Integration Guide

Duo Security Authentication

Revised: 23 March 2016

About This Guide

Guide Type

Documented Integration —WatchGuard or a Technology Partner has provided documentation demonstrating integration

Guide Details

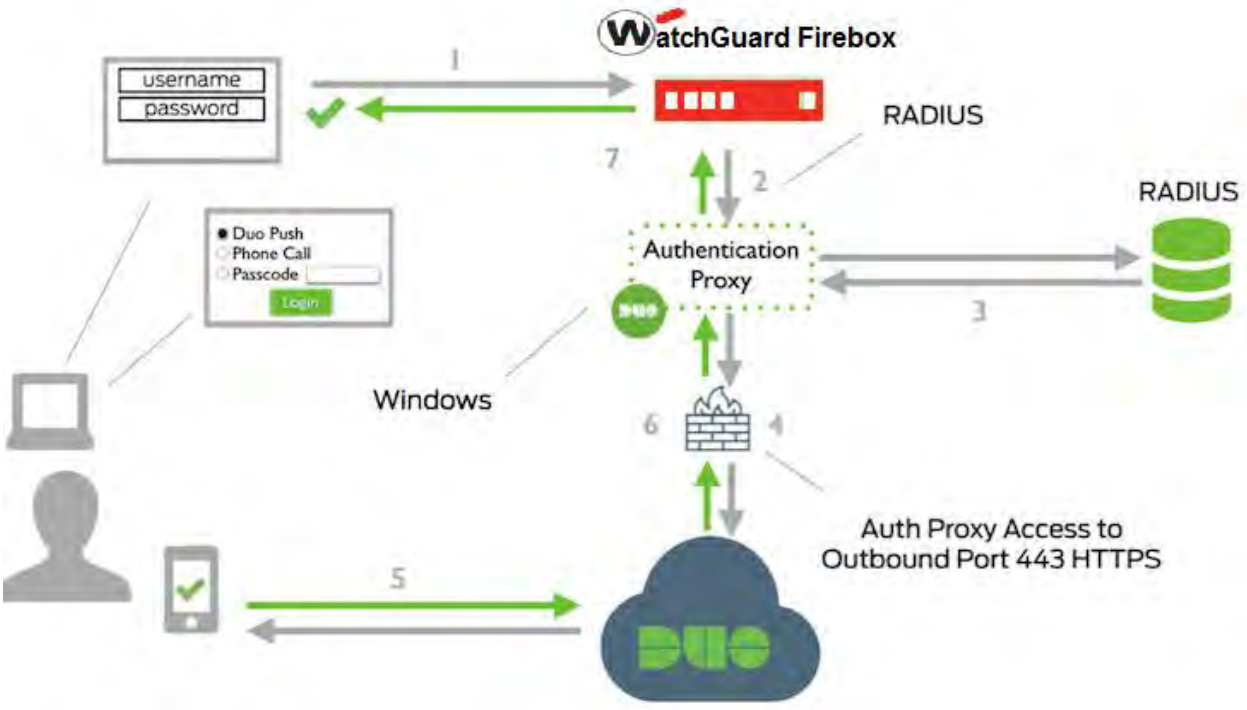
WatchGuard provides integration instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a third-party product, see the documentation and support resources for that product.

Duo Security Integration Overview

This document describes the steps to integrate WatchGuard Mobile VPN with SSL client software download access and Mobile VPN with SSL client authentication with Duo Security's two-factor authentication solution.

Duo Security offers user authentication by passcode, push, phone or SMS. All of these authentication methods have been successfully verified for use with Mobile VPN with SSL client software download access and to connect to the Firebox with the Mobile VPN with SSL client.

The workflow for two-factor authentication through integration with Duo is shown here:



1. The user initiates primary authentication to the WatchGuard Firebox.
2. The Firebox sends an authentication request to Duo's Authentication Proxy.
3. The Authentication Proxy completes primary authentication using RADIUS.
4. The Authentication Proxy establishes a secure connection to the Duo Security service.
5. Secondary authentication is conducted through the Duo Security service.
6. The Authentication Proxy receives a secondary authentication result from the Duo Security service.
7. The Firebox grants the user access.

