

WatchGuard® Mobile User VPN Administrator Guide

WatchGuard Mobile User VPN v7.3
Revised: 09/18/2007



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 - 2007 WatchGuard Technologies, Inc. All rights reserved.

Complete copyright, trademark, patent, and licensing information can be found in the WatchGuard System Manager User Guide. You can find it online at:
<http://www.watchguard.com/help/documentation/>

All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Client Software: MUVPN 7.3
Management Software: WSM 9.1
Appliance Software: WFS 7.5 and Fireware 9.1
Document Version: 9.1-352-2836-002

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT:

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

SALES:

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

ABOUT WATCHGUARD

WatchGuard is a leading provider of network security solutions for small- to mid-sized enterprises worldwide, delivering integrated products and services that are robust as well as easy to buy, deploy and manage. The company's Firebox X family of expandable integrated security appliances is designed to be fully upgradeable as an organization grows and to deliver the industry's best combination of security, performance, intuitive interface and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of the security landscape with vulnerability alerts, software updates, expert security instruction and superior customer care. For more information, please call (206) 613-6600 or visit www.watchguard.com.

Contents

CHAPTER 1

Preparing a WFS Firebox to Use MUVPN	1
Purchasing a Mobile User VPN license	2
Adding License Keys	2
Configuring WINS and DNS Servers	2
Preparing Mobile User VPN Profiles	3
Defining a User for a Firebox Authenticated Group	3
Using Extended Authentication	6
Setting Advanced Preferences	8
Configuring Services to Allow Incoming MUVPN Traffic	9
Regenerating End-User Profiles	10
Saving the Profile to a Firebox	10
Distributing the Software and Profiles	10
Making Outbound IPSec Connections From Behind a Firebox	11
Configuring Debugging Options for MUVPN	11
Terminating Tunnels on Optional or Trusted Interfaces	12
Terminating IPSec Connections	12

CHAPTER 2

Using Fireware Policy Manager to Configure MUVPN	13
Configuring WINS and DNS Servers	13
Preparing Mobile User VPN Profiles	14
Defining an MUVPN User Group	15
Setting Advanced Preferences	21
Configuring Policies to Filter MUVPN Traffic	22
Re-creating End-User Profiles	23
Saving the Profile to a Firebox	23
Distributing the Software and Profiles	23

Additional MUVPN Topics	24
CHAPTER 3	
MUVPN Client Preparation, Installation, and Connection	27
Prepare the Remote Computers	27
Installing and Uninstalling the MUVPN Client	34
Connect and Disconnect the MUVPN Client	36
Monitor the MUVPN Client Connection	39
CHAPTER 4	
Troubleshooting Tips for the MUVPN Client	41
CHAPTER 5	
The ZoneAlarm Personal Firewall	45
ZoneAlarm Features	45
Allowing Traffic through ZoneAlarm	46
Shutting Down ZoneAlarm	47
Uninstalling ZoneAlarm	47

1

Preparing a WFS Firebox to Use MUVPN

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

MUVPN requires configuration of the Firebox® and the remote client computers. The Firebox administrator has detailed control of the client configuration through a group of settings known as an end-user profile.

MUVPN users authenticate either to the Firebox or to a separate authentication server. Authentication occurs either with shared keys or certificates.

The complete procedure for using MUVPN is documented in the rest of this guide, and in the end-user brochures distributed for specific client operating systems. This chapter describes the Firebox configuration you must do for a Firebox III or Firebox X Core that uses WFS appliance software. These procedures should be done before you use the rest of this guide.

For information on how to configure a Firebox X Core or Firebox X Peak with Fireware appliance software, see the subsequent chapter, “Using Fireware Policy Manager to Configure MUVPN,” on page 13. For information on how to configure a Firebox SOHO 6, see the *SOHO 6 User Guide*. For information on how to configure a Firebox X Edge, see the *Firebox X Edge User Guide*.



If you are creating an MUVPN tunnel to a SOHO 6 or Firebox X Edge, WatchGuard recommends that you obtain a static IP address. If you use a dynamically addressed SOHO 6 or Firebox X Edge, you must reconfigure your MUVPN client every time the address changes.

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 use of the personal firewall included with the MUVPN client. These brochures, customized separately for the supported Windows operating systems, are available on our web site at

<http://www.watchguard.com/help/documentation/>

Purchasing a Mobile User VPN license

WatchGuard® Mobile User VPN is an optional feature available for most Firebox® model lines. Although the management software automatically includes the administrative tools to configure Mobile User VPN, you must purchase a license for each installation of the client software to activate the feature.

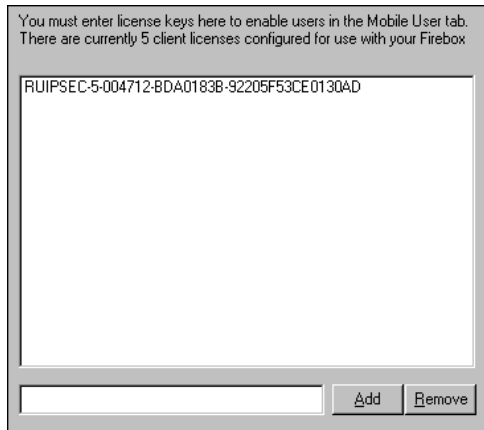
A license is available through your local reseller or at:

<http://www.watchguard.com/sales>

Adding License Keys

The first step in configuring the Firebox for MUVPN is to type the license key or keys into the Firebox configuration file. The Firebox automatically restricts the number of Mobile User VPN connections to the sum of the number of seats each license key provides. From Policy Manager:

- 1 Select **Network > Remote User**. Click the **Mobile User Licenses** tab.
The Mobile User licenses information appears as shown below.



- 2 Type the license key in the text field to the left of **Add**. Click **Add**.
The license key appears in the list of client licenses configured for use with the Firebox. Repeat the process until all your keys are added.

Encryption levels

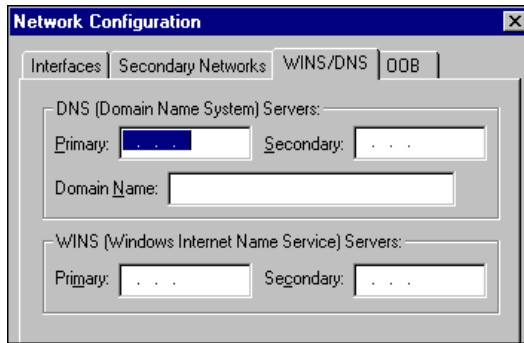
Because strict export restrictions are put on exported high encryption software, WatchGuard® System Manager is available with two encryption levels. You must make sure you download and use WatchGuard System Manager with strong encryption when you use MUVPN because the IPsec standard requires 56-bit (medium) encryption at the minimum.

Configuring WINS and DNS Servers

RUVPN and MUVPN clients rely on shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server addresses. DNS translates host names into IP addresses, while WINS resolves Net-BIOS names to IP addresses. These servers must be available from the Firebox® trusted interface.

Make sure you use only an internal DNS server. Do not use external DNS servers.

- 1 From Policy Manager, select **Network > Configuration**. Click the **WINS/DNS** tab.
The information for the WINS and DNS servers appears, as shown in the following figure.
- 2 Type the primary and secondary addresses for the WINS and DNS servers. Type a domain name for the DNS server.



Preparing Mobile User VPN Profiles

With Mobile User VPN, the network security administrator controls end-user profiles. Policy Manager is used to define the name of the end user and generate a profile with the extension .wgx. The .wgx file contains the shared key, user identification, IP addresses, and settings required to create a secure tunnel between the remote computer and the Firebox. This file is then encrypted with a key consisting of eight characters or greater which is known to the administrator and the remote user. When the .wgx file is installed in the remote client, this key is used to decrypt the file for use in the client software.

If you want to lock the profile for mobile users by making it read-only, see "Setting Advanced Preferences" on page 8.

The IPSec client allows for the deployment of the software in situations where the client does not have a static IP address, for example, with a DSL connection. This is the default profile and allows for the conversion of existing profiles (with the .exp extension) to the newer version (with the .wgx extension). New keys are generated as a part of this process; they must then be distributed to the users in the field.

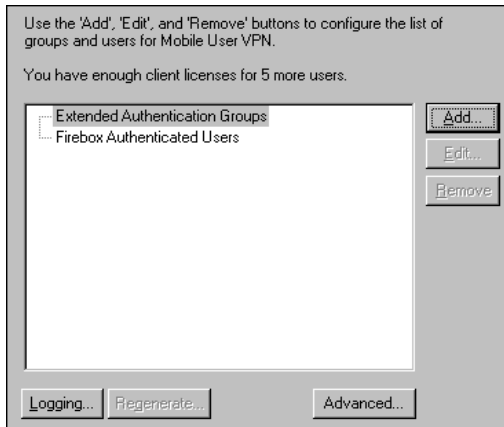
Defining a User for a Firebox Authenticated Group

You can use the Firebox® as an authentication server. If you want to add a new user who uses the Firebox to authenticate, use the following procedure to define that user. If the new user uses a third-party

Defining a User for a Firebox Authenticated Group

authentication server for authentication, use the procedure described in “Using Extended Authentication” on page 6.

- 1 From Policy Manager, select **Network > Remote User**. Click the **Mobile User VPN** tab.
The Mobile User VPN information appears, as shown in the following figure.



- 2 Select **Firebox Authenticated Users**. Click **Add**. Click **Next**.
The Mobile User VPN Wizard - Firebox Authenticated User appears.
- 3 Select the User Name from the drop-down list or if the User Name is not listed, click **Add New**.
The Setup New User dialog box appears.
- 4 Type the **User Name** and **Password** of the new user. Retype the **Password** to confirm. Click **OK**.
- 5 Type a shared key for the account and retype to confirm.
This key will be used to negotiate the encryption and/or authentication for the MUVPN tunnel.
- 6 If you are connecting with a Pocket PC, select the applicable check box. Click **Next**.
- 7 Select if you will use the shared key or a certificate for authentication. Click **Next**.
- 8 If you specified certificates, type the configuration passphrase of your certificate authority. Click **Next**.
- 9 Specify the network resource to which this user will be allowed to connect.
In the default configuration, the IP address of the Trusted network appears in the Allow user access to field.
- 10 If you plan to use a virtual adapter and route all of the remote user's Internet traffic through the IPsec tunnel, select the check box marked **Use default gateway on remote network**. This option also allows you to route MUVPN traffic through the HTTP proxies on the Firebox. For more information on this option, see “Allowing Internet connections through MUVPN tunnels” on page 5.



