

WatchGuard Integration

Contents

- 1 Introduction
- 2 Integration Overview
- 3 Platform and Software
- 4 Configuration
 - ◆ 4.1 Configure the RADIUS Server and NAS entry in Swivel Sentry
- 5 Configure Swivel Sentry for Two-Factor Authentication using Email
 - ◆ 5.1 Configure Challenge and Response Authentication
 - ◆ 5.2 Create an Email OTC Group
 - ◆ 5.3 Create an Email Transport Type
 - ◆ 5.4 Configure an SMTP Gateway
 - ◆ 5.5 Add an Authentication User in Swivel Sentry
- 6 Configure the Firebox to use a RADIUS Authentication Server
 - ◆ 6.1 Configure Users and Groups on the Firebox
 - ◆ 6.2 Configure Mobile VPN with SSL on the Firebox
- 7 Download Mobile VPN with SSL Software with Swivel Sentry
- 8 Mobile VPN with SSL Client Authentication
- 9 Troubleshooting

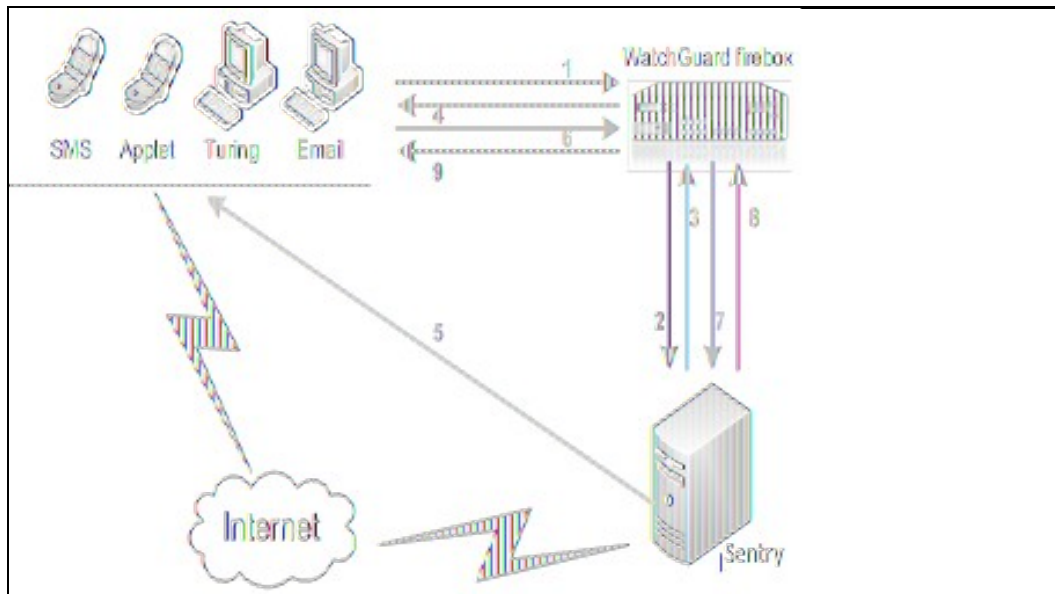
Introduction

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 provide a two-factor authentication solution, called Sentry. Future references to the Swivel authentication solution, will simply be referred to as Swivel Sentry.

Integration Overview

Swivel Sentry 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's Sentry two-factor authentication solution.

This diagram shows the workflow for two-factor authentication through integration with Swivel Sentry, 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 Swivel Sentry.
3. Swivel Sentry 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 Swivel Sentry is set to Dual Challenge On Demand, Swivel Sentry 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 TURING image, mobile phone client applicationapp, 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. Swivel Sentry 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 Swivel Sentry.
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 appliance server v2, and Swivel Sentry v.10.5.3030 installed on a Windows computer
? FreeRADIUS server 2.2.3

Configuration

Configure the RADIUS Server and NAS entry in Swivel Sentry

1. Verify that the RADIUS server has been enabled in Swivel Sentry. To do this, open the Swivel Sentry Management Console. Select RADIUS > Server and make sure 'Server enabled' in the drop-down list 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
Session TTL:	60
Permit empty attributes:	No
Radius Groups:	No
Radius Group Keyword:	
Additional RADIUS logging:	Both
Enable debug:	No


Apply Reset

2. From the Swivel Sentry 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.

RADIUS>NAS 

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the authentication services of the Swivel server via the RADIUS interface.