Platform and Software

The hardware and software used to complete the steps outlined in this document include:

- Firebox XTM 5 Series device installed with Fireware v11.10.x
- Duoauthproxy-2.4.14 on Windows
- Freeradius-server-2.2.3
- Duo Mobile Application 3.9.7 on Android

Two-Factor Authentication Methods

When using two-factor authentication, you can use any of the four secondary authentication methods supported by Duo in the Password field when you log in to the Firebox.

In the examples below, the username is *leezy*, the password is *password* and the Duo provided passcode is *nnnnnn*.[1]

1. <password>,<passcode>

   In addition to the password, the user provides a passcode obtained through the Duo Mobile App.

   Example:

Username:	*leezy*
Password:	*password*, *nnnnnn*

2. <password>,push

   After the username, password and key word "push" are submitted to the Firebox, the user must approve the subsequent authentication request in Duo's Mobile App on their phone.

   Example:

Username	*leezy*
Password	*password*,push

3. <password>,phone.

   After the username, password, and key word *phone* are submitted to the Firebox, the user must approve the subsequent authentication request by pressing any digit on their phone panel.

   Example:

Username	*leezy*
Password	*password*,phone

4. <password>, sms

   The initial submission of username, password and key word *sms* to the Firebox (this authentication attempt is expected to fail) causes the user to receive ten passcodes on their phone through SMS. The user then conducts a new authentication request, this time specifying one of the received passcodes (as shown in option 1 above).

   Example:

[1] In the actual Firebox provided authentication UI, the password will be obscured; the password field contents are shown here in clear text solely for purposes of illustration.

Username	*leezy*
Password	*password*,sms

Configuration

To complete this integration, you must have:

- Duo account
- Duo Authentication Proxy
- RADIUS server
- WatchGuard Firebox

The Duo account is used to log in to the Duo Service to manage applications, enroll users, and get integration keys. The Duo Authentication Proxy acts as a bridge, communicating with the RADIUS server, the Duo Security service in the cloud, the WatchGuard Firebox, and the Duo Mobile App. The RADIUS server is used for primary user authentication.

In the tested configuration, the Duo Authentication Proxy and the RADIUS server were located on the same subnet.

Create a Duo Account

To create a Duo account:

1. Sign up for a Duo account.
2. Log in to the Duo Admin Panel and select **Applications**.
3. Select **Protect an Application** and find RADIUS in the applications list.
4. Select **Protect this Application** to get an integration key, secret key, and API hostname.
5. Select **User** and enroll the user as defined on the RADIUS server into Duo, including the user's phone number.
6. After enrollment, activate the user.

Configure the Duo Authentication Proxy for Primary Authentication

The Duo Authentication proxy is the system that validates users' existing passwords. In most cases you must configure the proxy to communicate with a RADIUS server. To configure the proxy, add a `[radius_client]` section at the top of the file that includes properties described below. All properties are required.

Properties	Description
`host`	The IP address of the RADIUS server
`secret`	A secret to be shared between the proxy and the RADIUS server

For example:

```
[radius_client]
```

```
host=172.16.1.28
secret=password
```

Make sure that the RADIUS server is configured to accept authentication requests from the Duo Authentication Proxy.

Configure the Duo Authentication Proxy to Work with the Firebox

To set up the Duo Authentication Proxy to work with the Firebox, create a `[radius_server_auto]` section in the Proxy configuration file that includes the properties described below. All properties are required. Make sure to save the configuration file when you are done.

Properties	Description
`ikey`	The integration key, as referenced in the Create a Duo Account section of this document.
`skey`	The secret key, as referenced in the Create a Duo Account section of this document.
`api_host`	The api host, as referenced in the Create a Duo Account section of this document.
`radius_ip_1`	The IP address of the Firebox that is connected to the Proxy.
`radius_secret_1`	A secret to be shared between the Proxy and the Firebox.
`client`	Set this to **radius client**, which means the proxy will use RADIUS for primary authentication. Make sure a `[radius_client]` section as described above is configured.

