# SafeNet Authentication Service

# Integration Guide

## SAS using RADIUS Protocol with WatchGuard XTMv

## Document Information

| | |
|---|---|
| **Document Part Number** | 007-012745-001, Rev. A |
| **Release Date** | October 2014 |

## Trademarks



## Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

| Contact Method | Contact Information |
|---|---|
| **Mail** | SafeNet, Inc.<br>4690 Millennium Drive<br>Belcamp, Maryland  21017, USA |
| **Email** | TechPubs@safenet-inc.com |

# Contents

# Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as WatchGuard XTMv.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

# Description

SafeNet Authentication Service delivers a fully automated, versatile, and strong authentication-as-a-service solution. With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

WatchGuard's virtual solutions provide you with unmatched deployment flexibility. You can choose to deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform. WatchGuard virtual appliances feature all of the security and networking services found in our physical appliances and can be deployed in per-customer, -department, or -app scenarios for your virtual infrastructure.

WatchGuard® XTM security devices deliver:

- Application-layer content inspection that recognizes and blocks threats that stateful packet firewalls cannot detect.
- Best-of-breed security services, including intrusion prevention, spam blocking, and URL filtering—boosting protection in critical attack areas.
- Multiple VPN choices for flexibility in remote access.
- Monitoring and reporting tools that support industry and regulatory compliance.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in WatchGuard XTMv using SafeNet OTP authenticators managed by SafeNet Authentication Service.
- Configure WatchGuard XTMv to work with SafeNet Authentication Service in RADIUS mode.

This document assumes that the WatchGuard XTMv environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

WatchGuard XTMv can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with SafeNet Authentication Service.

# Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)** — SafeNet's cloud-based authentication service.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)** — A server version that is used by Service Providers to deploy instances of SafeNet Authentication Service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)** — A server version that is used to deploy the solution on-premises in the organization.

# Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service (SAS)** – SafeNet's cloud-based authentication service.
- **WatchGuard XTMv** - running on Fireware XTM OS 11.9.1

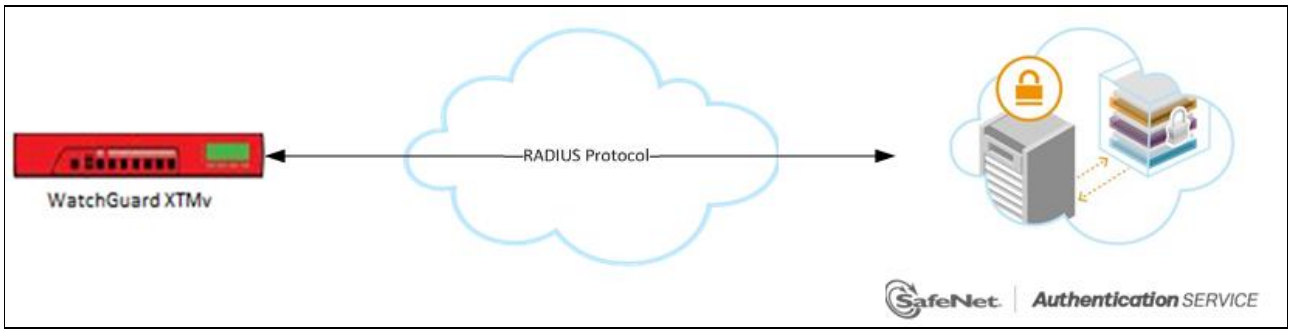
# Audience

This document is targeted to system administrators who are familiar with WatchGuard XTMv and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

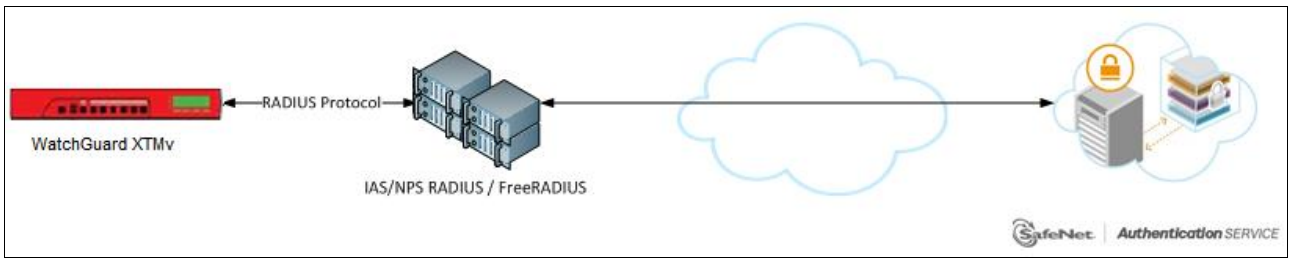
# RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

- **SAS cloud-hosted RADIUS service** – A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.




