneling Protocol (PPTP)** or **Layer-2 Tunneling Protocol (L2TP)** server type option, verify that the selected tunneling protocol is supported by the VPN server.

  By default, a computer running Windows Server 2003 Server and the Routing and Remote Access

service is a PPTP and L2TP server with five L2TP ports and five PPTP ports. To create a PPTP-only server, set the number of L2TP ports to zero. To create an L2TP-only server, set the number of PPTP ports to zero.

Solution: Verify that the appropriate number of PPTP or L2TP ports is configured.

See the Windows Server 2003 Help and Support Center for more information about how to add PPTP or L2TP ports. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: The VPN client and the VPN server in conjunction with a remote access policy are not configured to use at least one common authentication method.

  Solution: Configure the VPN client and the VPN server in conjunction with a remote access policy to use at least one common authentication method.

  See the Windows Server 2003 Help and Support Center for more information about how to configure authentication. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: The VPN client and the VPN server in conjunction with a remote access policy are not configured to use at least one common encryption method.

  Solution: Configure the VPN client and the VPN server in conjunction with a remote access policy to use at least one common encryption method.

  See the Windows Server 2003 Help and Support Center for more information about how to configure encryption. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: The VPN connection does not have the appropriate permissions through dial-in properties of the user account and remote access policies.

  Solution: Verify that the VPN connection has the appropriate permissions through dial-in properties of the user account and remote access policies. For the connection to be established, the settings of the connection attempt must:
  - Match all of the conditions of at least one remote access policy.
  - Be granted remote access permission through the user account (set to **Allow access**) or through the user account (set to **Control access through Remote Access Policy**) and the remote access permission of the matching remote access policy (set to **Grant remote access permission**).
  - Match all the settings of the profile.
  - Match all the settings of the dial-in properties of the user account.

  See the Windows Server 2003 Help and Support Center for an introduction to remote access policies, and for more information about how to accept a connection attempt. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: The settings of the remote access policy profile are in conflict with properties of the VPN server.

  The properties of the remote access policy profile and the properties of the VPN server both contain settings for:
  - Multilink.
  - Bandwidth allocation protocol (BAP).
  - Authentication protocols.

  If the settings of the profile of the matching remote access policy are in conflict with the settings of the VPN server, the connection attempt is rejected. For example, if the matching remote access policy profile specifies that the Extensible Authentication Protocol - Transport Level Security (EAP-TLS) authentication protocol must be used and EAP is not enabled on the VPN server, the connection attempt is rejected.

  Solution: Verify that the settings of the remote access policy profile are not in conflict with properties of the VPN server.

  See the Windows Server 2003 Help and Support Center for more information about additional information about multilink, BAP and authentication protocols. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: The answering router cannot validate the credentials of the calling router (user name, password, and domain name).

  Solution: Verify that the credentials of the VPN client (user name, password, and domain name) are correct and can be validated by the VPN server.

- **Cause**: There are not enough addresses in the static IP address pool.

  Solution: If the VPN server is configured with a static IP address pool, verify that there are enough addresses in the pool. If all of the addresses in the static pool have been allocated to connected VPN clients, the VPN server cannot allocate an IP address, and the connection attempt is rejected. If all of the addresses in the static pool have been allocated, modify the pool. See the Windows Server 2003 Help and Support Center for more information about TCP/IP and remote access, and how to create a

static IP address pool. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: The VPN client is configured to request its own IPX node number and the VPN server is not configured to permit IPX clients to request their own IPX node number.

  Solution: Configure the VPN server to permit IPX clients to request their own IPX node number.

  See the Windows Server 2003 Help and Support Center for more information about IPX and remote access. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: The VPN server is configured with a range of IPX network numbers that are being used elsewhere on your IPX network.

  Solution: Configure the VPN server with a range of IPX network numbers that is unique to your IPX network.

  See the Windows Server 2003 Help and Support Center for more information about IPX and remote access. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: The authentication provider of the VPN server is improperly configured.

  Solution: Verify the configuration of the authentication provider. You can configure the VPN server to use either Windows Server 2003 or Remote Authentication Dial-In User Service (RADIUS) to authenticate the credentials of the VPN client.

  See the Windows Server 2003 Help and Support Center for more information about authentication and accounting providers, and how to use RADIUS authentication. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: The VPN server cannot access Active Directory.

  Solution: For a VPN server that is a member server in a mixed-mode or native-mode Windows Server 2003 domain that is configured for Windows Server 2003 authentication, verify that:
  - The **RAS and IAS Servers** security group exists. If not, create the group and set the group type to Security and the group scope to Domain local.
  - The **RAS and IAS Servers** security group has Read permission to the **RAS and IAS Servers Access Check** object.
  - The computer account of the VPN server computer is a member of the **RAS and IAS Servers** security group. You can use the **netsh ras show registeredserver** command to view the current registration. You can use the **netsh ras add registeredserver** command to register the server in a specified domain.

    If you add (or remove) the VPN server computer to the **RAS and IAS Servers** security group, the change does not take effect immediately (because of the way that Windows Server 2003 caches Active Directory information). To immediately effect this change, restart the VPN server computer.
  - The VPN server is a member of the domain.

