

Copyright and Patent Information

Copyright© 1998 - 2002 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

WatchGuard® Mobile User VPN Client End User Brochure—Windows XP

WatchGuard Mobile User VPN (MUVPN) client version 6.0 creates a secure tunnel between a remote computer and a company network over the Internet. In other words, you can connect to the Internet from home or on the road and then communicate safely and security with your company network to read mail, browse Network Neighborhood, or access shared files.

What do I need?

Every computer used as a MUVPN client remote computer *must* have the following requirements.

System Requirements

- PC-compatible computer with minimum 233 MHz Pentium processor or equivalent
- Minimum RAM for Microsoft Windows XP: 64 MB
- Minimum 1.5 GB hard disk space
- Native Microsoft TCP/IP communications protocol
- Ethernet for network connections
- Microsoft Internet Explorer 5.0 or later
- An Internet Service Provider account
- A Dial-Up or Broadband (DSL or Cable modem) Connection

MUVPN client requirements

To install and use the MUVPN client, you *must* receive the following from your network administrator:

MUVPN installation file

Either a `Muvpn.exe` or `MuvpnLite.exe` file.

The end-user profile

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 end-user profile has the filename: `username.wgx`

Two certificates files—if you are authenticating by way of certificates.

These are the `.p12` file, an encrypted file containing the certificate, and the `ca.cert.pem` file, which contains the root (CA, or Certificate Authority) certificate.

Shared Key

In order to install the end-user profile (the `.wgx` file), the user is prompted for a shared key. This key decrypts the file and imports the security policy into the MUVPN client.

NOTE

Write the shared key down and keep it in a secure place as it will be needed during the final steps of the installation process.

Username and Password—if you are authenticating by way of Extended Authentication.

These are used once a connection is made to authenticate you as a legitimate user.

Preparation

Network configurations *must* be prepared and set up to use the remote WINS and DNS servers on the network behind the Firebox.

However, if you are using the MUVPN client virtual adapter, the WINS and DNS settings are *not* configured on the client computers, but rather on the Firebox by your network administrator.

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.

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.

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...

The Windows operating system verifies and maps networks 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.

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

From the Windows desktop:

- 1 Select **Start** ⇒ **Control Panel** ⇒ **Network Connections**, then select the connection you use to access the Internet.
The connection window appears.
- 2 Click 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** ⇒ **Control** ⇒ **Network Connections**, then select the connection you use to access the Internet.
The connection window appears.
- 2 Click 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** ⇒ **Control** ⇒ **Network Connections**, then select the connection you use to access the Internet.
The connection window appears.
- 2 Click 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

From the Windows desktop:

- 1 Select **Start** ⇒ **Control** ⇒ **Network Connections**, then select the connection you use to access the Internet.
The connection window appears.
- 2 Click 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.

Configuring the WINS and DNS settings

From the Windows desktop:

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

NOTE

The ZoneAlarm personal firewall settings are preserved under the following default directory, `c:\windows\internet logs\`. If you wish to disregard these settings, delete the contents.

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

Troubleshooting Tips

WatchGuard maintains a knowledge base 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 the Mobile User VPN client icon.
- 3 Select **Disconnect All**.
The MUVPN client closes all VPN tunnels.
- 4 Right-click 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 the ZoneAlarm icon and select **Shutdown ZoneAlarm**.
The ZoneAlarm dialog box appears.
- 6 Click the **Yes** button when prompted to quit ZoneAlarm.

Update or Uninstall the MUVPN Client

At some point, it may become necessary to either update or completely uninstall the MUVPN client.

Updating the end-user profile

From the Windows desktop:

- 1 Locate and run the end-user profile (the .wgx file) file.
If the WatchGuard Policy Import tool does not prompt you with the .wgx file to import, click **Browse** 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 computer is now ready to use MUVPN. The Security Policy is automatically activated.

