

WatchGuard®

Mobile User VPN

Administrator Guide

WatchGuard® Mobile User VPN (MUVPN) uses Internet Protocol Security (IPSec) to establish a secure connection over an unsecured network from a remote host computer to a protected network. In other words, MUVPN connects an employee on the road or working from home to trusted and optional networks behind a Firebox using a standard Internet connection without compromising security.

The Mobile User VPN client can also be installed with a personal firewall (ZoneAlarm®) in order to provide further security for your remote users.

This guide describes how to configure a remote host computer for MUVPN including instructions on how to install the MUVPN client. For information on configuring the Firebox, please see the WatchGuard Firebox™ System User Guide, Chapter 18 titled, “Configuring the Firebox for Remote User VPN”.

Prepare the Client Computers

Every computer used as a MUVPN remote host must have the following system requirements. Further, each platform variation must also be setup properly and be configured to use the remote WINS and DNS servers on the network behind the Firebox.

System Requirements

- PC-compatible computer with Pentium processor or equivalent
- Compatible operating systems and minimum RAM:
 - Microsoft Windows 98: 32 MB
 - Microsoft Windows ME: 64 MB
 - Microsoft Windows NT 4.0 Workstation: 32 MB
 - Microsoft Windows 2000 Professional: 64 MB
- 10 MB hard disk space
- Native Microsoft TCP/IP communications protocol
- Microsoft Internet Explorer 4.0 or later
- An Internet Service Provider account
- A Dial-Up or Broadband (DSL or Cable modem) Connection

The Mobile User VPN Adapter, which supports L2TP, installs only if these network components are already installed on your computer:

- Windows 98/ME: Dial-Up Networking
- Windows NT: Remote Access Server (RAS)

If these components are not installed, follow these instructions:

Installing Remote Access Server on Windows NT

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
- 2 Select the **Services** tab.
- 3 Click the **Add** button.
- 4 Select **Remote Access Services** from the list, then click the **OK** button.
- 5 Enter the path to the Windows NT install files or insert your system installation CD, then click the **OK** button.
The Remote Access Setup dialog box appears.
- 6 Click the **Yes** button to add a RAS capable device and enable you to add a modem.
- 7 Click the **Add** button and complete the Install New Modem wizard

NOTE

If there is no modem installed, you can enable the **Don't detect my modem; I will select it from a list** checkbox then add a Standard 28800 modem.

- 8 Select the modem added in the last step in the Add RAS Device dialog box, then click the **OK** button.
- 9 Click the **Continue** button, then click the **Close** button.
- 10 Reboot your computer.

Installing Dial-up Networking on Windows 98/ME

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Add/Remove Programs** icon.
The Add/Remove Properties window appears.
- 2 Click on the **Windows Setup** tab.
The Windows Setup dialog box appears and searches for installed components.
- 3 Enable the **Communications** checkbox and click the **OK** button.
The Copying Files dialog box appears and copies the necessary files.
- 4 The Dial-Up Networking Setup dialog appears and prompts you to restart the computer. Click the **OK** button.
The computer reboots.

Windows 98/ME Platform Setup

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
The Network window appears.
- 2 Verify that Client for Microsoft Networks is installed.
If Client for Microsoft Networks is not installed, you must install it. For instructions, please see the following section of this document titled, "Installing the Client for Microsoft Networks".
- 3 Click the **Identification** tab.
- 4 Enter a name for the remote client.
This must be a unique name on the remote network.
- 5 Enter the domain name you are connecting to.
This should be the same as the Logon to Windows NT domain value.

-
- 6 Enter a description for your computer (optional).
 - 7 Click **OK**. Click **OK** to close and save changes to the Network control panel.
Click **Cancel** if you do not want to save any changes.
 - 8 Reboot the machine.

Installing the Client for Microsoft Networks

From the Networks window:

- 1 Click the **Configuration** tab. Click **Add**.
The Select Network Component Type window appears.
- 2 Select **Client**. Click **Add**.
The Select Network Client window appears.
- 3 Select **Microsoft** from the list on the left. Select **Client for Microsoft Networks** from the list on the right. Click **OK**.
- 4 Select **Client for Microsoft Networks**.
- 5 Click **Properties**.
- 6 Enable the **Log on to Windows NT domain** option.
- 7 In the Windows NT Domain field, type the domain name.
For example, your domains might be sales, office, and warehouse.
- 8 Enable the **Logon and Restore Network Connections** option.

Windows NT Platform Setup

Adding a Domain Name to a Windows NT Workstation

Often remote clients need to connect to a domain behind the firewall. To do this, the remote client must be able to recognize the domains to which they belong. Adding a domain requires the installation of the Computer Browser Network Service.

Installing the Computer Browser

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
The Network dialog box appears.
- 2 Click the **Services** tab.
- 3 Click **Add**.

- 4 Select **Computer Browser**.
- 5 Browse to locate the installation directory. Click **OK**.
- 6 Reboot the workstation.

Adding a New Domain

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
The Network dialog box appears.
- 2 Click the **Protocols** tab.
- 3 Select **Computer Browser**. Click **Properties**.
- 4 Add the remote network domain name.
You can add multiple domain names during the same configuration session.
- 5 Click **OK**.
- 6 Reboot the workstation.

Windows 2000 Platform Setup

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Network and Dial-up Connections**, then select the Dial-up connection you use to access the Internet.
The connection window appears.
- 2 Click on the **Properties** button.
- 3 Select the **Networking** tab.
- 4 Verify that the following components are present and enabled:
 - Internet Protocol (TCP/IP)
 - File and Printer Sharing for Microsoft Networks
 - Client for Microsoft Networks

If these components are not present they will need to be installed.

Installing the Internet Protocol (TCP/IP) Network Component

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Network and Dial-up Connections**, then select the Dial-up connection you use to access the Internet.
The connection window appears.

-
- 2 Click on the **Properties** button.
 - 3 Select the **Networking** tab and then click the **Install** button.
The Select Network Component Type window appears.
 - 4 Double click the **Protocol** network component.
The Select Network Protocol window appears.
 - 5 Select the **Internet Protocol (TCP/IP)** Network Protocol and then click the **OK** button.

Installing the File and Printer Sharing for Microsoft Networks

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Network and Dial-up Connections**, then select the Dial-up connection you use to access the Internet.
The connection window appears.
- 2 Click on the **Properties** button.
- 3 Select the **Networking** tab and then click the **Install** button.
The Select Network Component Type window appears.
- 4 Double click the **Services** network component.
The Select Network Service window appears.
- 5 Select the **File and Printer Sharing for Microsoft Networks** Network Service and then click the **OK** button.

