WatchGuard PINsafe Integration

Table of Contents

1. Introduction

This document describes the integration of PINsafe with the WatchGuard VPN solutions

2. Overview

2.1. Prerequisites

PINsafe 3.x
Watchguard Firewall with VPN

2.2. Baseline

PINsafe 3.7
Watchguard Firebox X750e Core

2.3. Architecture

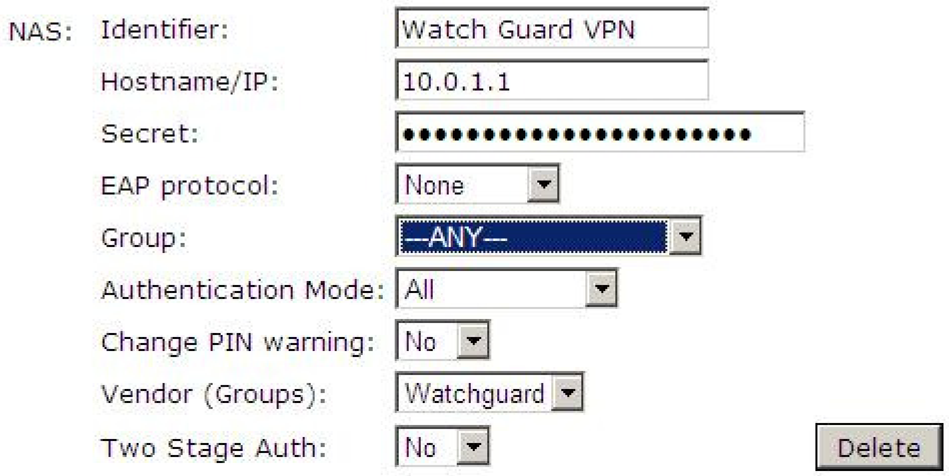
The WatchGuard Firebox accepts VPN connections by SSL or VPN client and uses RADIUS to authenticate users against the PINsafe server by checking the users username and One Time Code.

3. Installation

3.1. Configure The PINsafe Server

Configure a RADIUS NAS entry

1. Ensure the RADIUS server is running on PINsafe, on the PINsafe Management Console select RADIUS/Server, Server Enabled should be Yes
2. On the PINsafe Management Console select RADIUS NAS
3. Enter a name for the NAS
4. Enter the WatchGuard internal IP address
5. Enter the shared secret
6. Optionally if RADIUS groups are to be used then set the Vendor (Groups): to WatchGuard. When a RADIUS request is made this will return Filter ID 11, with the Group Nmae that the user is a member of. This can be used for assigning policies to users based on group membership.
7. Click on Apply to save changes

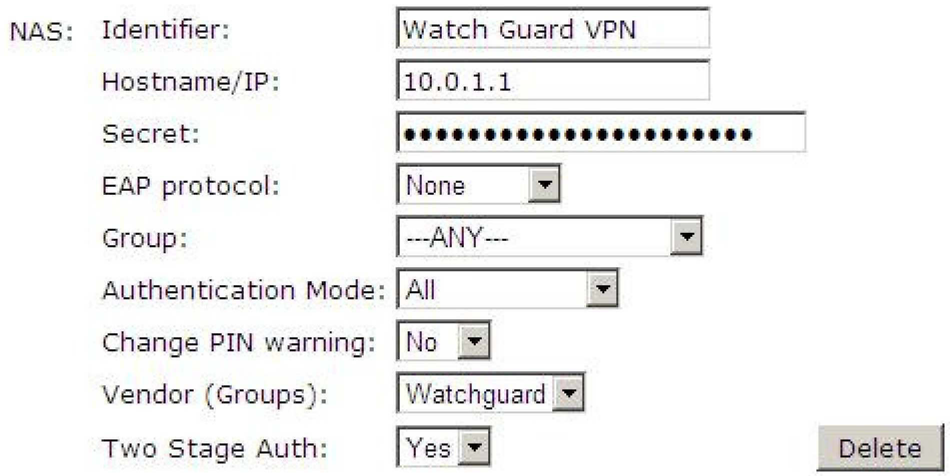


NAS:	Identifier:	Watch Guard VPN
	Hostname/IP:	10.0.1.1
	Secret:	••••••••••••••••••••••
	EAP protocol:	None
	Group:	---ANY---
	Authentication Mode:	All
	Change PIN warning:	No
	Vendor (Groups):	Watchguard
	Two Stage Auth:	No

3.1.1. Optional: Two Stage Authentication

This is where a user enters a password, and then is taken to a second page for a One Time Code. The user must have a password for authentication.

To Allow Two Stage Authentication, on the PINsafe Administration Console select Radius/NAS, ensure Two Stage Authentication is set to Yes.

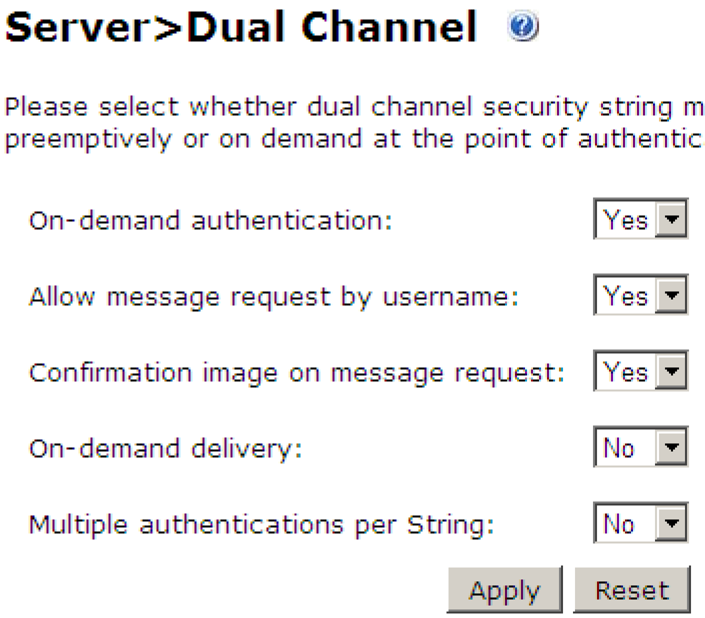


NAS:	Identifier:	Watch Guard VPN
	Hostname/IP:	10.0.1.1
	Secret:	••••••••••••••••••••••
	EAP protocol:	None
	Group:	---ANY---
	Authentication Mode:	All
	Change PIN warning:	No
	Vendor (Groups):	Watchguard
	Two Stage Auth:	Yes

3.1.2. Optional: Challenge and Response Using SMS

This is where a user enters a password, and if this is correct the user will then be sent automatically a One Time Code for authentication by their transport.

To Allow Challenge and Response Authentication using SMS, first configure Two Stage Authentication. On the PINsafe Administration Console select Server/Dual Channel, and ensure On-Demand Authentication is set to Yes.

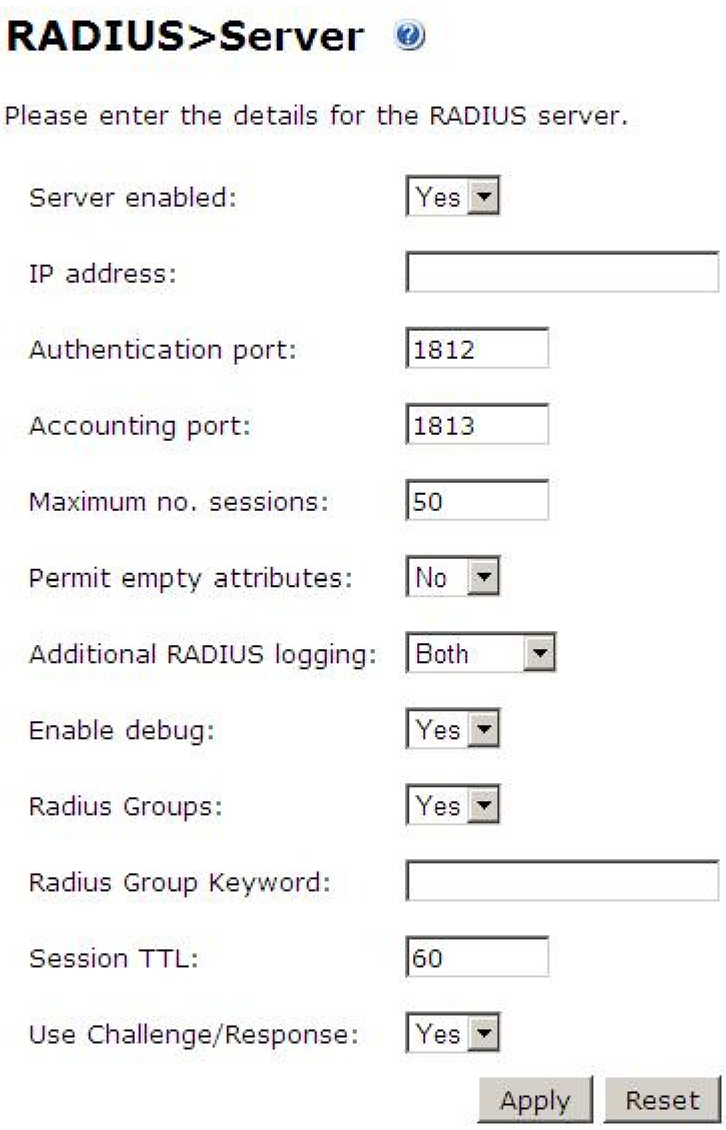


Server>Dual Channel

Please select whether dual channel security string messages are delivered preemptively or on demand at the point of authentication.

On-demand authentication:	Yes
Allow message request by username:	Yes
Confirmation image on message request:	Yes
On-demand delivery:	No
Multiple authentications per String:	No

Then select on the PINsafe Administration Console RADIUS/Server, ensure the Use Challenge/Response is set to Yes.



RADIUS>Server

Please enter the details for the RADIUS server.