An example configuration file that uses RADIUS could look like this:

```
[radius_client]
host=172.16.1.28
secret=password
pass_through_all=true

[radius_server_auto]
ikey=DI5G8WL3F2SPLZIBVHED
skey=sEyhfVljR2ork5og8rwvKxiXXXXXXXXX
api_host=api-77800a8d.duosecurity.com
radius_ip_1=172.16.1.1
radius_secret_1=password
client=radius_client
port=1812
failmode=safe
pass_through_all=true
```

Start the Duo Authentication Proxy

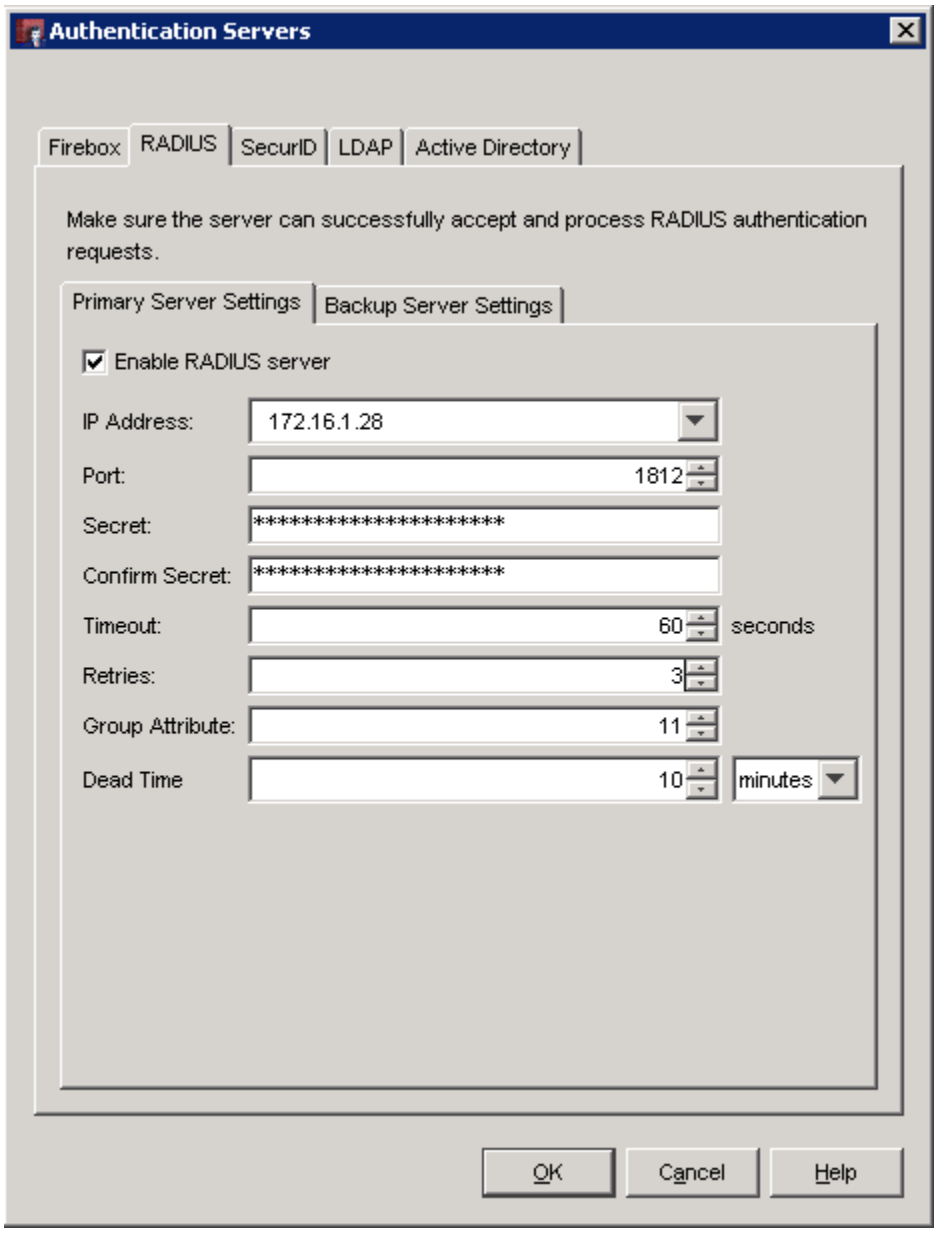
On the Windows computer where the Duo Authentication Proxy is installed, open an Administrator command prompt and type the command:

```
net start DuoAuthProxy
```

Configure RADIUS Authentication Server on the Firebox

From WatchGuard System Manager, open Policy Manager and configure the Firebox to use RADIUS authentication.