Installing the Client for Microsoft Networks Network Client

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Network and Dial-up Connections**, then select the Dial-up connection you use to access the Internet.
The connection window appears.
- 2 Click on the **Properties** button.
- 3 Select the **Networking** tab and then click the **Install** button.
The Select Network Component Type window appears.
- 4 Double click **the Client** network component.
The Select Network Protocol window appears.
- 5 Select the **Client for Microsoft Networks** Network Client and then click the **OK** button.
- 6 Click the **Cancel** button to close the Select Network Component Type window.
- 7 Click the **OK** button to preserve the installed components.

- 8 Click the **Cancel** button to close the Dial-up connection window.

Configure the WINS and DNS Server Settings

In order for Windows file and print sharing to occur through the MUVPN tunnel, the remote host computer must be configured to use the WINS and DNS servers on the trusted and optional networks behind the Firebox.

Windows 98/ME WINS and DNS settings

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
The Network window appears.
- 2 Select the network component **TCP/IP** ⇒ **Dial-Up Adapter**, then click the **Properties** button.
The TCP/IP Properties Information dialog box appears.
- 3 Click the **OK** button.
- 4 Click the **DNS Configuration** tab.
Verify that the Enable DNS option has been enabled.
- 5 Under the “DNS Server Search Order” heading, enter your DNS server IP address, then click the **Add** button.
If you have multiple remote DNS servers repeat this step.

CAUTION

Make certain that your DNS server on the Trusted network behind the Firebox is listed first.

- 6 Click the **WINS Configuration** tab.
- 7 Verify that the **Enable WINS Resolution** option has been enabled.
- 8 Under the “WINS Server Search Order” heading, enter your WINS server IP address, then click the **Add** button.
If you have multiple remote WINS servers repeat this step.
- 9 Click the **OK** button to close the TCP/IP Properties window.
- 10 Click the **OK** button to close the Network window.
The System Settings Change dialog box appears.
- 11 Click the **Yes** button to restart the computer and effect the changes.

Windows NT WINS and DNS settings

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
The Network window appears.
- 2 Click the **Protocols** tab.
- 3 Select the **TCP/IP** protocol and click the **Properties** button.
The Microsoft TCP/IP Properties window appears.
- 4 Click the **DNS** tab.
- 5 Click the **Add** button.
- 6 Enter your DNS server IP address in the appropriate.
If you have multiple remote DNS servers repeat the last two steps.

CAUTION

Make certain that your DNS server on the Trusted network behind the Firebox is listed first.

- 7 Click the **WINS Address** tab.
- 8 Enter your WINS server IP address in the appropriate field, then click the **OK** button.
If you have multiple remote WINS servers repeat this step.
- 9 Click the **Close** button to close the Network window.
The Network Settings Change dialog box appears.
- 10 Click the **Yes** button to restart the computer and effect the changes.

Windows 2000 WINS and DNS settings

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Network and Dial-up Connections**, then select the Dial-up connection you use to access the Internet.
The connection window appears.
- 2 Click on the **Properties** button.
- 3 Click the **Networking** tab.
- 4 Select the **Internet Protocol (TCP/IP)** component, then click the **Properties** button.
The Internet Protocol (TCP/IP) Properties window appears.

- 5 Click the **Advanced** button.
The Advanced TCP/IP Settings window appears.
- 6 Click the **DNS** tab.
- 7 Under the “DNS server addresses, in order of use” heading, click the **Add** button.
The TCP/IP DNS Server window appears.
- 8 Enter your DNS server IP address in the appropriate field, then click the **Add** button.
If you have multiple remote DNS servers repeat the last two steps.

CAUTION

Make certain that your DNS server on the Trusted network behind the Firebox is listed first.

- 9 Enable the **Append these DNS suffixes (in order)** option.
- 10 Click the **Add** button.
The TCP/IP Domain Suffix window appears.
- 11 Enter your Domain suffix in the appropriate field.
If you have multiple DNS suffixes repeat the last two steps.
- 12 Click the **WINS** tab.
- 13 Under the “WINS addresses, in order of use” heading, click the **Add** button.
The TCP/IP WINS Server window appears.
- 14 Enter your WINS server IP address in the appropriate field, then click the **Add** button.
If you have multiple remote DNS servers repeat the last two steps.
- 15 Click the **OK** button to close the Advanced TCP/IP Settings window.
- 16 Click the **OK** button to close the Internet Protocol (TCP/IP) Properties window.
- 17 Click the **OK** button to close the next window.
- 18 Click the **Cancel** button again to close the Dial-up connection window window.

Installation Requirements for Mobile User VPN

In addition to basic platform preparation, MUVPN requires the installation of the client software. For each remote host computer the network administrator must provide:

- Software installation package

The packages are located on the WatchGuard LiveSecurity site at:

www.watchguard.com/support

Enter the site using your LiveSecurity user name and password. Click the **Mobile User VPN** link.

- Configuration file

A file containing the user name, shared key, and settings that enable a remote computer to connect securely over the Internet to a protected, private computer network. The configuration file has the filename:

username.wgx

NOTE

The WatchGuard Firebox System Policy Manager also creates the prior MUVPN version configuration files: *username.exp*.

- Shared Key

In order to install the configuration file (.wgx), the user is prompted for a shared key. This key decrypts the file and imports the security policy into the MUVPN client. The key is set during the creation of the file at the Policy Manager. For instructions on creating this file, please see the WatchGuard User Guide, Chapter 18 subsection titled, "Preparing Mobile User VPN configuration files".

Install the Mobile User VPN Client

Install the MUVPN Client software on each remote host computer. The software installation packages are available from the LiveSecurity Service Web site, one with and one without the personal firewall.

The installation process consists of two steps: installing the software and setting up the client.

NOTE

In order to perform the installation process successfully, you must be logged into the remote host computer with local administrator rights.

Installing the Mobile User VPN Client Software

- 1 Copy the software installation package to the remote host computer.
- 2 Copy the end-user configuration file (.wgx) to the remote host computer's root directory.
The Policy Manager creates an end-user configuration file when you add a new user to the Firebox configuration file. For more information, please see the WatchGuard User Guide, Chapter 18 subsection titled, "Preparing Mobile User VPN configuration files".
- 3 Double-click the software installation package file.

NOTE

If for any reason you have missed a step, simply cancel the process and begin again.

- 4 The installation package welcomes you to the InstallShield Wizard. Click the **Next** button.