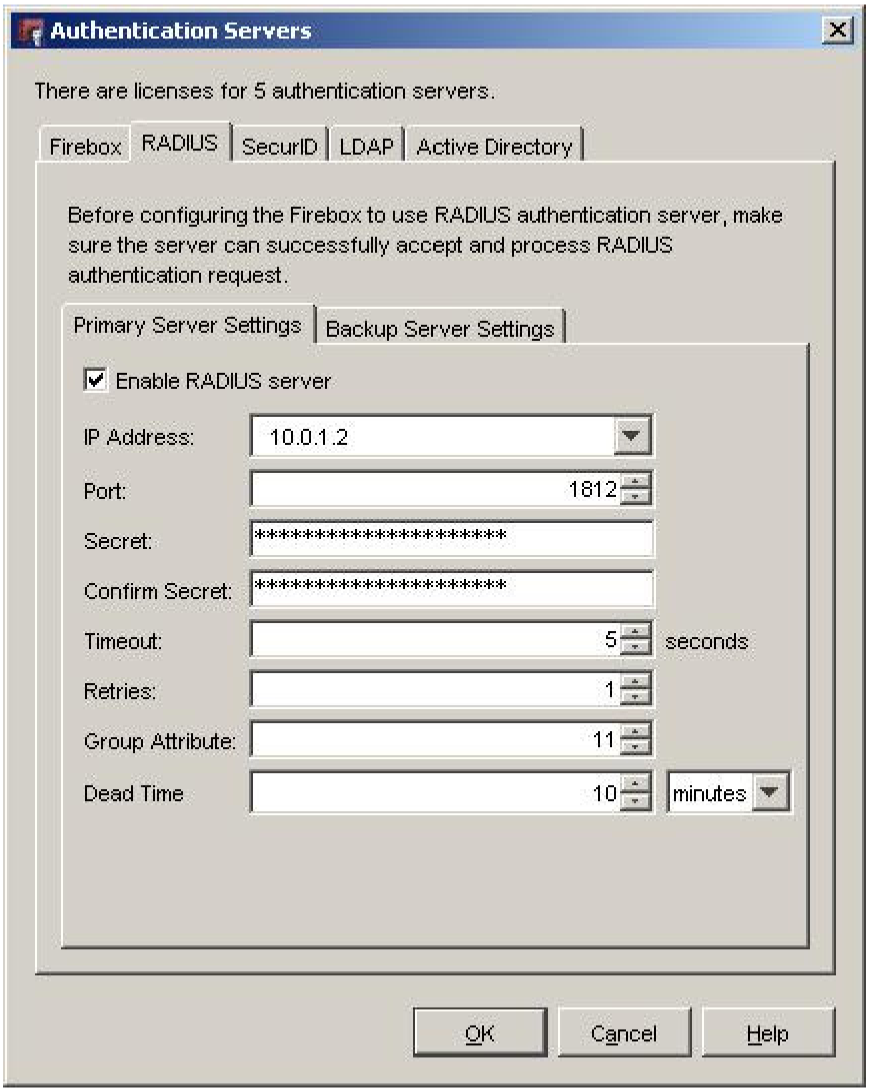
Server enabled:	Yes
IP address:	
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No
Additional RADIUS logging:	Both
Enable debug:	Yes
Radius Groups:	Yes
Radius Group Keyword:	
Session TTL:	60
Use Challenge/Response:	Yes

3.2. Configure The WatchGuard Server

3.2.1. Configure The Authentication Server Settings

On the WatchGuard Policy Manager create an authentication server

1. Select Setup/Authentication/Authentication Servers
2. From the Tabs select RADIUS (or also SecureID has been recommended as it has been designed for One Time Codes)
3. Configure the following settings:
    - IP Address of the PINsafe server
    - Port used for RADIUS, usually 1812
    - Shared Secret that has been entered on the PINsafe server
4. When settings have been configured click on OK.



There are licenses for 5 authentication servers.

Before configuring the Firebox to use RADIUS authentication server, make sure the server can successfully accept and process RADIUS authentication request.

☑ Enable RADIUS server

IP Address: 10.0.1.2

Port: 1812

Secret: *********************

Confirm Secret: *********************

Timeout: 5 seconds

Retries: 1

Group Attribute: 11

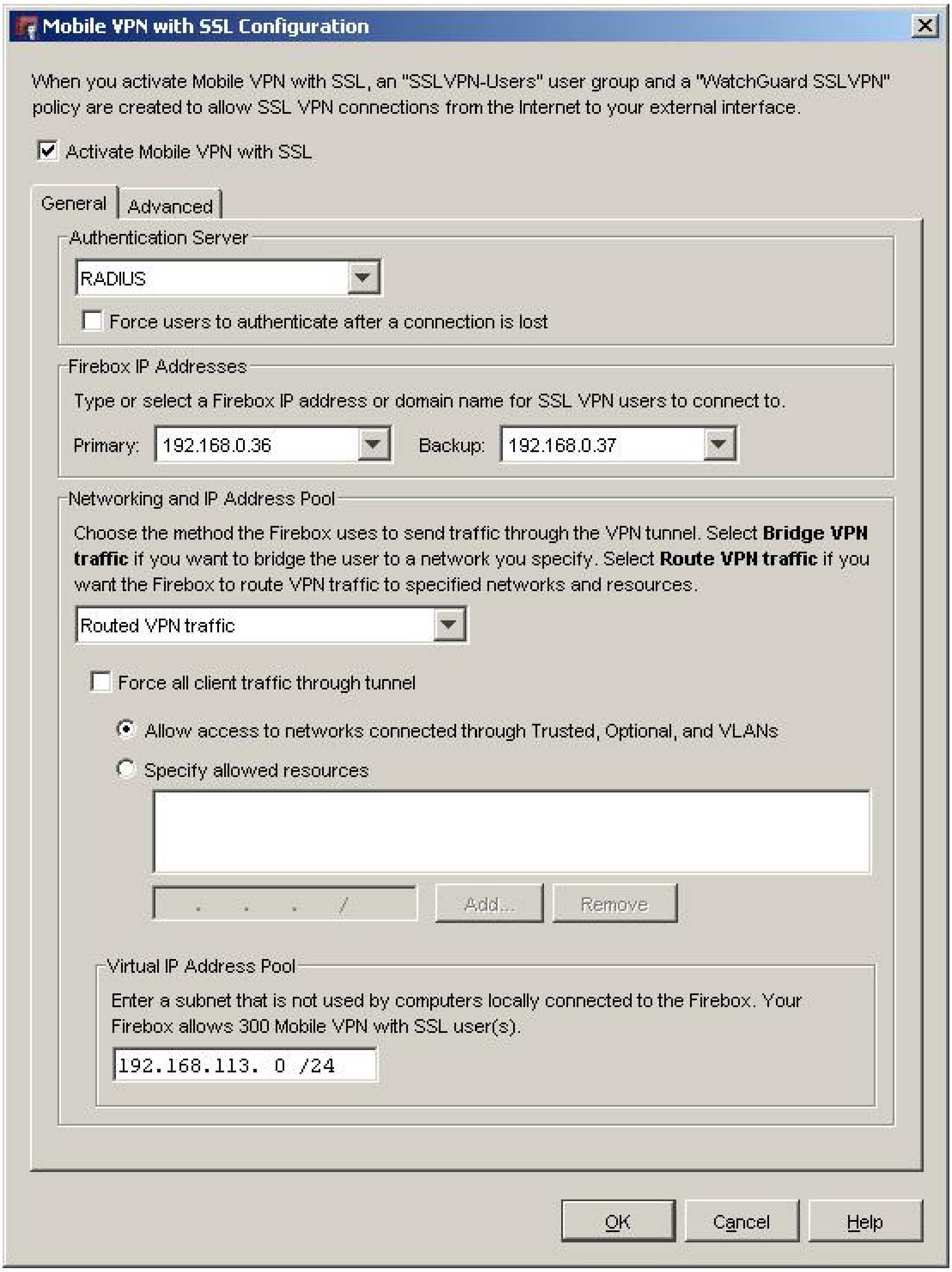
Dead Time 10 minutes

3.2.2. Configuration for Mobile SSL VPN

Configure the WatchGguard for Mobile SSL VPN use.

1. Select VPN/Mobile VPN/SSL.
2. In the Mobile VPN with SSL Configuration configure the following settings:
   - Ensure the Activate Mobile VPN with SSL is ticked.
   - Enter the previously configured Authentication Server
   - It is recommended to Force users to authenticate after a connection is lost by selecting the tick box.
   - Enter the IP Address or hostname for users to connect to
   - Configure Networking and IP address Pool as required
3. When completed click OK

Note: When you enable Mobile VPN with SSL, an SSLVPN-Users group is created automatically.



Mobile VPN with SSL Configuration

When you activate Mobile VPN with SSL, an "SSLVPN-Users" user group and a "WatchGuard SSLVPN" policy are created to allow SSL VPN connections from the Internet to your external interface.

☑ Activate Mobile VPN with SSL

Authentication Server

RADIUS

□ Force users to authenticate after a connection is lost

Firebox IP Addresses

Type or select a Firebox IP address or domain name for SSL VPN users to connect to.

Primary: 192.168.0.36 Backup: 192.168.0.37

Networking and IP Address Pool

Choose the method the Firebox uses to send traffic through the VPN tunnel. Select **Bridge VPN traffic** if you want to bridge the user to a network you specify. Select **Route VPN traffic** if you want the Firebox to route VPN traffic to specified networks and resources.

Routed VPN traffic

□ Force all client traffic through tunnel

● Allow access to networks connected through Trusted, Optional, and VLANs

○ Specify allowed resources

Virtual IP Address Pool

Enter a subnet that is not used by computers locally connected to the Firebox. Your Firebox allows 300 Mobile VPN with SSL user(s).

