

WatchGuard® Mobile User VPN Administration Guide

WatchGuard Mobile User VPN 6.1



Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright© 1998 - 2002 WatchGuard Technologies, Inc. All rights reserved.
Firebox, Firebox 1000, Firebox 2500, Firebox 4500, Firebox II, Firebox II Plus, Firebox II FastVPN, Firebox III, Firebox SOHO, Firebox SOHO|tc, Firebox V100, Firebox V80, Firebox V60, Firebox V10, LiveSecurity, RapidStream, RapidCore, WatchGuard, WatchGuard Technologies, Inc., AppLock, AppLock/Web, Designing peace of mind, DVCP technology, Enforcer/MUVPN, FireChip, HackAdmin, HostWatch, LockSolid, RapidCare, SchoolMate, ServerLock, ServiceWatch, Smart Security. Simply Done., SpamScreen, Vcontroller are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries.

© Hi/fn, Inc. 1993, including one or more U.S. Patents: 4701745, 5016009, 5126739, and 5146221 and other patents pending.

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.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

RC2 Symmetric Block Cipher, RC4 Symmetric Stream Cipher, RC5 Symmetric Block Cipher, BSAFE, TIPEM, RSA Public Key Cryptosystem, MD, MD2, MD4, and MD5 are either trademarks or registered trademarks of RSA Data Security, Inc. Certain materials herein are Copyright © 1992-1999 RSA Data Security, Inc. All rights reserved.

RealNetworks, RealAudio, and RealVideo are either a registered trademark or trademark of RealNetworks, Inc. in the United States and/or other countries.

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All right reserved.

© 1995-1998 Eric Young (eay@cryptsoft). All rights reserved.

© 1998-2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OPENSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

© 1995-1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2001 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."
4. The names "mod_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.
5. Products derived from this software may not be called "mod_ssl" nor may "mod_ssl" appear in their names without prior written permission of Ralf S. Engelschall.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Apache Software License, Version 1.1
Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)." Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <<http://www.apache.org/>>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.
Part No:

WatchGuard Technologies, Inc.
Mobile User VPN Software
End-User License Agreement

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE:

This Mobile User VPN End-User License Agreement (the "AGREEMENT") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc., ("WATCHGUARD") for the Mobile User VPN Software you have purchased, which includes computer software and any separately installed components, and any updates or modifications thereto, and which may include associated media, printed materials, and online or electronic documentation (the "SOFTWARE PRODUCT"). WATCHGUARD is willing to license the SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this AGREEMENT. Please read this AGREEMENT carefully. By installing or using the SOFTWARE PRODUCT you agree to be bound by the terms of this AGREEMENT. If you do not agree to the terms of this AGREEMENT, WATCHGUARD will not license the SOFTWARE PRODUCT to you, and you will not have any rights in the SOFTWARE PRODUCT. In that case, promptly

return the SOFTWARE PRODUCT, along with proof of payment, to the authorized dealer from whom you obtained the SOFTWARE PRODUCT for a full refund of the price you paid.

1. Ownership and License. The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement and NOT an agreement for sale. All title and copyrights in and to the SOFTWARE PRODUCT (including, but not limited to, any images, photographs, animations, video, audio, music, text, and applets incorporated into the SOFTWARE PRODUCT) and any copies of the SOFTWARE PRODUCT are owned by WATCHGUARD and its licensor(s), including SafeNet, Inc. Your rights to use the SOFTWARE PRODUCT are as specified in this AGREEMENT, and WATCHGUARD retains all rights not expressly granted to you in this AGREEMENT. Nothing in this AGREEMENT constitutes a waiver of the rights of WATCHGUARD under U.S. copyright law or any other law or treaty.

2. Permitted Uses. You are granted the following rights to the SOFTWARE PRODUCT:

(A) You may install and use the SOFTWARE PRODUCT on that number of computers at any one time as you have purchased licenses to do so.

(B) To use the SOFTWARE PRODUCT on more than one computer at once, you must purchase additional licenses for the SOFTWARE PRODUCT covering each additional computer on which you want to use it.

(C) You may make a single copy of the SOFTWARE PRODUCT for backup or archival purposes only.

3. Prohibited Uses. You may not, without express written permission from WATCHGUARD:

(A) Use, copy, modify, merge or transfer copies of the SOFTWARE except as provided in this AGREEMENT;

(B) Use any backup or archival copy of the SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective;

(C) Sublicense, lend, lease or rent the SOFTWARE PRODUCT;

(D) Transfer this license to another party unless:

(i) the transfer is permanent;

(ii) the third party recipient agrees to the terms of this AGREEMENT; and

(iii) you do not retain any copies of the SOFTWARE PRODUCT; or

(E) Reverse engineer, disassemble or decompile the SOFTWARE PRODUCT.