- **Local RADIUS hosted on-premises** - A RADIUS agent that is implemented in the existing customer's RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.




For more information on how to install and configure SAS Agent for IAS/NPS, refer to:
http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

For more details on how to install and configure FreeRADIUS, refer to the *SAS FreeRADIUS Agent Configuration Guide*.

This document demonstrates the solution using the SAS cloud-hosted RADIUS service.

# RADIUS-based Authentication using SAS-SPE and SAS-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)** – An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.
- **SafeNet Authentication Service – Private Cloud Edition (PCE)** – An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, SAS can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS) or the legacy Microsoft Internet Authentication Service (MS-IAS)** — SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.

  For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to the following document:

  http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

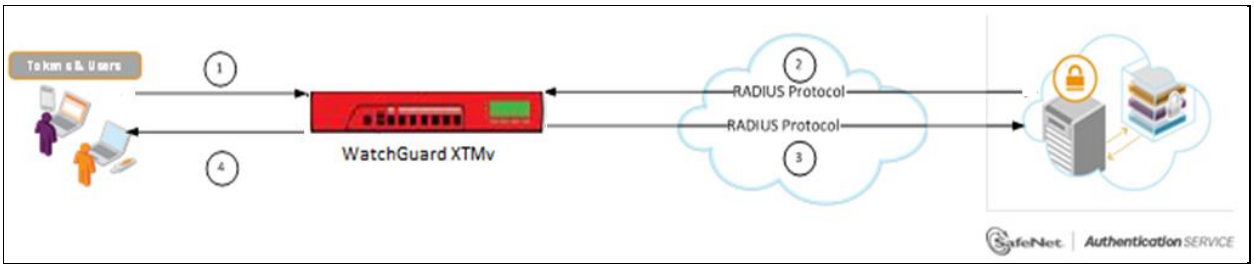
- **FreeRADIUS** — The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

# RADIUS Authentication Flow using SAS

SafeNet Authentication Service communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the dataflow of a multi-factor authentication transaction for WatchGuard XTMv.




1. A user attempts to log on to WatchGuard XTMv using an OTP authenticator.
2. WatchGuard XTMv sends a RADIUS request with the user's credentials to SafeNet Authentication Service for validation.
3. The SAS authentication reply is sent back to WatchGuard XTMv.
4. The user is granted or denied access to WatchGuard XTMv based on the OTP value calculation results from SAS.

# RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from WatchGuard XTMv, ensure the following:

- End users can authenticate through from the WatchGuard XTMv environment with a static password before configuring WatchGuard XTMv to use RADIUS authentication.
- Ports 1812/1813 are open to and from WatchGuard XTMv.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signature purposes.

# Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with WatchGuard XTMv using the RADIUS protocol requires:

- Synchronizing user stores to SAS
- Authenticator assignment in SAS
- Adding WatchGuard XTMv as an Authentication Node in SAS
- Checking the SAS RADIUS IP address

## Synchronizing User Stores to SafeNet Authentication Service

Before SAS can authenticate any user in your organization, you must create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time using the **Create User** shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory/LDAP server using the SAS Synchronization Agent

For further details on importing users to SafeNet Authentication Service, refer to the section on “creating users” in the *SafeNet Authentication Service Subscriber Account Operator Guide*:

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

## Authenticator Assignment in SAS

SAS supports a number of authentication methods that can be used as second authentication factor for users who are authenticating through WatchGuard XTMv.

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS tokens
- MP-1 software token
- GrIDsure authentication
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning** – Assign an authenticator to users one by one.
- **Provisioning rules** – The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change; an authenticator will be assigned automatically to the user.