To allow a connection to more than one network or computer, use the procedure that follows to change the policy.

- 11 Specify a virtual IP address for this mobile user. Click **Next**.
This can either be an unused IP address on the network you specified in the previous step or on a false network you have created.
- 12 Select an authentication method and encryption method for this mobile user's connections. Type a key expiration time in kilobytes or hours.

Authentication

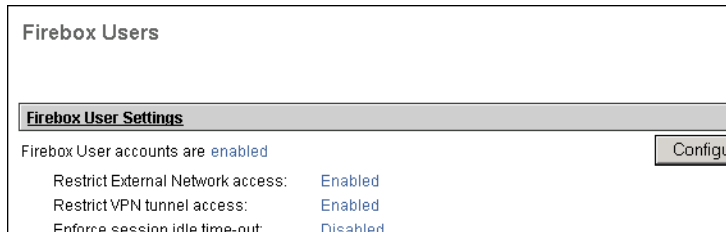
MD5-HMAC (128-bit algorithm), SHA1-HMAC (160-bit algorithm), or AES 128, 192, or 256 bit

Encryption

None (no encryption), DES-CBC (56-bit), 3DES-CBC (168-bit), or AES 128, 192, or 256 bit

13 Click **Next**. Click **Finish**.

The wizard closes and the user name appears on the **Mobile User VPN** tab. If you expand the plus signs (+) next to the entries, you can view the information as shown in the following figure.



Modifying an existing Mobile User VPN entry

Use the Mobile User VPN wizard to generate a new .exp or .wgx file every time you want to change an end-user profile. Reasons to change a profile include:

- Change the shared key
- Let a user connect to new computer or network
- Set the connection to one destination port, source port, or protocol
- Change the encryption or authentication parameters

1 From Policy Manager, select **Network > Remote User**.

2 In the list of user names and groups on the **Mobile User VPN** tab, click the user name or group you want to change.

3 Click **Edit**.

The **Mobile User VPN** wizard appears, displaying the form containing the user or group name and passphrase.

4 Use **Next** to step through the wizard. Configure the end-user profile to match your security policy requirements.

5 To add a connection for a new network or host, go to the Allowed Resources and Virtual IP Address screen in the Mobile User VPN wizard. Click **Add**.

You can also use this dialog box to change the virtual IP address assigned to the remote user.

6 In the **Advanced Mobile User VPN Policy Configuration** dialog box, use the drop-down list to select **Network** or **Host**. Type the IP address. Use the **Dst Port**, **Protocol**, and **Src Port** options to allow connections to only a specified port or protocol. Click **OK**.

7 Go completely through the wizard to the final screen. Click **Finish**.

You must click **Finish** to create a new .wgx file and write the modified settings to the Firebox configuration file.

8 Click **OK**.

Allowing Internet connections through MUVPN tunnels

You can enable remote users with virtual adapters to connect to the Internet through an MUVPN tunnel. However, this option has performance implications. For better performance, you can use *split tunneling*. Split tunneling refers to a remote user or site connecting to the Internet on the same computer as the VPN connection, without placing the Internet traffic inside the tunnel. Browsing the Web occurs directly through the user's ISP. However, split tunneling exposes the system to attack because the Internet traffic is not filtered or encrypted.

Despite the security risks of split tunneling, it offers a large performance boost compared to Internet connection through the MUVPN tunnel. When split tunneling is not allowed or supported, Internet-bound traffic must pass across the WAN bandwidth of the VPN gateway twice. This creates considerable load on the VPN gateway.



If you want the MUVPN client to be protected by an HTTP Proxy policy, you cannot use split tunneling. You must let users connect to the Internet through the MUVPN tunnel. For more information, see "Outgoing configuration to allow MUVPN traffic over proxies" on page 10.

One recommended solution is to allow split tunneling, but require that remote users have personal firewalls for computers behind the VPN endpoint.

To allow users to connect to the Internet only through the MUVPN tunnel:

- 1 When you are running the MUVPN wizard, select the check box marked **Use default gateway on remote network** on the network resource screen.
- 2 Create a dynamic NAT entry from VPN to the external interface. If you want to specify that only specified MUVPN users have this ability, create entries from <virtual IP address> to the external interface.
- 3 Add services as appropriate to allow outgoing connections for mobile users. Because this lets users connect to the Internet only through the tunnel, you use the **Incoming** tab to configure outgoing traffic.

Using Extended Authentication

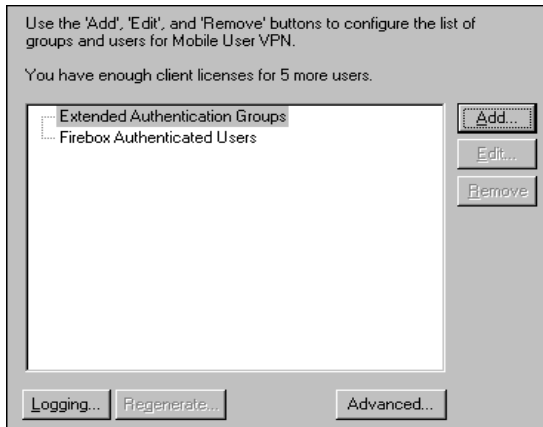
MUVPN with extended authentication allows users to authenticate to a Windows NT or RADIUS authentication server instead of to the Firebox. Instead of validating against its own data, the Firebox validates users against the third-party server. No user names or passwords need to be configured on the Firebox.

The advantage of MUVPN with extended authentication is that the network administrator does not have to continually synchronize user login information between the Firebox and the authentication server. MUVPN users log in to the corporate network from remote locations with the same user name and password they use when they are at their desks inside the company.

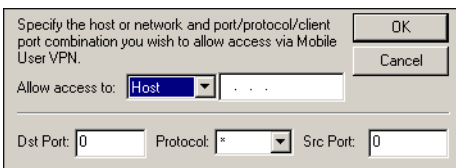
If you want to use a third-party server for authentication, you must set an extended authentication group on the Firebox. The user names and passwords for MUVPN users are kept on the authentication server and not on the Firebox. Note that users actually connect and authenticate to the Firebox; the third-party server only supplies the user database.

Define an extended authentication group

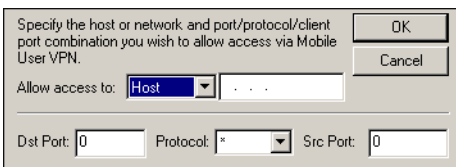
- 1 From Policy Manager, select **Network > Remote User**. Click the **Mobile User VPN** tab. *The Mobile User VPN information appears, as shown in the following figure.*



- 2 Select **Extended Authentication Groups**. Click **Add**. Click **Next**. *The Mobile User VPN Wizard - Extended Authentication Group appears.*
- 3 Specify a name for the extended authentication group. Specify the passphrase used to encrypt the .wgx file for this group. Click **Next**.
- 4 Select an authentication server for this group from the drop-down list. Click **Next**. *You must use the Authentication Server dialog box before you do this step. For more information, see the WFS Configuration Guide.*
- 5 Select if this group will use a shared key or a certificate for authentication. Click **Next**.



- 6 If you specified certificates, type the configuration passphrase of your Certificate Authority. This can be the Firebox or a third-party CA device. Click **Next**. *If you specify the passphrase of the Firebox, CA must be active on the Firebox. For information on activating the CA, see the chapter on certificates and the Certificate Authority in the Firebox documentation.*
- 7 Specify the network resources to which this group will be allowed to connect. To add a new resource, click **Add**. *The Advanced Mobile User VPN Policy Configuration dialog box appears.*



- 8 Use the **Allow Access to** drop-down list to select **Network** or **Host**. Type the IP address. Use the **Dst Port**, **Protocol**, and **Src Port** options if you want the client to use only a specified port or protocol.

Setting Advanced Preferences

- 9 If you plan to use a virtual adapter and route all of the remote users' Internet traffic through the IPsec tunnel, select the check box marked **Use default gateway on remote network**. Click **Next**.
- 10 Specify the virtual IP address pool (these can be virtual IP addresses on a false network). To add addresses, click **Add** and type an address or address range. Click **Next**.
- 11 Select an authentication method and encryption method for the connection this group uses. Type a key expiration frequency in kilobytes or hours.
If you type a value for kilobytes and hours, the key expires when the traffic matches one of the criteria.

Authentication

MD5-HMAC (128-bit algorithm) or SHA1-HMAC (160-bit algorithm)

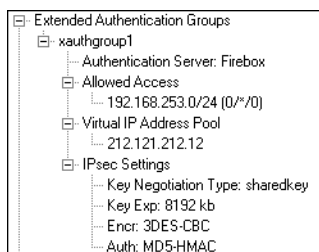
Encryption

None (no encryption), DES-CBC (56-bit), or 3DES-CBC (168-bit)

- 12 Click **Next**. Click **Finish**.
The wizard closes and the group name appears on the Mobile User VPN tab. If you expand the plus signs (+) next to the entries, you can see the information as shown in the following figure.

Configuring the external authentication server

Define a group on the server that has the same name as the extended authentication remote gateway. All MUVPN users that authenticate to the server must belong to this group.



Setting Advanced Preferences

Advanced settings include specifying a virtual adapter rule, allowing MUVPN connections on any interface, and locking down the end-user profile so that users can see the settings but not change them. Locking down the profile is the recommended setting, because users usually cannot make effective changes to the profile without making corresponding modifications to the Firebox®.

- 1 Click **Advanced** on the **Mobile User VPN** tab.
The Advanced Export File Preferences dialog box appears.
- 2 To prevent users from changing their profile, select the **Make the security policy read-only in the MUVPN client** check box.
- 3 To allow MUVPN tunnels from any interface, select the **Allow MUVPN connects from all interfaces** check box.
- 4 A virtual adapter is used to assign client IP addresses and network parameters such as WINS and DNS. Select the virtual adapter rule for the mobile user:

Disabled

(Recommended) The mobile user does not use a virtual adapter to connect to the MUVPN client.

Preferred

If the virtual adapter is in use or not available, address assignment is performed without it.

Required

The mobile user must use a virtual adapter to connect to the MUVPN client.