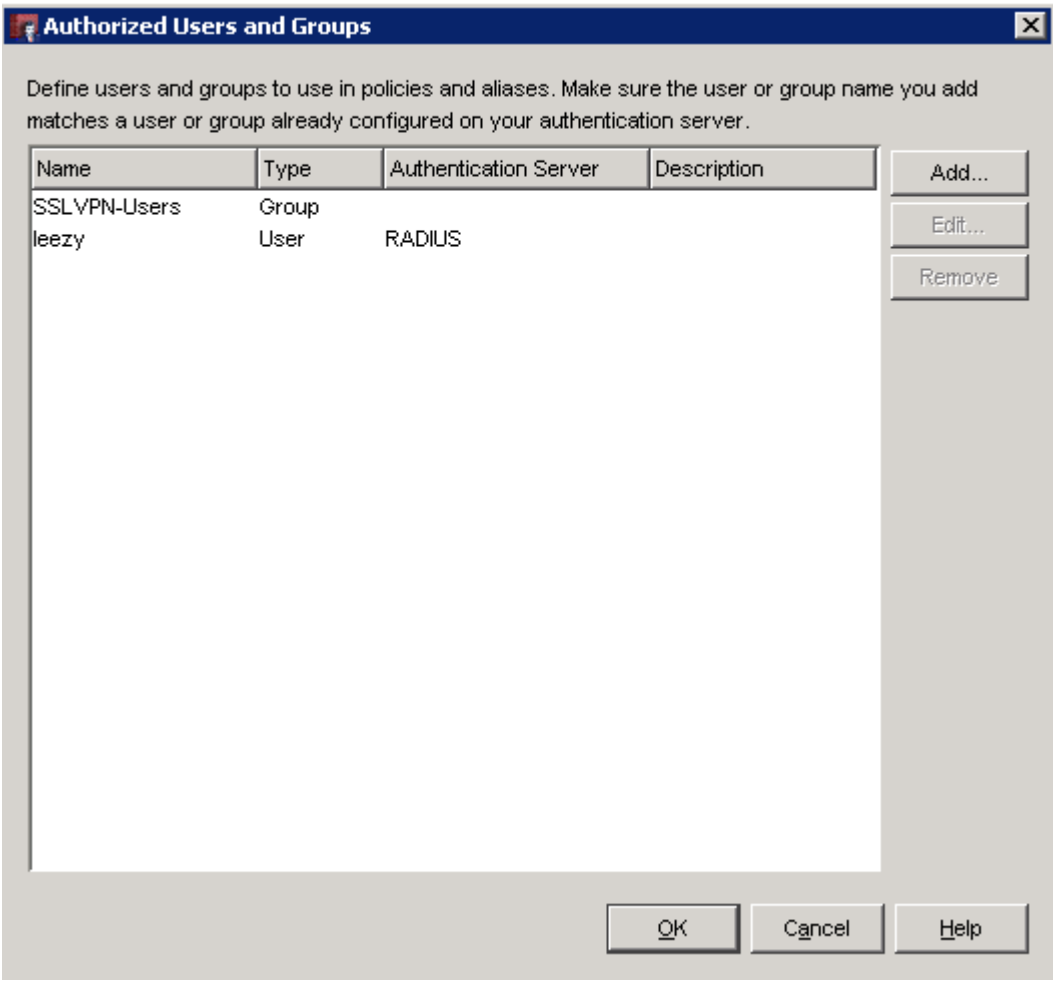
1. From Policy Manager, select **Setup > Authentication > Authentication Servers**.
2. On the RADIUS tab, configure these properties:
    a. *IP Address* – the IP address of the Duo Authentication Proxy
    b. *Secret* – the RADIUS secret configured on the Duo Authentication Proxy
    c. *Timeout* – Set this to at least 60 seconds