NOTE

During the Setup Status portion of the install procedure, the InstallShield may detect ReadOnly Files. If this occurs, click the **Yes** button for each event in order to continue the install.

- 5 The installation package again welcomes you to the InstallShield Wizard. Once more, click the **Next** button.
The Software Licence Agreement appears.
- 6 Click the **Yes** button, to accept the terms of the License Agreement and to continue with the installation.
The Setup Type window appears.
- 7 Select the type of setup, by default Typical is enabled—this is the setup recommended by WatchGuard. Click the **Next** button.
- 8 If you are installing the client on a Windows 2000 host, the InstallShield will detect the native Windows 2000 L2TP component.

The client will use this component and not need to install its own. Click the **OK** button to continue with the install.

The Select Components window appears.

- 9 Keep the default components, click the **Next** button.

The Start Copying Files window appears.

- 10 Click the **Next** button to begin copying files.

NOTE

A command prompt window will appear while the `dni_vapmp` file is installed—this is normal. When it is complete, the installation will continue.

- 11 When the InstallShield Wizard is complete, click the **Finish** button.

- 12 The InstallShield Wizard then searches for the configuration file (`.wgx`) at the computer's root directory, `c:\`, click the **Next** button. If the file was not copied to this default directory, you must use the **Browse** button to locate and select the proper folder.

- 13 The InstallShield Wizard has completed the install of the MUVPN Client, verify that the option **Yes, I want to restart my computer now** is enabled and click the **Finish** button.

The computer reboots.

CAUTION

The ZoneAlarm personal firewall may interfere with regular Local network traffic preventing access to network resources. If the remote host computer is connected to the network after reboot, this may disrupt the network logon process. If in doubt, log on to the computer locally the first time after installation.

Importing the Configuration File

Once you have restarted the machine, the WatchGuard Policy Import dialog box appears. Import the MUVPN configuration file (`.wgx`) and provide the Shared Key used to decrypt the file.

- 1 The WatchGuard Policy Import window should locate the configuration file (`.wgx`) in the directory specified during the installation.

NOTE

If the WatchGuard Policy Import tool does not locate the .wgx file, click the **Browse** button and locate the file.

- 2 Enter the Shared key in the appropriate field. Then click the **OK** button.
- 3 You have finished setting up the MUVPN client. Click **OK**.
The remote host computer is now ready to use MUVPN.

To reconfigure the MUVPN client with a new configuration file, please see the section of this document titled, "Update the Configuration File" on page 39.

NOTE

The ZoneAlarm personal firewall may immediately begin to display alerts on your Windows desktop. For more information regarding ZoneAlarm please see the section of this document titled, "The ZoneAlarm Personal Firewall" on page 19.

Connect Using the Mobile User VPN Client

The MUVPN client enables the remote host computer to establish a secure, encrypted connection to a protected network over the Internet. To do this, you must first connect to the Internet and then use the MUVPN client to connect to the protected network.

- 1 First establish an Internet connection through either Dial-Up Networking or directly through a local area network (LAN) or wide area network (WAN).

From the Windows desktop system tray:

- 2 Verify the MUVPN client status—it must be activated. If it is not, right-click on the icon and select **Activate Security Policy**.
For information on how to determine the status of the MUVPN icon, please see the following section of this document titled, "The Mobile User VPN Client Icon".

Then, from the Windows desktop:

- 3 Select **Start ⇒ Programs ⇒ Mobile User VPN ⇒ Connect**.
The WatchGuard Mobile User Connect widow appears.
- 4 Click the **Yes** button.

The Mobile User VPN Client Icon

The Mobile User VPN icon exists in the Windows desktop system tray and displays several different status images. The following lists these images and provides a brief description of each:

Deactivated



The MUVPN Security Policy has been deactivated or the Windows operating system did not start a necessary Mobile User VPN service properly and the remote host computer must be restarted (if this continues you may need to reinstall the MUVPN client).

Activated



The MUVPN client is ready to establish a secure, VPN tunnel connection.

Activated and Transmitting Unsecured Data



The MUVPN client is ready to establish a secure, VPN tunnel connection and the red bar on the right of the icon indicates that the client has begun transmitting unsecured data.

Activated and Connected



The MUVPN client has established at least one secure, VPN tunnel connection but is not transmitting data.

Activated, Connected and Transmitting Unsecured Data



The MUVPN client has established at least one secure, VPN tunnel connection and the red bar on the right of the icon indicates that the client is transmitting only unsecured data.

Activated, Connected and Transmitting Secured Data



The MUVPN client has established at least one secure, VPN tunnel connection and the green bar on the right of the icon indicates that the client is transmitting only secured data.

Activated, Connected and Transmitting both Secure and Unsecured Data

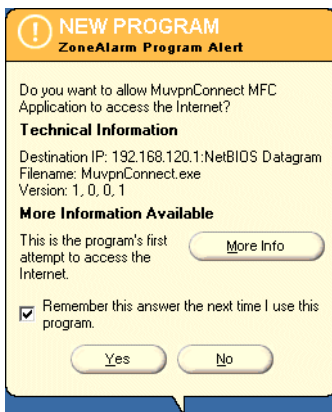


The MUVPN client has established at least one secure, VPN tunnel connection and the red and green bars on the right of the icon indicate that the client is transmitting both secured and unsecured data.

Allowing Mobile User VPN through the Personal Firewall

The ZoneAlarm personal firewall will detect the attempt of the Mobile User Connect application to access the Internet. You must allow a couple of programs associated with this application access to the internet in order to establish the VPN tunnel.

The New Program alert dialog box appears requesting access for the MuvpnConnect.exe program.



From the ZoneAlarm alert dialog box:

- 1 Enable the **Remember this answer the next time I use this program** option and click the **Yes** button.

This will enable ZoneAlarm to allow the MuvpnConnect.exe program through each time you attempt to make a MUVPN connection.

The New Program alert dialog box appears requesting access for the IreIKE.exe program.

- 2 Enable the **Remember this answer the next time I use this program** option and click the **Yes** button.

This will enable ZoneAlarm to allow the IreIKE.exe program through each time you attempt to make a MUVPN connection.

Disconnecting Mobile User VPN

The MUVPN tunnel is independent of the Internet connection. Close the MUVPN tunnels when the remote computer encounters either of the following events.

- Loses the Internet connection
- No longer needs the MUVPN tunnel


From the Windows desktop system tray:

- 1 Right-click on the Mobile User VPN Client icon.
- 2 Select **Disconnect All**.
- 3 Right-click on the Mobile User VPN Client icon and select **Deactivate Security Policy**.

