Integration Guide

Swivel Secure Authentication

Revised: 21 February 2016

About This Guide

Guide Type

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

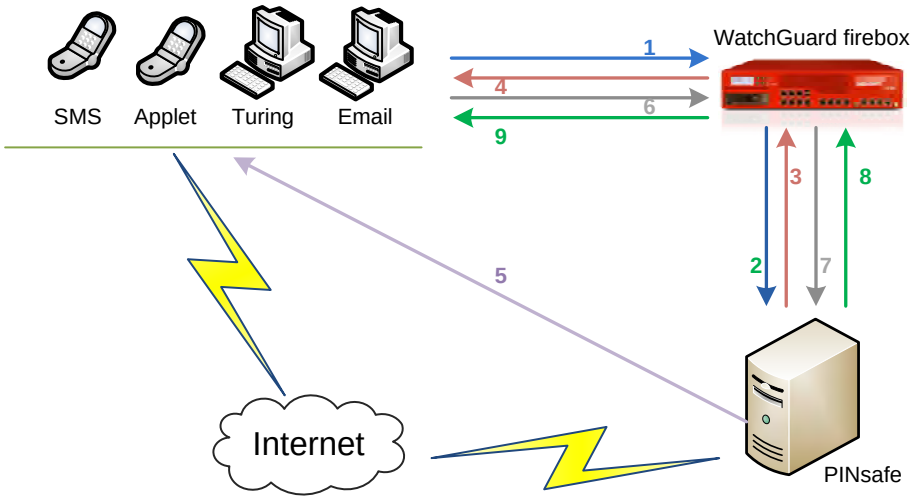
Guide Details

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.

Swivel Secure Integration Overview

The Swivel Secure PINsafe server is RADIUS compatible and can be used as a RADIUS server. This document describes the steps necessary to integrate the WatchGuard Mobile VPN with SSL client software download process and Mobile VPN with SSL client authentication with Swivel Secure's two-factor authentication solution.

This diagram shows the workflow for two-factor authentication through integration with Swivel's PINsafe server, which is described below:



At a high level:

1. A user initiates primary authentication to the WatchGuard Firebox.
2. The Firebox sends an authentication request to PINsafe.
3. PINsafe checks the password. If it is correct, it responds with a RADIUS challenge (one-time code) to the Firebox.
4. The user is prompted with a second dialog box.
5. If the user types a correct passphrase and PINsafe is set to Dual Challenge On Demand, PINsafe will send a dual channel message security string message as a one-time code to the user in a specified format (SMS text message, Turing image, mobile phone client application, or email).
6. The user submits their one-time code in the second dialog box and sends a second authentication request to the Firebox.
7. PINsafe authenticates the user based on the password submitted in the first authentication request and the one-time code submitted in the second authentication request.
8. The Firebox receives the authentication results from PINsafe.
9. The Firebox grants the user access.

Platform and Software

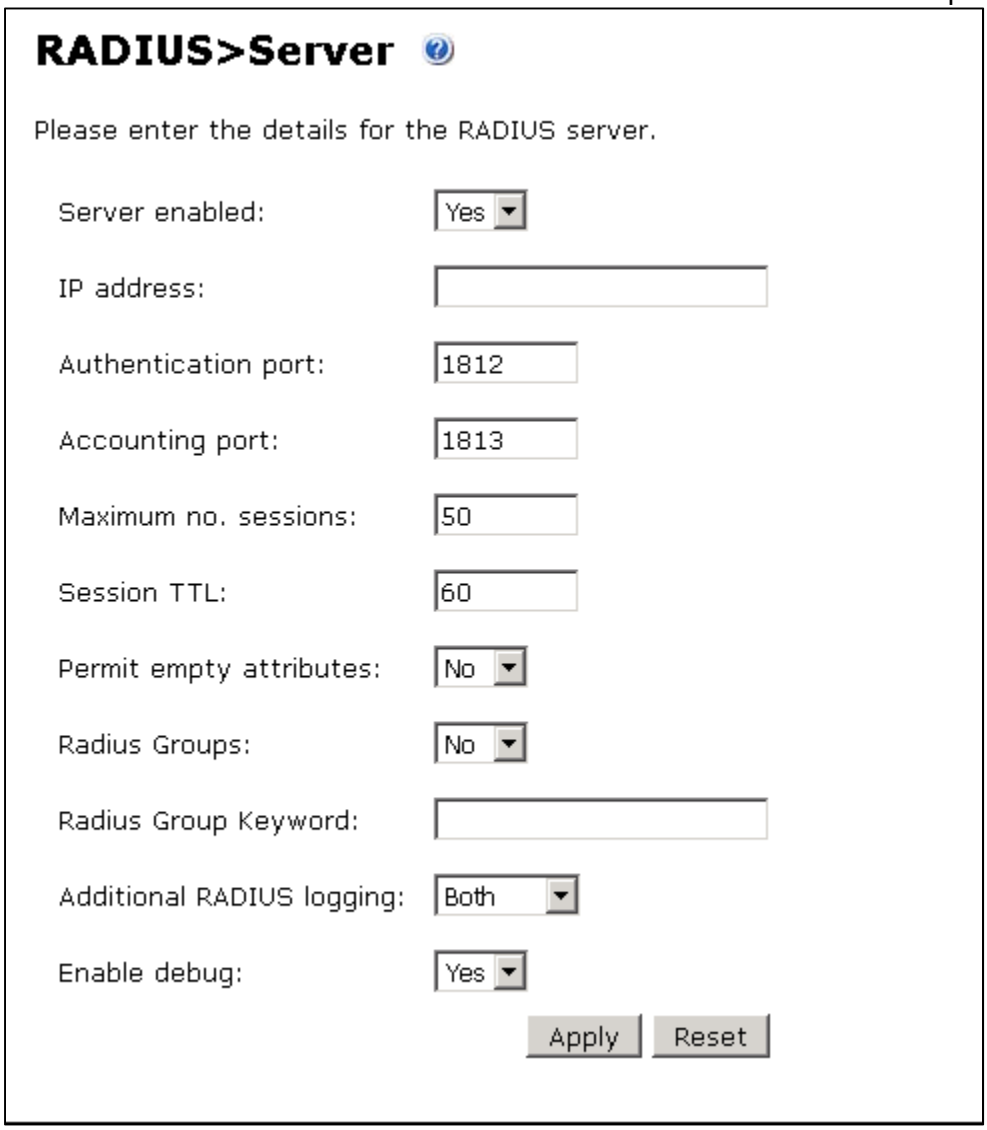
The hardware and software used to complete the steps outlined in this document include:

- Firebox M400 installed with Fireware v11.10.5
- Swivel Secure PINsafe server v2.10.5.3030 installed on a Windows computer
- FreeRADIUS server 2.2.3