4. Limited Warranty. WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer:

(A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase.

(B) SOFTWARE PRODUCT. The SOFTWARE PRODUCT will materially conform to the documentation that accompanies it. If the SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return the SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase, specifying the problems, and such authorized dealer will provide you with a new version of the SOFTWARE PRODUCT or a full refund, at their election.

Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ITS LICENSORS, INCLUDING SAFENET, INC., AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD OR ITS LICENSORS, INCLUDING SAFENET, INC., EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY THAT THE SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD OR ITS LICENSORS, INCLUDING SAFENET, INC., AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE SOFTWARE PRODUCT).

Limitation of Liability. WATCHGUARD'S LIABILITY AND THE LIABILITY OF ITS LICENSORS, INCLUDING SAFENET, INC., (WHETHER IN CONTRACT, TORT, OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) WITH REGARD TO THE SOFTWARE PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD OR ITS LICENSORS, INCLUDING SAFENET, INC., BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF WATCHGUARD AND ITS LICENSORS, INCLUDING SAFENET, INC., HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5. United States Government Restricted Rights. The enclosed SOFTWARE PRODUCT and documentation are provided with Restricted Rights. Use, duplication or disclosure by the U.S. Government or any agency or instrumentality thereof is subject to restrictions as set forth in DFARS 227.7202-3 (Commercial Computer Software) and DFARS 252.227-7015(b) (Technical Data-Commercial Items) -- Restricted Rights Clause at FAR 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Incorporated, 505 Fifth Avenue, South, Suite 500, Seattle, WA 98104.

6. Export Controls. You agree not to directly or indirectly transfer the SOFTWARE PRODUCT or documentation to any country to which such transfer would be prohibited by the U.S. Export Administration Act and the regulations issued thereunder.

7. Termination. This license and your right to use the SOFTWARE PRODUCT will automatically terminate in the event you (i) fail to comply with any provisions of this AGREEMENT; (ii) destroy all copies of the SOFTWARE PRODUCT in your possession, or; (iii) voluntarily return the SOFTWARE PRODUCT to WATCHGUARD. Upon termination you will destroy all copies of the SOFTWARE PRODUCT and documentation remaining in your control or possession.

8. Miscellaneous Provisions. This AGREEMENT will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire AGREEMENT between us relating to the contents of this package, and supersedes any prior purchase order, communications, advertising or representations concerning the contents of this package AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. No change or modification of this AGREEMENT will be valid unless it is in writing, and is signed by WATCHGUARD.

9. Canadian Transactions: If you obtained this SOFTWARE PRODUCT in Canada, you agree to the following: The parties hereto have expressly required that the present AGREEMENT and its Exhibits be drawn up in the English language. / Les parties aux presentes ont expressement exige que la presente conventions et ses Annexes soient redigees en la langue anglaise.

Contents

CHAPTER 1 Preparation, Installation, and Connection	1
Prepare the Remote Computers	2
System requirements	2
Windows 98/ME operating system setup	3
Windows NT operating system setup	6
Windows 2000 operating system setup	8
Windows XP operating system setup	11
MUVPN client requirements	14
Install and Uninstall the MUVPN Client	16
Update the end-user profile	18
Uninstall the MUVPN client	18
Connect and Disconnect the MUVPN Client	19
Connecting the MUVPN Client	20
The Mobile User VPN client icon	21
Allowing the MUVPN client through the personal firewall	22
Disconnecting the MUVPN client	23
Monitor the MUVPN Client Connection	24
The Log Viewer	24
The Connection Monitor	25

CHAPTER 2 The ZoneAlarm Personal Firewall	27
ZoneAlarm Features	28
Allowing Traffic through ZoneAlarm	28
Shutting Down ZoneAlarm	30
Uninstalling ZoneAlarm	30
CHAPTER 3 Troubleshooting Tips for the MUVPN Client	31
My computer is hung up just after installing the MUVPN client...	31
I have attempted to connect several times, but nothing is happening...	32
I have to enter my network log in information even when I'm not connected to the network...	32
I am <i>not</i> prompted for my user name and password when I turn my computer on...	32
Is the Mobile User VPN tunnel working...	33
My mapped drives have a red X through them...	33
How to map a network drive...	33
I sometimes get prompted for a password when I am browsing the company network...	34
It takes a really long time to shut down the computer after sing Mobile User VPN...	34
I lost the connection to my ISP, and now I can't use the company network...	34
No matter what I do, I can't use the company network...	34
Index	35

Preparation, Installation, and Connection

WatchGuard® Mobile User VPN (MUVPN)TM client uses Internet Protocol Security (IPSec) to establish a secure connection over an unsecured network from a remote computer to your protected network.