Uninstalling 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 the **Add/Remove Programs** icon.
The Add/Remove Programs window appears.
- 3 Select **Mobile User VPN** and click 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.
A command prompt window will appear while the dni_vapmp file is uninstalled—this is normal. When it is complete the process will continue. The Uninstall Security Policy dialog box appears.
- 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

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 WINS 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.

Installation

In order to perform the installation process successfully, you *must* log into the remote computer with local administrator rights. The process consists of two steps: installing the MUVPN client and importing the end-user profile (.wgx) into the client.

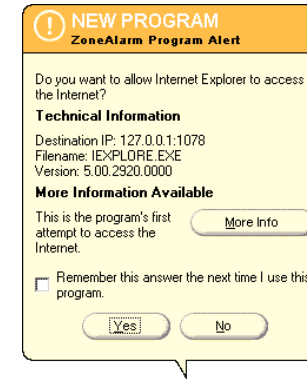
Follow these instructions to install the MUVPN client:

- 1 Copy the MUVPN installation file to the Windows desktop.
- 2 Copy the end-user profile (.wgx file) to the computer's c:\ directory.
If using certificates to authenticate, copy these files to the same directory.
- 3 Double-click the software installation package executable file.

- 4 The installation welcomes you to the InstallShield Wizard. Click the **Next** button.
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 welcomes you again. 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.
- 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 and click the **Next** button.
- 10 Click the **Next** button to begin copying files.
A command prompt window will appear while the `dn1_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 `.wgx` end-user profile at the computer's root directory, `c:\`. 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.

NOTE

The ZoneAlarm personal firewall may interfere with regular Local network traffic preventing access to network resources. If the remote 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.



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 5.x</i>	IEXPLORE.exe
<i>Netscape 6.1</i>	netscp6.exe
<i>Standard Windows network applications</i>	lsass.exe services.exe svchost.exe winlogon.exe

Disconnect the MUVPN client

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 the Mobile User VPN client icon.
- 2 Select **Disconnect All**.
The MUVPN client closes all VPN tunnels. This process does not affect your connection to the Internet. You *must* disconnect from the Internet separately.
- 3 Right-click 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 the ZoneAlarm icon and select **Shutdown ZoneAlarm**.
The ZoneAlarm dialog box appears.
- 2 Click the **Yes** button when prompted to quit ZoneAlarm.

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.

Import the end-user profile

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

- 1 The WatchGuard Policy Import window should locate the end-user profile (.wgx) in the directory specified during the installation.
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 and click the **OK** button.
- 3 You have finished setting up the Mobile User VPN client. Click **OK**.
The remote computer is now ready to use Mobile User VPN.

Connection

The MUVPN client enables the remote 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.

NOTE

You *must* disable the Windows XP Internet Connection Firewall. The MUVPN client cannot be used with this built-in software firewall.

From the Windows desktop system tray:

- 4 Verify the MUVPN client status—it *must* be activated. If it is not, right-click the icon and select **Activate Security Policy**.

Then, from the Windows desktop:

- 5 Select **Start ⇒ Programs ⇒ Mobile User VPN ⇒ Connect**.
The WatchGuard Mobile User Connect window appears.
- 6 Click the **Yes** button.

At this point, if you are using Extended Authentication, you will be prompted for the Username and Passphrase created previously on the authentication server. Enter these values and click **OK**.

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 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, MUVPN tunnel connection.

Activated and Transmitting Unsecured Data



The MUVPN client is ready to establish a secure, MUVPN 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, MUVPN tunnel connection but is not transmitting data.

Activated, Connected, and Transmitting Unsecured Data



The MUVPN client has established at least one secure, MUVPN 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, MUVPN 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, MUVPN 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.

With the ZoneAlarm 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 MUVPN 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.
- 2 The New Program alert dialog box appears requesting access for the IreIKE.exe program.
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 IreIKE.exe program through each time you attempt to make a MUVPN connection.