Refer to “provisioning rules” in the *SafeNet Authentication Service - Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.

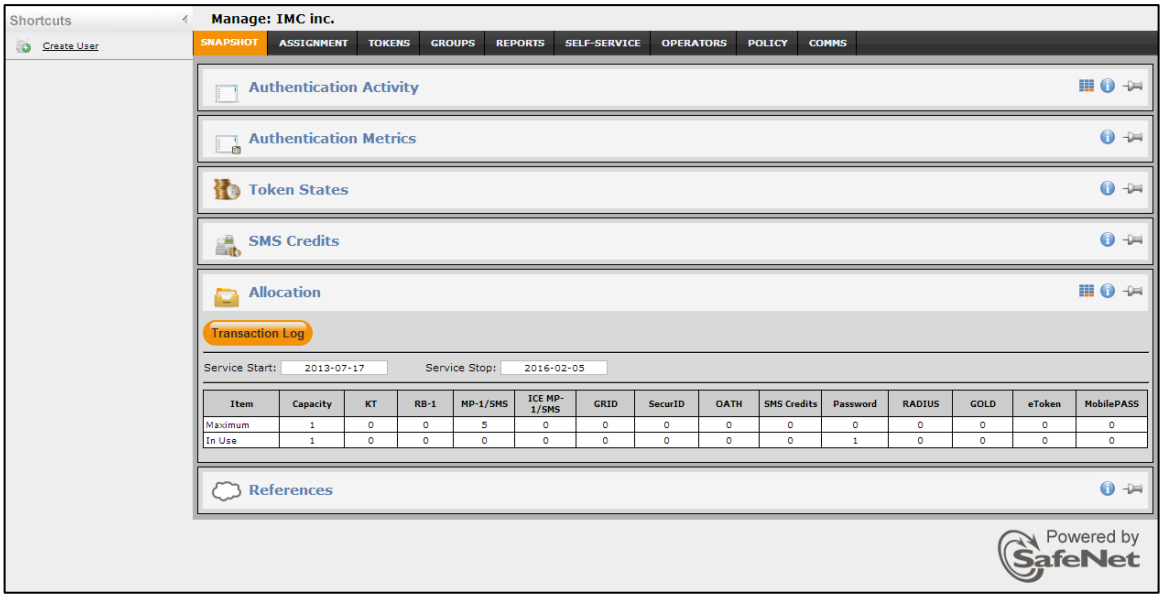
http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

# Adding WatchGuard XTMv as an Authentication Node in SAS

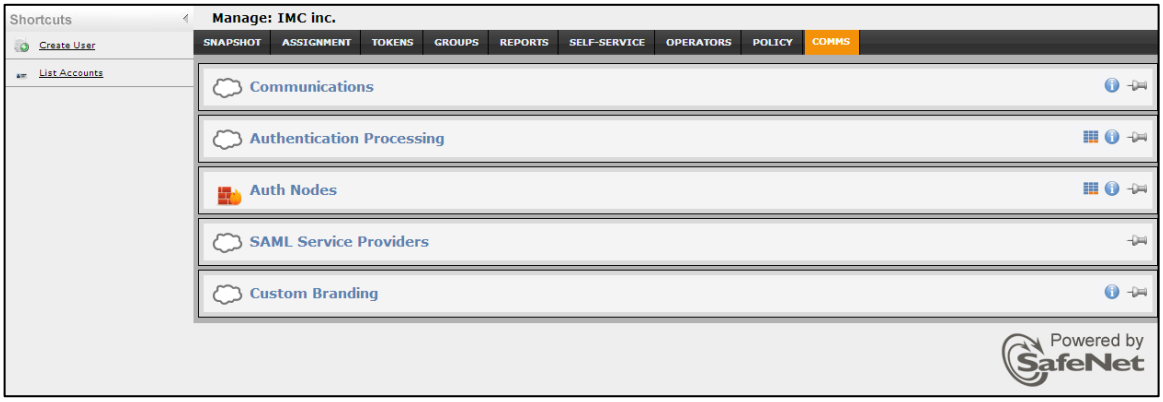
Add a RADIUS entry in the SAS **Authentication Nodes** module to prepare it to receive RADIUS authentication requests from WatchGuard XTMv. You will need the IP address of WatchGuard XTMv and the shared secret to be used by both SAS and WatchGuard XTMv.