NAS: 

Identifier:	<input type="text" value="Watch VPN"/>
Hostname/IP:	<input type="text" value="172.16.1.1"/>
Secret:	<input type="password" value="*****"/>
Group:	<input type="text" value="---ANY---"/>
EAP protocol:	<input type="text" value="None"/>
Authentication Mode:	<input type="text" value="All"/>
Vendor (Groups):	<input type="text" value="Watchguard"/>
Change PIN warning:	<input type="text" value="No"/>
Two Stage Auth:	<input type="text" value="Yes"/>
Allow blank password at Stage One:	<input type="text" value="No"/>
Send Security String after Stage One:	<input type="text" value="Yes"/>
Even if User as Valid String:	<input type="text" value="Yes"/>
Check password with repository:	<input type="text" value="No"/>
Authenticate non-user with just password:	<input type="text" value="No"/>
Username attribute for repository:	<input type="text"/>
Allow alternative usernames:	<input type="text" value="No"/>
Alternative username attributes:	<input type="text"/>
OTC timeout (mins):	<input type="text" value="0"/>
Internal IP ranges:	<input type="text"/>
Send username in challenge:	<input type="text" value="No"/>

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

Configure Swivel Sentry 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 OTC for the second authentication. The code can be distributed through an SMS text message, email, TURring image, or mobile phone client application. In this example, we will configure Swivel Sentry to send the one-time code through email.

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

RADIUS>NAS 

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the authentication services of the Swivel server via the RADIUS interface.

NAS: 

Identifier:	<input type="text" value="Watch VPN"/>
Hostname/IP:	<input type="text" value="172.16.1.1"/>
Secret:	<input type="password" value="*****"/>
Group:	<input type="text" value="---ANY---"/>
EAP protocol:	<input type="text" value="None"/>
Authentication Mode:	<input type="text" value="All"/>
Vendor (Groups):	<input type="text" value="Watchguard"/>
Change PIN warning:	<input type="text" value="No"/>
Two Stage Auth:	<input type="text" value="Yes"/>
Allow blank password at Stage One:	<input type="text" value="No"/>

Configure Challenge and Response Authentication

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

1. From the Swivel Sentry Administration Console, select Server > Dual Channel.
2. Make sure the **On-demand authentication** drop-down box 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

On-Demand Delivery: No

Allow message request by username: Yes

Allow alternative usernames: No

Verification Mode: Standard - OTC

Alternative username attributes:

Multiple authentications per String: No

Confirmation image on message request: Yes

In Bound OTC Rule: None

Confirmation key: 1

Call/Notification gap (s): 10

In Bound SMS Timeout (ms): 500

Domain Allowed to get OTC:

Apply Reset

Create an Email OTC Group

A group is needed to give authentication rights to users via email. This group could be linked to AD, but for the example, we will use local users created in Swivel Sentry:

1. From the Swivel Sentry Management Console, select Repository > Groups.
2. In the empty fields at the bottom of the screen, type in SwivelEmailOTC as a group name.
3. Select the Dual and PINless tick boxes.
4. In the Local XML field, type in SwivelEmailOTC as the name.

Repository>Groups

Please enter the repository group information to be used by the Swivel server. This includes group privileges and Active Directory/LDAP definition. For XML repository, please copy the group name into the definition.

	Single	Dual	OneTouch	Mobile Client	Admin	Helpdesk	PINless	OATH
Name: SwivelImage	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Definitions:								
Local XML: SwivelImage								
Name: SwivelAdmin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Definitions:								
Local XML: SwivelImage								
Name: SwivelEmailOTC	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Definitions:								
Local XML: SwivelEmailOTC								

Apply Reset Group Rights

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

Create an Email Transport Type

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

1. From the Swivel Sentry 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 **SwivelEmailOTC**.
4. From the **Alert repository group** drop-down list, select **SwivelEmailOTC**.

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:

Identifier:

Class:

Strings per message:

Copy to alert transport:

Destination attribute:

Strings Repository Group:

Alert repository group:

OneTouch repository group:

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

Configure an SMTP Gateway

You must define an email gateway for Swivel to use.

1. From the Swivel Sentry 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.

Server > SMTP

Please enter the details of an SMTP relay to be used for delivering mail.