192.168.113. 0 /24

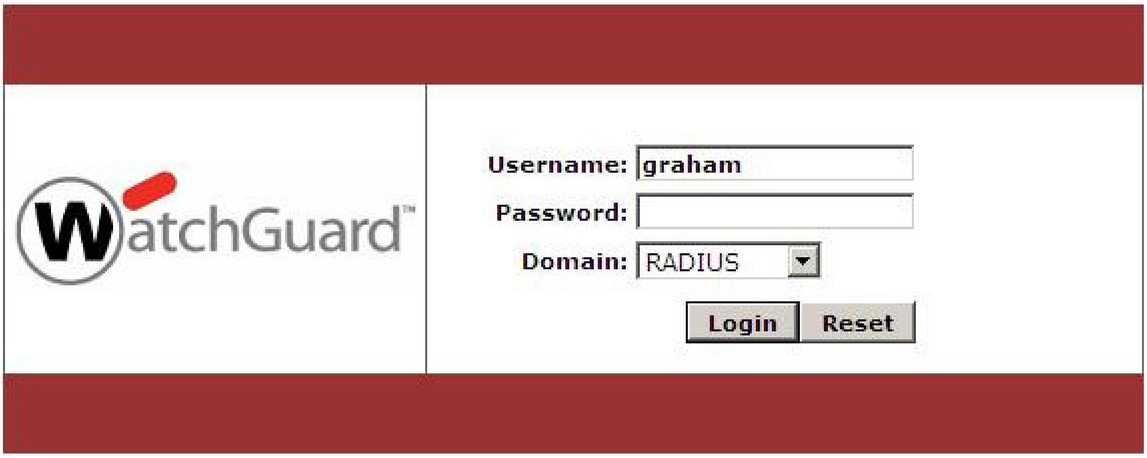
To Allow Mobile VPN with SSL users to access a trusted network

1. Click the plus (+) icon on the Policy Manager toolbar. You can also select Edit/Add Policies.
2. In the The Add Policies dialog box, click the plus (+) icon on the left side of Packet Filters.
3. A list of templates for packet filters appears, select Any and click Add.
4. In the New Policy Properties dialog box, enter a name for the policy in the Name text box. Choose a name that will help you identify this policy in your configuration.
5. On the Policy tab, in the From area, select Any-Trusted and click Remove.

6. In the From area, click Add.
7. The Add Address dialog box opens and The Add Member dialog box appears. Click Add User. For the two Type drop-down lists, select SSL VPN for the first and Group for the second.
8. Select SSLVPN-Users and click Select.
9. Click OK to close the Add Address dialog box.
10. In the From area, select Any-External and click Remove.
11. In the To area, click Add.
12. In the Add Address dialog box select the Available Members list, and select Any-Trusted and click Add.
13. Click OK twice and click Close.
14. Save the changes to the WatchGuard device.

3.2.3. Connecting using the Mobile SSL VPN

Open a web browser and connect to the WatchGuard SSL VPN portal



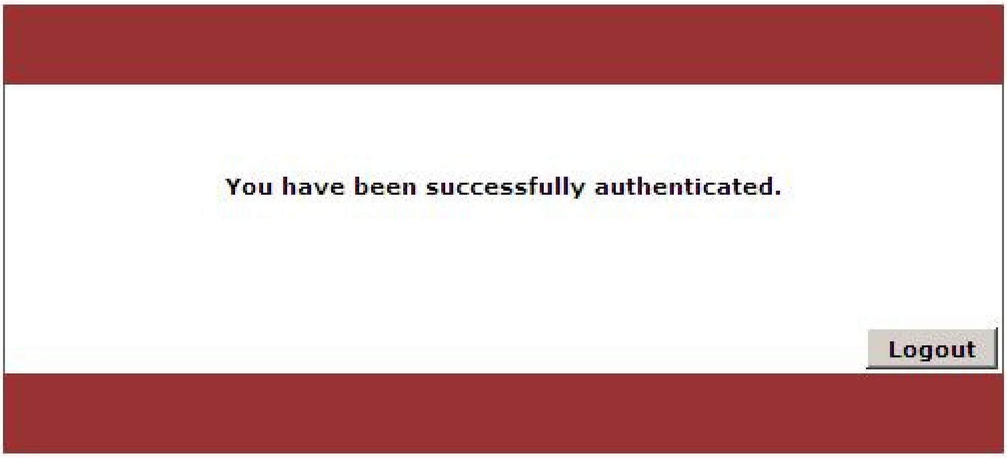
Username: graham

Password:

Domain: RADIUS

Enter the username, then enter the PINsafe One Time Code, possible sources of the One Time Code are:

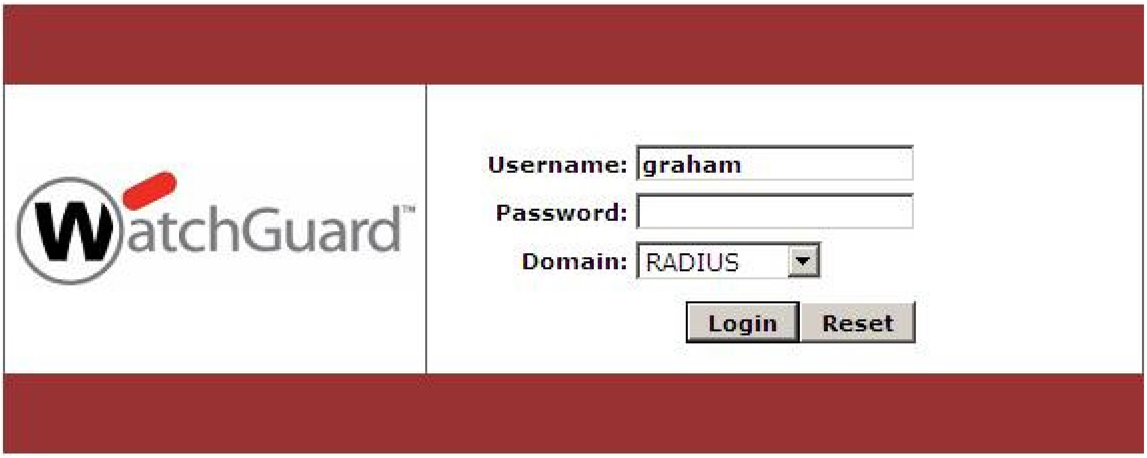
- SMS Text Message
- PINsafe Taskbar utility or Single Channel image
- Mobile Phone Applet



You have been successfully authenticated.

3.2.4. Optional: SSL VPN Authentication using Two Stage or Two Stage and Challenge and Response

Enter Username and Password

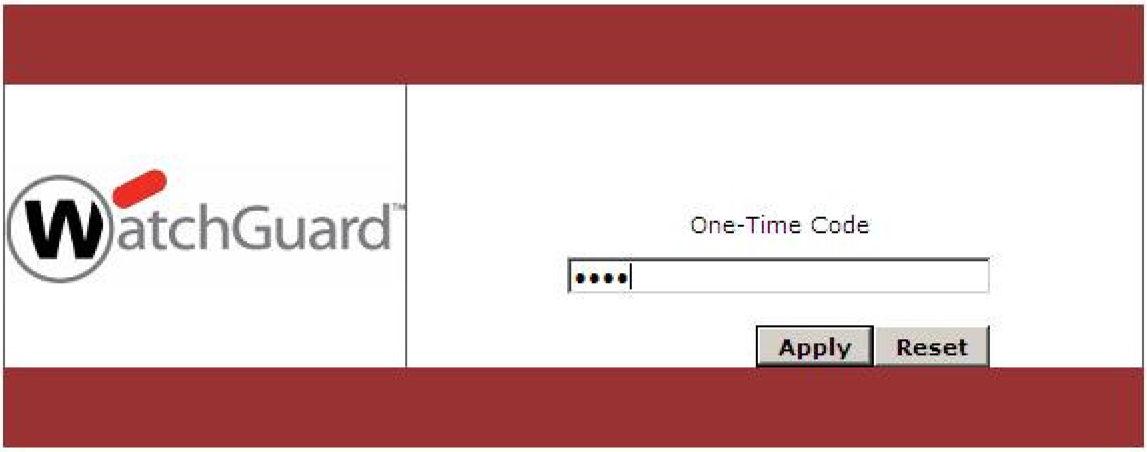


Username: graham

Password:

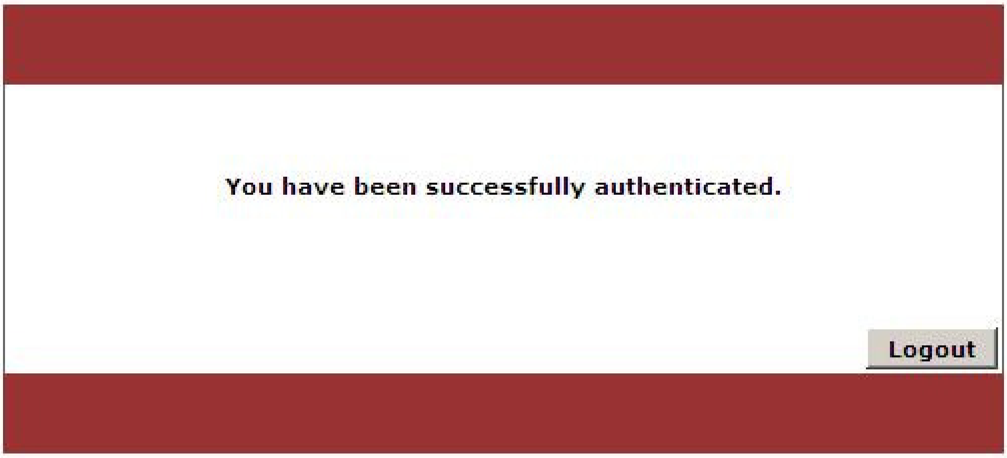
Domain: RADIUS

Enter One Time Code



One-Time Code

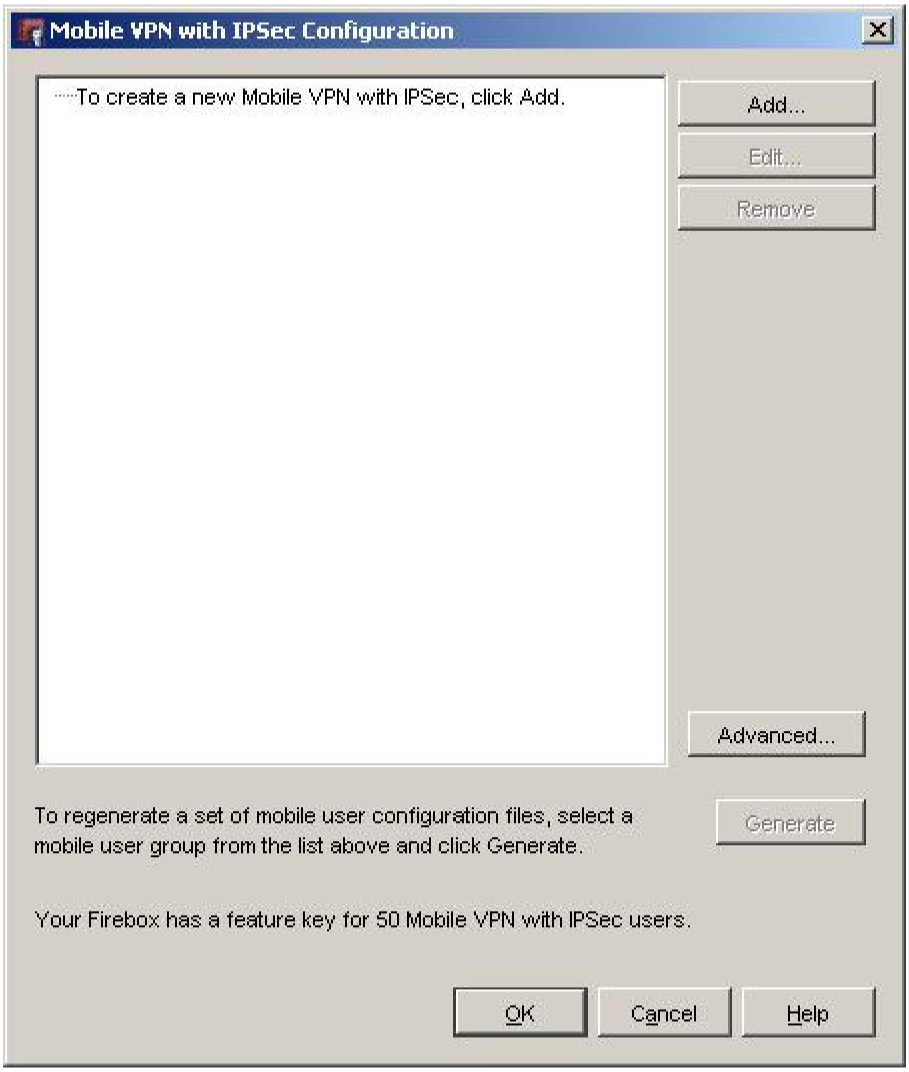
••••



You have been successfully authenticated.

3.2.5. Configuration of VPN Gateway for VPN IPSEC Client

1. From the WatchGuard Policy Manager select VPN/Mobile VPN/IPSec… then click Add.



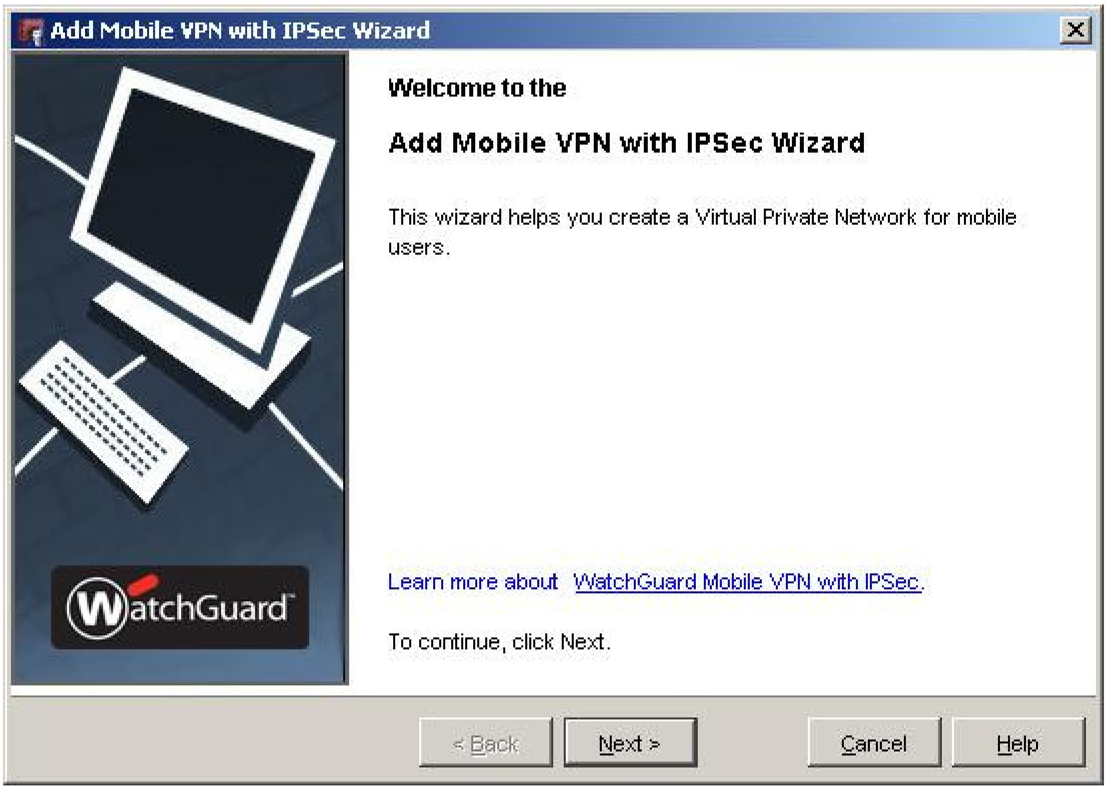
Mobile VPN with IPSec Configuration

To create a new Mobile VPN with IPSec, click Add.

To regenerate a set of mobile user configuration files, select a mobile user group from the list above and click Generate.

Your Firebox has a feature key for 50 Mobile VPN with IPSec users.

2. The Add Mobile VPN with IPSec Wizard starts, click Next.



Welcome to the

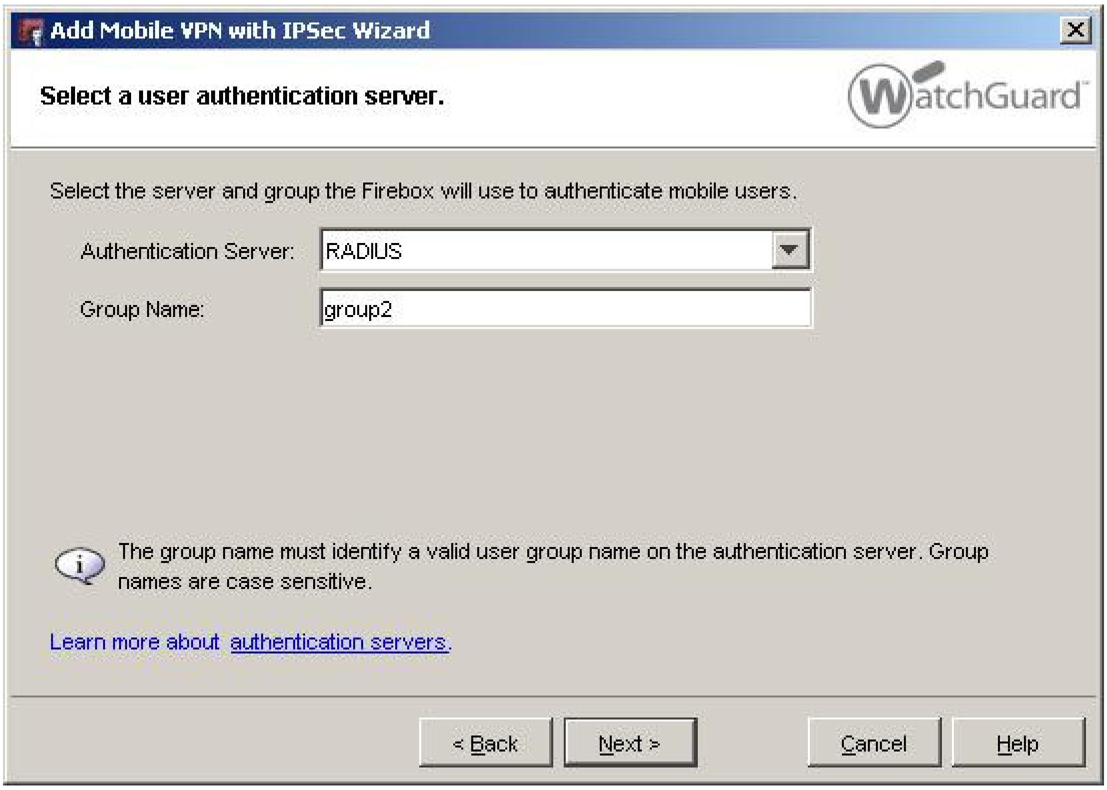
Add Mobile VPN with IPSec Wizard

This wizard helps you create a Virtual Private Network for mobile users.

Learn more about WatchGuard Mobile VPN with IPSec.

To continue, click Next.

3. Select the authentication server, and enter a group name.



Select a user authentication server.

Select the server and group the Firebox will use to authenticate mobile users.

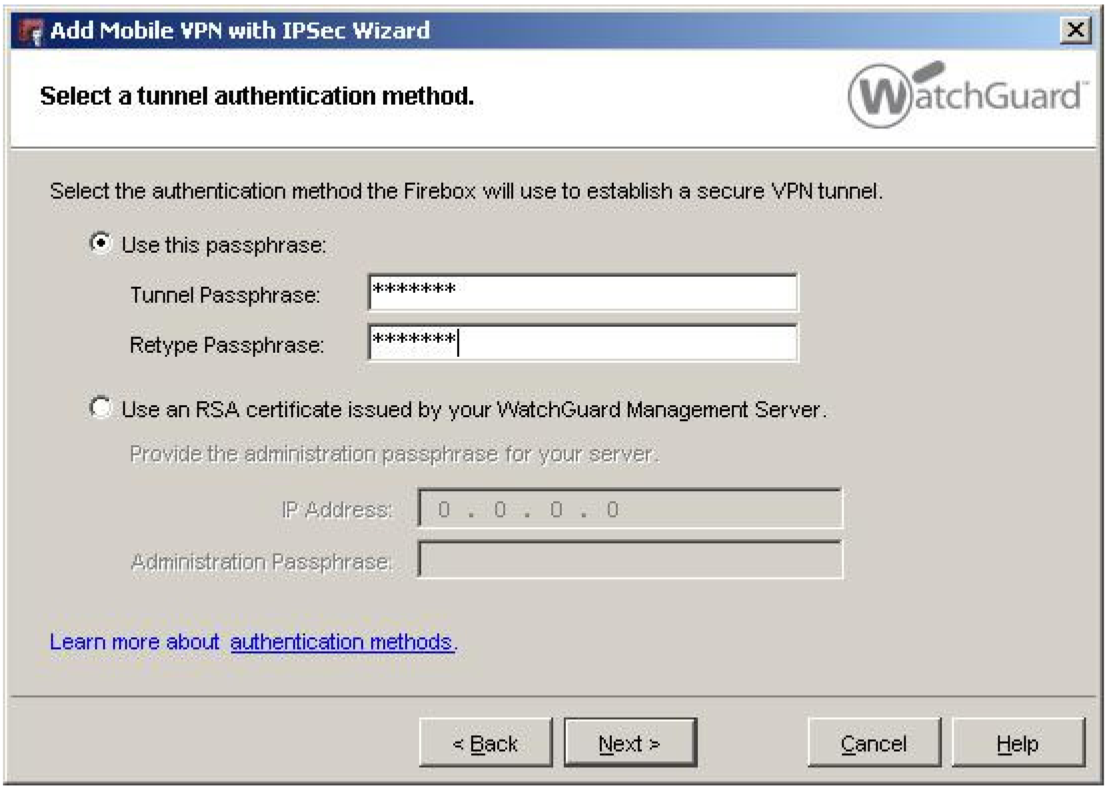
Authentication Server: RADIUS

Group Name: group2

The group name must identify a valid user group name on the authentication server. Group names are case sensitive.