3. Click **OK** to add the new RADIUS server.

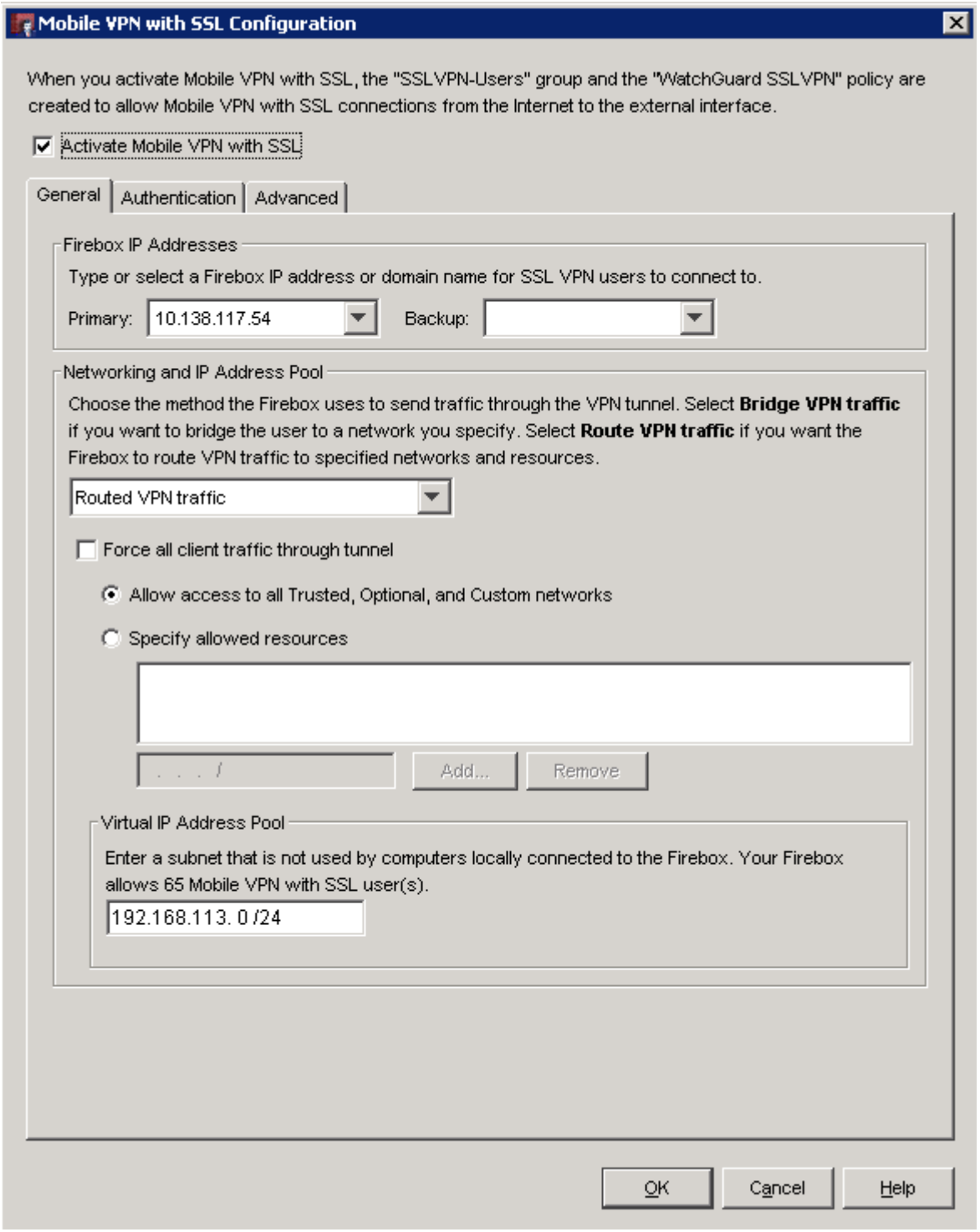
Configure a User Group on the Firebox

1. Select **Setup > Authentication > Authorized Users/Groups** and add a user.
2. If you want, you can use the default SSLVPN-Users group for authentication. Or, you can add the names of users and groups to match those defined on your RADIUS server.