Configuration

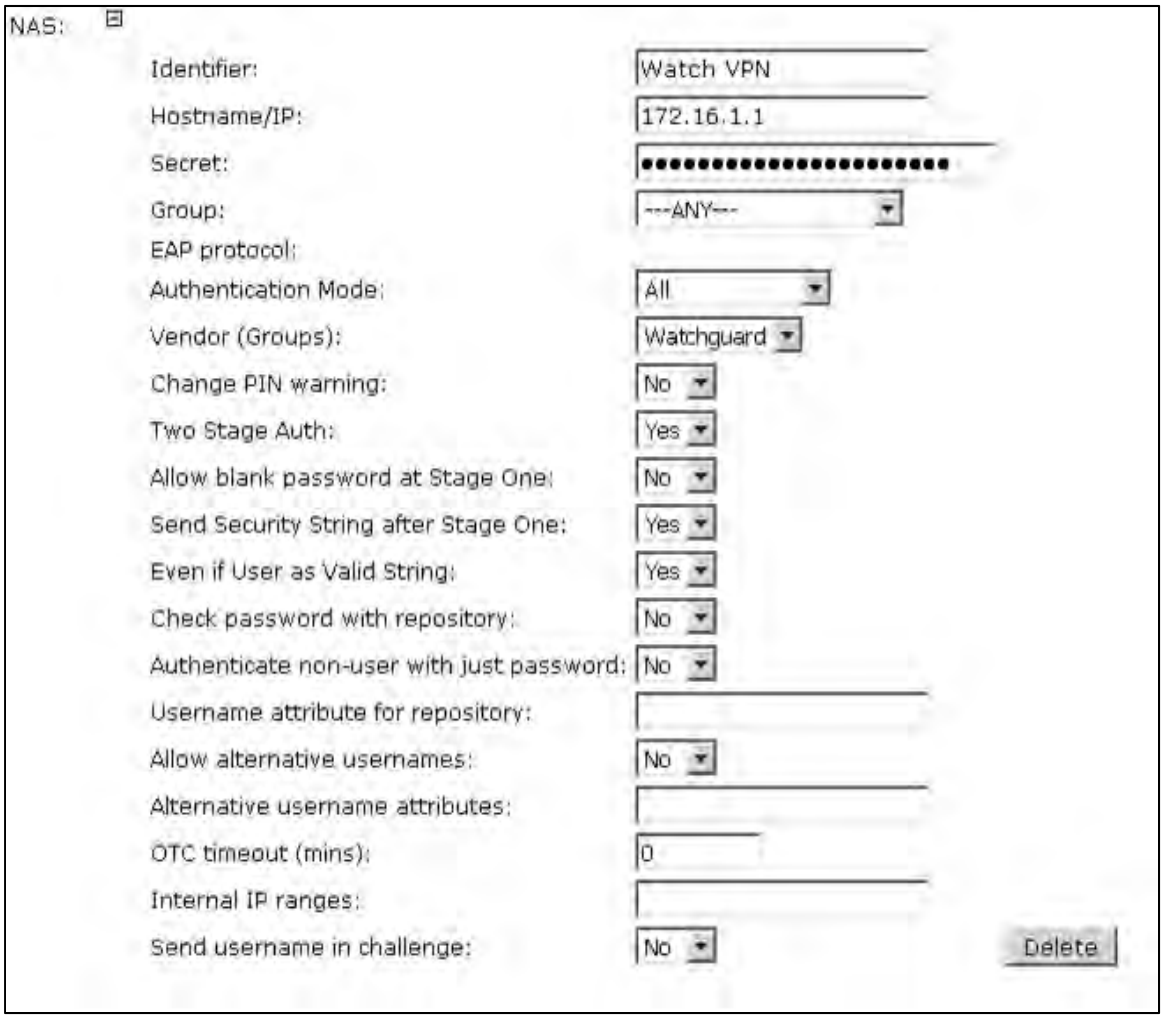
Configure the RADIUS Server and NAS entry in PINsafe

1. Verify that the RADIUS server has been enabled in PINsafe. To do this, open the PINsafe Management Console. Select **RADIUS/Server** and make sure the **Server enabled** drop-down list is set to **Yes**.



2. From the PINsafe Management Console, select **RADIUS NAS**.
3. In the **Identifier** text box, type a name for the NAS.

4. In the **Hostname/IP** text box, type the trusted interface IP address of your Firebox. In our example, we used 172.16.1.1, but your IP address could be different.
5. In the **Secret** text box, type the shared secret to use for communication between the Firebox and RADIUS NAS.

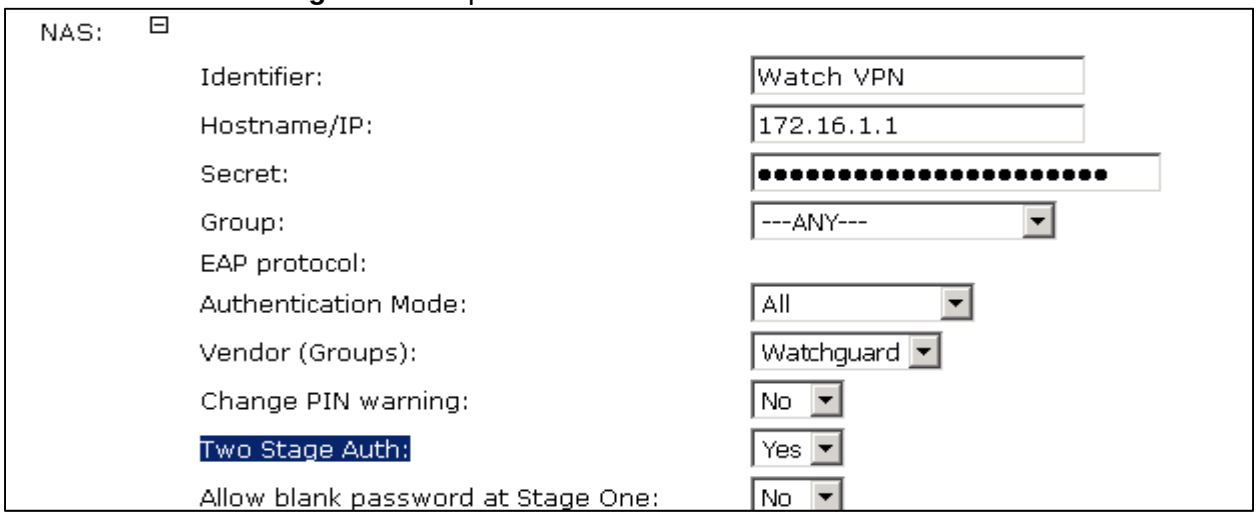


6. Click **Apply** to save changes.

Configure PINsafe for Two-Factor Authentication using Email

When a user authenticates with two-factor authentication, they enter their passphrase to authenticate and are then presented with a second dialog box to enter a one-time code. This code is used as the passphrase for the second authentication. The code can be distributed through an SMS text message, email, Turing image, or mobile phone client application. In this example, we will configure PINsafe to send the one-time code through email.