**To add an Authentication Node in SAS:**

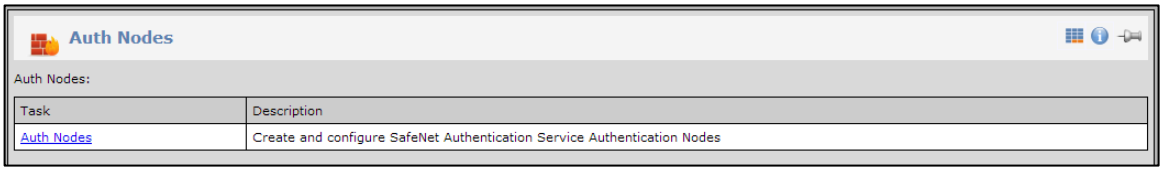
1. Log in to the SAS console with an Operator account.



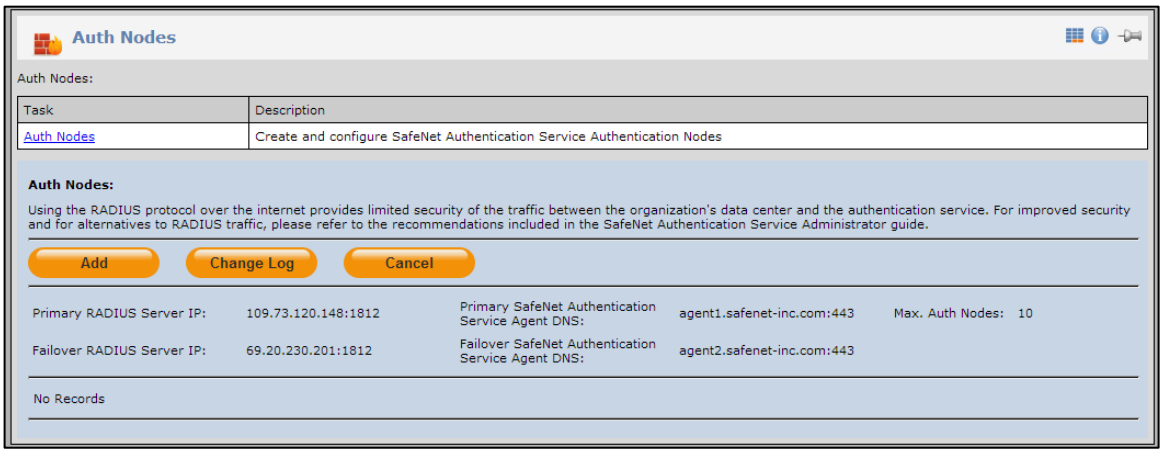

2. Click the **COMMS** tab, and then select the **Auth Nodes** module.




3. In the **Auth Nodes** module, click the **Auth Nodes** link.

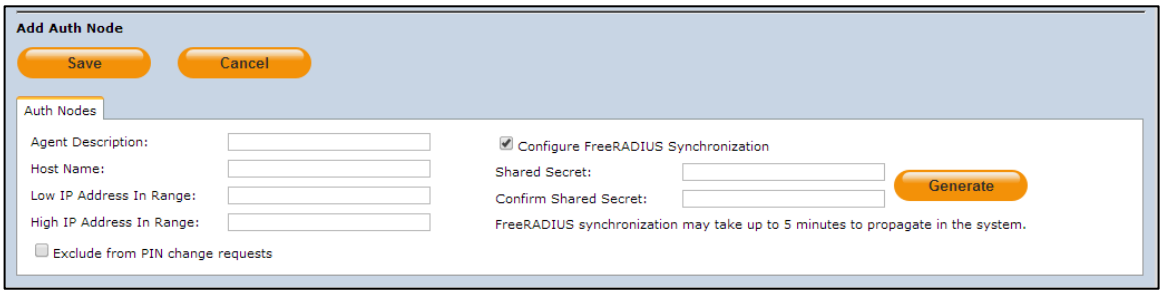


4. Click **Add**.

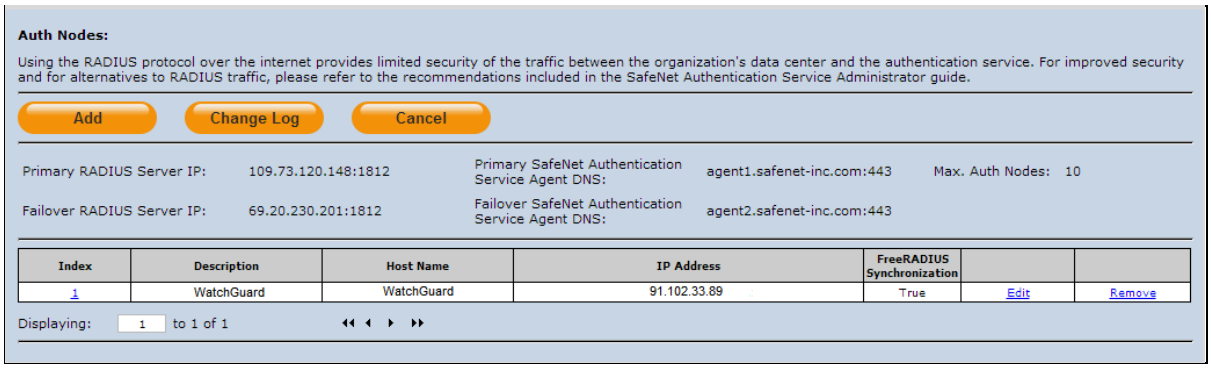



5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

| | |
|---|---|
| **Agent Description** | Enter a host description. |
| **Host Name** | Enter the name of the host that will authenticate with SAS. |
| **Low IP Address In Range** | Enter the IP address of the host that will authenticate with SAS. |
| **Configure FreeRADIUS Synchronization** | Select this option. |
| **Shared Secret** | Enter the shared secret key. |
| **Confirm Shared Secret** | Re-enter the shared secret key to confirm it. |




The Auth Node is added to the system.