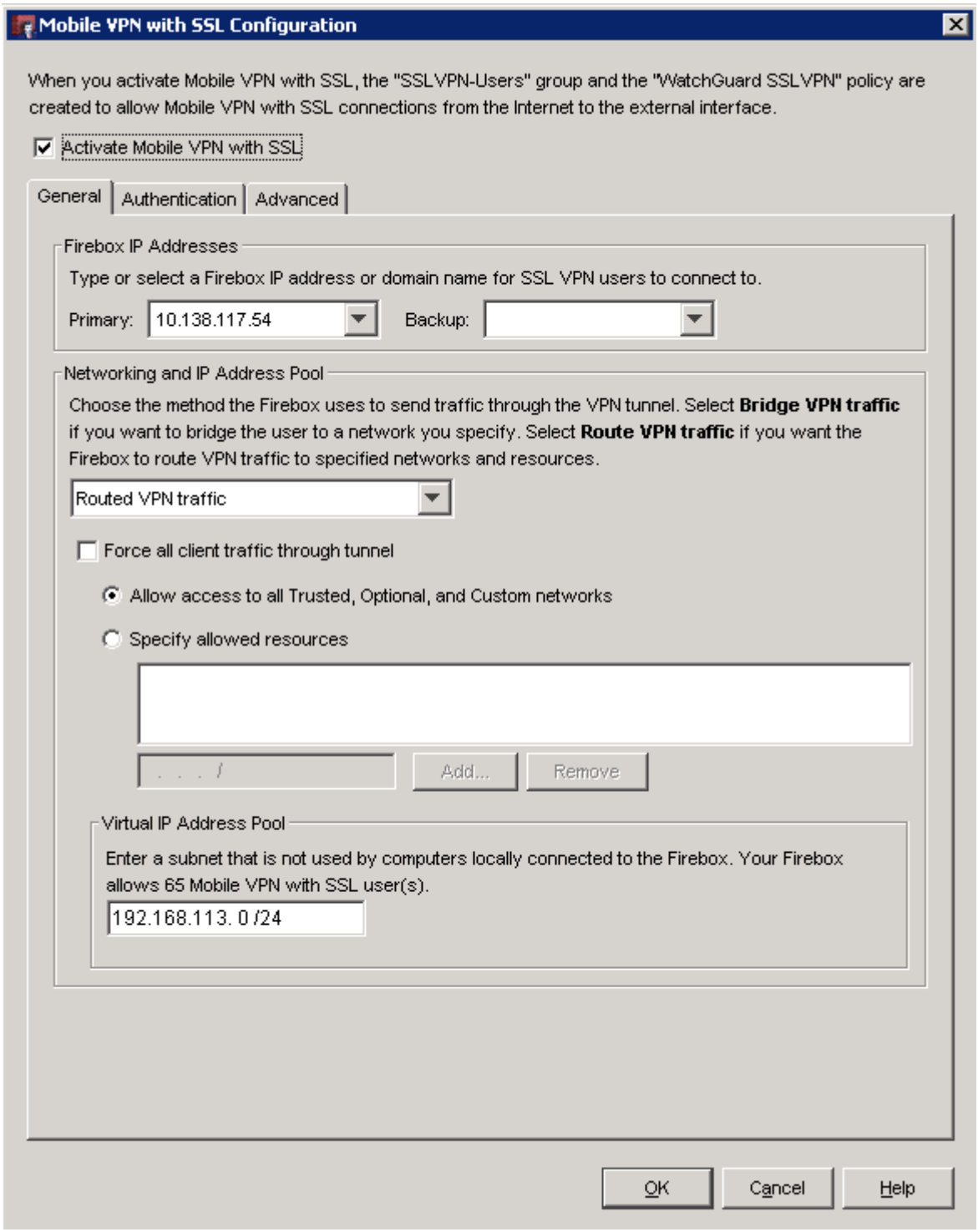


Configure Mobile VPN with SSL on the Firebox

1. From Policy Manager select **VPN > Mobile VPN > SSL**.
2. Configure these settings on the General tab:
   - Select the **Activate Mobile VPN with SSL** check box.
   - Type the IP address or domain name to which the mobile clients will connect.
   - Configure networking settings and add and IP address pool if required.