For example, the MUVPN client is installed on an employee's computer, on the road or working from home. The employee establishes a standard Internet connection and activates the MUVPN client. The MUVPN client then creates an encrypted tunnel to your company's trusted and optional networks, protected by a WatchGuard Firebox System. The MUVPN client allows you to provide remote access to your internal networks without compromising security.

For information on configuring the WatchGuard Firebox System for use with the MUVPN client, see the WatchGuard *VPN Guide*, Chapter 5 "Preparing to use MUVPN".

ZoneAlarm®, a personal firewall software application, is included as an optional feature with the MUVPN client to provide further security for your end users.

The purpose of this guide is to assist users of the WatchGuard Firebox System to set up the MUVPN client on an end-user's remote computer and to explain the features of the personal firewall.

MUVPN Brochures

Along with this guide, WatchGuard has compiled end-user documentation regarding the preparation, installation, and connection of the Mobile User VPN Client as well as the usage of the personal firewall, is available on our Web site. The documentation exists as separate brochures customized to the various Windows operating systems.

These brochures can be found on the WatchGuard Web site at:

www.watchguard.com/documentation

The rest of this chapter describes the basic tasks involved in preparing the remote computers to use the MUVPN client as well as the installation and connection procedures for the client.

Prepare the Remote Computers

The MUVPN client is only compatible with the Windows operating system. Every Windows system used as a MUVPN remote computer *must* have the following system requirements.

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
 - Microsoft Windows XP: 64 MB
- The latest service packs for each operating system are recommended, but not necessarily required.
- 10 MB hard disk space
- Native Microsoft TCP/IP communications protocol
- Microsoft Internet Explorer 5.0 or later
- An Internet Service Provider account

- A Dial-Up or Broadband (DSL or Cable modem) Connection

Additionally, in order for Windows file and print sharing to occur through the MUVPN client tunnel each Windows operating system *must* have the proper components installed and configured to use the remote WINS and DNS servers on the trusted and optional networks behind the Firebox.

NOTE

However, if you plan to use the MUVPN client virtual adapter, the WINS and DNS settings are *not* configured on the client computers, but rather on the Firebox.

Windows 98/ME operating system setup

The following networking components *must* be configured and installed on a remote computer running Windows 98/ME in order for the MUVPN client to function properly.

Configuring networking names

From the Windows desktop:

- 1 Select **Start** ⇒ **Settings** ⇒ **Control Panel**. Double-click the **Network** icon.
The Network window appears.
- 2 Verify that the Client for Microsoft Networks is installed.
If Client for Microsoft Networks is not installed, you *must* install it. For instructions, see the following section, "Installing the Client for Microsoft Networks".
- 3 Click the **Identification** tab.
- 4 Enter a name for the remote computer.
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.

Installing Dial-Up Networking

The Mobile User VPN Adapter, which supports L2TP, installs only if Dial-up Networking is already installed on your computer. If Dial-up Networking is *not* installed, follow these instructions.

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 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 box appears and prompts you to restart the computer. Click the **OK** button.
The computer reboots.

Further, Windows 98 requires that the Dial-up Networking component be updated with the 1.4 patch. Please see the Microsoft Web site to receive this free update.

Configuring the WINS and DNS settings

You *must* configure the remote computer to use the WINS and DNS servers of the trusted network behind the Firebox only if you do *not* plan to use the MUVPN client's virtual adapter.

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.

NOTE

You *must* list the DNS server on the Private network behind the Firebox 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 implement the changes.

Windows NT operating system setup

The following networking components *must* be installed and configured on a remote computer running Windows NT in order for the MUVPN client to function properly.

Installing Remote Access Services on Windows NT

The Mobile User VPN Adapter, which supports L2TP, installs only if the Remote Access Services (RAS) network component is already installed on the computer.

Follow the Windows desktop:

- 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. Windows NT requires at least one RAS device such as a modem if the RAS component is installed. If no modems are available, a dial-up networking, serial cable between two computers can be selected.

- 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.