Hostname/IP:

Port:

Authentication enabled:

Username:

Password:

Timeout (secs):

2. Make sure that there is connectivity between the Swivel Sentry server appliance and the mail gateway.

Add an Authentication User in Swivel Sentry

1. From the Swivel Sentry 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*.

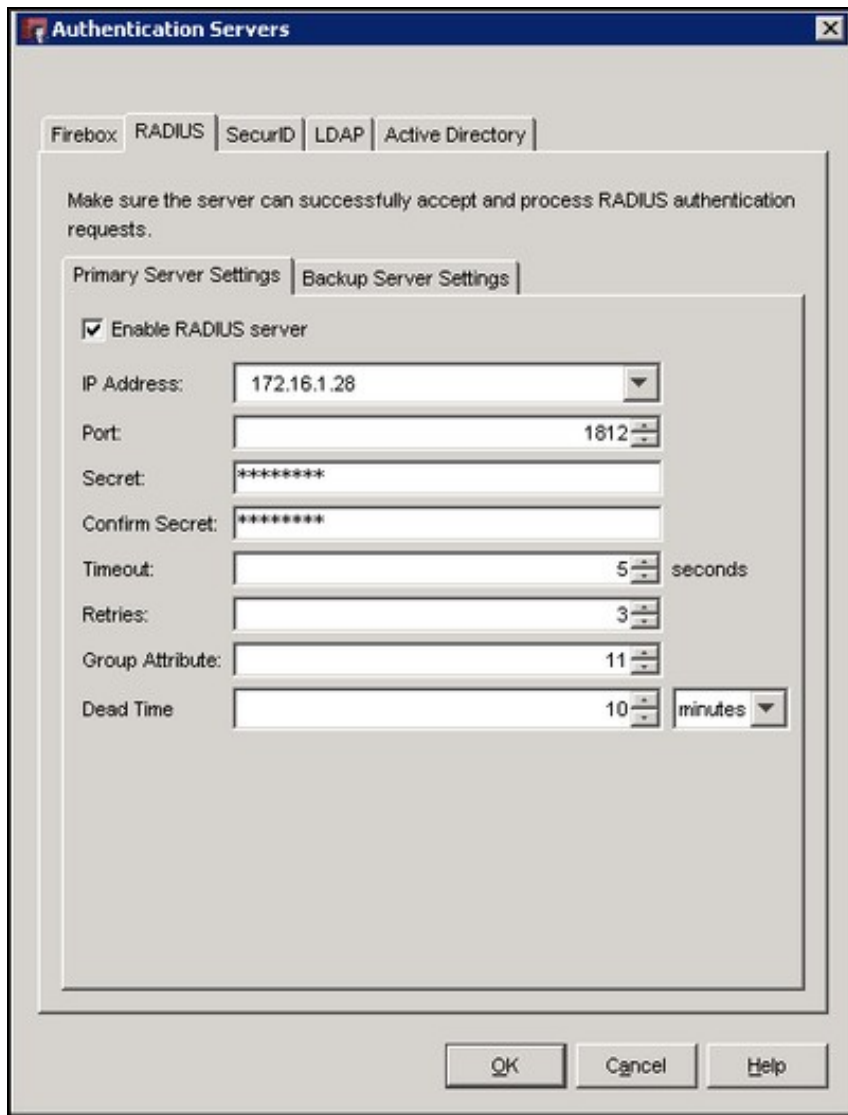
Username:	<input type="text" value="leezy"/>
First name:	<input type="text" value="Li"/>
Last name:	<input type="text" value="Leezy"/>
Email address:	<input type="text" value="leezy.li@watchguard.com"/>
Phone number:	<input type="text"/>
PIN:	<input type="text" value="****"/>
Password:	<input type="text" value="*****"/>
Expiry Date:	<input type="text"/>
Custom attribute:	<input type="text"/>
Disabled	<input type="button" value="No"/> ▾
Server groups:	
SwivelEmailOTC	<input checked="" type="checkbox"/>
SwivelImage	<input type="checkbox"/>
SwivelAdmin	<input type="checkbox"/>
<input type="button" value="Reset"/>	<input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>

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

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.