3. Configure these settings on the Authentication tab:
   - Select the RADIUS server.
   - We recommend that you enable the option **Force users to authenticate after a connection is lost** but it is not required.



4. Click **OK**.

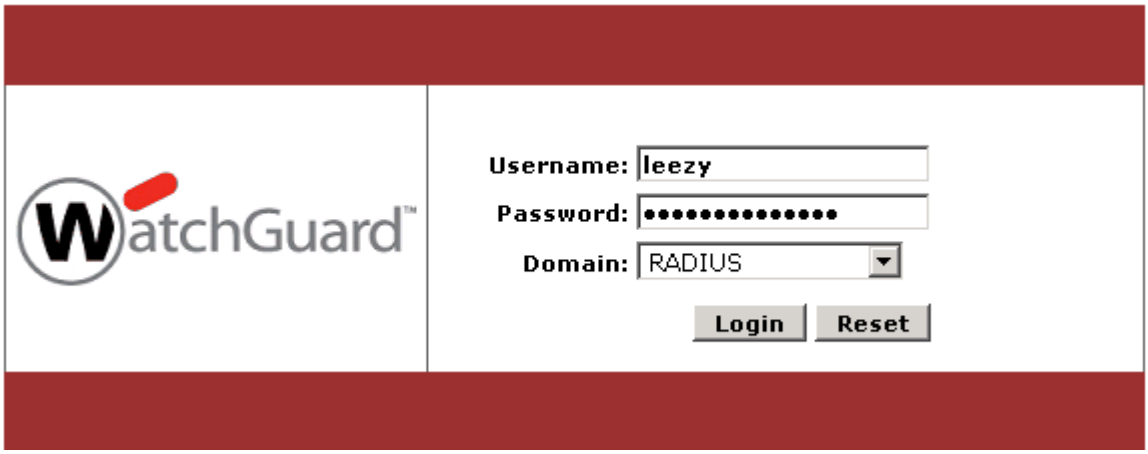
Note: When Mobile VPN with SSL is activated, an SSLVPN-Users user group and a WatchGuard SSLVPN policy are automatically created and added to your configuration to allow SSL VPN connections from the Internet to the external interface. It is possible to use these groups or create new groups that match the user group names defined on the authentication server.

Mobile VPN with SSL Client Software Download

To download Mobile VPN with SSL client software, connect to your Firebox with this URL:

https://[device_interface_IP_address]:410/sslvpn.html

Here is an example of the authentication page:



You can use any of the four supported two-factor authentication methods described in the Two-Factor Authentication Methods section above. Review the content carefully for syntax, but usually you will type the password followed by a comma and the additional information required for the method you choose.

The options are:

- <password>,<passcode>
- <password>,push
- <password>,phone
- <password>,sms

When authentication is successful, this is what you see:

From this page you can download the Mobile VPN with SSL client software that matches your computer operating system.

Mobile VPN with SSL Client Authentication

After the Mobile VPN with SSL client is downloaded and configured on your computer, you can use any of the four supported two-factor authentication methods to connect to your Firebox with the Mobile VPN client software. These methods are described in the Two-Factor Authentication Methods section above. Review the content carefully for syntax, but usually you will type the password followed by a comma and the additional information required for the method you choose.

The options are:

- <password>,<passcode>
- <password>,push
- <password>,phone
- <password>,sms

The authentication screen looks like this:


WatchGuard Mobile VPN with SSL
WatchGuard
Firebox SSL
Server:
10.138.117.54
User name:
leezy
Password:
Automatically reconnect
Connect
Cancel
Version 11.10.0 (Build 468314)