Configuring the WINS and DNS settings

You *must* configure the remote computer to use the WINS and DNS servers of the trusted network behind the Firebox only if you do *not* plan to use the MUVPN client's virtual adapter.

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 field.
If you have multiple remote DNS servers repeat the previous three steps.

NOTE

You *must* list the DNS server on the Private network behind the Firebox 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 implement the changes.

Windows 2000 operating system setup

The following networking components *must* be installed and configured on a remote computer running Windows 2000 in order for the MUVPN client to function properly.

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 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

Install these components if they are not already present.

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 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 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** ⇒ **Settings** ⇒ **Network and Dial-up Connections**, then select the Dial-up 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

You *must* configure the remote computer to use the WINS and DNS servers of the trusted network behind the Firebox only if you do *not* plan to use the MUVPN client's virtual adapter.

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 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

You *must* list the DNS server on the Private network behind the Firebox 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.

Windows XP operating system setup

The following networking components **must** be installed and configured on a remote computer running Windows XP in order for the MUVPN client to function properly.

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

Install these components if they are not already present.

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

You *must* configure the remote computer to use the WINS and DNS servers of the trusted network behind the Firebox only if you do *not* plan to use the MUVPN client's virtual adapter.

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

You *must* list the DNS server on the Private network behind the Firebox 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.

MUVPN client requirements

In addition to basic operating system preparation, the MUVPN client requires the following, files, documentation, and passphrases.

MUVPN installation file

The installation files—one with the personal firewall (Muvpn.exe) and one without the personal firewall (MuvpnLite.exe)—are available from the WatchGuard Web site at:

www.watchguard.com/support

Enter the site using your LiveSecurity user name and password. Click the **Latest Software** link, then click **Add-ons/Upgrades** on the left side, and then the **Mobile User VPN** link.

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 your trusted network. The end-user profile has the filename:

username.wgx

The Policy Manager creates an end-user profile when you add a new MUVPN user to the Firebox. For more instructions on creating this file, see the WatchGuard *VPN Guide*, Chapter 5 “Preparing to Use MUVPN”.

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

The Policy Manager creates two files when the you select to authenticate using a certificate. These are the .p12 file, an encrypted file containing the certificate, and the cacert.pem file, which contains the root (CA or Certificate Authority) certificate. For instructions on using certificates for authentication, see the *VPN Guide*, Chapter 5, subsection “Preparing Mobile User VPN Profiles.”

For more information regarding using certificates, see the *VPN Guide*, Chapter 3, “Activate the Certificate Authority on the Firebox.”

User documentation

End-user brochures developed by WatchGuard are located on the WatchGuard Web site at:

www.watchguard.com/support

Enter the site using your LiveSecurity user name and password. Click the **Product Documentation** link and then click the **VPN** link.

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. The key is set during the creation of the file at the Policy Manager.

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.

You *must* supply the end user with the Username and Password for their authentication account. This is defined on the relevant authentication server.

For instructions on using Extended Authentication, see the *VPN Guide*, Chapter 5, subsection, “Defining an Extended Authentication Group.”

Install and Uninstall the MUVPN Client

The installation process consists of two parts: installing the client software on the remote computer and importing the end-user profile into the client.

NOTE

In order to perform the installation process successfully, you *must* log into the remote computer with local administrator rights.

Follow these steps to install the client:

- 1 Copy the MUVPN installation file to the remote computer.
- 2 Copy the end-user profile (the .wgx file) to the remote computer's root directory.
If using certificates to authenticate, copy these files to the root directory as well.
- 3 Double-click the MUVPN installation file.
If at any time during the installation process you inadvertently skip a step, simply cancel the process and begin again.
- 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 **Yes** 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.
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 detects the native Windows 2000 L2TP component. The client uses this component and does 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.
The Start Copying Files window appears.
- 10 Click the **Next** button to begin copying files.
A command prompt window appears while the `dn_i_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 end-user profile (the .wgx file) 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.

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. For more information, see Chapter 2 "The ZoneAlarm Personal Firewall" on page 27.

Importing the end-user profile

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

- 1 The WatchGuard Policy Import window should locate the end-user profile (the .wgx file) in the directory specified during the installation. If the WatchGuard Policy Import tool does not locate the .wgx file, click **Browse** 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 MUVPN client. Click **OK**.
The remote computer is now ready to use MUVPN.

For instructions on how to reconfigure the MUVPN client with a new end-user profile, see "Update the end-user profile" on page 18.