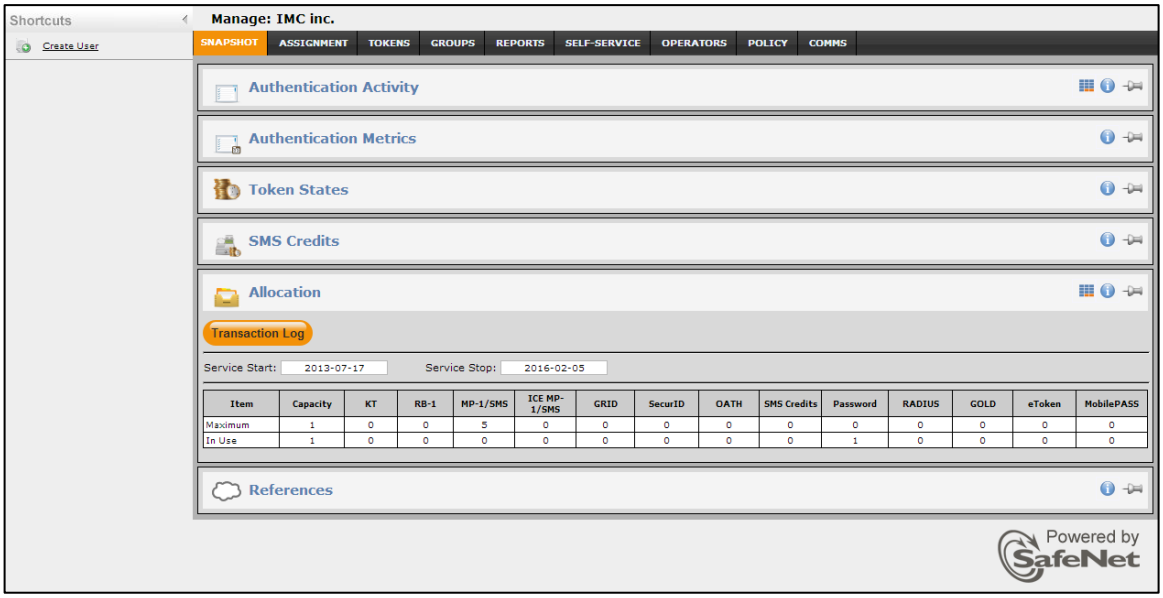


# Checking the SAS RADIUS IP Address

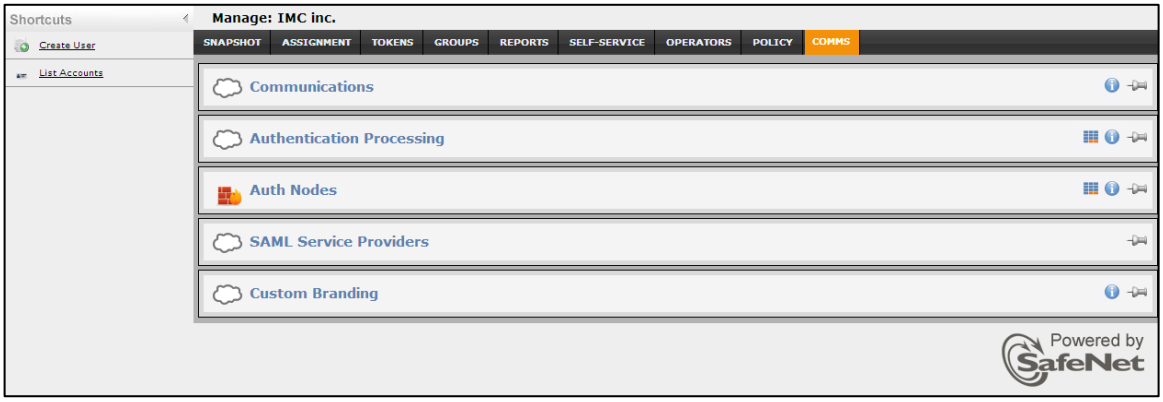
Before adding SafeNet Authentication Service as a RADIUS server in WatchGuard XTMv, check the IP address of the SAS RADIUS server. The IP address will then be added to WatchGuard XTMv as a RADIUS server at a later stage.