Configuring Services to Allow Incoming MUVPN Traffic

In the default configuration, MUVPN users cannot connect to computers on the trusted or optional protected by your Firebox. To allow remote users to connect to those resources, you must add their user names, extended authentication group (for MUVPN users who authenticate to an external server), or the ipsec_users group (for MUVPN users authenticating to the Firebox) to service icons in the Services Arena. Note that extended authentication groups must be added to services because these users are not members of ipsec_users.

We recommend two methods for configuring services for MUVPN traffic: by individual service or by using the Any service. Configuring the Any service “opens a hole” through the Firebox®, allowing all traffic to flow unfiltered between specific hosts.

To allow traffic to be filtered by WatchGuard’s proxies, follow this procedure, with the slight Service modifications shown at “Outgoing configuration to allow MUVPN traffic over proxies” on page 10.

By individual service

In the Services Arena, double-click a service that you want to enable for your VPN users. Set the following properties on the service:

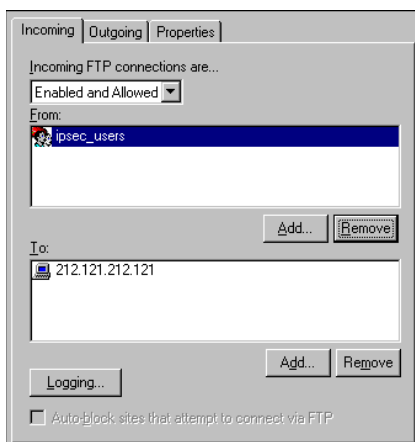
Incoming

- Enabled and allowed
- From: ipsec_users or extended authentication group
- To: trusted interface, optional interface, network or host IP address, or alias

Outgoing

- Enabled and allowed
- From: trusted interface, optional interface, network or host IP address, or alias
- To: ipsec_users or extended authentication group

This figure shows an example of how you might define incoming properties for a service.



Outgoing configuration to allow MUVPN traffic over proxies

The following Services configuration allows MUVPN traffic to be filtered by a proxy.

- Enabled and allowed
- From: ipsec_users, pptp_users, or extended authentication group
- To: trusted interface, optional interface, network or host IP address, or alias

Using the Any service

Add the Any service with the following properties:

Incoming

- Enabled and allowed
- From: ipsec_users or extended authentication group
- To: trusted interface, optional interface, network or host IP address, or alias

Outgoing

- Enabled and allowed
- From: trusted interface, optional interface, network or host IP address, or alias
- To: ipsec_users or extended authentication group



You cannot use the Any service to allow outgoing traffic To the external interface. Use the Outgoing service to allow outgoing traffic To the external interface.

Make sure you save your configuration file to the Firebox after you make these changes.

Regenerating End-User Profiles

The WatchGuard® MUVPN configuration gives you the ability to regenerate end-user profiles for your existing MUVPN users. You do not need to create a new profile when you regenerate. Regeneration creates new end-user profiles with the same settings for the current MUVPN users.

To generate new end-user profiles for current MUVPN users, on the **Mobile User VPN** tab, click **Regenerate**. If you use WatchGuard System Manager v9.0 with WFS, profiles are kept in C:\Documents and Settings\All Users\Shared WatchGuard\muvpn\[firebox.ip.address]\wgx\.

You can now distribute these end-user profiles as necessary.

Saving the Profile to a Firebox

To activate a new Mobile User profile, you must save the configuration file to the Firebox®. Select **File > Save > To Firebox**.

Distributing the Software and Profiles

We recommend distributing end-user profiles by encrypted email or some other secure method. Each client computer must have:

- Software installation package

The packages are located on the WatchGuard® LiveSecurity® Service web site at:
<http://www.watchguard.com/support>

Enter the site using your LiveSecurity Service user name and password. Click the **Latest Software** link, then click either **Any Firebox III Model** or **Any Firebox X model** from the drop-down list. Click the **MUVPN Software** download.

- The end-user profile
This file contains 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 *user name.wgx*
- Two certificate files—if you authenticate with certificates
These are the .p12 file, an encrypted file containing the certificate, and cacert.pem, which contains the root Certificate Authority (CA) certificate.
- User documentation
End-user brochures developed by WatchGuard are located on the WatchGuard LiveSecurity Service 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 **Firebox System** link.
- Shared key
To install the end-user profile, 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 in Policy Manager.

Making Outbound IPSec Connections From Behind a Firebox

It can be necessary sometimes to make an IPSec connection to a Firebox® from behind a second Firebox. An example is a mobile user from your company, at a different location that also has a Firebox, who must connect to your corporate network. For the local Firebox to correctly transmit the outgoing IPSec connection, you must set up the IPSec service. For information on services, see “Configuring Filtered Services” in the *WFS Configuration Guide*.

Because the IPSec service enables a tunnel to the IPSec server and does not examine the traffic for suspicious traffic at the firewall, we recommend that you do not use this service for as a standard policy.

Configuring Debugging Options for MUVPN

WatchGuard® System Manager includes a selection of log options that you can set to get information and help you with troubleshooting. When you enable these diagnostic options, the log message volume increases. This can have negative effects on Firebox performance. We recommend that you use these options only to troubleshoot MUVPN problems.

- 1 From Policy Manager, click **Network > Remote User VPN**.
The Remote User setup window appears with the Mobile User VPN tab selected.
- 2 Click **Logging**.
The IPSec Logging dialog box appears.

Terminating Tunnels on Optional or Trusted Interfaces

- 3 Click the logging options you want to activate.
For a description of each option, right-click it, and then click What's This?
- 4 Click **OK**. Save the configuration file to the Firebox.

Terminating Tunnels on Optional or Trusted Interfaces

Because the Firebox® can accept IKE traffic (IPSec key negotiation on the optional port), the IPSec peer can be connected directly to the optional port and can route traffic to the trusted network. To enable this feature, on the Safenet Client's security policy editor, set the IP address of the remote gateway to the Firebox's optional IP address.

Terminating IPSec Connections

To stop a VPN connection, you must restart the Firebox. If you delete only the IPSec service, active connections to the Firebox do not stop.

2

Using Fireware Policy Manager to Configure MUVPN

The full procedure for using MUVPN is included in this guide and in the operating system–specific MUVPN end-user brochures. This chapter supplies the Firebox® procedures you must perform.

Like RUVPN with PPTP, when you use Mobile User VPN (MUVPN) you must configure the Firebox and the remote client computers. However, with MUVPN you or another Firebox administrator can make the client configuration. You make end-user profiles to set parameters for the client.

MUVPN users authenticate either to the Firebox or to another authentication server. You can authenticate with shared keys or certificates.



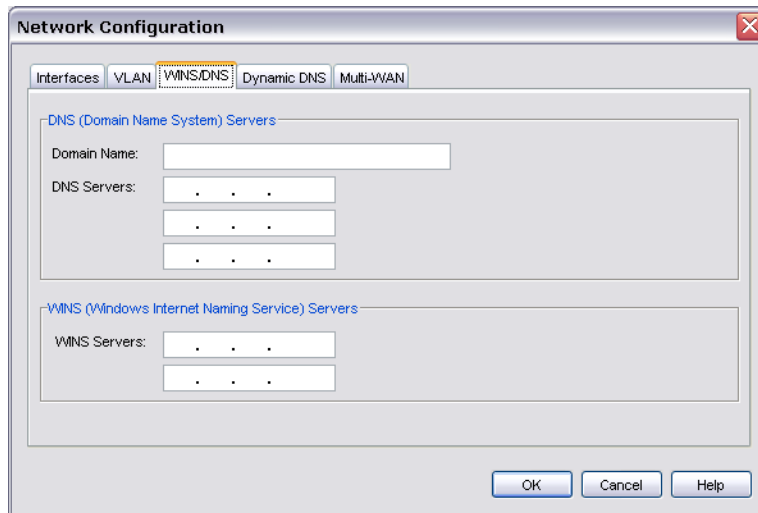
Because strict export restrictions are put on exported high encryption software, WatchGuard® System Manager is available with two encryption levels. You must make sure you download and use WatchGuard System Manager with strong encryption when you use MUVPN because the IPSec standard requires 56-bit (medium) encryption at the minimum.

Configuring WINS and DNS Servers

RUVPN and MUVPN clients rely on shared Windows Internet Name Server (WINS) and Domain Name System (DNS) server addresses. DNS translates host names into IP addresses. WINS resolves NetBIOS names to IP addresses. These servers must be accessible from the Firebox® trusted interface.

Make sure you use only an internal DNS server. Do not use external DNS servers.

- 1 From Policy Manager, click **Network > Configuration**. Click the **WINS/DNS** tab.
The information for the WINS and DNS servers appears.
- 2 Type a domain name for the DNS server.
- 3 In the **DNS Servers** and **WINS Servers** text boxes, type the addresses for the WINS and DNS servers.



Preparing Mobile User VPN Profiles

With Mobile User VPN, the network security administrator controls end-user profiles. Policy Manager is used to set the name of the end user and create a profile with the extension .wgx. The .wgx file contains the shared key, user identification, IP addresses, and settings that are used to create a secure tunnel between the remote computer and the Firebox®. This file is encrypted with a key that is eight characters or greater in length. This key must be known to the administrator and the remote user. When the .wgx file is installed in the remote client, this key is used to decrypt the file for use in the client software.

If you want to lock the profiles for mobile users by making them read-only, see “Setting Advanced Preferences” on page 21.

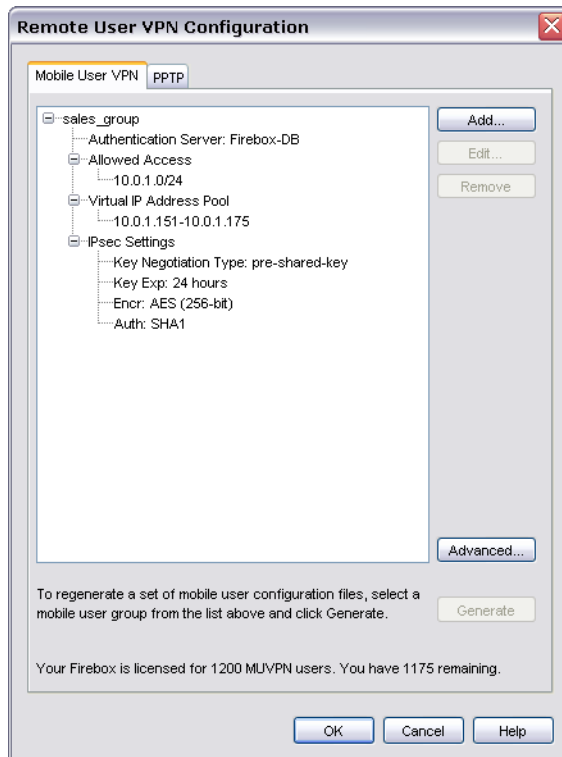
Mobile users connect to the network with MUVPN client software. The MUVPN client allows you to deploy the software in the situation where the client does not have a static IP address, such as with a DSL connection.

