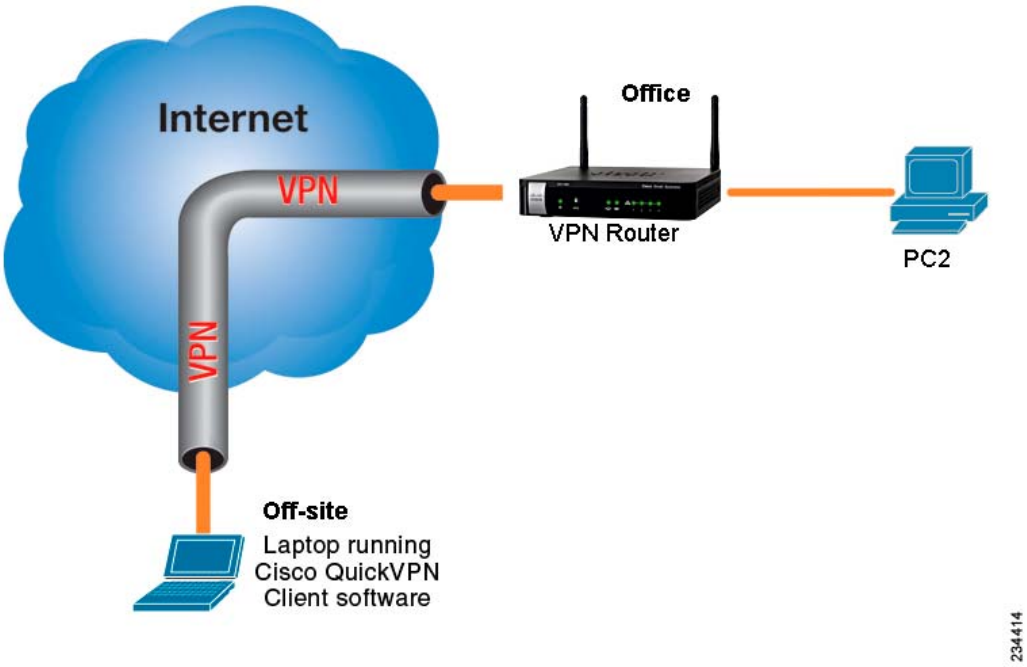
Easy and Secure Remote Access with Cisco QuickVPN

With the widespread use of mobile technology and an increased reliability of wireless networks, more businesses can separate “work” from “place.” It is now easy to connect from anywhere. The telecommuter can check email and back up files, whether working from home or attending the kids’ soccer practice. The salesperson can retrieve the latest presentations and submit updated proposals, whether staffing a trade show booth or visiting a customer site. The business traveler can remain productive, whether sitting in a hotel room or waiting at an airport. As more small businesses retain contractors to reduce overhead, they must extend secure connectivity beyond the walls of the office.

To achieve these goals and protect your network, you need an encrypted Virtual Private Network (VPN). A VPN is a communications tunnel between a remote worker’s computer and your network. Encryption and authentication features prevent unauthorized entry and keep communications secure. The benefits are clear, but setting up a VPN can be daunting because of confusing technical terminology and numerous configuration options. Cisco QuickVPN provides an easy way to ensure secure remote access. As shown below, with Cisco QuickVPN installed on a computer and a few simple settings configured on the router, an off-site user can securely access network resources from anyplace with an Internet connection.



Key Benefits

Cisco QuickVPN provides a cost-effective and simple way to set up a VPN.

- **Free software.** Cisco QuickVPN is available free of charge from Cisco.com.
- **Easy installation & setup.** Your employees easily can install the QuickVPN client themselves. Optionally, you can generate certificates that they can install for extra protection.
- **Simple management.** There’s no need to configure VPN policies on the router. Typically the only requirement is to create the user accounts. Some router models may require that you enable a remote access port.

Requirements

Cisco QuickVPN requires Windows computers, a compatible router, and Windows Firewall. For best performance, ensure that the router and the users' computers have the latest software at all times. Details are listed below.

- **A Windows operating system.** Users can have Windows 7 (32-bit and 64-bit editions), Windows XP (32-bit), and WIndows Vista (32-bit and 64-bit editions). QuickVPN is not available for the Mac.
- **A compatible router.** Cisco QuickVPN is compatible with the following Cisco Small Business routers:
  - RV110W Wireless-N VPN Firewall
  - RV120W Wireless-N VPN Firewall
  - RV220W Wireless Network Security Firewall
  - RV016 16-port 10/100 VPN Router - Multi WAN
  - RV042 4-port 10/100 VPN Router - Dual WAN
  - RV082 8-port 10/100 VPN Router - Dual WAN
  - RVS4000 4-port Gigabit Security Router - VPN
  - SA520 Security Appliance
  - SA520W Security Appliance
  - SA540 Security Appliance
  - WRV200 Wireless-G VPN Router - RangeBooster
  - WRV210 Wireless-G VPN Router - RangeBooster
  - WRVS4400N Wireless-N Gigabit Security Router - VPN V2.0
  - WRVS4400N Wireless-N Gigabit Security Router - VPN V1.0 & V1.1

  Note: To avoid address conflicts between the LAN settings of your router and VPN users' routers, do not configure your LAN with a common IP address range such as 192.168.1.x.
- **Administrative rights on the PC.** The user must have administrative rights to use the Cisco QuickVPN software.
- **Windows Firewall.** Because of the way that Windows handles IPsec service, Windows Firewall must be enabled for QuickVPN to function properly. The user must uninstall third-party firewall software that conflicts with or disables Windows Firewall.
  Note: As a best practice, users should enable Windows Firewall (via the Control Panel) even if the network has a router firewall. Doing so helps to block viruses from other computers on the LAN.