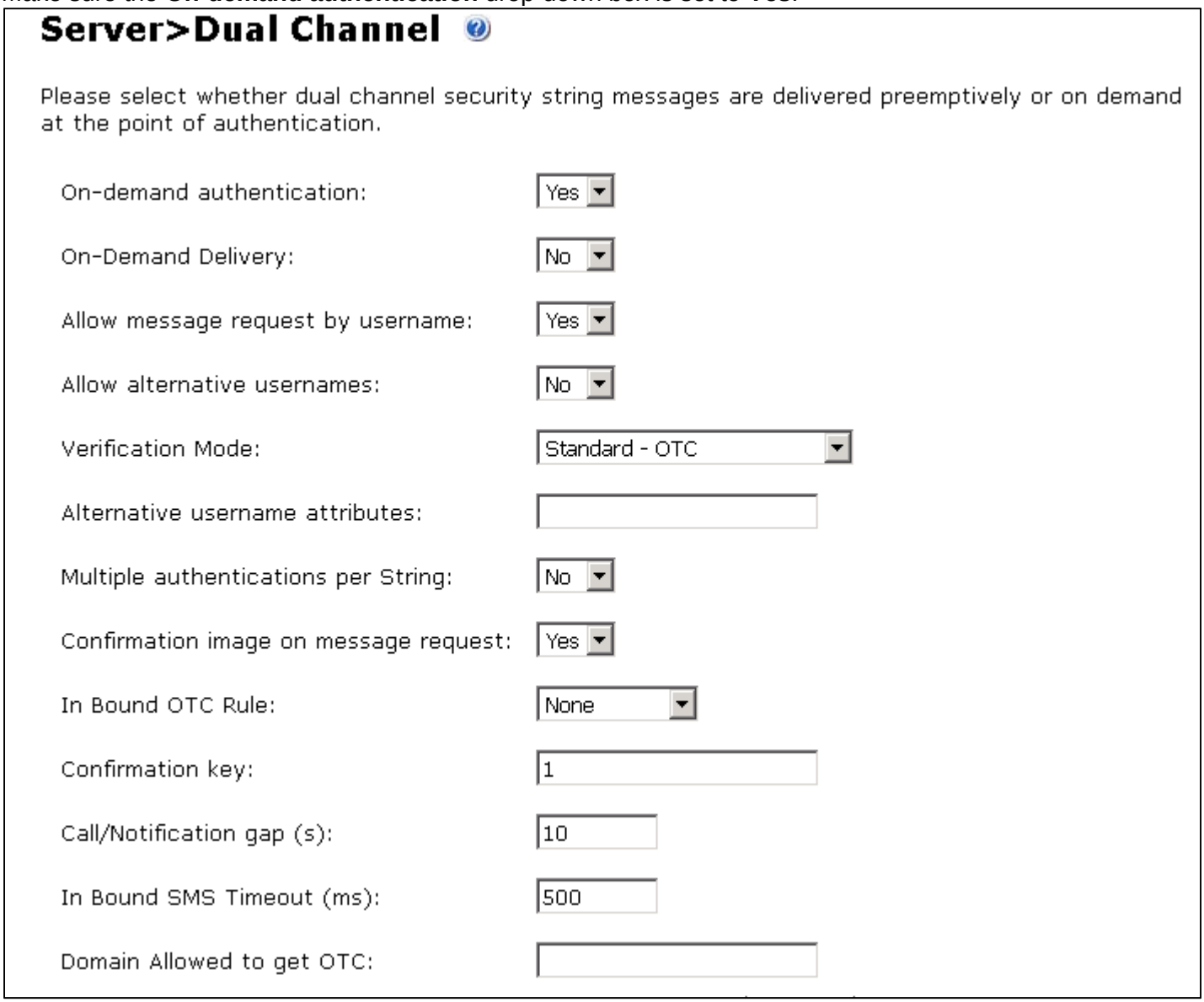
1. From the PINsafe Administration Console, select **RADIUS/NAS**.
2. Make sure the **Two Stage Auth** drop-down list is set to **Yes**.



Configure Challenge and Response Authentication

To allow challenge and response authentication through email, you must first configure PINsafe for two stage authentication:

1. From the PINsafe Administration Console, select **Server/Dual Channel**.
2. Make sure the **On-demand authentication** drop-down box is set to **Yes**.

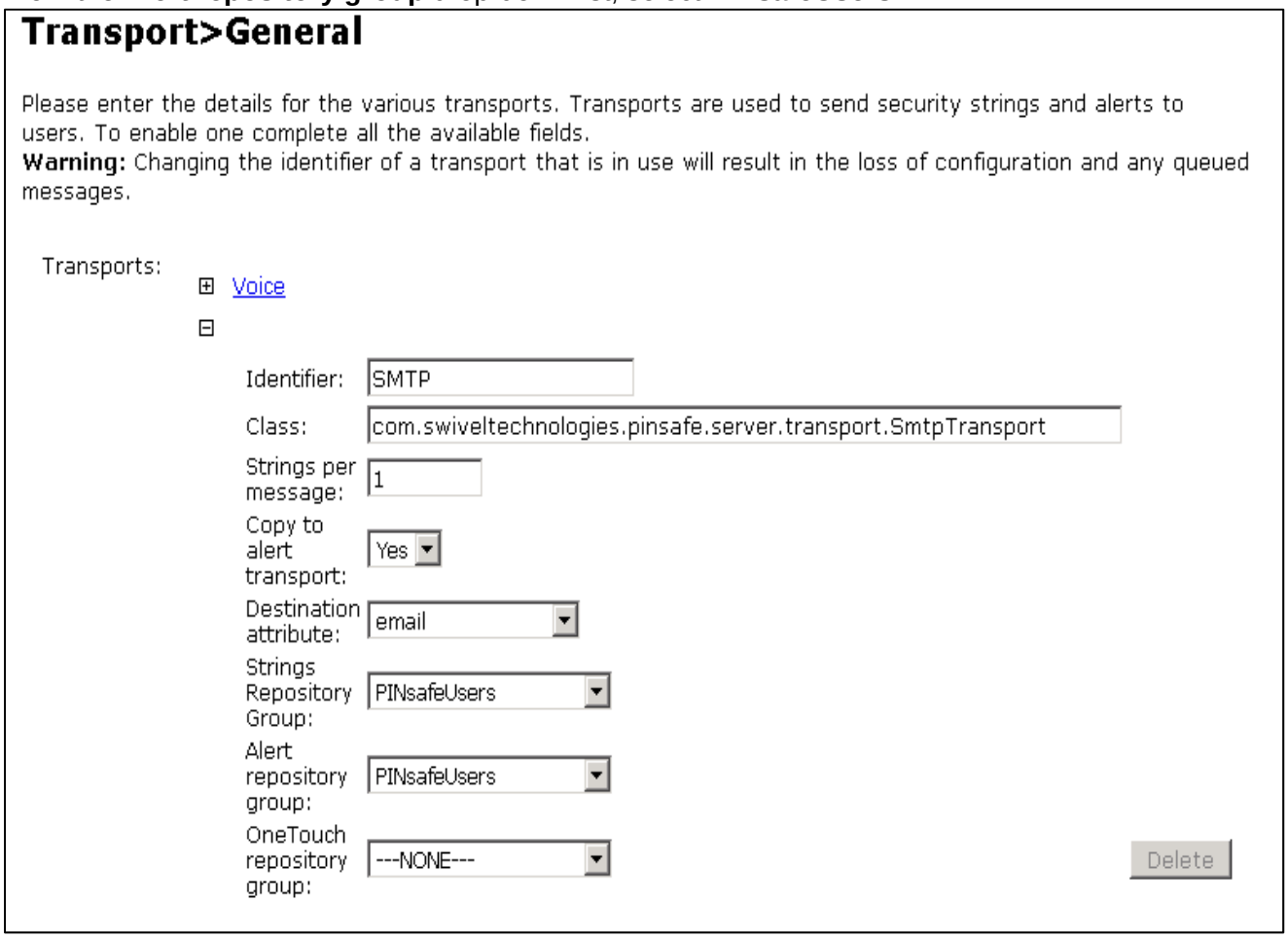


Create an Email Transport Type

A transport is a method of delivering security strings or other information as one-time code. To set the PINsafe transport type to email:

1. From the PINsafe Management Console, select **Transport/General**.
2. From the **Destination Attribute** drop-down list, select **email**.
3. From the **Strings Repository Group** drop-down list, select **PINsafeUsers**.

4. From the **Alert repository group** drop-down list, select **PINsafeUsers**.

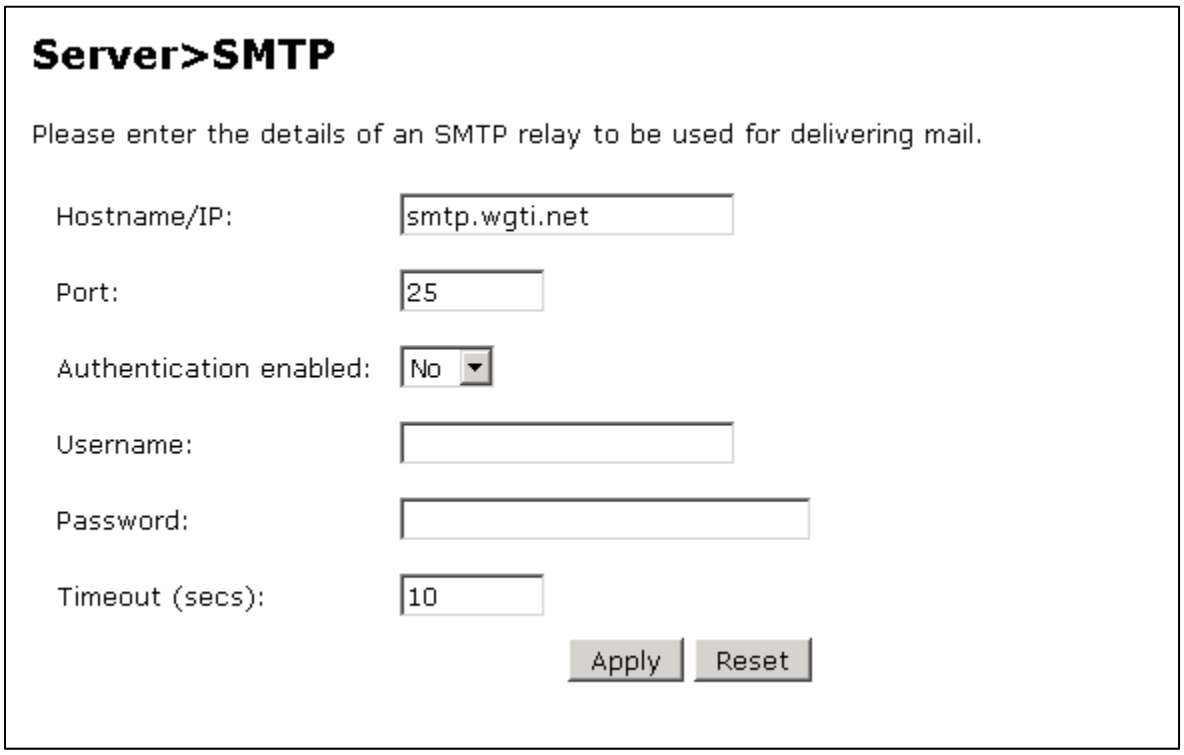


5. Click **Apply** to save changes to your configuration.

Configure an SMTP Gateway

You must define an email gateway for PINsafe to use.

1. From the PINsafe Management Console, select **Server/SMTP** and configure your email gateway. In this example, the gateway is set to `smtp.wgti.net` but your email gateway name/IP address will be different.