The MUVPN icon will display a red slash to indicate that the Security Policy has been deactivated.

If you are using the ZoneAlarm personal firewall, deactivate this as well.

From the Windows desktop system tray:

- 1 Right-click on the ZoneAlarm icon  and select **Shutdown ZoneAlarm**.
- 2 Click the **Yes** button when prompted to quit ZoneAlarm.

Monitor the Mobile User VPN connection

There are two tools that accompany the MUVPN client which can be used to monitor your connection and diagnose problems that may occur: the Log Viewer and the Connection Monitor.

The Log Viewer

The Log Viewer displays the communications log, a diagnostic tool that lists the negotiations that occur during the MUVPN client connection.

From the Windows desktop system tray:

- 1 Right-click on the Mobile User VPN Client icon.
- 2 Select **Log Viewer**.

The Log Viewer window appears.

The Connection Monitor

The Connection Monitor displays statistical and diagnostic information for each active connection in the security policy. This module shows the actual security policy settings and the security association (SA) information established during Phase 1 IKE negotiations and Phase 2 IPSec negotiations.

From the Windows desktop system tray:

- 1 Right-click on the Mobile User VPN Client icon.
- 2 Select **Connection Monitor**.

The Connection Monitor window appears.

An icon displays to the left of the connection name:

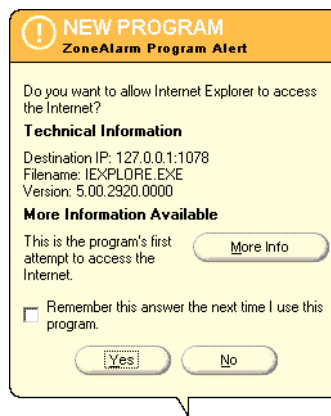
- SA indicates that the connection has only a Phase 1 IKE SA. This occurs when connecting to a secure gateway tunnel or when a Phase 2 IPSec SA fails to establish or has not been established yet.
- A key indicates that the connection has a Phase 2 IPSec SA, or both a Phase 1 and Phase 2 SA.
- A key with a black line moving below it indicates that the client is processing secure IP traffic for that connection.
- When there is a single Phase 1 SA to a gateway that is protecting multiple Phase 2 SAs, there will be a single Phase 1 connection with the SA icon and individual Phase 2 connections with the key icon displayed above that entry.

The ZoneAlarm Personal Firewall

A personal firewall is a barrier between your computer and the outside world. The computer is most vulnerable at its doors, called ports. Without ports, no connection to the Internet is possible.

ZoneAlarm protects these ports by following a simple rule: Block all incoming and outgoing traffic unless you explicitly allow it for trusted programs.

When using ZoneAlarm, you often see Program Alert dialog boxes similar to the image below.



This alert appears whenever one of your programs (in this example, Internet Explorer) attempts to access the Internet or your local network. This powerful feature means no information leaves your computer unless you give it permission.

If you enable the “Remember the answer each time I use this program” checkbox you will only have to answer this question once for each program.

ZoneAlarm Features

The ZoneAlarm personal firewall provides a brief tutorial of the product immediately after installation of the MUVPN client. Carefully read each step to familiarize yourself with the application.

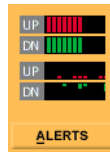
There are five buttons on the ZoneAlarm personal firewall panel. These are described in detail below.

The Alerts Panel

The Alert messages generated by ZoneAlarm contain information on what ZoneAlarm is blocking.

Up and Down Graphs

Notice the two sets of UP and DN (Up and Down) graphs on the ZoneAlarm Panel. Whenever data is being sent to the Internet, red bars are displayed inside the two UP graphs. Whenever data is being received, green bars are displayed inside the DN graphs. If there is no activity to or from the Internet, ZoneAlarm will display "ZA" on a red and yellow background.




- The two graphs in the top portion of the icon display Internet traffic as it occurs.
- The two graphs in the lower portion of the icon display a chronological history of Internet traffic as it is generated on your machine.
- Whenever red or green flashing bars appear in the Alerts icon, the application receiving or sending traffic is shown as a blinking icon inside the Programs icon.

NOTE

You might also notice traffic being displayed when you are not on the Internet. This is local broadcast traffic from your computer.

Expanded Alert Panel

Click on the  button to display the entire Alerts panel.

At the top of the panel, Today's Summary shows the total amount of data sent and received by all applications. The middle portion of the panel details Current Alerts. In the Alert Settings area, at the bottom of the panel, there are options to display and save alerts.



Pressing the “More Info” button launches the Zone Labs Alert Analyzer Web page which provides additional information on traffic blocked by ZoneAlarm.

The Lock Panel

The purpose of the lock is to block all network activity inbound and outbound from your computer. Therefore, only use the lock during extended inactivity of your PC.

A locked or unlocked padlock is displayed in the middle of the icon. To immediately turn Internet access on or off for all the applications installed on your machine that are not set to bypass the lock, click directly on the padlock.




- When the bar below the Lock button is green, the Internet Lock is not on. This means that ZoneAlarm is allowing Internet traffic in and out of your computer.

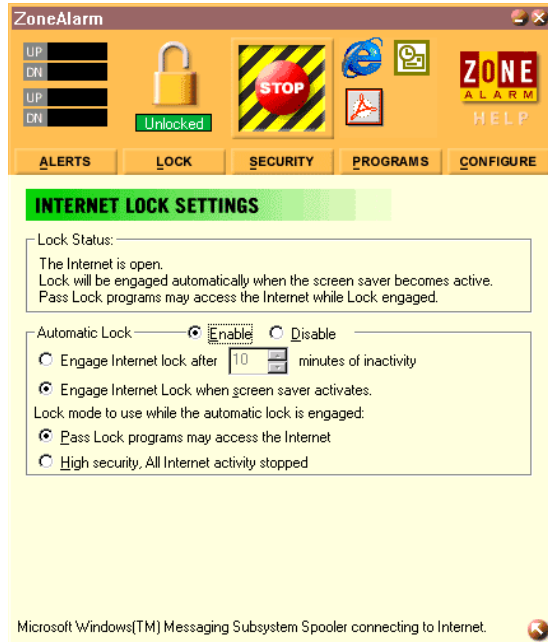
If the bar displays a countdown timer, this is the time remaining before the Automatic Lock will engage.



- When the bar is red, the lock is closed and no Internet traffic is allowed. When the lock is closed, the countdown timer counts upwards, showing the amount of time the lock has been active.