NOTE

The ZoneAlarm personal firewall may immediately begin to display alerts on your Windows desktop. For more information regarding ZoneAlarm see the Chapter 2 "The ZoneAlarm Personal Firewall" on page 27.

Update the end-user profile

At some point, it may become necessary to reconfigure the MUVPN end-user profile (the .wgx file).

For example:

- The shared key changes
- The certificate files are reissued
- The Extended Authentication account is changed to a different server. For example, from NT authentication to RADIUS.
- The network configuration changes
- The remote computer is transferred to a new end-user

First, use the Policy Manager to edit and create a new MUVPN end-user profile (the .wgx file). For more information, see the WatchGuard *VPN Guide*, Chapter 5 “Preparing to Use MUVPN”.

From the remote computer:

- 1 Locate and double-click 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.

Uninstall the MUVPN 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.

First, disconnect all existing tunnels and dial-up connections and reboot the remote computer. Then, 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**. 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 appears while the `dni_vapmp` file is installed—this is normal. When it is complete, the installation 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

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\`
Windows XP: `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.

Connect and Disconnect the MUVPN Client

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.

Connecting the MUVPN Client

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

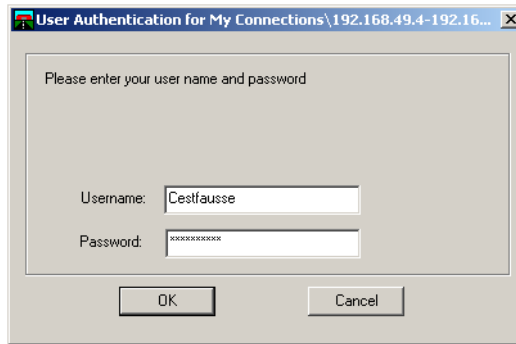
From the Windows desktop system tray:

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

Then, from the Windows desktop:

- 3 Select **Start** ⇒ **Programs** ⇒ **Mobile User VPN** ⇒ **Connect**.
The WatchGuard Mobile User Connect window appears.
- 4 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**.



For more information regarding Extended Authentication, see the *VPN Guide*, Chapter 5, subsection “Defining an Extended Authentication Group.”

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 is 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. 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. 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. 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



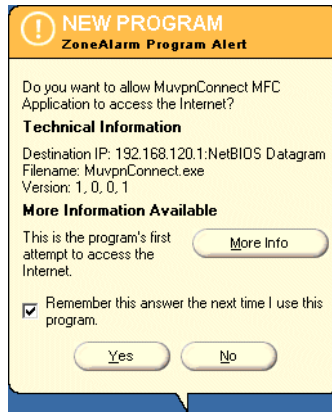
The MUVPN client has established at least one secure, MUVPN tunnel connection. The red and green bars on the right of the icon indicate that the client is transmitting both secured and unsecured data.

Allowing the MUVPN client through the personal firewall

There are a couple of programs associated with the MUVPN client, which you *must* allow through the personal firewall in order to establish the MUVPN tunnel:

- MuvpnConnect.exe
- IreIKE.exe

The personal firewall will detect the attempt of these programs to access the Internet. 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 enables 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 enables ZoneAlarm to allow the IreIKE.exe program through each time you attempt to make a MUVPN connection.

Disconnecting 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 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 displays a red slash to indicate a deactivated Security Policy.

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.

Monitor the MUVPN Client 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.

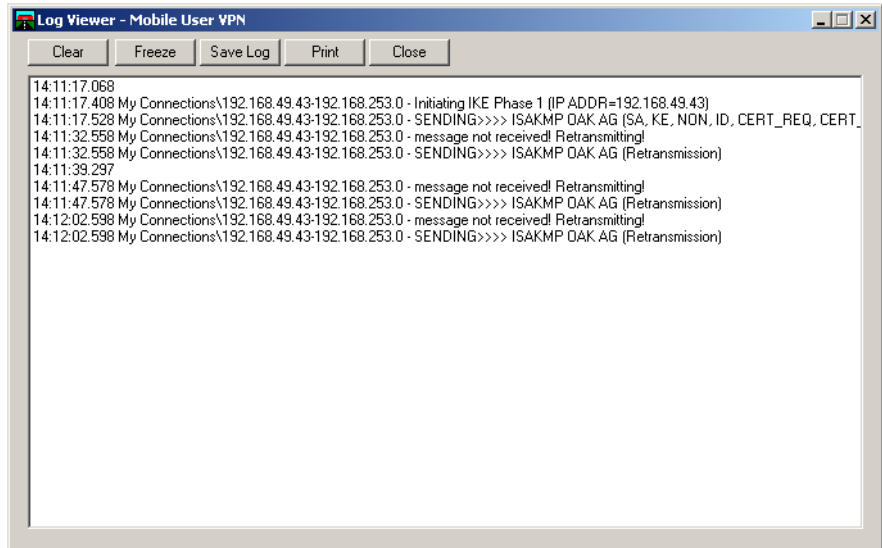
The Log Viewer

The LogViewer 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 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 the **Mobile User VPN** client icon.
- 2 Select **Connection Monitor**.
The Connection Monitor window appears.