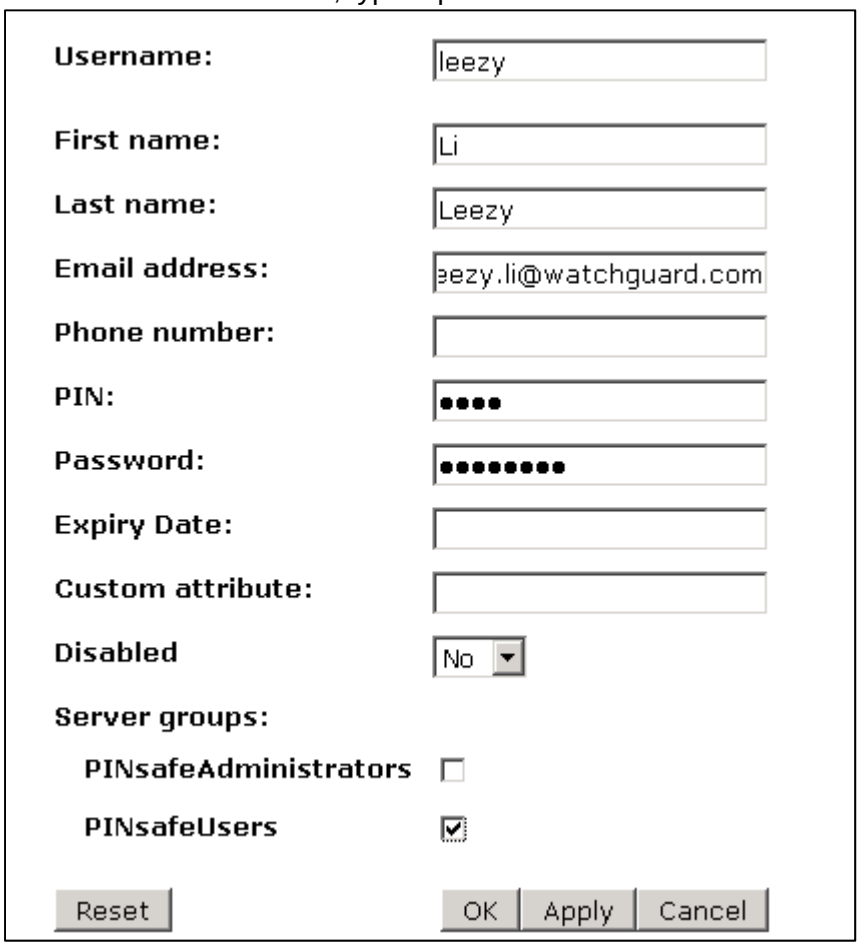


2. Make sure that there is connectivity between the PINsafe server and the mail gateway.

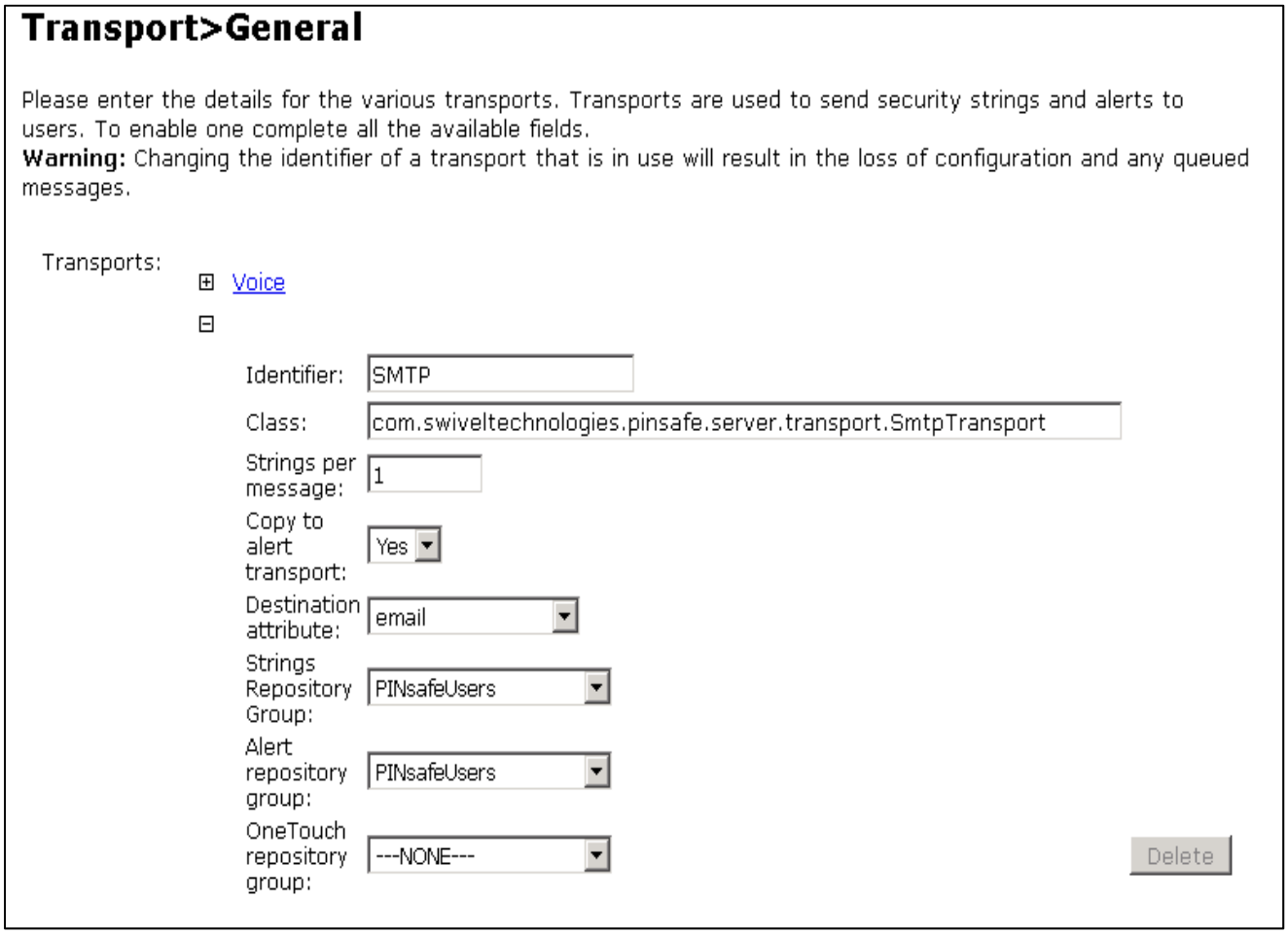
Add an Authentication User in PINsafe

1. From the PINsafe Management Console, select **Reporting/User administration**.
2. Click **Add user**.
3. In the **Username** text box, type a name for the authentication user. In this example, we use the username `leezy`.
4. In the **Email address** text box, type the email address for the authentication user. In this example, we use the email address leezy.li@watchguard.com.
5. In the PIN text box, type a number to be used as the PIN. In this example, we use `1234`.

6. In the **Password** text box, type a password to use for this user. In this example, we use `zG$t@cdc`.



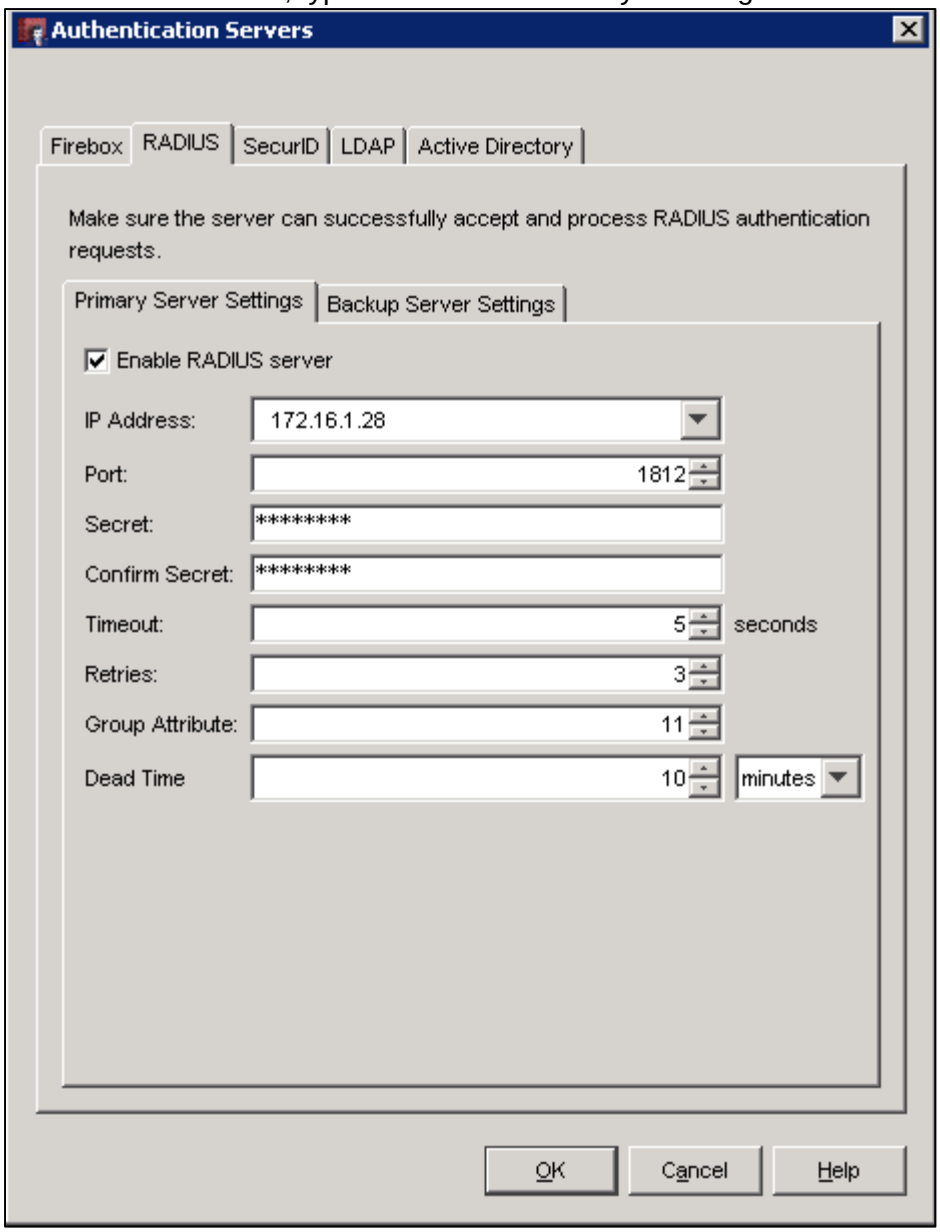
7. Make sure the **PINsafeUsers** check box is selected.