**To check the IP address of the SAS RADIUS server:**

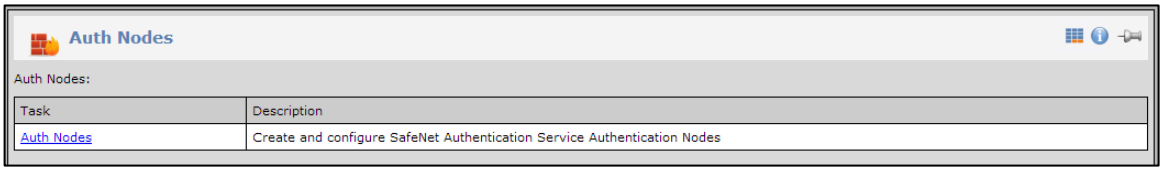
1. Log in to the SAS console with an Operator account.



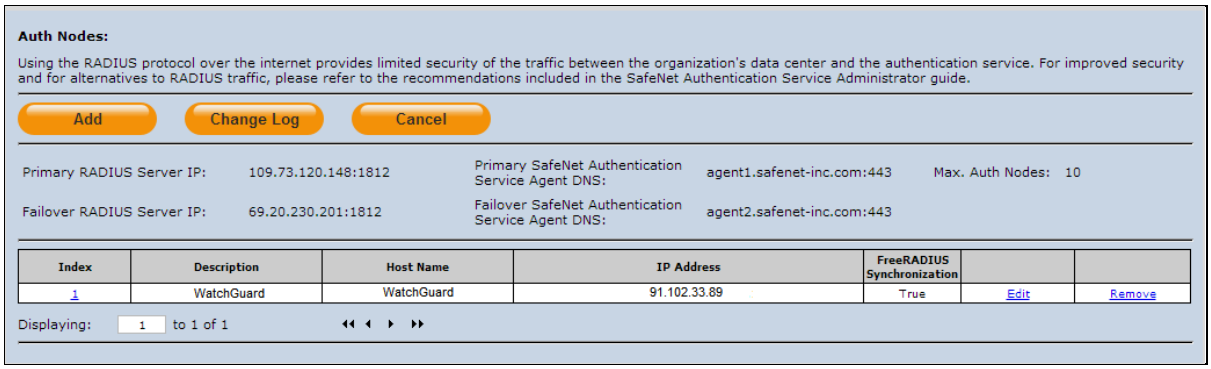

2. Click the **COMMS** tab, and then select the **Auth Nodes** module.




3. Click the **Auth Nodes** link.



The SAS RADIUS server details are displayed.