This is the default profile and allows for the conversion of existing profiles (with the .exp extension) to the newer version (with the .wgx extension). New keys are created as a part of this process. They must then be given to the remote users in the field.

Defining an MUVPN User Group

You can use this procedure if the new user group you create uses the Firebox® for authentication, or if it will use a third-party authentication server for authentication.

- 1 From Policy Manager, click **VPN > Remote Users**.
The *Remote User VPN configuration dialog box* appears.



- 2 Click **Add**.
The *Add Mobile User VPN Wizard* appears.
- 3 Click **Next**.
- 4 Select an authentication server from the **Authentication Server** drop-down list. You can authenticate users with the internal Firebox database (Firebox-DB) or with a RADIUS, SecurID, LDAP, or Active Directory server. Make sure that this method of authentication is enabled in Policy Manager (select **Setup > Authentication > Authentication Servers**).
See the "Authentication" chapter in the *WatchGuard® System Manager User Guide* for more information.
- 5 Type a group name in the **Group Name** field. Make sure the name is unique among MUVPN group names as well as all interface and tunnel names. Click **Next**.



The group name cannot include a dash (-). The MUVPN client cannot import files that use a dash in the name.

- 6 Select the authentication method.
If you select passphrase, type and retype the passphrase in the fields. If you use an RSA certificate, provide the address and passphrase for your server.
- 7 Click **Next**.

- 8 Select an option for Internet traffic. You can allow all Internet traffic between the MUVPN client and the Internet to use the ISP of the client, or you can make all Internet traffic use the VPN tunnel. If you make sure all Internet traffic goes through the tunnel, more processing power and bandwidth is used. However, the configuration is more secure.
- 9 Add the networks and computers to which this user can have access. Click **Add** to add a host IP address or a network IP address. Type an address and click **OK** in the **Add Address** dialog box. Do this step again to add more resources.
- 10 Click **Next**.
- 11 Add virtual IP addresses. MUVPN users will use these IP addresses when they connect to your network.
Click **Add** to add one IP address or an IP address range. Do this step again to add more virtual IP addresses.
If High Availability is configured, you must add two virtual IP addresses for each MUVPN user.
- 12 Click **Next**. The success dialog box appears. The MUVPN profile is saved in the My Documents folder at the location
My Watchguard\Shared WatchGuard\muvpn\ip_address\MUVPN\wgx. Click **Finish**.
- 13 The **Remote User VPN Configuration** dialog box appears.
 - To add users to this group, use the procedure for adding users in the "Authentication" chapter in the *WatchGuard System Manager User Guide*.

Configuring the external authentication server

If you create an MUVPN user group that authenticates to a third-party server, make sure you create a group on the server that has the same name as the extended authentication remote gateway. All MUVPN users that authenticate to the server must belong to this group.

Modifying an existing Mobile User VPN entry

After you use the Mobile User VPN wizard to create a new .wgx file, you can change the profile to:

- Change the shared key
 - Add access to more hosts or networks
 - Restrict access to a single destination port, source port, or protocol
 - Change the Phase 1 or Phase 2 settings.
- 1 From Policy Manager, click **VPN > Remote Users**.
 - 2 From the list of user names and groups on the **Remote User VPN** dialog box, click the user name or group to change.

3 Click **Edit**.

The *Edit MUVPN Extended Authentication Group* dialog box appears.

Use the following fields to edit the group profile:

Authentication Server

Select the authentication server to use for this MUVPN group.

To configure your authentication server, select

Setup > Authentication > Authentication Servers from the menu bar in Policy Manager.

Passphrase

Type a passphrase to encrypt the MUVPN profile (.wgx file) that you distribute to users in this group.

Confirm

Type the passphrase again.

Primary

Select or type the primary external IP address to which MUVPN users in this group can connect. MUVPN users connect on port 4100.

Backup

Select or type a backup external IP address to which MUVPN users in this group can connect. This backup IP address is optional.

Session

Type the maximum time in minutes that an MUVPN session can be active.

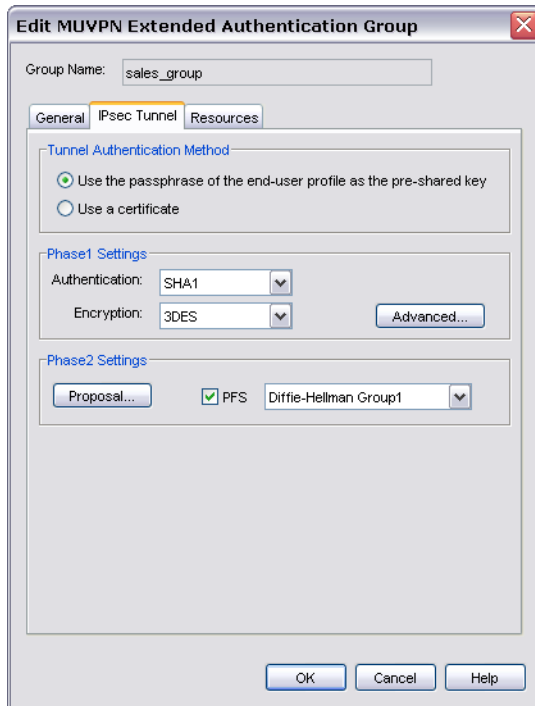
Idle

Type the time in minutes before the Firebox closes an idle MUVPN session.

The session and idle timeout values are the default timeouts if the authentication server does not return specific timeout values. If you use the Firebox as the authentication server, the timeouts for the MUVPN group are always ignored.

The session and idle timeouts cannot be longer than the value in the **SA Life** field. To set this field, from the **IPsec Tunnel** tab of the **Edit MUVPN Extended Authentication Group** dialog box, click **Advanced**. The default value is 8 hours.

- 4 Click the **IPSec Tunnel** tab.



- 5 Use the following fields to edit the IPSec settings:

Use the passphrase of the end-user profile as the pre-shared key

Select this setting to use the passphrase of the end-user profile as the pre-shared key for tunnel authentication. You must use the same shared key on the remote device, and this shared key can use only standard ASCII characters.

Use a certificate

Select this setting to use a certificate for tunnel authentication. You must start the Certificate Authority if you select certificate-based authentication. You must also use the WatchGuard Log Server for log messages.

CA IP address

(This field appears only if you select to use a certificate) Type the IP address for the certificate authority (CA).

Timeout

(This field appears only if you select to use a certificate) Type the time in seconds before the certificate authority request times out.

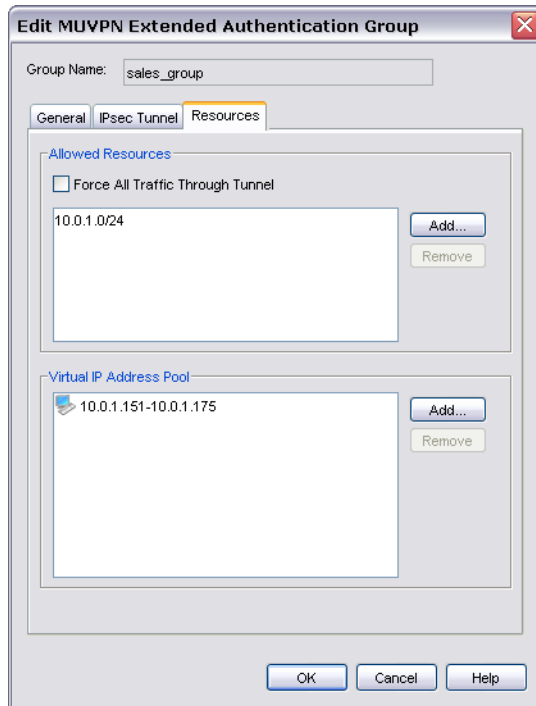
Phase1 Settings

Select the authentication and encryption methods for the MUVPN tunnel. These settings must be the same for both VPN endpoints. To configure advanced settings, such as NAT Traversal or the key group, click the **Advanced** button, and see the procedure described in "Defining advanced Phase 1 settings" on page 19.

Phase2 Settings

Select the proposal and key expiration settings for the MUVPN tunnel. You can also enable Perfect Forward Secrecy (PFS) or set the Diffie-Hellman group. These settings must be the same for both VPN endpoints. To change other proposal settings, click the **Proposal** button, and see the procedure described in "Defining advanced Phase 2 settings" on page 20.

- 6 Click the **Resources** tab.



- 7 Use the following fields to add and remove allowed network resources and virtual IP addresses:

Force All Traffic Through Tunnel

Select this check box to send all MUVPN user Internet traffic through the VPN tunnel. When this is selected, MUVPN user Internet traffic is sent safely, but web sites can be slower for those users. If this is not selected, MUVPN user Internet traffic is not sent safely, but users can browse the Internet more quickly.

Allowed Resources list

This list shows the resources that users in the MUVPN authentication group can get access to on the network. Click **Add** to add an IP address or IP address range to the network resources list. Click **Remove** to clear the selected IP address or IP address range from the network resources list.

Virtual IP Address Pool

This list shows the internal IP addresses that are used by MUVPN users over the tunnel. These addresses are used only when they are needed. Click **Add** to add an IP address or IP address range to the virtual IP address pool. Click **Remove** to clear the selected IP address or IP address range from the virtual IP address pool.

- 8 Click **OK**.
You return to the Remote Users Configuration dialog box.



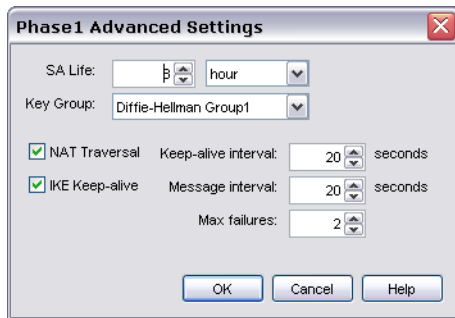
End-user profiles (.wgx) for the profile you edited are automatically regenerated. You must distribute new end-user profiles to the affected users and groups.*

Defining advanced Phase 1 settings

To define advanced Phase 1 settings for an MUVPN user profile:

- From the **IPSec Tunnel** tab of the **Edit MUVPN Extended Authentication Group** dialog box, select **Advanced**.
The Phase1 Advanced Settings dialog box appears.