  See the Windows Server 2003 Help and Support Center for more information about how to add a group, how to verify permissions for the RAS and IAS security group, and about **netsh** commands for remote access. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: A Windows NT 4.0-based VPN server cannot validate connection requests.

  Solution: If VPN clients are dialing in to a VPN server running Windows NT 4.0 that is a member of a Windows Server 2003 mixed-mode domain, verify that the Everyone group is added to the Pre-Windows 2000 Compatible Access group with the following command:

  "net localgroup "Pre-Windows 2000 Compatible Access""

  If not, type the following command at a command prompt on a domain controller computer, and then restart the domain controller computer:

  net localgroup "Pre-Windows 2000 Compatible Access" everyone /add

  See the Windows Server 2003 Help and Support Center for more information about Windows NT 4.0 remote access server in a Windows Server 2003 domain. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: The VPN server cannot communicate with the configured RADIUS server.

  Solution: If you can reach your RADIUS server only through your Internet interface, do one of the following:
  - Add an input filter and an output filter to the Internet interface for UDP port 1812 (based on RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)"). –or-
  - Add an input filter and an output filter to the Internet interface for UDP port 1645 (for older RADIUS servers), for RADIUS authentication and UDP port 1813 (based on RFC 2139, "RADIUS Accounting"). -or-
  -

-or- Add an input filter and an output filter to the Internet interface for UDP port 1646 (for older RADIUS servers) for RADIUS accounting.

See the Windows Server 2003 Help and Support Center for more information about how to add a packet filter. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: Cannot connect to the VPN server over the Internet using the Ping.exe utility.

  Solution: Because of the PPTP and L2TP over IPSec packet filtering that is configured on the Internet interface of the VPN server, Internet Control Message Protocol (ICMP) packets used by the ping command are filtered out. To turn on the VPN server to respond to ICMP (ping) packets, add an input filter and an output filter that permit traffic for IP protocol 1 (ICMP traffic).

  See the Windows Server 2003 Help and Support Center for more information about how to add a packet filter. Click **Start** to access the Windows Server 2003 Help and Support Center.

Cannot Send and Receive Data

- **Cause**: The appropriate demand-dial interface has not been added to the protocol being routed.

  Solution: Add the appropriate demand-dial interface to the protocol being routed.

  See the Windows Server 2003 Help and Support Center for more information about how to add a routing interface. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: There are no routes on both sides of the router-to-router VPN connection that support the two-way exchange of traffic.

  Solution: Unlike a remote access VPN connection, a router-to-router VPN connection does not automatically create a default route. Create routes on both sides of the router-to-router VPN connection so that traffic can be routed to and from the other side of the router-to-router VPN connection.

  You can manually add static routes to the routing table, or you can add static routes through routing protocols. For persistent VPN connections, you can turn on Open Shortest Path First (OSPF) or Routing Information Protocol (RIP) across the VPN connection. For on-demand VPN connections, you can automatically update routes through an auto-static RIP update. See Windows Server 2003 online Help for more information about how to add an IP routing protocol, how to add a static route, and how to perform auto-static updates. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: A two-way initiated, the answering router as a remote access connection is interpreting router-to-router VPN connection.

  Solution: If the user name in the credentials of the calling router appears under **Dial-In Clients** in Routing and Remote Access, the answering router may interpret the calling router as a remote access client. Verify that the user name in the credentials of the calling router matches the name of a demand-dial interface on the answering router. If the incoming caller is a router, the port on which the call was received shows a status of **Active** and the corresponding demand-dial interface is in a **Connected** state.

  See Windows Server 2003 online Help for more information about how to check the status of the port on the answering router, and how to check the status of the demand-dial interface. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: Packet filters on the demand-dial interfaces of the calling router and answering router are preventing the flow of traffic.

  Solution: Verify that there are no packet filters on the demand-dial interfaces of the calling router and answering router that prevent the sending or receiving of traffic. You can configure each demand-dial interface with IP and IPX input and output filters to control the exact nature of TCP/IP and IPX traffic that is permitted into and out of the demand-dial interface.

  See Windows Server 2003 online Help for more information about how to manage packet filters. Click **Start** to access the Windows Server 2003 Help and Support Center.

- **Cause**: Packet filters on the remote access policy profile are preventing the flow of IP traffic.

  Solution: Verify that there are no configured TCP/IP packet filters on the profile properties of the remote access policies on the VPN server (or the RADIUS server if Internet Authentication Service is used) that are preventing the sending or receiving of TCP/IP traffic. You can use remote access policies to configure TCP/IP input and output packet filters that control the exact nature of TCP/IP traffic permitted on the VPN connection. Verify that the profile TCP/IP packet filters are not preventing the flow of traffic.

  See Windows Server 2003 online Help for more information about how to configure IP options. Click **Start** to access the Windows Server 2003 Help and Support Center.

APPLIES TO

- Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
- Microsoft Windows Server 2003, Standard Edition (32-bit x86)
- Microsoft Windows Small Business Server 2003 Standard Edition
- Microsoft Windows Small Business Server 2003 Premium Edition

Keywords: kbpubtypekc kbnetwork kbhowtomaster KB323441