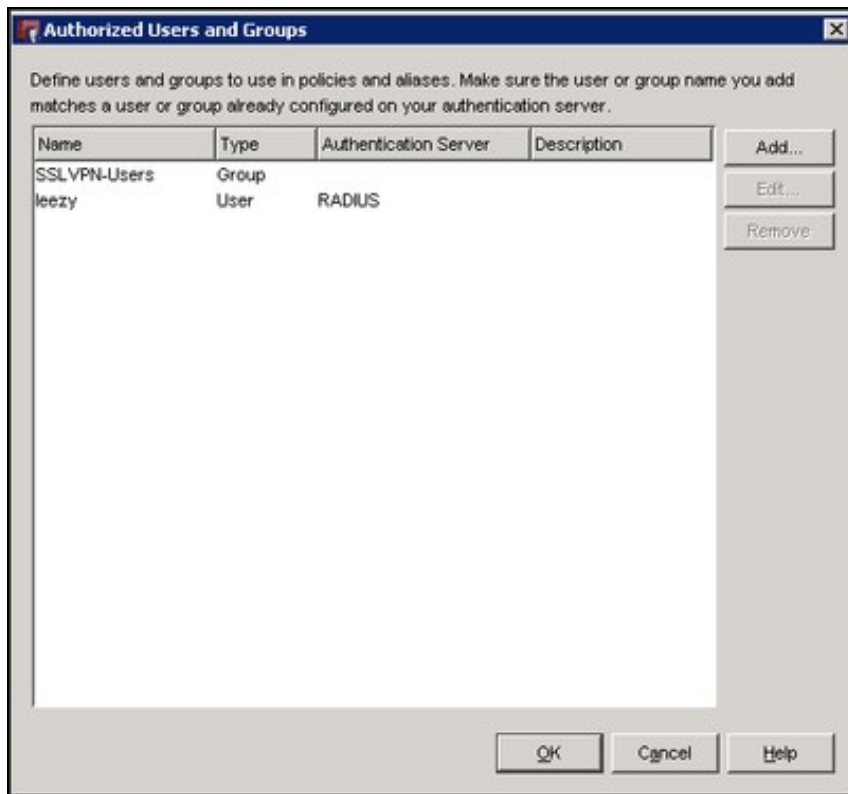
1. From Policy Manager, select Setup > Authentication > Authentication Servers.
2. Select the **RADIUS** tab.
3. In the **IP address** field, type or select the IP address of the Swivel Sentry appliance.
4. In the **Secret text** box, type the RADIUS secret you configured on the Swivel Sentry.



5. Click **OK**.

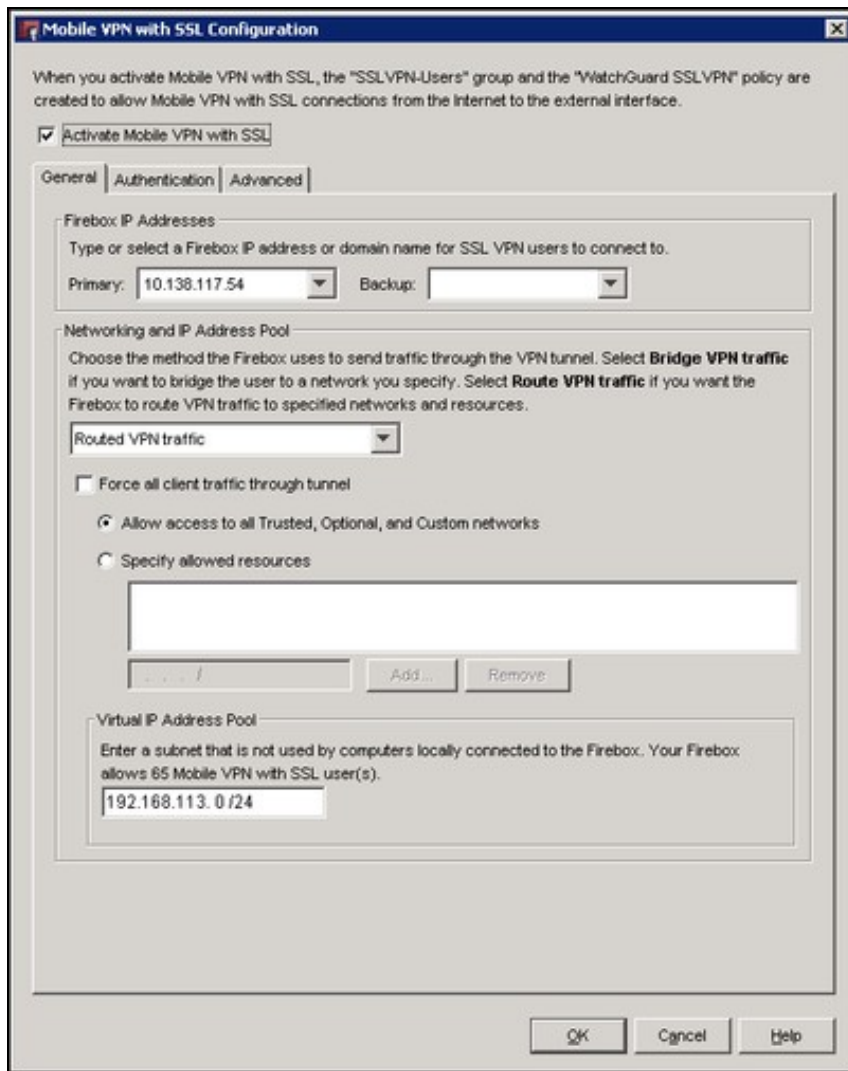
Configure Users and Groups on the Firebox

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.