Learn more about authentication servers.

4. Enter a passphrase for the VPN Tunnel



Add Mobile VPN with IPSec Wizard

Select a tunnel authentication method.

Select the authentication method the Firebox will use to establish a secure VPN tunnel.

● Use this passphrase:

Tunnel Passphrase: *******

Retype Passphrase: *******

○ Use an RSA certificate issued by your WatchGuard Management Server.

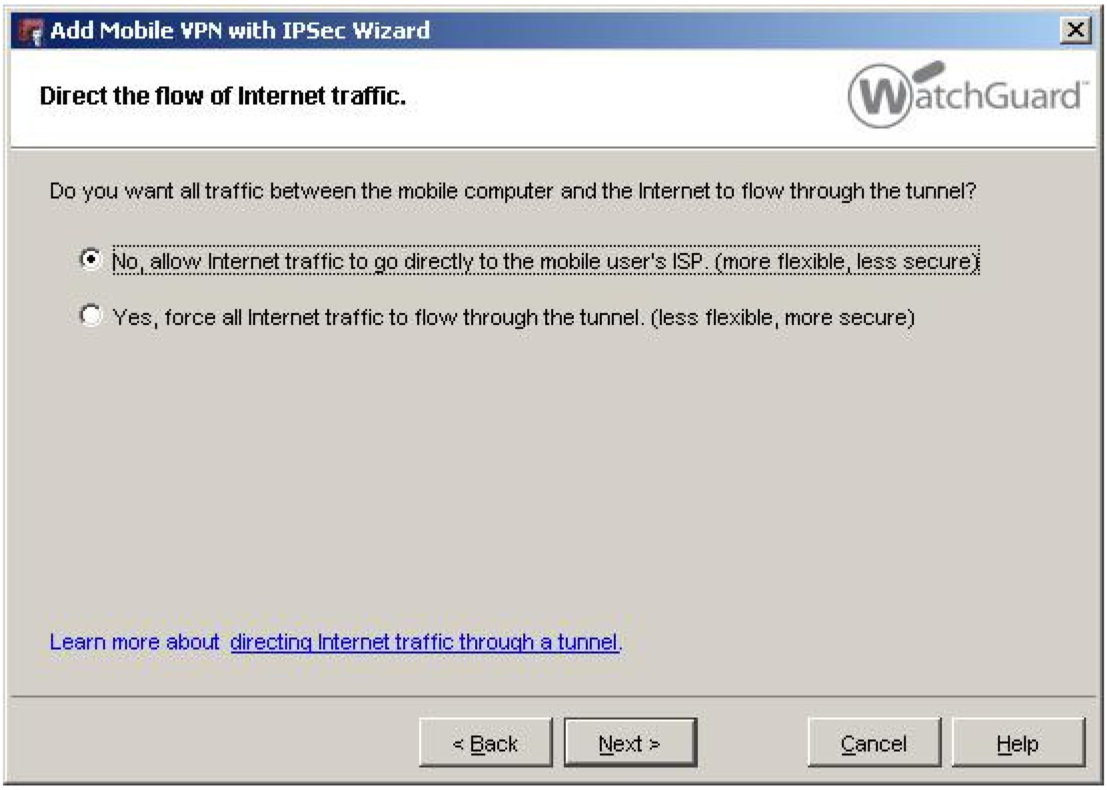
Provide the administration passphrase for your server.

IP Address: 0 . 0 . 0 . 0

Administration Passphrase:

Learn more about authentication methods.

5. Select how users traffic will be routed.



Add Mobile VPN with IPSec Wizard

Direct the flow of Internet traffic.

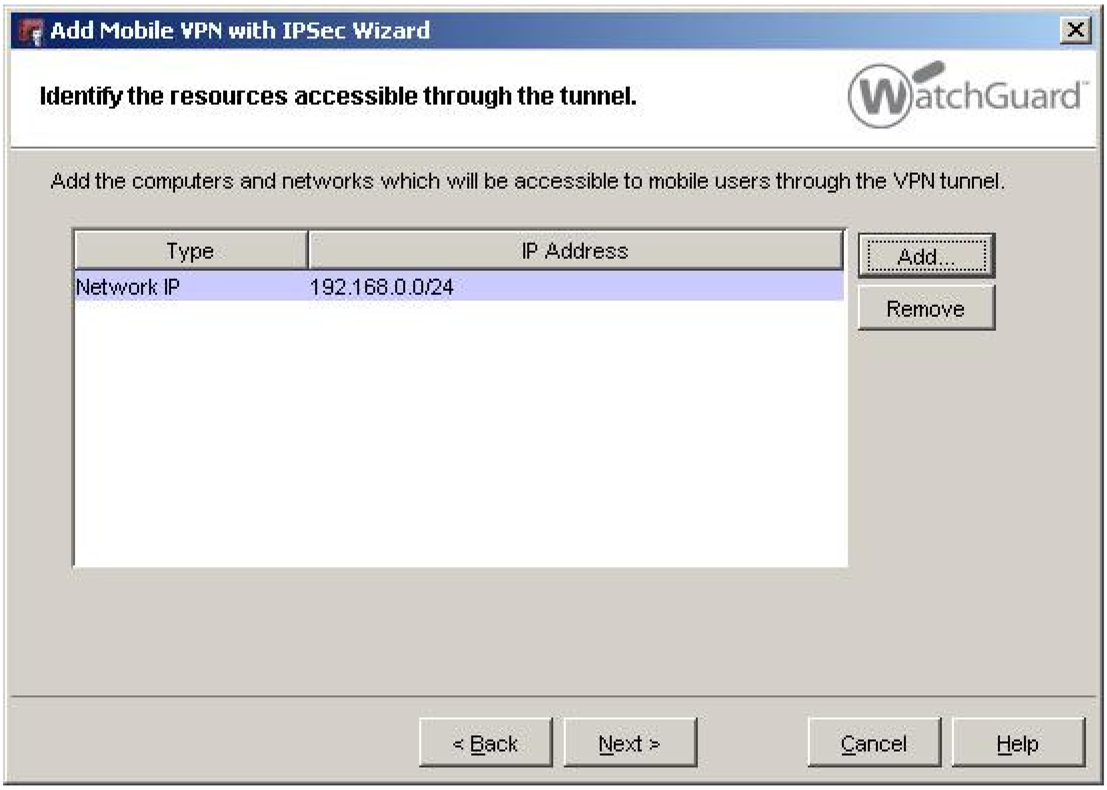
Do you want all traffic between the mobile computer and the Internet to flow through the tunnel?

● No, allow Internet traffic to go directly to the mobile user's ISP. (more flexible, less secure)

○ Yes, force all Internet traffic to flow through the tunnel. (less flexible, more secure)

Learn more about directing Internet traffic through a tunnel.

6. Enter the resources that are available through the VPN



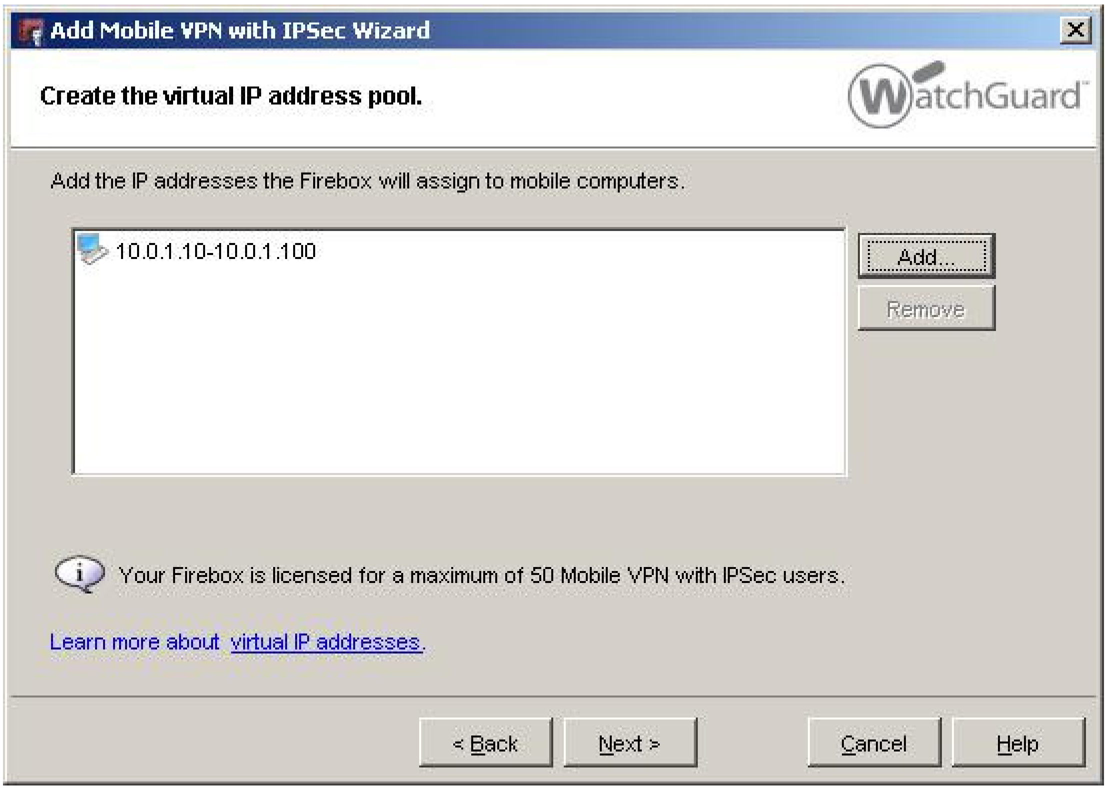
Add Mobile VPN with IPSec Wizard

Identify the resources accessible through the tunnel.