Expanded Lock Panel

Click on the  button to display the entire Lock panel.



The Automatic Lock will activate at whatever set intervals you select. You can program the Automatic Lock to activate in the following situations:

- Whenever your computer has not been used for a preset number of minutes
- Whenever the screen saver takes control of your desktop

NOTE

If Internet access is locked when the screen saver activates, it will be unlocked when the screen saver is deactivated.

The option “Pass Lock programs may access the Internet” allows Internet activity for applications that have been given rights to bypass the lock. Using this bypass feature, you can allow programs like your email client to check for mail during intervals when the Automatic Lock is in effect for all your other applications.

The High Security setting will *stop* all applications' Internet activity regardless of the program's access settings. Please see the section of this document titled, "The Programs Panel" for more information.

Undoing an Inactivity Lock

If you have activated the Automatic Lock using the minutes-of-inactivity option, unlock the lock by clicking on the padlock inside the Lock icon. After clicking on the padlock to deactivate the lock, the bar under the padlock will be set to green. This means that the lock is no longer stopping Internet traffic.

The Stop Button

Clicking on the STOP button immediately stops *all* network traffic. This includes local traffic as well, regardless if you are on a LAN, WAN, or stand-alone workstation. The only reason to use this button is if you are monitoring activity and encounter a compromise in progress.



The STOP button overrides the Pass Lock settings in the Programs panel. This is useful for stopping Trojan horses and other malicious programs that want to gain access to the Internet from your PC. To reactivate Internet access, press the stop button again.

NOTE

Using the emergency stop button completely cuts off connections to the Internet. Connections and data transfer by all programs on your computer must be restarted.

The Security Panel

The Security panel is used to regulate ZoneAlarm's protection levels.

The Local and Internet Zone each have a security level selector, that you drag up and down to change the security level. Local Zone security is displayed in green, and Internet Zone security in blue.

The default security settings are *medium* for the Local Zone and *high* for the Internet Zone.

For all three security levels, the application privileges in the Program panel are enforced. The following is a description of the three security levels:

Low

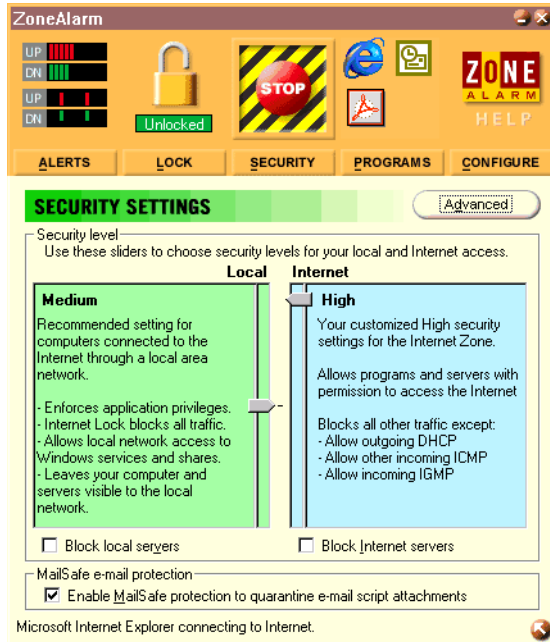
This is the minimal security setting. The Internet Lock feature allows only application traffic, not server traffic (that is, traffic outbound from the computer but not inbound from the network). All local network access to and from your computer and server applications are allowed, such as Windows file and print shares.

Medium

This is the recommended setting for computers connected to the Internet through a LAN or WAN. The Internet Lock feature blocks *all* traffic. All local network access to and from your computer and server application is allowed, such as Windows file and print shares.

High

This is the maximum security setting. The Internet Lock feature blocks *all* traffic. All local network access to and from your computer and server application is blocked, such as Windows file and print shares. All ports not in use are hidden.



Use the block servers checkbox for each zone to prevent all programs from acting as servers for that zone. By checking this option, no application will be allowed to listen for incoming connections in that zone, even if you've checked the Allow Server option in the Programs panel.

Definition of Zones

ZoneAlarm divides traffic into two separate zones: the Local Zone and the Internet Zone.


The purpose of the Local Zone is to enable ZoneAlarm to recognize what you as the user, deem as permissible traffic.

The Local Zone is made up of the computers and resources you have defined as trusted. These are usually resources on your local network but they can include any resource of your choosing. Use the Advanced button on the Security panel to define and modify the components of the Local Zones.

The members of the Internet Zone are defined as all computers and addresses you have not included in your trusted Local Zone for protection.

Members of the Local Zone can include hosts, Web sites, trusted IP Addresses, IP Subnets, and IP Ranges.

Configuring the Local Zone

Click on the  button in the Security panel to display the Local Zone Properties.

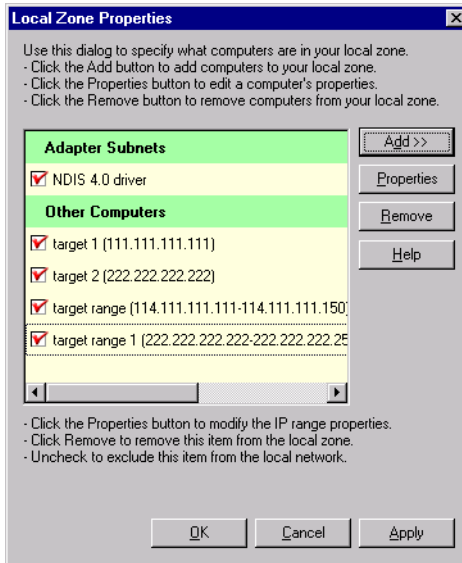
Use the Local Zone Properties to add the following:

- Web sites
- IP addresses or ranges of IPs
- Subnets

Click the Add button to add any of these elements and the Remove button to remove items from your Local Zone list. Click on the Properties button to modify the name or IP address of any element of your Local Zone properties.

The Adapter Subnets section lists all the Network Interface Cards (NICs) on your machine. Checking an adapter automatically adds the network adapter's local subnet to the Local Zone.

If you are on a local area network, checking an adapter automatically adds any computers and other devices such as printers using that subnet to your Local Zone. On a LAN or WAN using multiple subnets, you would need to add these individually.