Defining an MUVPN User Group

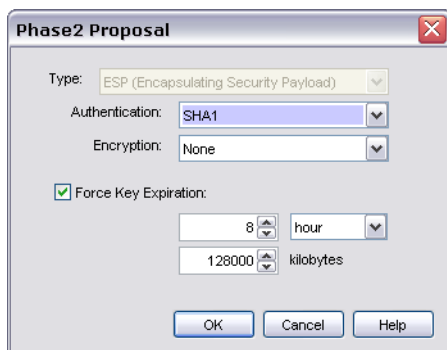


- 2 To change the SA (security association) lifetime, type a number in the **SA Life** field, and select **Hour** or **Minute** from the drop-down list
- 3 From the **Key Group** drop-down list, select the Diffie-Hellman group you want. WatchGuard supports groups 1, 2, and 5.
Diffie-Hellman groups determine the strength of the master key used in the key exchange process. The higher the group number, the greater the security but the more time is required to make the keys.
- 4 If you want to build an MUVPN tunnel between the Firebox and another device that is behind a NAT device, select the **NAT Traversal** check box. NAT Traversal, or UDP Encapsulation, allows traffic to get to the correct destinations. To set the **Keep-alive interval**, type the number of seconds or use the value control to select the number of seconds you want.
- 5 To have the Firebox send messages to its IKE peer to keep the tunnel open, select the **IKE Keep-alive** check box. To set the **Message interval**, type the number of seconds or use the value control to select the number of seconds you want.
- 6 To set the maximum number of times the Firebox tries to send an IKE keep-alive message before it tries to negotiate Phase 1 again, type the number you want in the **Max failures** box.
- 7 Click **OK**.

Defining advanced Phase 2 settings

To define advanced Phase 2 settings for an MUVPN user profile:

- 1 From the **IPSec Tunnel** tab of the **Edit MUVPN Extended Authentication Group** dialog box, select **Proposal**.
The Phase2 Advanced Settings dialog box appears.



- 2 From the **Type** drop-down list, select **ESP** or **AH** as the proposal method. Only ESP is supported at this time.

- 3 From the **Authentication** drop-down list, select **SHA1** or **MD5** for the authentication method.
- 4 From the **Encryption** drop-down list, select the encryption method.
The options are None, DES, 3DES, and AES 128, 192, or 256 bit which appear in the list from the most simple and least secure to most complex and most secure.
- 5 To make the gateway endpoints generate and exchange new keys after a quantity of time or amount of traffic passes, select the **Force Key Expiration** check box. In the fields below, enter a quantity of time and a number of bytes after which the key expires.
If **Force Key Expiration** is disabled, or if it is enabled and both the time and kBytes are set to zero, the Firebox tries to use the key expiration time set for the peer. If this is also disabled or zero, the Firebox uses a key expiration time of 8 hours.
You can set the time up to one year.
- 6 Click **OK**.

Allowing Internet access through MUVPN tunnels

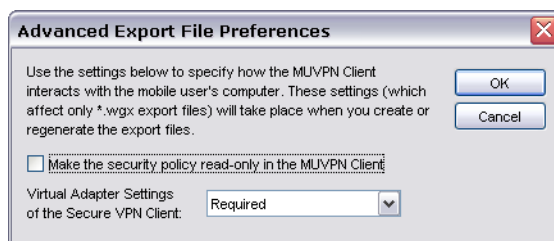
To give remote users with virtual adapters access to the Internet through an MUVPN tunnel:

- When you use the MUVPN wizard, select the **Yes, force all Internet traffic to flow through the tunnel** radio button on the "Direct the flow of Internet traffic" screen.
This option adds Any-External as an allowed resource, which means that traffic destined to go out any external interface is allowed.

Setting Advanced Preferences

Advanced settings include assigning a virtual adapter rule and locking down the end-user profile so that users can see the settings but not change them. Locking down the profile is the recommended setting, because users cannot make effective changes to the profile without making corresponding changes to the Firebox®.

- 1 Click **Advanced** on the **Mobile User VPN** tab.
The Advanced Export File Preferences dialog box appears.



- 2 To give mobile users only read-only access to their profiles, select the **Make the security policy read-only in the MUVPN Client** check box.
- 3 You can use a virtual adapter to assign client IP addresses and network settings that include WINS and DNS. Select the virtual adapter rule for the mobile user:

Disabled

(Recommended) The mobile user does not use a virtual adapter to connect to the MUVPN client.

Preferred

If the virtual adapter is in use or is not available, addresses are assigned without the adapter.

Required

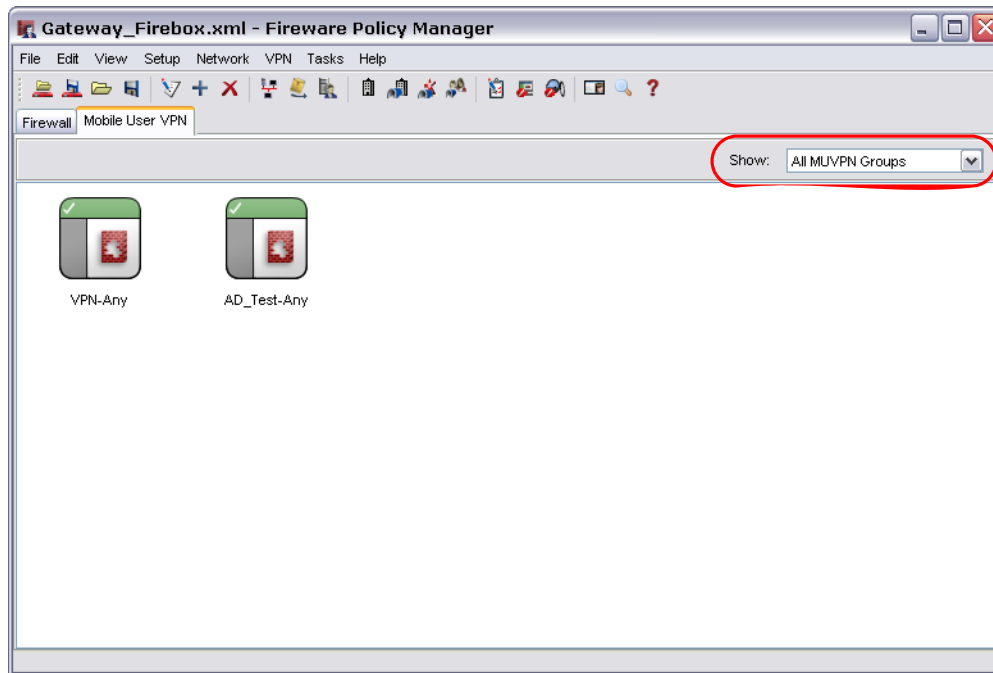
The mobile user must use a virtual adapter to connect to the MUVPN client.

Configuring Policies to Filter MUVPN Traffic

In a default configuration, MUVPN users have full access privileges through a Firebox®, with the Any policy. To put limits on MUVPN users, you must add policies to the **MUVPN** tab in Policy Manager.

Add individual policies

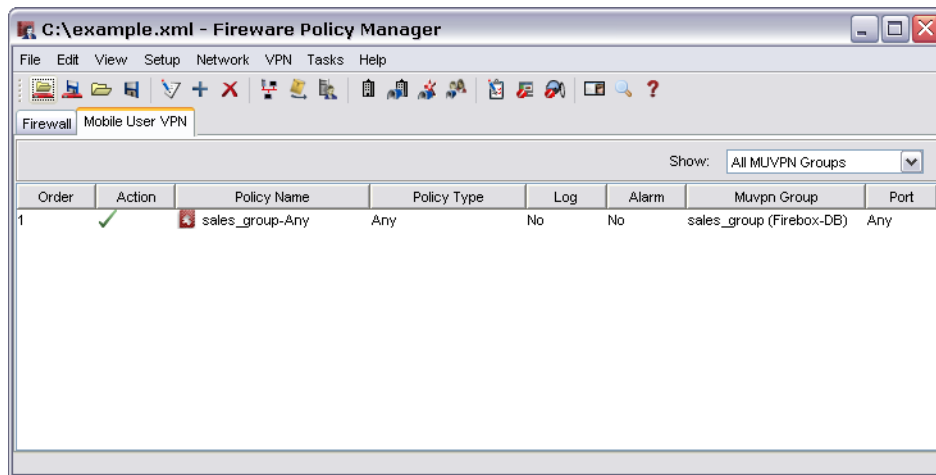
- 1 In Policy Manager, click the **MUVPN** tab.



- 2 From the **Show** drop-down list, select the name of the MUVPN group for which you are adding a policy. You must select a group before you add a policy.
- 3 Add, edit, and delete policies as described in the "Policies" chapter in the *WatchGuard® System Manager User Guide*. Make sure you save your configuration file to the Firebox after you make these changes.

Seeing details on an MUVPN policy

To see more information on an MUVPN policy in Policy Manager, select **View > Details**.



Under **MUVPN Group**, Policy Manager displays the authentication server, in parentheses, for the MUVPN group.

Using the Any Policy

The Any policy is added to all MUVPN user groups by default.

Re-creating End-User Profiles

The WatchGuard® MUVPN configuration gives you the ability to re-create end-user profiles for your existing MUVPN users. You do not have to create a new profile when you re-create. Use this procedure to create new end-user profiles with the same settings for the current MUVPN users. This file is located in Documents and Settings\All Users\Shared Watch-guard\muvpn\ip_address\config_name\wgx\config_name.wgx. If the tunnel is authenticated with certificates, the certificates are also created.

To create new end-user profiles for current MUVPN users, on the **Mobile User VPN** tab, select the MUVPN group and click **Generate**.

You can now distribute these end-user profiles as necessary.

Saving the Profile to a Firebox

To activate a new Mobile User profile, you must save the configuration file to the Firebox®. From the **File** menu, click **Save > To Firebox**.