Transport>General
Please enter the details for the various transports. Transports are used to send security strings and alerts to users. To enable one complete all the available fields.
Warning: Changing the identifier of a transport that is in use will result in the loss of configuration and any queued messages.
Transports:
Voice
Identifier:
SMTP
Class:
com.swiveltechnologies.pinsafe.server.transport.SmtpTransport
Strings per message:
1
Copy to alert transport:
Yes
Destination attribute:
email
Strings Repository Group:
PINsafeUsers
Alert repository group:
PINsafeUsers
OneTouch repository group:
---NONE---
Delete

Configure the Firebox to use a RADIUS Authentication Server

In this procedure, we configure the Firebox to use RADIUS authentication. You can use Policy Manager or Fireware Web UI. In this example, we use Policy Manager.

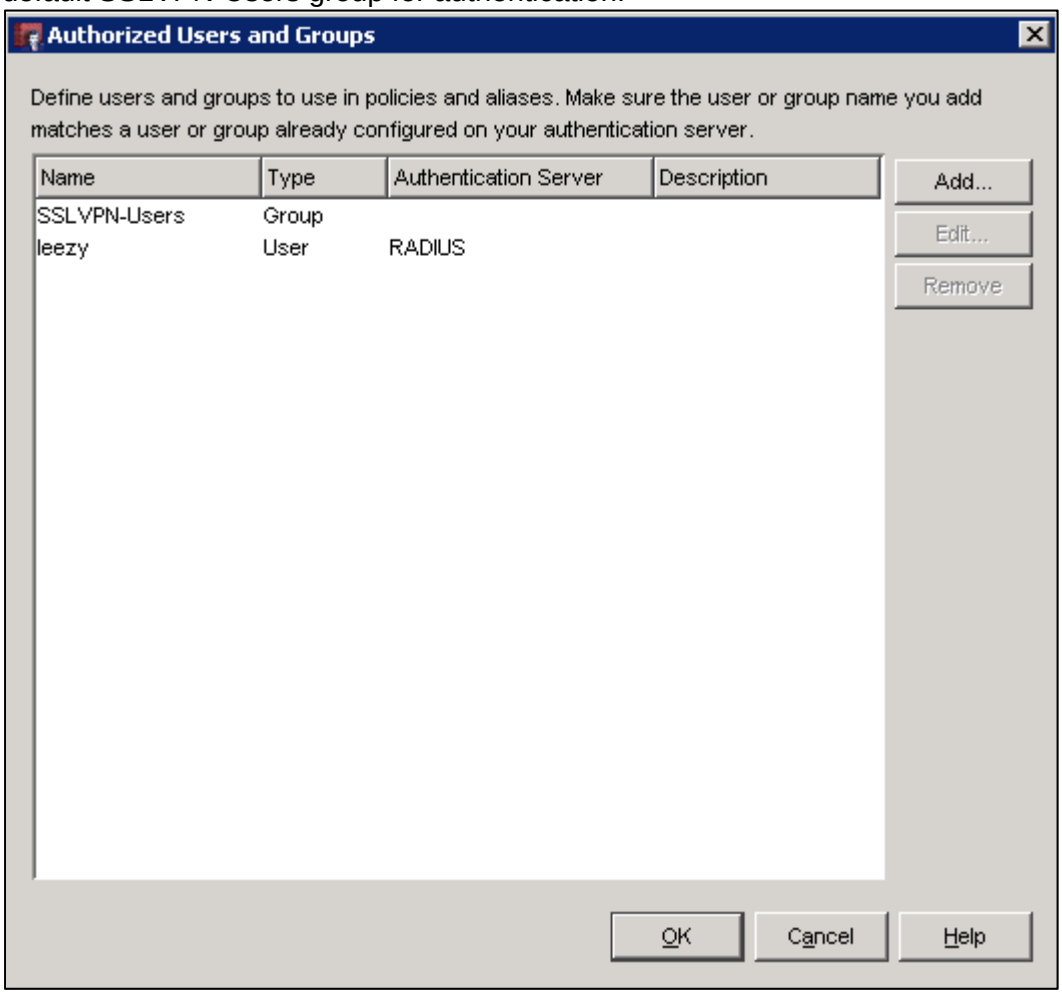
1. From Policy Manager, select **Setup > Authentication > Authentication Servers**.
2. Select the **RADIUS** tab.
3. In the **IP address** field, type or select the IP address of the Swivel PINsafe server.
4. In the **Secret** text box, type the RADIUS secret you configured on the PINsafe server.