Add the computers and networks which will be accessible to mobile users through the VPN tunnel.

Type	IP Address
Network IP	192.168.0.0/24

7. Enter the IP address ranges that are available to users



Add Mobile VPN with IPSec Wizard

Create the virtual IP address pool.

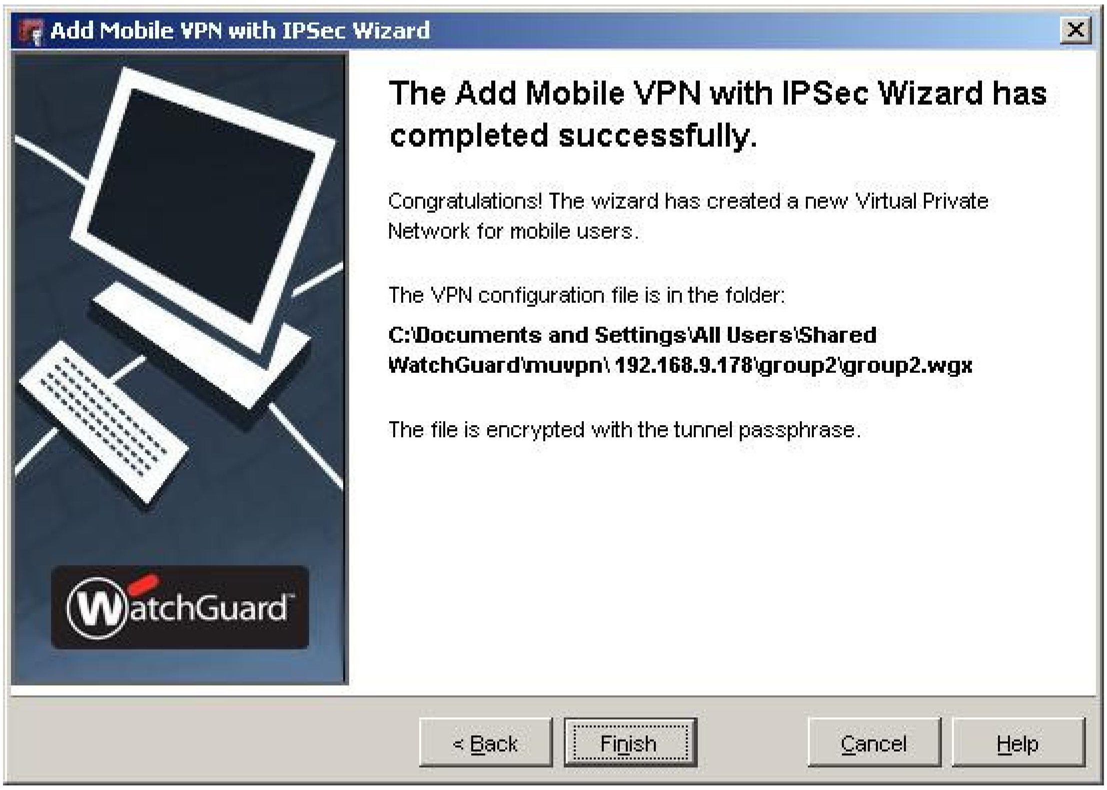
Add the IP addresses the Firebox will assign to mobile computers.

10.0.1.10-10.0.1.100

Your Firebox is licensed for a maximum of 50 Mobile VPN with IPSec users.

Learn more about virtual IP addresses.

8. When complete click on Finish



The Add Mobile VPN with IPSec Wizard has completed successfully.

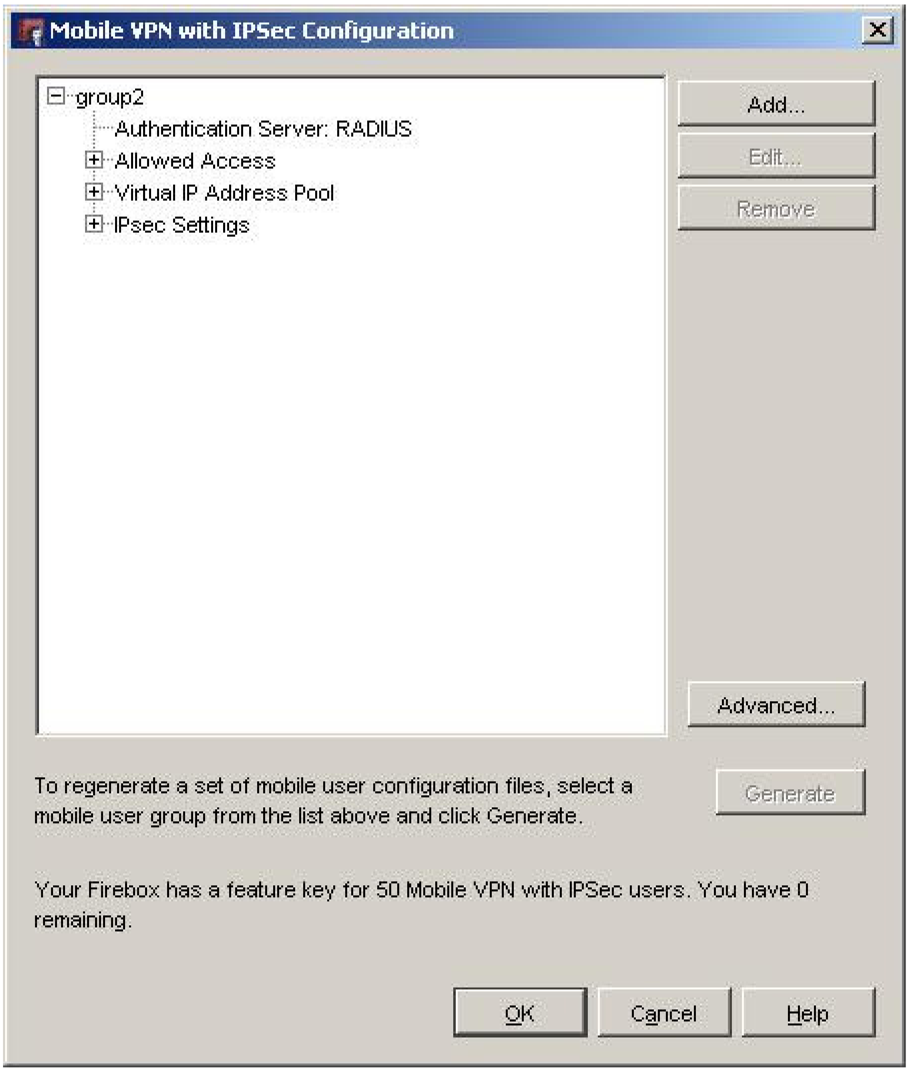
Congratulations! The wizard has created a new Virtual Private Network for mobile users.

The VPN configuration file is in the folder:

C:\Documents and Settings\All Users\Shared WatchGuard\muvpn\ 192.168.9.178\group2\group2.wgx

The file is encrypted with the tunnel passphrase.

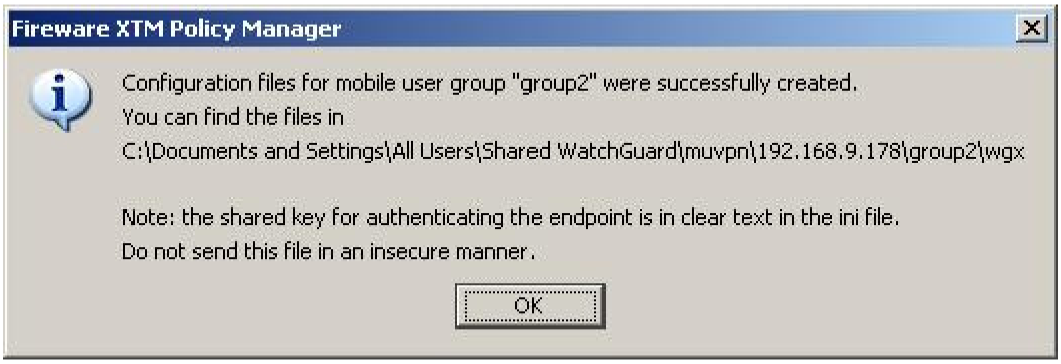
9. Select the Group and click on Generate to create the Client policy.



To regenerate a set of mobile user configuration files, select a mobile user group from the list above and click Generate.

Your Firebox has a feature key for 50 Mobile VPN with IPSec users. You have 0 remaining.

10. The configuration files can be imported into the VPN Client software.

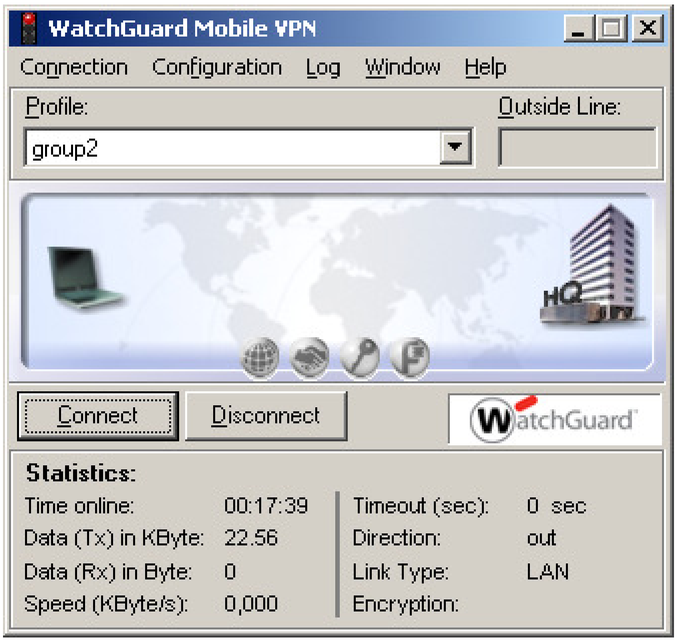


Configuration files for mobile user group "group2" were successfully created.
You can find the files in
C:\Documents and Settings\All Users\Shared WatchGuard\muvpn\192.168.9.178\group2\wgx

Note: the shared key for authenticating the endpoint is in clear text in the ini file.
Do not send this file in an insecure manner.