Distributing the Software and Profiles

WatchGuard® recommends distributing end-user profiles by encrypted email or with some other secure method. Each client computer must have:

- Software installation package
The packages are located on the WatchGuard LiveSecurity® Service web site at: <http://www.watchguard.com/support>
Log in to the site using your LiveSecurity Service user name and password. Click the **Latest Software** link, click **Add-ons/Upgrades** on the left side, and then click the **Mobile User VPN** link.
- The end-user profile
This file contains the group 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 file name **groupname.wgx**.
- Two certificate files—if you are authenticating with certificates
These are the .p12 file, an encrypted file containing the certificate, and cacert.pem, which contains the root (CA) certificate.
- User documentation
End-user brochures supplied by WatchGuard are located at: www.watchguard.com/help/documentation
- Shared key
To install the end-user profile, the user is requested to type 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 in Policy Manager.

Additional MUVPN Topics

This section describes special topics for MUVPN.

Making outbound IPSec connections from behind a Firebox

A user could have to make IPSec connections to a Firebox® from behind another Firebox. For example, if a mobile employee travels to a customer site that has a Firebox, that user can make IPSec connections to their network using IPSec. For the local Firebox to correctly handle the outgoing IPSec connection, you must set up an IPSec policy that includes the IPSec packet filter. For information on enabling policies, see the “Policies” chapter in the *WatchGuard System Manager User Guide*.

Because the IPSec policy enables a tunnel to the IPSec server and does not do any security checks at the firewall, only add users that you trust to this policy.

Terminating IPSec connections

In order to fully stop VPN connections, the Firebox must be restarted. Removing the IPSec policy does not stop current connections.

Global VPN settings

Global VPN settings on your Firebox apply to all manual BOVPN tunnels, managed tunnels, and MUVPN tunnels. You can use these settings to:

- Enable IPSec pass-through.
- Clear or maintain the settings of packets with Type of Service (TOS) bits set.
- Use an LDAP server to verify certificates.

To change these settings, from Policy Manager, select **VPN > VPN Settings**. For more information on these settings, see the “Basic Configuration Setup” chapter in the *WatchGuard System Manager User Guide*.

Seeing the number of MUVPN licenses

To see the number of MUVPN licenses that are installed, from Policy Manager, select **Setup > Feature Keys**. From the **Firebox Feature Keys** dialog box, click **Active Features**. Scroll down to the value **MUVPN_USERS** and look at the number in the **Capacity** column. This is the number of installed MUVPN licenses.

Purchasing additional MUVPN licenses

WatchGuard Mobile User VPN is an optional feature of the WatchGuard Firebox[®] System. Each Firebox X device includes a number of MUVPN licenses. You can purchase more licenses for MUVPN.

Licenses are available through your local reseller or at:

<http://www.watchguard.com/sales>

Adding feature keys

For information on adding feature keys, see “Working with Feature Keys” in the *WatchGuard System Manager User Guide*.

MUVPN and VPN failover

You can configure VPN tunnels to fail over to a backup endpoint if the primary endpoint becomes unavailable. For more information on VPN failover, see the *WatchGuard System Manager User Guide*.

If VPN failover is configured and failover occurs, MUVPN sessions do not continue. You must authenticate your MUVPN client again to make a new MUVPN tunnel.

To configure VPN failover for MUVPN tunnels, on the **General** tab of the **Edit MUVPN Extended Authentication Group** dialog box, enter a backup WAN interface in the **Backup** field in the **Firebox IP** box. You can specify only one backup interface for tunnels to fail over to, even if you have additional WAN interfaces.

3

MUVPN Client Preparation, Installation, and Connection

The WatchGuard® MUVPN client is installed on an employee computer, whether the employee travels or works from home. The employee uses a standard Internet connection and activates the MUVPN client. The MUVPN client then creates an encrypted tunnel to your trusted and optional networks, which are protected by a WatchGuard Firebox®. The MUVPN client allows you to supply remote access to your internal networks and not compromise your security.

You must configure your Firebox to work with MUVPN. If you have not, see the previous chapters that describe how to configure your Firebox when you use a particular type of appliance software.

ZoneAlarm is a personal firewall software application that is included as an optional feature with the MUVPN client. ZoneAlarm gives an end user added security when they use MUVPN.

Prepare the Remote Computers

The MUVPN client is compatible only with the Windows operating system. Each Windows system you use as an MUVPN remote computer must match these system requirements:

System requirements

- PC-compatible computer with a Pentium processor or equivalent
- Compatible operating systems and minimum RAM:
 - Microsoft Windows NT 4.0 Workstation: Minimum 32 MB
 - Microsoft Windows 2000 Professional: Minimum 64 MB
 - Microsoft Windows XP: Minimum 64 MB



The MUVPN client does not work with the Microsoft Vista operating system.

- We recommend that you use the most current service pack for each operating system, but this is not a requirement.
- 10 MB of hard disk space
- Native Microsoft TCP/IP communication protocol

Prepare the Remote Computers

- Microsoft Internet Explorer 5.0 or later
- An account with an Internet Service Provider
- A dial-up connection or broadband (DSL or Cable modem) connection

To make sure that Windows file and print sharing can occur through the MUVPN client tunnel, you must configure each Windows operating system to use the remote WINS and DNS servers on the trusted networks and optional networks behind the Firebox.



If you want to use the MUVPN client virtual adapter, the WINS and DNS settings are not configured on the client computers, but are configured on the Firebox®.

Windows NT operating system setup

You must install and configure some network components on a remote computer that uses Windows NT to make the MUVPN client operate successfully. You must remove any other client-based IPsec VPN software from the computer before you install MUVPN.

Installing Remote Access Services on Windows NT

The Mobile User VPN Adapter, which makes it possible to use L2TP, is installed only if the Remote Access Services (RAS) network component is installed on the employee computer.

From the Windows desktop:

- 1 Click **Start > Settings > Control Panel**, and then double-click the **Network** icon.
- 2 Click the **Services** tab.
- 3 Click **Add**.
- 4 From the drop-down list, select **Remote Access Services**, and then click **OK**.
- 5 Type the path to the Windows NT install files, or put in your system installation CD, and then click **OK**.
The Remote Access Setup dialog box appears.
- 6 Click **Yes** to add a RAS-capable device, which lets you add a modem.
- 7 Click **Add** and complete the **Install New Modem** wizard.



*If no modem is installed, you can enable the **Don't detect my modem; I will select it from a list** check box then add a Standard 28800 modem. To use Windows NT with RAS you must have one or more RAS-compatible devices, such as a modem, installed in your network. If there are no modems available, you can use a dial-up network serial cable between two computers.*

- 8 Select the modem you added in the previous step in the **Add RAS Device** dialog box, and then click **OK**.
- 9 Click **Continue** and click **Close**.
- 10 Restart your computer.

Configuring the WINS and DNS settings

You *must* configure the remote computer to use the WINS and DNS servers for the trusted network behind the Firebox only if you do not want to use the virtual adapter on the MUVPN client computer.

From the Windows desktop:

- 1 Click **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 **Properties**.
The Microsoft TCP/IP Properties window appears.
- 4 Click the **DNS** tab.
- 5 Click **Add**.
- 6 Type the IP address of your DNS server in the applicable text box.
If you have two or more remote DNS servers, complete the previous three steps again.



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

- 7 Click the **WINS Address** tab.
- 8 Type the IP address of your WINS server in the applicable text box and click **OK**.
If you have multiple remote WINS servers repeat this step.
- 9 Click **Close** to close the Network window.
The Network Settings Change dialog box appears.
- 10 Click **Yes** to restart the computer and make the setting changes.

Windows 2000 operating system setup

To use Windows 2000 you must install the TCP/IP protocol, File and Printer Sharing for Microsoft Networks, and Client for Microsoft Networks on the employee computer. You must also remove any other client-based IPsec VPN software from the computer before you install MUVPN.

From the Windows desktop:

- 1 Click **Settings > Network and Dial-up Connections**, and then select the dial-up connection you use to connect to the Internet.
The connection window appears.
- 2 Click **Properties**.
- 3 Click the **Networking** tab.
- 4 Make sure that these components are 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 Click **Start > Settings > Network and Dial-up Connections**, and then select the dial-up connection you use to connect to the Internet.
The connection window appears.
- 2 Click **Properties**.
- 3 Click the **Networking** tab and click **Install**.
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 click **OK**.

Installing the File and Printer Sharing for Microsoft Networks

From the Windows desktop:

- 1 Click **Start > Settings > Network and Dial-up Connections**, and then select the dial-up connection you use to connect to the Internet.
The connection window appears.
- 2 Click **Properties**.
- 3 Click the **Networking** tab and click **Install**.
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 click **OK**.

Installing the Client for Microsoft Networks

From the Windows desktop:

- 1 Click **Start > Settings > Network and Dial-up Connections**, and then select the dial-up connection you use to connect to the Internet.
The connection window appears.
- 2 Click **Properties**.
- 3 Click the **Networking** tab and click **Install**.
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 click **OK**.
- 6 Click **Cancel** to close the Select Network Component Type window.
- 7 Click **OK** to save your changes.
- 8 Click **Cancel** 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 for the trusted network behind the Firebox only if you do not want to use the virtual adapter on the MUVPN client computer.

From the Windows desktop:

- 1 Click **Start > Settings > Network and Dial-up Connections**, and then select the dial-up connection you use to connect to the Internet.
The connection window appears.
- 2 Click **Properties**.
- 3 Click the **Networking** tab.
- 4 Select the **Internet Protocol (TCP/IP)** component and click **Properties**.
The Internet Protocol (TCP/IP) Properties window appears.
- 5 Click **Advanced**.
The Advanced TCP/IP Settings window appears.
- 6 Click the **DNS** tab.

- 7 Below the **DNS server addresses, in order of use** heading, click **Add**.
The TCP/IP DNS Server window appears.
- 8 Type the IP address of your DNS server in the applicable text box and click **Add**.
If you have multiple remote DNS servers repeat the last two steps.



You must list the DNS server on the private network behind the Firebox first.

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

Windows XP operating system setup

To use Windows XP you must install the TCP/IP protocol, File and Printer Sharing for Microsoft Networks, and Client for Microsoft Networks on the employee computer. You must also remove any other client-based IPsec VPN software from the computer before you install MUVPN.

From the Windows desktop:

- 1 Click **Start > Settings > Network Connections**, and then select the connection you use to get access to the Internet.
The connection window appears.
- 2 Click **Properties**.
- 3 Click the **Networking** tab.
- 4 Make sure that these components are 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 Click **Start > Settings > Network Connections**, and then select the connection you use to get access to the Internet.
The connection window appears.

- 2 Click **Properties**.
- 3 Click the **Networking** tab and click **Install**.
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 click **OK**.