To add items to the Local Zone, follow these instructions:

- 1 At the Security panel, click the **Advanced** button.
The Local Zone Properties window appears.
- 2 Click **Add** and select Host/Site (where you have the URL of the remote server Web site rather than the IP address), IP address, IP Range or Subnet.
- 3 Under Description, enter a name for the entry. This description can be anything and has no bearing on functionality. It is intended to help you distinguish multiple entries in the Local Zone.
- 4 Enter the name of the Host/Site, IP Address, IP Range, or Subnet.
For example, www.addhostsitesite.com or 10.10.10.1
- 5 Click the **OK** (or **Next** if adding a Host/Site) button.
- 6 Click **Finish** (if adding a Host/site).
- 7 Click the **OK** button to close the Local Zone Properties window.

NOTE

The MUVPN client should add the VPN destinations contained within the configuration file (.wgx) to the Local Zone by default.

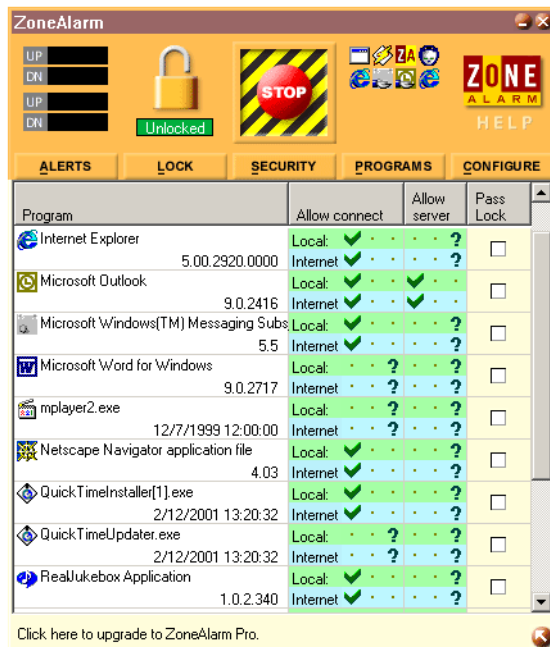
The Programs Panel

The programs panel displays programs that have attempted to access the Internet.

The extended portion of the Programs panel is the Program List. This is the list of programs installed on your machine that have attempted to connect to the Internet. Use the checkboxes in this panel to control the connection behavior of any program on the list or to specify each program's access rights for the Local Zone or the Internet Zone.

The same functions are available by bringing up the popup menu by right-clicking on a program name in the Program list.

In the Program List, the Allow server column allows you to control which applications can perform server functions. The Allow connect column allows you to control which applications make outgoing connections to the Internet or the Local Zone. Run your mouse pointer over the Programs List or right-click on an entry in the list to see more statistics.



Using the Panel

Go to the Allow connect column in the main body of the panel to change a program's permissions. Click directly on the dots within the column to change the access level.



In the same way, you can change the settings in the Allow server column.

- The question mark indicates that ZoneAlarm will prompt you each time that particular program attempts to pass traffic to or from the either the Internet or Local zones.



- The checkmark indicates that ZoneAlarm will allow that program access to the selected zone.



- The red X indicates that ZoneAlarm will deny that program access to the selected zone.



- The column labeled “Allow connect” is for a program which is attempting to make a connection out to the Internet.
- The column labeled “Allow server” is for a program which is attempting to make a connection in to your computer.
- The column labeled “Pass Lock” allows an exception to the Internet lock feature.


In the Program column, the program's name and version number are displayed. Run your mouse over the program name to see more statistics:

- Product name
- The name of the file used to access the Internet
- The location of the file
- Product version
- Creation date and file size

See the section of this document titled, “Allowing Traffic through ZoneAlarm” for more information on allowing a few common applications and all of their necessary programs through the ZoneAlarm personal firewall.

The Configuration Panel

Use the configuration panel to set the basic operational characteristics for ZoneAlarm.

Click the  button to display the Configuration panel. This button is located directly below the Help button in the top right corner of ZoneAlarm. Use the checkboxes and buttons in the Configuration Panel to determine the following:

- ZoneAlarm should be displayed on top of other applications on your computer screen when Internet activity is selected.
- The Desk Band Tool bar should be displayed (applies to Windows 98 and NT 4 only).
- ZoneAlarm should load when you start your computer.
- To check for product updates.
- To change the registration information you've submitted to Zone Labs.



The first checkbox on the Configuration Panel is On top during Internet activity. This checkbox controls whether or not ZoneAlarm will be displayed *on top* of other applications whenever Internet activity is detected.

The Load ZoneAlarm at Startup checkbox is selected by default. This causes ZoneAlarm to be loaded when you start your computer. If you disable this checkbox, Internet traffic monitoring will not begin until you start ZoneAlarm on your machine.

NOTE

The ZoneAlarm personal firewall may interfere with regular Local network traffic. Please see the troubleshooting item in this document titled, "Why am I not prompted for my user name and password when I turn my computer on?"

Older versions of Windows NT (those without the Windows Shell Update) allow you to choose a "Show shell toolbar" option. Under newer

versions and Windows 98/ME or Windows 2000, this option is part of the Windows Shell.

The Check for update button contacts the web for ZoneAlarm product updates.

The Change Registration button allows you to review and change your ZoneAlarm registration information

Frequently Asked Questions about ZoneAlarm

What is Internet Traffic?

ZoneAlarm keeps an eye on all Internet traffic.

Internet traffic includes all data movement to and from the Internet. It also includes all connection attempts from your machine to the Internet and vice versa.

The ZoneAlarm personal firewall only stops undesired traffic. When it does stop an instance of traffic, ZoneAlarm will issue an alert. The alert can be displayed and stored in a number of places. Data movement and connection attempts that are allowed according to your rules in ZoneAlarm, will be allowed to pass through the firewall.

What is an Internet Alert?

An alert is basically a blocked Internet connection. When ZoneAlarm blocks some kind of inbound or outbound Internet traffic, an alert is produced based on the rules you've set up in the various ZoneAlarm panels.

By going to the Alerts panel, you can easily find out the basic information behind an alert.

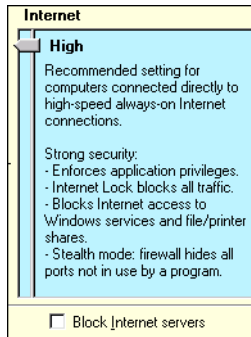
What Will ZoneAlarm Block?

What ZoneAlarm blocks is the result of how selections are made in ZoneAlarm panels in these two ways:

- Default settings that were installed with the product that you did not change.
- Modifications made to those settings by you or your system administrator.

The higher the security setting in a zone, the more ZoneAlarm will block. In the Security panel, if you allow overall security for the Internet Zone to be set to high, the firewall will block, and

create an alert, for the three events shown in the lower part of the example below.