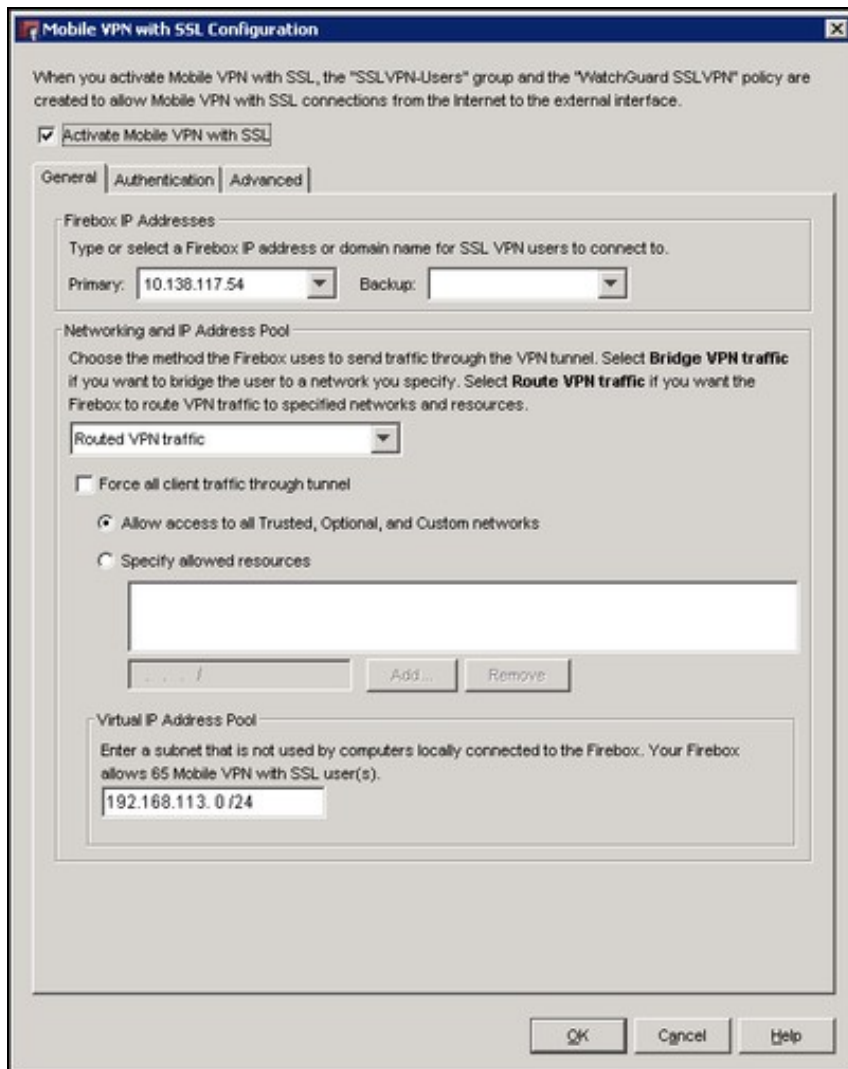
Configure Mobile VPN with SSL on the Firebox

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 Swivel Sentry

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:

Swivel One Time Code
637485

3. When prompted, enter the Swivel Sentry One Time Code. In our example the one-time code to enter is 637485.



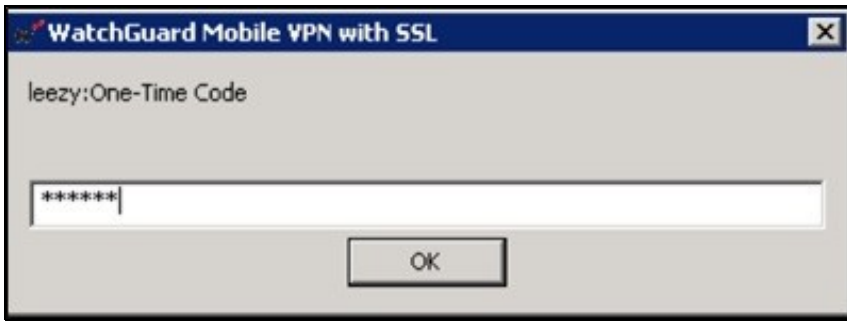
4. When authentication is successful, you will see the Mobile VPN with SSL client software download page and you can select the client software for your computer operating system. For more information, see Fireware Help.



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.





Troubleshooting