11. Start the VPN Client and select Configuration/Profiles. Click on Configuration then Profile Import.

3.2.6. Configuration of VPN IPSEC Client



Profile: group2

Outside Line:

Statistics:

Time online: 00:17:39

Data (Tx) in KByte: 22.56

Data (Rx) in Byte: 0

Speed (KByte/s): 0,000

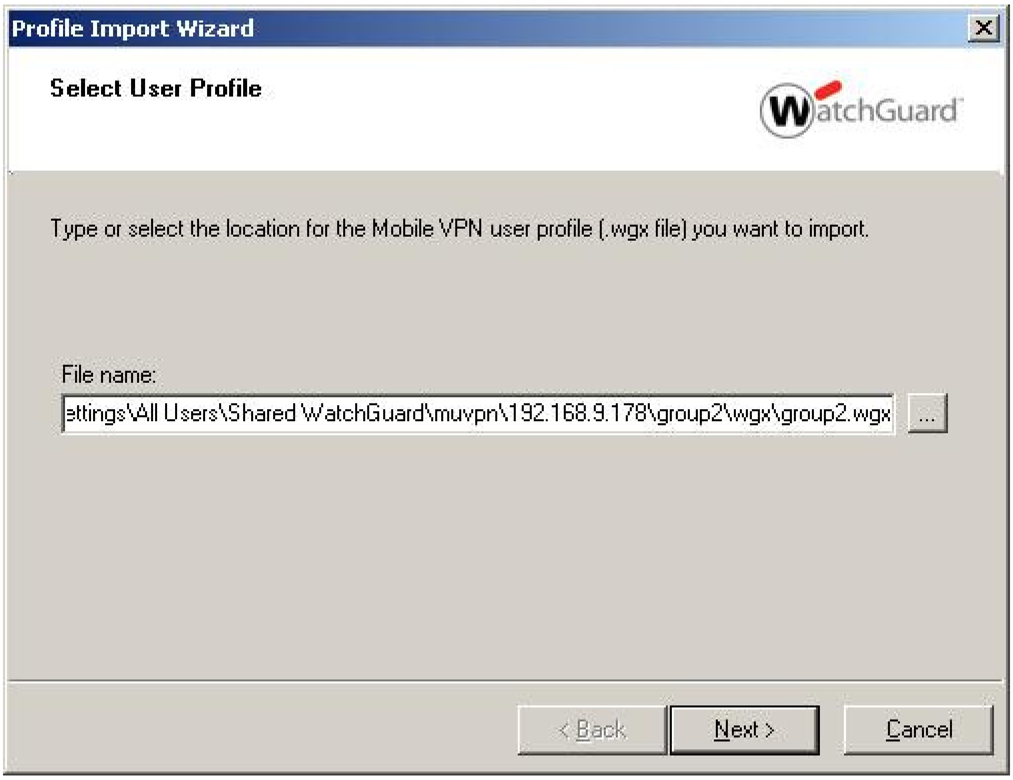
Timeout (sec): 0 sec

Direction: out

Link Type: LAN

Encryption:

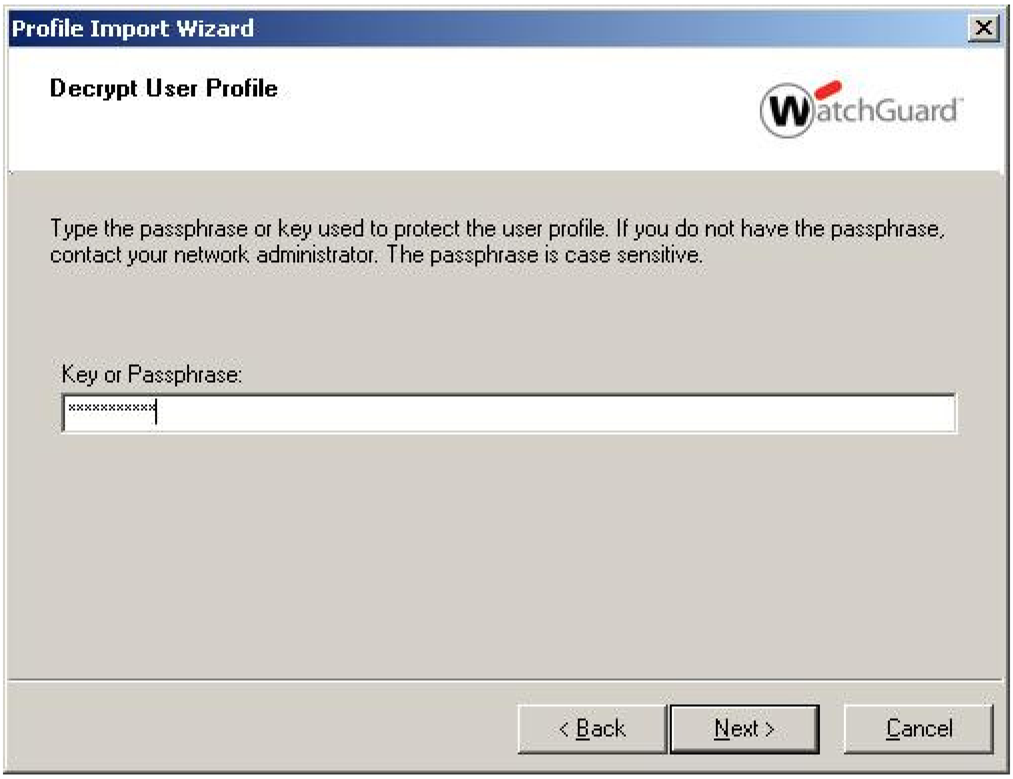
1. Select the Configuration file created above, then click on Next.



Type or select the location for the Mobile VPN user profile (.wgx file) you want to import.

File name: ettings\All Users\Shared WatchGuard\muvpn\192.168.9.178\group2\wgx\group2.wgx

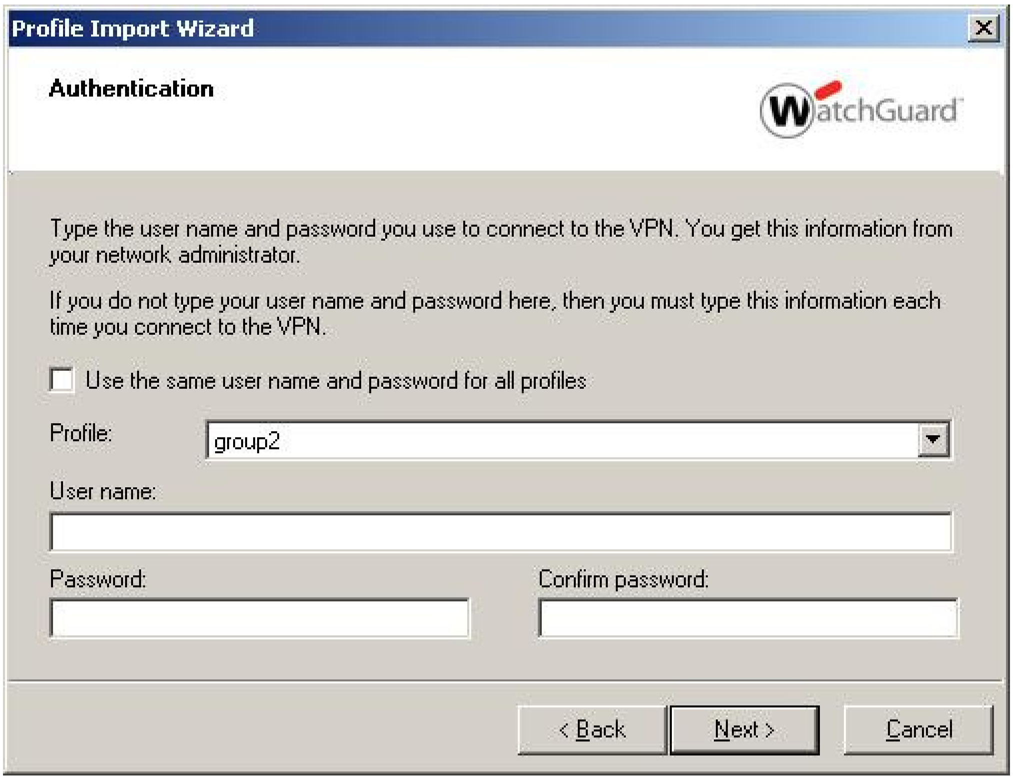
2. Enter the passphrase used above then click on Next.



Type the passphrase or key used to protect the user profile. If you do not have the passphrase, contact your network administrator. The passphrase is case sensitive.

Key or Passphrase:
****

3. Enter the Authentication information, if you wish to enter the User ID: for the profile, enter the required User ID:, leave the Password field empty then click on Next.



Type the user name and password you use to connect to the VPN. You get this information from your network administrator.

If you do not type your user name and password here, then you must type this information each time you connect to the VPN.