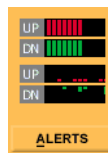
What Are the Red and Green Traffic Indicators

The most visible Internet traffic indicators are the red and green bars you can see at any time inside the first box on the left side of the DeskBand Toolbar.



Red bars indicate data being sent; green bars indicate data being received. These indicators don't indicate alerts or illegal traffic, but simply that Internet traffic is occurring.

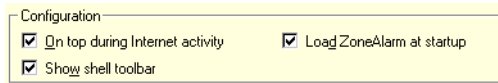
When you open the product, you see a larger version of these indicators on the Alerts icon:



Whenever red or green flashing bars appear in the Alerts icon, the application receiving or sending traffic is shown as a blinking icon inside the Programs icon.

How Do I View My Internet Traffic?

If you really want to see Internet traffic every single time it occurs, make sure the first checkbox below, located on the Configuration panel, is enabled.

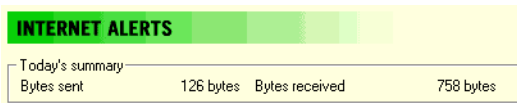


This means that, in addition to being able to view the red and green bars, you will also see the main ZoneAlarm panel displayed on top of all the other applications on your desktop.

This will make it obvious that Internet traffic is occurring. Since so much Internet traffic can occur when you have a live Internet connection, many ZoneAlarm users disable this checkbox and rely on the red and green bars only.

How Do I Know How Many Bytes Are Sent and Received?

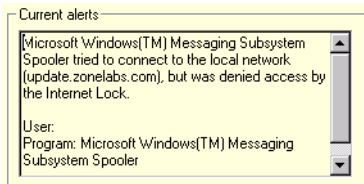
About Internet traffic, you can always view how many bytes have been sent to your PC and how many have been received since you launched ZoneAlarm. These statistics are available at the top of the Alerts panel as shown below.



Why Did I Get That Alert?

Just below the Bytes received area in the Alerts panel, statistics are always available immediately after your ZoneAlarm personal firewall detects an Internet connection attempt that it is being blocked by the firewall rules you've set up throughout ZoneAlarm.

The example below shows that a connection attempt by Internet Explorer was blocked.



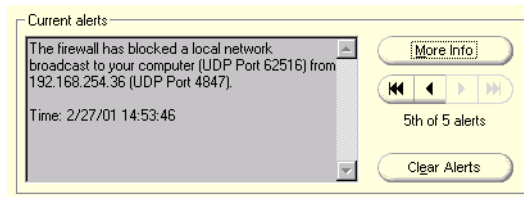
A number of rules could be responsible for this alert. One possibility is that, in the Allow connect column of the Programs

panel, you have established a rule to block Internet Explorer's access to the Zone where the IP address mentioned in the alert. In this case, the IP address would be in the Internet zone, because the Red X is in the Internet Zone area.



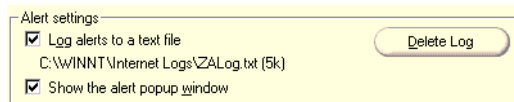
How Do I Get More Info about a Particular Alert

Clicking on the More Info button, located to the right of the alert description, gives you access to the Alert Analyzer, located on the Zone Labs web site.



How Do I Control ZoneAlarm for Displaying Alerts?

The area at the bottom of the Alerts panel allows you to control whether you want the Alert Log to be created, and whether or not you want alert popups to be displayed each time there is an alert.

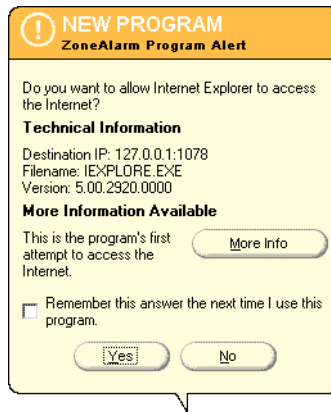


If you enable the second checkbox, you'll get a display like the example below each time firewall rules trigger an alert.



Allowing Traffic through ZoneAlarm

When an application requires access through the ZoneAlarm personal firewall, a Program Alert will be displayed on the Windows desktop informing the user which particular program needs access. Often, the program associated with the application is not readily indicative of the application the user is attempting to execute.



In the example above, the Internet Explorer Web browser application has been launched and is attempting to access the users home page. The program which actually needs to pass through the firewall is "IEXPLORE.EXE".

In order to allow this program access each time the application is executed, enable the **Remember the answer each time I use this program** checkbox.

Here is a list of a few essential programs which will need access through the ZoneAlarm personal firewall in order to operate some important applications.

Programs Which *Must* Be Allowed


<i>MUVPN client</i>	IreIKE.exe MuvpnConnect.exe
<i>MUVPN Connection Monitor</i>	CmonApp.exe
<i>MUVPN Log Viewer</i>	ViewLog.exe

Programs Which *May* be Allowed

<i>MS Outlook</i>	OUTLOOK.exe
<i>MS Internet Explorer</i>	IEXPLORE.exe
<i>Netscape 6.1</i>	netscp6.exe
<i>Opera Web browser</i>	Opera.exe
<i>Standard Windows network applications</i>	lsass.exe services.exe svchost.exe winlogon.exe

Shutting Down ZoneAlarm

From the Windows desktop system tray:

- 1 Right-click on the ZoneAlarm icon  and select **Shutdown ZoneAlarm**.
The ZoneAlarm dialog box appears.
- 2 Click the **Yes** button when prompted to quit ZoneAlarm.

Uninstalling ZoneAlarm

From the Windows desktop:

- 1 Select **Start** ⇒ **Programs** ⇒ **Zone Labs** ⇒ **Uninstall ZoneAlarm**.
The Confirm Uninstall dialog box appears.
- 2 Click the **Yes** button.
The ZoneLabs TrueVector service dialog box appears.

- 3 Click the **Yes** button to continue with uninstalling the TrueVector service and disable its Internet Security features.
The Select Uninstall Method window appears.
- 4 Verify that **Automatic** is selected and then click the **Next** button.
- 5 Click the **Finish** button to perform the uninstall.

NOTE

The Remove Shared Component window may appear. During the initial installation of ZoneAlarm, some files were installed that could be shared by other programs on the system. Click the **Yes to All** button to completely remove all of these files.

- 6 The Install window appears and prompts you to restart the computer. Click the **OK** button to reboot your system.

Update the Configuration File

At some point, it may become necessary to reconfigure the MUVPN Security Policy configuration file (.wgx).