Installing the File and Printer Sharing for Microsoft Networks

From the Windows desktop:

- 1 Click **Start > Settings > Network Connections**, and then select the connection you use to get access to the Internet.
The connection window appears.
- 2 Click **Properties**.
- 3 Click the **Networking** tab and click **Install**.
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 click **OK**.

Installing the Client for Microsoft Networks

From the Windows desktop:

- 1 Click **Start > Settings > Network Connections**, and then select the connection you use to get access to the Internet.
The connection window appears.
- 2 Click **Properties**.
- 3 Click the **Networking** tab and click **Install**.
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 click **OK**.
- 6 Click **Cancel** to close the Select Network Component Type window.
- 7 Click **OK** to save your changes.
- 8 Click **Cancel** 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 for the trusted network behind the Firebox only if you do not want to use the virtual adapter on the MUVPN client computer.

From the Windows desktop:

- 1 Click **Start > Settings > Network and Dial-up Connections**, and then select the dial-up connection you use to connect to the Internet.
The connection window appears.
- 2 Click **Properties**.
- 3 Click the **Networking** tab.

- 4 Select the **Internet Protocol (TCP/IP)** component and click **Properties**.
The Internet Protocol (TCP/IP) Properties window appears.
- 5 Click **Advanced**.
The Advanced TCP/IP Settings window appears.
- 6 Click the **DNS** tab.
- 7 Below the **DNS server addresses, in order of use** heading, click **Add**.
The TCP/IP DNS Server window appears.
- 8 Type the IP address of your DNS server in the applicable text box and click **Add**.
If you have multiple remote DNS servers repeat the last two steps.



You must list the DNS server on the private network behind the Firebox first.

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

MUVPN client requirements

After you prepare the operating system, you must install the components in the following list. You must remove any other client-based IPsec VPN software from the computer before you install the MUVPN software.

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 web site using your LiveSecurity® user name and password. Click the **Latest Software** link, then click on your Firebox model. Scroll down to MUVPN Software and click the link for the version you want.

The end-user profile

A file that contains the user name, shared key, and settings that let a remote computer make a secure connection to your trusted network across the Internet. The end-user profile has the filename: *username.wgx*

Policy Manager creates an end-user profile when you add a new MUVPN user to the Firebox.

Two certificates files—if you use certificates to authenticate

Policy Manager creates two files when the you select to authenticate using a certificate. These are the .p12 file, an encrypted file that contains the certificate, and the cacert.pem file, which contains the root certificate (CA or Certificate Authority).

User documentation

End-user brochures developed by WatchGuard are located on the WatchGuard web site at: www.watchguard.com/help/documentation



Note that the MUVPN brochures are formatted for printing and are not designed to be read online, therefore the page numbers in the PDF files are not sequential.

Shared Key

Before an end user can install the end-user profile (the .wgx file), the software prompts them for a shared key. This key decrypts the file and imports the security policy into the MUVPN client. The key is set when the file is created in Policy Manager.



Write the shared key down and keep it in a secure location because you must use it during the final steps of the installation procedure.

Username and Password—if you use Extended Authentication to authenticate

You must supply the end user with the Username and Password for their authentication account. This is defined on the applicable authentication server. For instructions on using Extended Authentication, see “Define an extended authentication group” on page 7

Installing and Uninstalling 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.



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

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 root directory on the remote (client or employee) computer.
If you use 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 you do not complete a step by mistake, you can cancel the procedure, and start again.
- 4 The InstallShield wizard appears. Click **Next**.
During the Setup Status portion of the install procedure, the InstallShield sometimes can find ReadOnly Files only. If this occurs, click Yes for each event to continue the installation.
- 5 A welcome screen appears. Click **Next**.
The Software Licence Agreement appears.
- 6 Click **Yes** to accept the terms of the License Agreement and to continue the installation.
The Setup Type window appears.
- 7 Click the setup type you want. By default, Typical is selected—this is the setup that we recommend. Click **Next**.
- 8 If you install the client on a Windows 2000 host, the InstallShield detects the native Windows 2000 L2TP component. The client uses the native L2TP component and does not install its own L2TP component. Click **OK** to continue the installation.
The Select Components window appears.
- 9 Keep the default components and click **Next**.
The Start Copying Files window appears.

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

A command prompt window appears while the `dni_vapmp` file is installed—this is normal. When this procedure is completed, the installation continues.

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

- 12 The InstallShield Wizard then searches for the end-user profile (the `.wgx` file) in the root directory of the computer, `c:\`. Click **Next**. If the file was not copied to this default directory, you must click the **Browse** button to find and select the correct folder.

- 13 When the InstallShield Wizard is complete, make sure that the check box **Yes, I want to restart my computer now** is enabled and click **Finish**.

The computer restarts.



The ZoneAlarm personal firewall can cause problems with regular local network traffic and prevent access to network resources. If the remote computer is connected to the network after it restarts, this can cause a problem with the network logon process. If in doubt, log on to the computer locally the first time after the installation.

Importing the end-user profile

When the computer restarts, the **WatchGuard Policy Import** dialog box appears. Import the MUVPN end-user profile (the `.wgx` file) and use the shared key that decrypts the file.

- 1 The **WatchGuard Policy Import** window looks for the end-user profile (the `.wgx` file) in the directory you selected during the installation.

If the WatchGuard Policy Import tool does not find the `.wgx` file, click Browse and find the file.

- 2 Type the shared key in the applicable text box and click **OK**.

- 3 You set up the MUVPN client successfully. 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 “Updating the end-user profile” on page 35.



The ZoneAlarm personal firewall may immediately begin to display alerts on your Windows desktop. For more information on ZoneAlarm, see “The ZoneAlarm Personal Firewall,” on page 45.

Updating the end-user profile

At some point, it can become necessary to edit 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 Windows NT authentication to RADIUS.
- The network configuration changes
- A different end user gets the remote computer

First, use Policy Manager to edit and create a new MUVPN end-user profile (the `.wgx` file). For more information, see the previous chapters that describe how to configure your Firebox® when you use a particular type of appliance software.

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, then click Browse and find the file.
- 2 Type or paste the shared key in the applicable text box and click **OK**.
- 3 The MUVPN client is updated. Click **OK**.
The remote computer is now ready to use MUVPN. The Security Policy is automatically activated.

Uninstalling the MUVPN client

At some point, it can become necessary to uninstall the MUVPN client. WatchGuard recommends that you use the Windows Add/Remove Programs tool to uninstall the MUVPN client.

Before you start, disconnect all tunnels and dial-up connections, and then restart the remote computer. Then, from the Windows desktop:

- 1 Click **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 **Change/Remove**.
The InstallShield Wizard window appears.
- 4 Click **Remove** and click **Next**.
The Confirm File Deletion dialog box appears.
- 5 Click **OK** to completely remove all of the components.
A command prompt window appears while the dni_vapmp file is installed—this is normal. When this procedure is completed, the installation continues. The Uninstall Security Policy dialog box appears.
- 6 Click **Yes** to delete the Security Policy Personal Certificates and Private/Public Keys.
The InstallShield Wizard window appears.
- 7 Make sure the option **Yes, I want to restart my computer now** is enabled and click **Finish**.
The computer will restart.



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

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

Windows XP: c:\windows\internet logs

If you want to ignore these settings, delete the contents.

- 8 When the computer restarts, click **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 make a secure, encrypted connection to a protected network across 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, make an Internet connection through Dial-Up Networking, through a local area network (LAN), or wide area network (WAN).

From the Windows desktop system tray:

- 2 Make sure that the MUVPN client is activated. If it is not, right-click the icon and select **Activate Security Policy**.

For information on how to find the status of the MUVPN icon, see the section “The Mobile User VPN client icon”.

Then, from the Windows desktop:

- 3 Click **Start > Programs > Mobile User VPN > Connect**.
The WatchGuard® Mobile User Connect widow appears.
- 4 Click **Yes**.

If you are using Extended Authentication, you are prompted for the username and passphrase you created on the authentication server. Type the name and passphrase and click **OK**.



For more information regarding Extended Authentication, see “Define an extended authentication group” on page 7.

The Mobile User VPN client icon

The Mobile User VPN icon is in the Windows desktop system tray and shows different status images. A list of the images and a brief description of each follows:

Deactivated



The MUVPN Security Policy is deactivated or the Windows operating system did not start a necessary Mobile User VPN service correctly 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 make a secure, MUVPN tunnel connection.

Activated and Transmitting Unsecured Data



The MUVPN client is ready to make a secure, MUVPN tunnel connection. The red bar on the right side of the icon shows that the client is transmitting unsecured data.

Activated and Connected



The MUVPN client makes one secure, MUVPN tunnel connection but is not transmitting data.

Activated, Connected and Transmitting Unsecured Data



The MUVPN client makes one secure, MUVPN tunnel connection. The red bar on the right side of the icon shows that the client is transmitting only unsecured data.

Activated, Connected and Transmitting Secured Data



The MUVPN client makes one secure, MUVPN tunnel connection. The green bar on the right side of the icon shows that the client is transmitting only secured data.

Activated, Connected and Transmitting both Secure and Unsecured Data



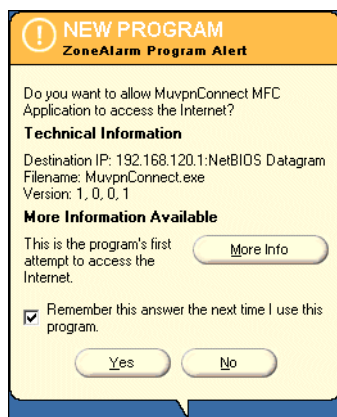
The MUVPN client makes one secure, MUVPN tunnel connection. The red and green bars on the right side of the icon shows that the client is transmitting secured and unsecured data.

Allowing the MUVPN client through the personal firewall

There are two software applications associated with the MUVPN client, which you *must* allow through the personal firewall to make an MUVPN tunnel:

- MuvpnConnect.exe
- IrelKE.exe

The personal firewall detects when these software applications try to connect to the Internet. The **New Program Alert** dialog box appears and requests a connection for the MuvpnConnect.exe program.



From the ZoneAlarm alert dialog box:

- 1 Select the **Remember this answer the next time I use this program** option and click **Yes**.
This lets ZoneAlarm allow the MuvpnConnect.exe program through each time you try to make a MUVPN connection.
The New Program alert dialog box appears requesting access for the IrelKE.exe program.