5. Click **OK**.

Configure Users and Groups on the Firebox

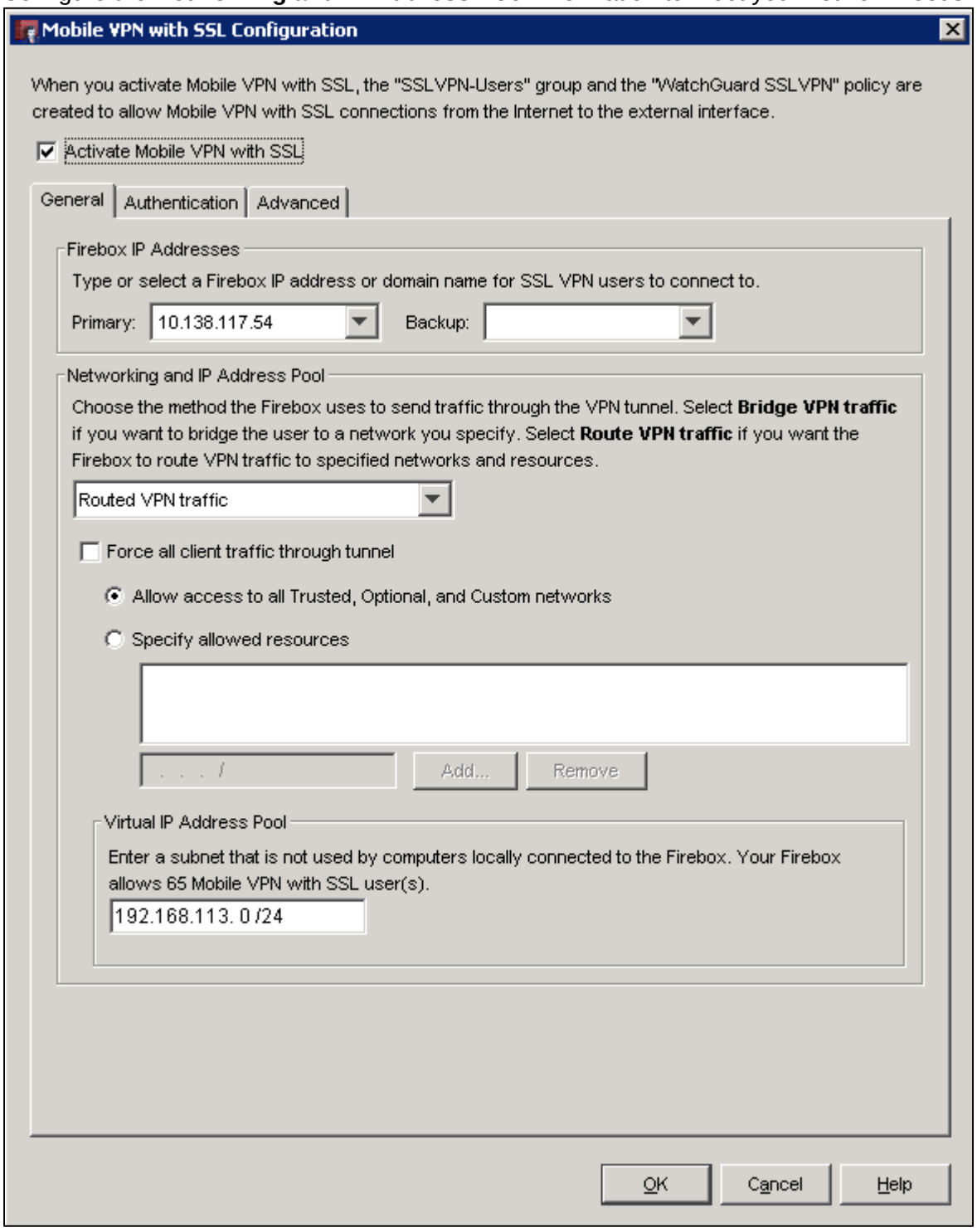
1. From Policy Manager, select **Setup > Authentication User/Group**.
2. From here, you can add users or groups to match those defined on your RADIUS server or use the default SSLVPN-Users group for authentication.



Configure Mobile VPN with SSL on the Firebox

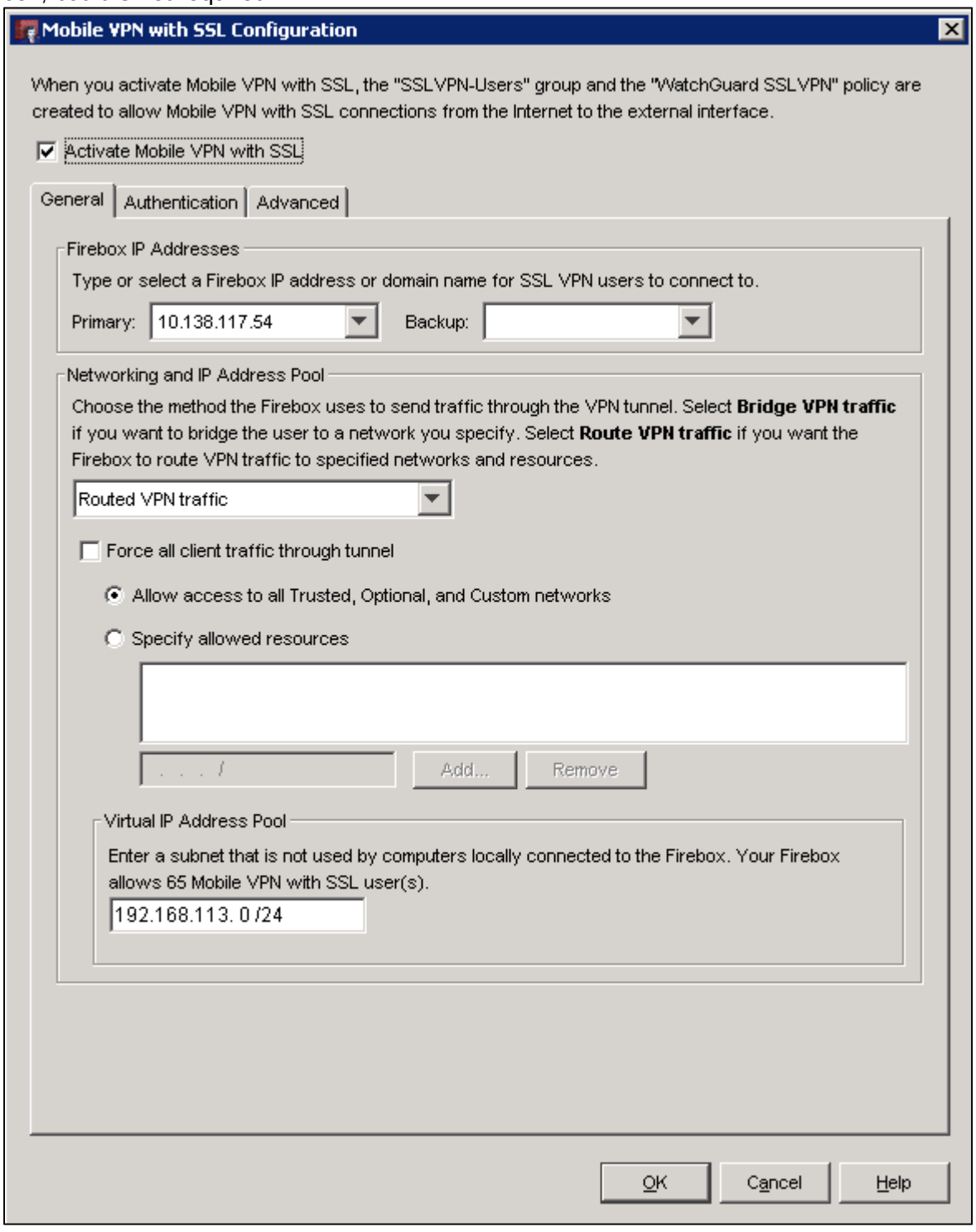
1. From Policy Manager, select **VPN > Mobile VPN > SSL**.
2. Select the **Activate Mobile VPN with SSL** check box.
3. From the **Firebox IP Addresses** drop-down list, select the IP address or domain name to which Mobile VPN clients will connect.

4. Configure the **Networking and IP Address Pool** information to meet your network needs.



5. On the Authentication tab, select the RADIUS server.

6. We recommend that you enable the **Force users to authenticate after a connection is lost** check box, but it is not required.