For example:

- The shared key changes
- The network configuration changes
- The remote host computer is transferred to a new end-user

First, use the Policy Manager to edit and create a new end-user MUVPN configuration file (.wgx). For more information, please see the WatchGuard Firebox System User Guide, Chapter 18 subsection titled, "Modifying an existing Mobile User VPN entry".

From the remote host computer:

- 1 Locate and run the configuration file (.wgx) file.

NOTE

If the WatchGuard Policy Import tool does not prompt you with the .wgx file to import, click the **Browse** button and locate the file.

-
- 2 Enter the Shared key in the appropriate field. Then click the **OK** button.
 - 3 You have finished updating the MUVPN client. Click **OK**.
The remote host computer is now ready to use MUVPN. The Security Policy is automatically activated.

Uninstall the Mobile User VPN Client

At some point, it may become necessary to completely uninstall the MUVPN client. WatchGuard recommends a complete uninstall using the Windows Add/Remove Programs tool.

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**.
The Control Panel window appears.
- 2 Double click on the **Add/Remove Programs** icon.
The Add/Remove Programs window appears.
- 3 Select **Mobile User VPN** and click on the **Change/Remove** button.
The InstallShield Wizard window appears.
- 4 Select **Remove** and click the **Next** button.
The Confirm File Deletion dialog box appears.
- 5 Click the **OK** button to completely remove all of the components.

NOTE

A command prompt window will appear while the `dni_vapmp` file is uninstalled—this is normal. When it is complete the process will continue.

- 6 Click the **Yes** button to delete the Security Policy Personal Certificates and Private/Public Keys.
The InstallShield Wizard window appears.
- 7 Verify that the option **Yes, I want to restart my computer now** is enabled and click **Finish**.
The computer will reboot.

NOTE

The ZoneAlarm personal firewall settings are preserved under the following default directories.

Windows 98: c:\\windows\\internet logs\
 Windows NT and 2000: c:\\winnt\\internet logs\\

If you wish to disregard these settings, delete the contents.

- 8 When the computer has restarted, select **Start** ⇒ **Programs**.
- 9 Right-click on **Mobile User VPN** and select **Delete** to remove this selection from your Start Menu.

Troubleshoot Tips for Mobile User VPN

WatchGuard maintains a knowledgebase on our Web site, including an In-Depth FAQ section on configuring and using the MUVPN client. This is available at:

www.watchguard.com/support

A few of the most common issues found in installing, configuring, and using the MUVPN client are described below.

My computer is hung up just after installing the MUVPN client...


This is most likely due to either the ZoneAlarm personal firewall application interfering with regular Local network traffic or the MUVPN client is active and is unsuccessfully attempting to create VPN tunnels.

When the MUVPN client is not in use, ZoneAlarm should be shutdown and the client deactivated.

From the Windows desktop system tray:

- 1 First, reboot your computer
- 2 Right-click on the Mobile User VPN Client icon.
- 3 Select **Disconnect All**.

The MUVPN Client closes all VPN tunnels.

-
- 4 Right-click on the Mobile User VPN Client icon and select **Deactivate Security Policy**.
The MUVPN icon will display a red slash to indicate that the Security Policy has been deactivated.
 - 5 Right-click on the ZoneAlarm icon  and select **Shutdown ZoneAlarm**.
The ZoneAlarm dialog box appears.
 - 6 Click the **Yes** button when prompted to quit ZoneAlarm.

I have to enter my network log in information even when I'm not connected to the network...

When you start your computer, you are prompted to enter your Windows network user name, password and domain. It is very important that you enter this information correctly, just as you would if you were at the office connected to the network. Windows stores the information for use by network adapters and networked applications. Later, when you connect to your ISP and start the MUVPN client, your computer uses the stored user name, password, and domain to connect to the company network.

I am not prompted for my user name and password when I turn my computer on...

This is most likely due to the ZoneAlarm personal firewall application. This program is very good at what it does: keeping your computer secure from unauthorized incoming or outgoing traffic. Unfortunately, it may block your computer from broadcasting its network information thereby preventing the machine from sending the necessary login information. You should be certain to shut down ZoneAlarm each time you disconnect the MUVPN connection.

Is the Mobile User VPN tunnel is working...

The Mobile User VPN client icon, which appears in the Windows desktop system tray once it has been launched, will display a key within the icon once the client has connected.

To test the connection, ping a computer on your company network.

- Select **Start** ⇒ **Run**. Type ping and the IP address of a computer on your company network.

My mapped drives have a red X through them...

Windows 98/ME, NT, and 2000 verifies and maps network drives automatically when the computer starts. Because there is no way for you to establish a remote session with the company network before the computer actually starts, drive mapping fails during the boot process and a red X appears on the drive icon. Establish a MUVPN tunnel and open the network drive. The red X should disappear.

How to map a network drive

Due to a Windows operating system limitation, mapped network drives disappear when you work remotely. To remap a network drive from the Windows desktop:

- 1 Right-click on **Network Neighborhood**.
- 2 Select **Map Network Drive**.
The Map Network Drive dialog box appears.
- 3 Use the drop list to select a drive letter.
Either use the drop list or type a network drive path. For example:
`\\techsupport\share2\rodolfo`
- 4 Click **OK**.

The mapped drive appears in the My Computer window. Even if you enable the "Reconnect at Logon" checkbox, the mapped drive will not appear the next time you start your computer unless it is physically connected to the network.

I sometimes get prompted for a password when I am browsing the company network...

Due to a Windows networking limitation, remote user virtual private networking products only allow access to a single network domain. If your company is large enough to require subnetting (multiple networks connected together), you will only be able to browse your own domain. Attempts to access other domains will result in a password prompt. Unfortunately, even providing the correct information will not open these additional networks.

It takes a *really* long time to shut down the computer after using Mobile User VPN...

If you open and browse a mapped network drive during a MUVPN session, the Windows operating system waits for a signal from the network before it times out and completes the shut down cycle.

I lost the connection to my ISP, and now I can't use the company network...

If you lose Internet connection long enough, MUVPN also loses the secure tunnel. Follow the steps to close the tunnel. Then connect to the Internet and restart the MUVPN client.

No matter what I do, I can't use the company network...

There may be a problem with the configuration file (.wgx) or shared passwords.

Copyright and Patent Information

Copyright© 1998 - 2001 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, Firebox, Mobile User VPN, and MUVPN are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and other countries. This product is covered by one or more pending patent applications.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT® and Windows® 2000 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks and tradenames are the property of their respective owners. Printed in the United States of America.

Part No: 1200016