# Configuring WatchGuard XTMv

This section covers how to configure WatchGuard XTMv to use a RADIUS server for user authentication on an SSL VPN.

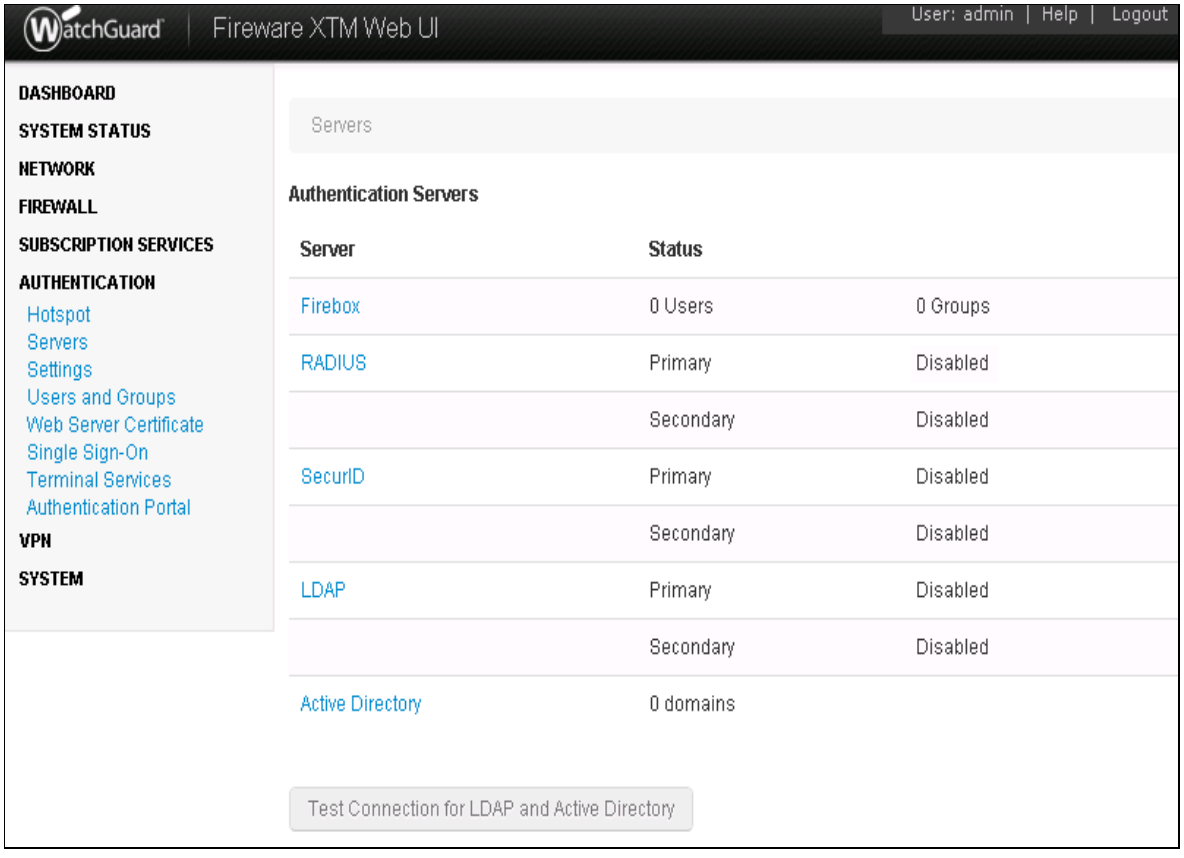
To configure WatchGuard XTMv, you need to:

- Configure WatchGuard XTMv to use RADIUS server authentication
- Activate WatchGuard Mobile VPN with SSL
- Select an authentication server and add a user

## Configuring WatchGuard XTMv to Use RADIUS Server Authentication

To use RADIUS server authentication with your XTMv device, you must enable and specify the RADIUS server in your XTMv device configuration.