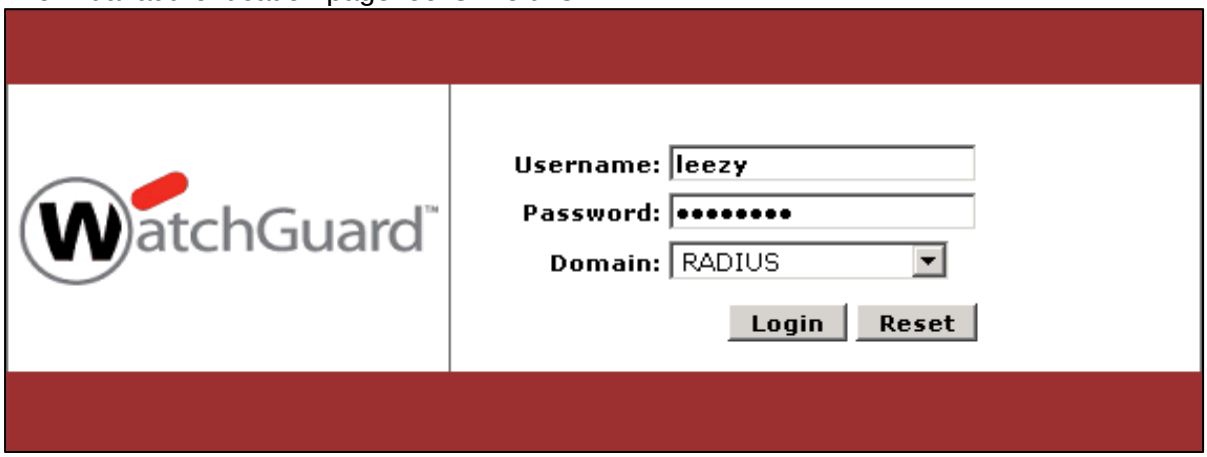


7. Click **OK**.

When Mobile VPN with SSL is enabled, an SSLVPN-Users user group and a WatchGuard SSLVPN policy are automatically created in your Firebox configuration to allow SSL VPN connections from the Internet to the external interface of your Firebox. You can use these groups or create new groups to match the user group names defined on the authentication server.

Download Mobile VPN with SSL Software with PINsafe

1. From the web browser of a client computer, open the Mobile VPN with SSL client software download page on the WatchGuard Firebox. The URL for this page follows this pattern:
   https://<device interface IP address>:4100/sslvpn.html
   The initial authentication page looks like this:

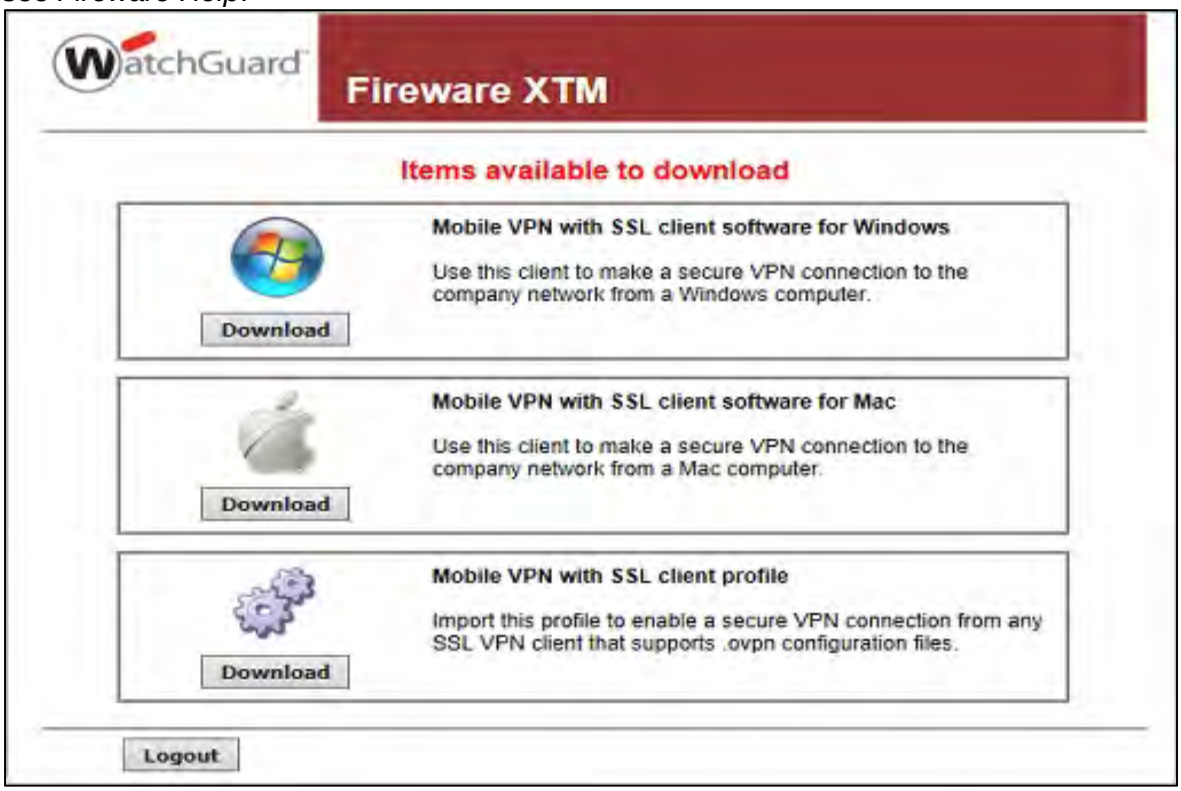


2. After you click **Login**, you will receive an email that contains a one-time code. The email should include content similar to this:

```
PINsafe Security String Message
1234567890
6374859201
```

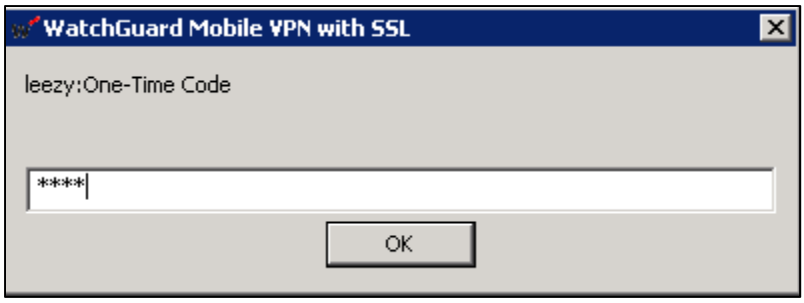
3. When prompted, enter the PINsafe One Time Code. Because the user PIN in our example is set to 1234, the one-time code to enter is 6374.

4. When authentication is successful, you will see the Mobile VPN with SSL client software download page and you can select the client software for your computer operating system. For more information, see *Fireware Help*.



Mobile VPN with SSL Client Authentication

After you download and install the Mobile VPN with SSL client on your computer, you can use the same authentication process to connect to the Firebox with the SSL VPN client.


WatchGuard Mobile VPN with SSL
leezy:One-Time Code
****
OK