□ Use the same user name and password for all profiles

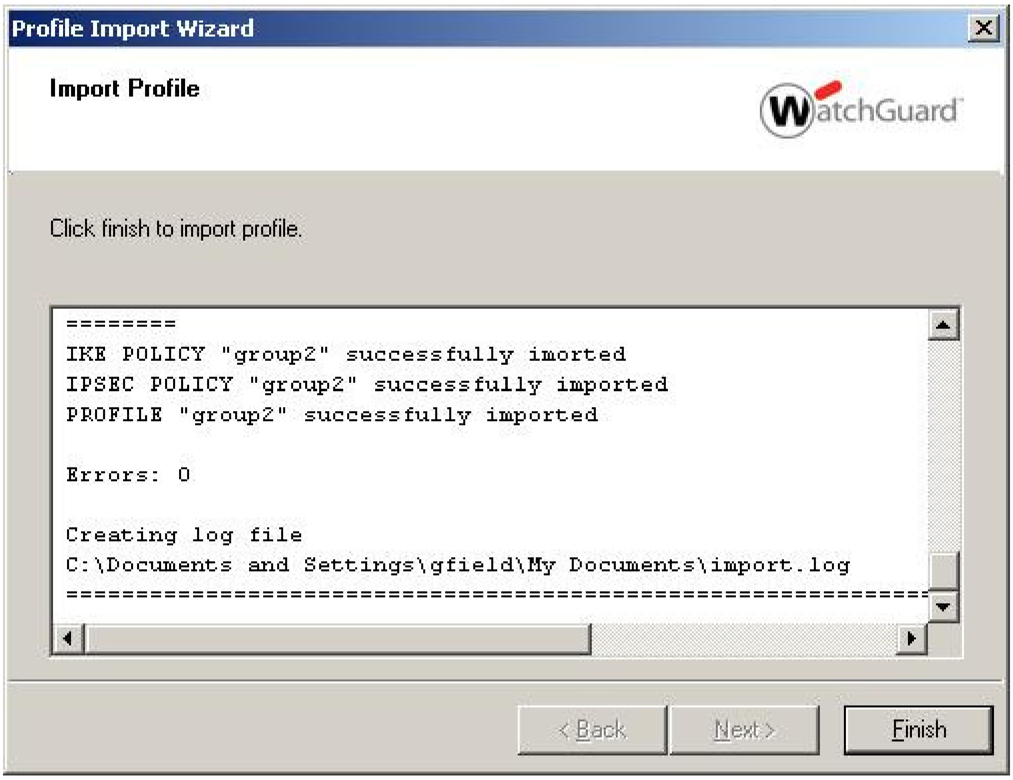
Profile: group2

User name:

Password:

Confirm password:

4. The profile is completed, then click on Finish.



Click finish to import profile.

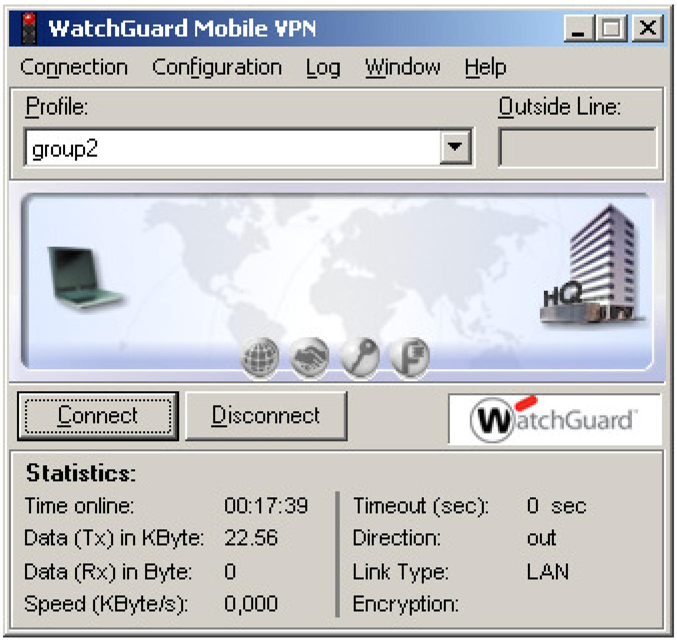
```
========
IKE POLICY "group2" successfully imorted
IPSEC POLICY "group2" successfully imported
PROFILE "group2" successfully imported

Errors: 0

Creating log file
C:\Documents and Settings\gfield\My Documents\import.log
=============================================================
```

3.2.7. Connecting using the VPN IPSEC Client

1. Select the required profile and then click Connect



Profile: group2

Outside Line:

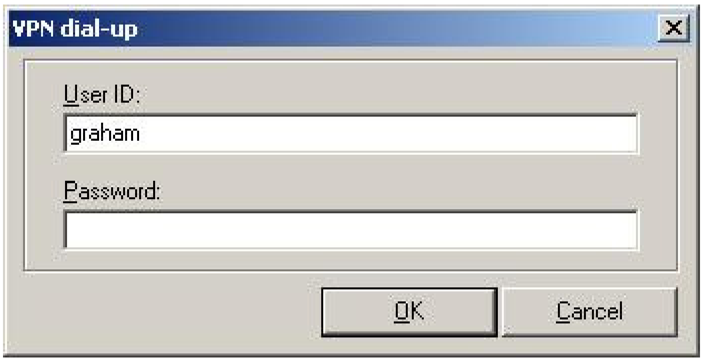
Statistics:

Time online:	00:17:39	Timeout (sec):	0 sec
Data (Tx) in KByte:	22.56	Direction:	out
Data (Rx) in Byte:	0	Link Type:	LAN
Speed (KByte/s):	0,000	Encryption:	

2. Select the required profile and then click Connect

Enter the username (unless pre-defined above), then enter the PINsafe One Time Code, possible sources of the One Time Code are:

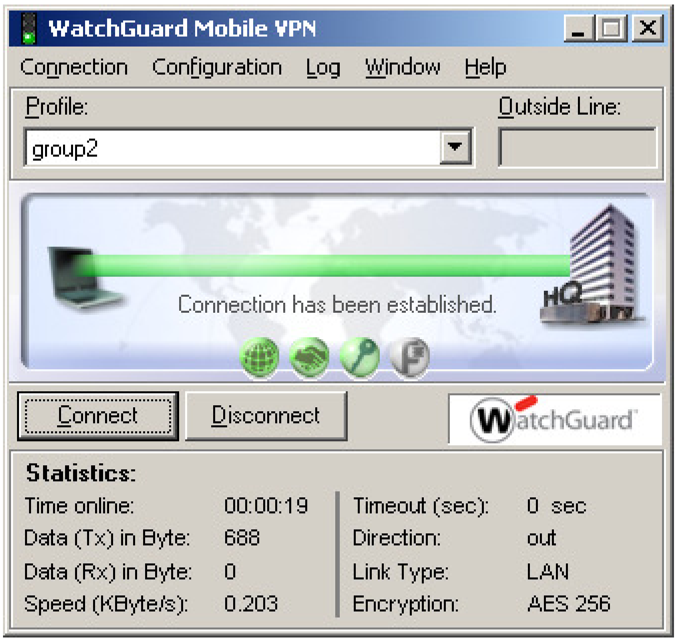
- SMS Text Message
- PINsafe Taskbar utility or Single Channel image
- Mobile Phone Applet



User ID: graham

Password:

3. If a correct One Time Code is entered, the VPN connection is established.



Profile: group2

Outside Line:

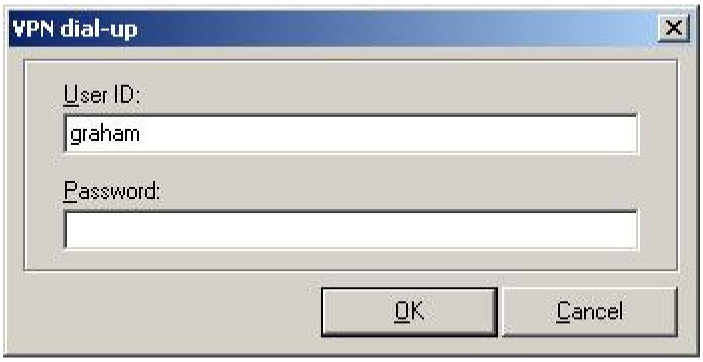
Connection has been established.

Statistics:

Time online:	00:00:19	Timeout (sec):	0 sec
Data (Tx) in Byte:	688	Direction:	out
Data (Rx) in Byte:	0	Link Type:	LAN
Speed (KByte/s):	0.203	Encryption:	AES 256

3.2.8. Optional: IPSec Authentication using Two Stage or Two Stage and Challenge and Response

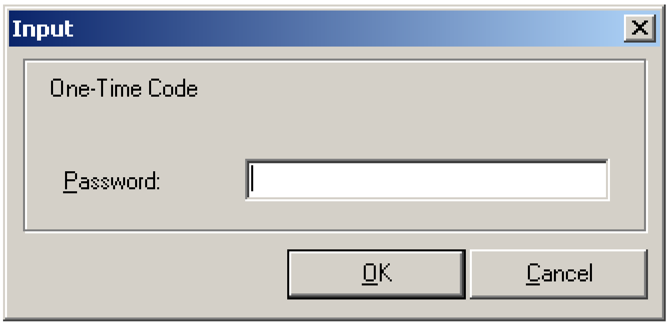
Enter Username and Password



User ID: graham

Password:

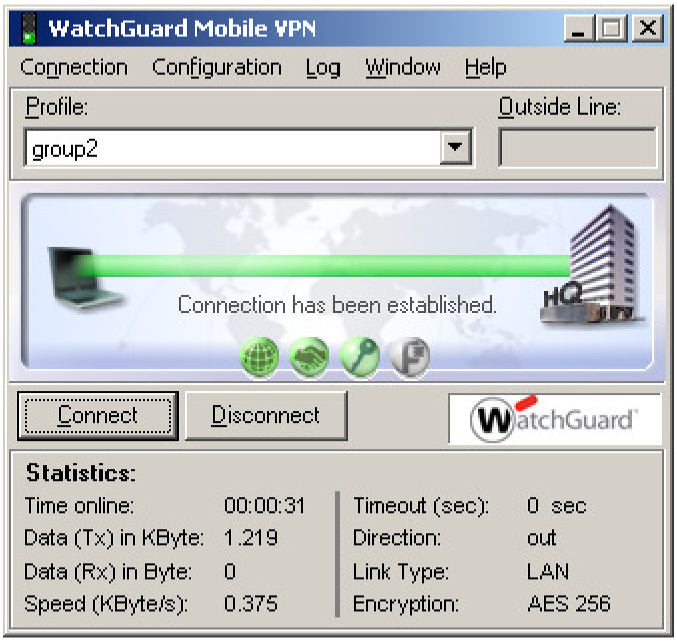
Enter One Time Code



One-Time Code

Password:

If a correct One Time Code is entered, the VPN connection is established.



Profile: group2

Outside Line:

Connection has been established.

Statistics:

Time online:	00:00:31	Timeout (sec):	0 sec
Data (Tx) in KByte:	1.219	Direction:	out
Data (Rx) in Byte:	0	Link Type:	LAN
Speed (KByte/s):	0.375	Encryption:	AES 256

4. Verifying the Installation

<How to check the install is working ok>

5. Troubleshooting

<If it does not work, what steps to try>

6. Known Issues and Limitations

<If there are any, if none write None >

7. Additional Information

For assistance in the PINsafe installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com