Cisco also recommends the following best practices:

- **Cisco QuickVPN updates.** Install the latest software when setting up users' computers. As a best practice, ensure that users install Cisco QuickVPN updates as they become available.
- **Windows updates.** As a best practice, enable Windows Automatic Updates to ensure that the computer is updated with critical patches from Microsoft.
  Note: For users with Windows XP, be aware of known issues with Service Pack 2. Install either Service Pack 3 (see http://www.microsoft.com/downloads/details.aspx?FamilyId=5B33B5A8-5E76-401F-BE08-1E1555D4F3D4&displaylang=en) or a special patch that Microsoft has issued (see http://support.microsoft.com/kb/889527/en-us).

Limitations

Cisco QuickVPN is a good choice if you want to set up a secure VPN easily and quickly. However, you may have additional requirements that would be better suited to another VPN solution. Consider the following points:

- **Cisco QuickVPN does not allow customization of settings.** Because it is designed for quick and easy setup, this solution does not offer the ability to specify the authentication and encryption settings.
- **Cisco QuickVPN is not a site-to-site solution.** Cisco QuickVPN is specifically designed to allow remote users to access resources on your network. It does not allow users at the main site to access resources at a remote site.
- **Cisco QuickVPN does not allow the use of network names.** At your site, users may be accustomed to accessing printers and other devices by using their assigned host names or by browsing the Windows Network Neighborhood. However, NetBIOS, the program that makes this possible, is not available via Cisco QuickVPN. You will need to provide your QuickVPN users with the IP addresses of the resources that they can access remotely.

Note: If Cisco QuickVPN does not suit your requirements, most Cisco Small Business routers support other VPN options such as IPsec and SSL VPN. Many models include a VPN setup wizard that simplifies the process of setting up the VPN policies. After using the wizard, you can use the web-based configuration utility to customize the settings for your business. For more information, refer to the documentation for your Cisco Small Business router.

Appendix A: How-To Information

How to Set Up Your Router for QuickVPN

Typically the only requirement is to create the user accounts. Some router models may require the extra step of enabling a remote access port. For details, refer to the router's administration guide.

How to Install QuickVPN on a PC

1. Get the software from Cisco.com:
   a. Go to www.cisco.com/go/software.
   b. Enter the router's model number in the search box and then click **Find**.
   c. In the list of links, click **Quick Virtual Private Network (QVPN) Utility**.
   d. Follow the on-screen instructions to download the software. Save it on your PC.
2. Extract the Zip file, and then double-click **Setup.exe** to install the software.

How to Use Cisco QuickVPN

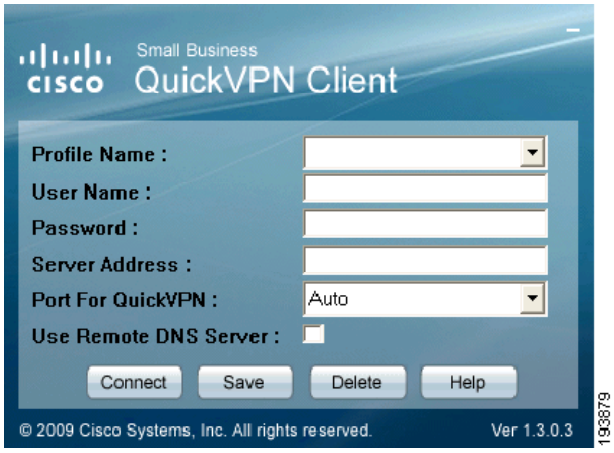
1. Double-click the Cisco QuickVPN software icon on your Desktop or System Tray, or go to **Start** > **Programs** > **Cisco Small Business** > **QuickVPN Client**.

QuickVPN Desktop Icon

2. Enter a new **Profile Name** or select a saved profile from the drop-down list. When creating a new profile, enter the following information:
   - **User Name:** Enter the username provided by the administrator.
   - **Password:** Enter your password.
     Note: The administrator will provide the password. After you connect, you can change your password, if allowed by the administrator.

- **Server Address:** Enter the IP address or domain name of the RV220W.
- **Port for QuickVPN:** Enter the port number specified by the administrator, or keep the default setting, Auto.
- **Use Remote DNS Server:** Check this box to use the server to resolve domain names, or uncheck this box to use your local network settings.

3. To save this profile for future use, click **Save**.



4. To begin your Cisco QuickVPN connection, click **Connect**. The connection's progress is displayed: *Connecting, Provisioning, Activating Policy,* and *Verifying Network*.
5. After your QuickVPN connection is established, the Cisco QuickVPN tray icon turns green, and the Cisco QuickVPN Status window appears. The window displays the IP address of the remote end of the VPN tunnel, the time and date the VPN tunnel began, and the total length of time the VPN tunnel has been active.

QuickVPN Tray Icon—Connection

The status window appears. You can now access network resources by using their IP addresses.

6. To terminate the VPN tunnel, click **Disconnect**.

   If allowed by the administrator, you can click **Change Password** to update your password. For information, click **Help**.

Where to Go From Here

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Downloads and Documentation	
Firmware	www.cisco.com/go/software (Enter the model number to search. Then choose to download the router firmware or Cisco QuickVPN.)
Cisco Small Business Routers Documentation	www.cisco.com/go/smallbizrouters (See the Technical Documentation links.)
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb

OL-25680-01