- 2 Select the **Remember this answer the next time I use this program** option and click **Yes**.
This lets ZoneAlarm allow the IrelKE.exe program through each time you try 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:

- 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 action does not change your connection to the Internet. You must disconnect from the Internet in a different procedure.
- 3 Right-click the **Mobile User VPN** client icon and select **Deactivate Security Policy**.
The MUVPN icon displays a red slash to show a deactivated Security Policy.

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

From the Windows desktop system tray:

- 1 Right-click the **ZoneAlarm** icon and select **Shutdown ZoneAlarm**.



The ZoneAlarm dialog box appears.

- 2 Click **Yes** when prompted to quit ZoneAlarm.

Monitor the MUVPN Client Connection

You can use two tools with the MUVPN client to monitor your connection and find problems that can occur: LogViewer and the Connection Monitor.

LogViewer

LogViewer displays the Communications Log, a diagnostic tool that includes 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 Click **Log Viewer**.
The Log Viewer window appears.

Connection Monitor

The Connection Monitor displays statistical and diagnostic information for each active connection in the security policy. This module shows the security policy settings and the security association (SA) information made 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, when a Phase 2 IPSec SA fails to make a connection, or when the connection is not yet made.
- 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 shows that the client is processing secure IP traffic for that connection.
- When one Phase 1 SA to a gateway protects many 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.

4

Troubleshooting Tips for the MUVPN Client

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 type your Windows network user name, password and domain. It is very important that you type 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 computer from sending the necessary login information. Make sure you 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, shows a key within the icon when 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 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-down 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” check box, 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 allow access to only a single network domain. If your company is large enough to require subnetting (multiple networks connected together), you can browse only your own domain. Attempts to access other domains result in a password prompt.

It takes a very 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 cannot 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 cannot use the company network

There may be a problem with the end-user profile (the .wgx file) or shared passwords.

I see ESP-Auth errors in Traffic Monitor. Is this a problem?

If you use an MUVPN client behind a NAT device, you can sometimes see error messages such as that shown below in Traffic Monitor. If your MUVPN traffic is not affected, you can safely ignore these messages.

```
2007-01-31 21:04:55 ESP-Auth-Error 8001 PRIMARY: ESP-Auth-Error detected, ESP
Authentication error, policy_id = 13, local_ip=100.0.0.1, peer_ip=10.10.100.1,
spi=1354113665, sa_id=1354113665, interface=0. proc_id="ma" time="Wed Jan 31
21:04:55 2007 (PST)" hostname="HA-X8500e.wgti.net"
```

```
2007-01-31 22:31:53 ESP-Auth-Error 8001 PRIMARY: ESP-Auth-Error detected, ESP
Authentication error, policy_id = 17, local_ip=100.0.0.1, peer_ip=10.10.100.1,
spi=1354113195, sa_id=1354113195, interface=0. proc_id="ma" time="Wed Jan 31
22:31:53 2007 (PST)" hostname="HA-X8500e.wgti.net"
```

I see many log messages that refer to "Invalid_SPI" on my MUVPN clients' Log Viewer. Is this a problem?

If your MUVPN user has no problems with their MUVPN connection, these messages can be safely ignored.

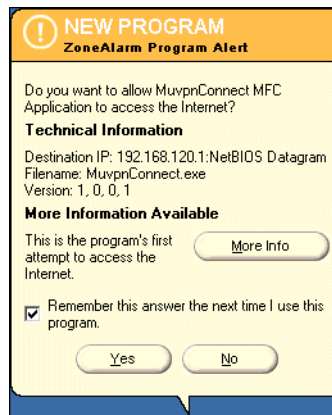
5

The ZoneAlarm Personal Firewall

A personal firewall is a barrier between your computer and outside threats. The computer is most vulnerable at its doors, which are referred to as ports. Without ports, no connection to the Internet is possible.

ZoneAlarm protects these ports by using a simple rule: Block all incoming traffic and outgoing traffic unless you explicitly allow the traffic.

When using ZoneAlarm, you frequently see **Program Alert** dialog boxes that look similar to the image below.



This dialog box appears when one of your software applications (in this example, Internet Explorer) tries to get access to the Internet or your local network. This powerful feature does not let information leave your computer without your permission.

If you enable the **Remember the answer each time I use this program** check box, then you only have to answer this question once for each program.

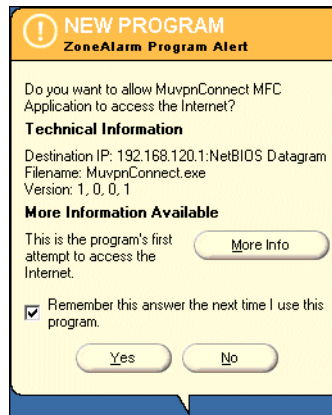
ZoneAlarm Features

The ZoneAlarm personal firewall gives you a short tutorial of the product immediately after you install the MUVPN client. Read each step carefully to get to know the software application.

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

Allowing Traffic through ZoneAlarm

When a software application requires access through the ZoneAlarm personal firewall, a Program Alert is displayed on the Windows desktop showing the user which application requires access. Frequently the program associated with the software application is not indicative of the application the user wants to use.



In the example above, the Internet Explorer web browser application is trying to connect with the user's home page. The program that actually must pass through the firewall is "IEXPLORE.EXE".

To allow the program through the firewall each time it executes, enable the **Remember the answer the next time I use this program** check box.

Here is a list of a few essential programs which must pass through the ZoneAlarm personal firewall to use some important software applications.

Programs that must be allowed

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

Programs that can be allowed

<i>MS Outlook</i>	OUTLOOK.exe
<i>MS Internet Explorer</i>	IEXPLORE.exe
<i>Mozilla Firefox</i>	firefox.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 **Yes** when prompted to quit ZoneAlarm.

Uninstalling ZoneAlarm

From the Windows desktop:

- 1 Click **Start > Programs > Zone Labs > Uninstall ZoneAlarm**.
The Confirm Uninstall dialog box appears.
- 2 Click **Yes**.
The ZoneLabs TrueVector service dialog box appears.
- 3 Click **Yes** to continue with uninstalling the TrueVector service and disable its Internet Security features.
The Select Uninstall Method window appears.
- 4 Make sure that **Automatic** is selected and click **Next**.
- 5 Click the **Finish** button to perform the uninstall.



*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 **OK** to restart your system.

Symbols

.exp files 3, 14
.p12 file 11, 24, 33
.wgx file 33
.wgx files 3, 14

A

Add Mobile User VPN wizard 15
Advanced Export File Preferences dialog box 8, 21
Advanced Mobile User VPN Policy Configuration dialog box 7
Any service
 and MUVPN 9, 10, 23
authentication server
 specifying 7
 types supported 6
authentication, extended. See extended authentication

C

ca-cert.pem 11, 24, 33
certificates
 files in end-user profile 11, 24
certificates, files required if authenticating using 33
Client for Microsoft Networks
 installing on Windows 2000 computers 30
Connection Monitor, monitoring MUVPN client through 39

D

dialog boxes
 Advanced Export File Preferences 8, 21
 IPSec Logging 11
Diffie-Hellman groups
 described 20
DNS servers, configuring 3

E

encryption
 and MUVPN 2, 13
end-user profile
 described 33
 importing 35
 updating 35
end-user profiles for MUVPN users
 described 1, 13
 distributing to remote users 10, 23
 locking 8, 21
 preparing 3, 14
 regenerating 10, 23
 saving 10, 23
extended authentication
 defining groups for 6
 specifying authentication method for 7
 specifying server 7

F

- File and Printer Sharing for Microsoft Networks
 - and Windows 2000 30
 - and Windows XP 32
- Fireboxes
 - configuring for MUVPN 1, 13

I

- IKE
 - and Diffie-Hellman group 20
- Internet
 - accessing through IPSec tunnel 5, 21
 - accessing through tunnel 5
- Internet Protocol (TCP/IP) Network Component
 - and Windows 2000 29
 - and Windows XP 31
- IPSec Logging dialog box 11
- ISAKMP
 - and Diffie-Hellman groups 20

M

- MD5-HMAC 4
- Mobile User VPN Wizard 15
- Mobile User VPN wizard 4, 5, 7
- Mobile User VPN. See MUVPN
- MUVPN
 - adding license keys 2, 25
 - allowing Internet access through 5, 21
 - and virtual adapters 8, 21
 - authentication for 1, 13
 - configuring debugging options 11
 - configuring services to allow 9, 22
 - configuring shared servers for 2, 13
 - connecting with Pocket PC 4
 - defining new user 3
 - described 1, 13
 - disconnecting 39
 - distributing end-user profiles 10, 23
 - encryption levels for 2, 13
 - end-user profiles. See end-user profiles for MUVPN users
 - making outbound connections behind Firebox 11, 24
 - modifying existing user 5, 16
 - preparing configuration files for 3, 14
 - preparing end-user profiles 3, 14
 - purchasing license for 2, 25
 - setting encryption for 5
 - specifying authentication method 4, 7
 - system requirements for 28
 - troubleshooting 42
 - with extended authentication 6
- MUVPN client
 - allowing through firewall 38
 - connecting using 36
 - icon for 37
 - installing 34
 - monitoring connection for 39
 - removing 36
- Muvpn.exe 33
- MuvpnLite.exe 33

N

NAT Traversal 20

O

Outgoing service 10

P

Pocket PC 4

R

Remote Access Server, installing on Windows NT 28

S

services

- configuring to allow MUVPN traffic 9, 22

SHA1-HMAC 4

shared key 34

split tunneling 5

- described 5

system requirements 27

T

troubleshooting tips 41

V

virtual adapter for MUVPN users 8, 21

VPNs

- design considerations 5

- split tunneling 5

- terminating 12, 24

W

Windows 2000

- installing Client for Microsoft Networks on 30

- installing File and Printer Sharing for Microsoft Networks on 30

- installing Internet Protocol (TCP/IP) Network Component on 29

- WINS and DNS settings 30

Windows NT

- installing Remote Access Server on 28

- WINS and DNS settings 28

Windows XP

- installing Client for Microsoft Networks on 32

- installing File and Printer Sharing for Microsoft Networks on 32

- installing Internet Protocol (TCP/IP) Network Component on 31

- WINS and DNS settings 32

WINS and DNS settings

- on Windows 2000 computers 30

- on Windows NT computers 28

- on Windows XP computers 32

WINS servers, configuring 3

Z

ZoneAlarm

allowing MUVPN client through 38

described 27

troubleshooting 41