An icon appears 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 a single Phase 1 SA to a gateway protects multiple Phase 2 SAs, there is 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.

For more information on ZoneAlarm features and configuration, please refer to the ZoneAlarm Help system. To access the Help system, select **Start =>Programs =>Zone Labs =>ZoneAlarm Help**.

Allowing Traffic through ZoneAlarm

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



In the example above, the Internet Explorer Web browser application 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 the program access each time it is executed, enable the **Remember the answer the next time I use this program** checkbox.

Here is a list of a few essential programs which 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 are installed that other programs on the system may share. 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.

Troubleshooting Tips for the MUVPN Client

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 it is because the MUVPN client is active and is unsuccessfully attempting to create VPN tunnels.

When the MUVPN client is not in use, you should shut down ZoneAlarm and deactivate the client.

First, reboot your computer, then from the Windows desktop system tray:

- 1 Right-click on the Mobile User VPN client icon and select **Deactivate Security Policy**.

The MUVPN client icon displays a red slash indicating that the Security Policy is deactivated.

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

I have attempted to connect several times, but nothing is happening...

The MUVPN client may have misloaded the end-user profile. Try reloading your security policy.

From the Windows desktop system tray:

- 1 Right-click the Mobile User VPN Client icon.
- 2 Select **Reload Policy**.
The MUVPN client reloads the end-user profile.
- 3 Now try to connect the client again.

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 and prevent the machine from sending the necessary login information. Be certain to shut down ZoneAlarm each time you disconnect the MUVPN connection.

Is the Mobile User VPN tunnel working...

The Mobile User VPN client icon, which appears in the Windows desktop system tray once it is launched, will display a key within the icon once the client is 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 **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, mobile 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 can only browse your own domain. Attempts to access other domains 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 your 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 end-user profile (the .wgx file) or shared passwords.

Index

Symbols

.p12 file 14
.wgx file 14

C

cacert.pem 14
certificates, files required if authenticating
 using 14
Client for Microsoft Networks
 installing on Windows 2000 computers 9
 installing on Windows 98/ME computers 4
Connection Monitor, monitoring MUVPN client
 through 25

E

end-user profile
 described 14
 importing 17
 updating 18

F

File and Printer Sharing for Microsoft Networks
 and Windows 2000 8
 and Windows XP 11

I

Internet Protocol (TCP/IP) Network Component
 and Windows 2000 8
 and Windows XP 11

L

LogViewer, monitoring MUVPN client
 through 24

M

Mobile User VPN. See MUVPN
MUVPN

 described 1
 disconnecting 23
 system requirements for 3
 troubleshooting 33

MUVPN client

 allowing through firewall 22
 connecting using 19
 files required to install 14
 icon for 21
 installing 14, 16
 monitoring connection for 24
 removing 18

Muvpn.exe 14

MuvpnLite.exe 14

R

Remote Access Server, installing on Windows
 NT 6

S

shared key 15
system requirements 2

T

troubleshooting tips 31

W

Windows 2000

 installing Client for Microsoft Networks on 9
 installing File and Printer Sharing for
 Microsoft Networks on 8
 installing Internet Protocol (TCP/IP) Network
 Component on 8
 WINS and DNS settings 9

Windows 98/ME

 configuring network names on 3
 installing Client for Microsoft Networks 4
 WINS and DNS settings 5

Windows NT

- installing Remote Access Server on 6
- WINS and DNS settings 7
- Windows XP
 - installing Client for Microsoft Networks on 12
 - installing File and Printer Sharing for Microsoft Networks on 11
 - installing Internet Protocol (TCP/IP) Network Component on 11
 - WINS and DNS settings 12
- WINS and DNS settings
 - on Windows 2000 computers 9
 - on Windows 98/ME computers 5
 - on Windows NT computers 7
 - on Windows XP computers 12

Z

- ZoneAlarm
 - allowing MUVPN client through 22
 - described 1
 - troubleshooting 31