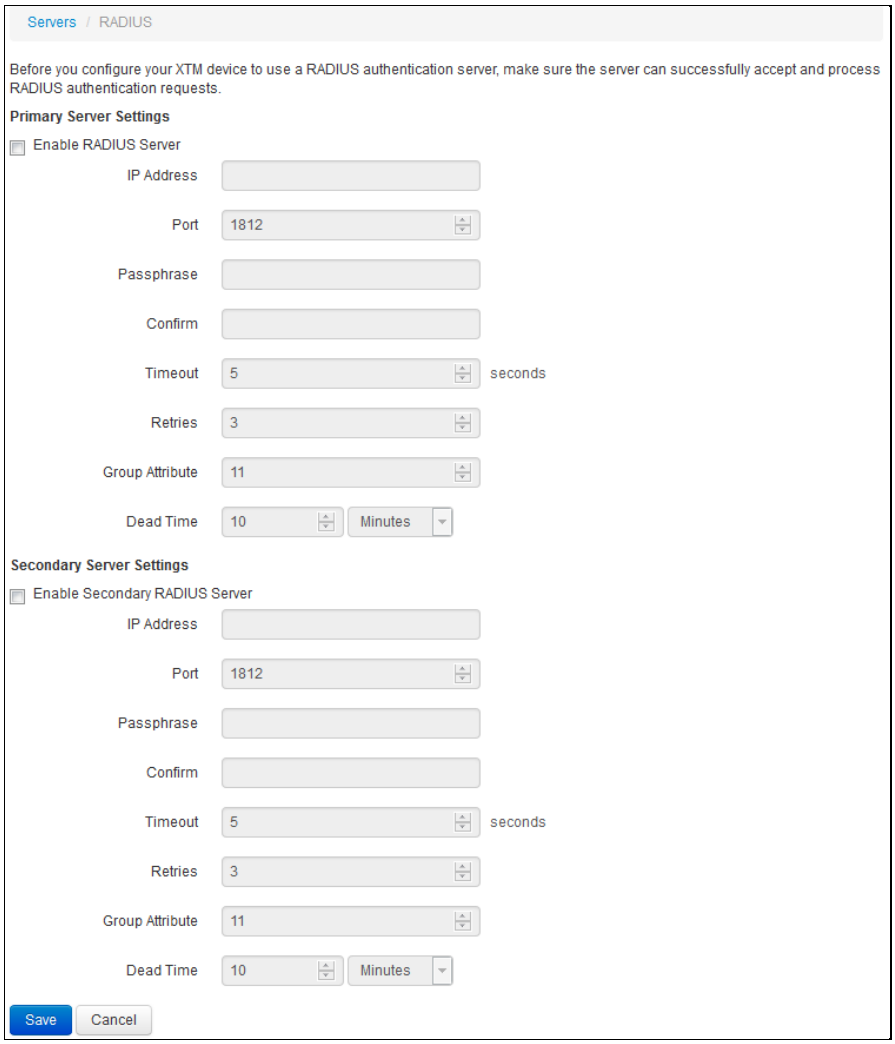
1. Log in to the **WatchGuard Web UI** console: **http://<IPAddress of WatchGuard>:<Port Number>/**. The default username/password combination is **admin/readwrite**.
2. On the **WatchGuard Web UI** console, in the left pane, click **Authentication > Servers**. In the right pane, under **Authentication Servers**, click the **RADIUS** link.




*(The screen image above is from WatchGuard® software. Trademarks are the property of their respective owners.)*

3. Under **Primary Server Settings**, complete the following fields, and then click **Save**.

| | |
|---|---|
| **Enable RADIUS server** | Select this option. |
| **IP Address** | Enter the IP address of the SAS RADIUS server.<br>To get the IP address of the SAS RADIUS server, refer to “Checking the SAS RADIUS IP Address” on page 11. |
| **Port** | Enter the port number through which the RADIUS server communicates. The default port number is 1812. |
| **Passphrase** | Enter the shared secret key.<br>This is the same key you specified in the section “<br>Adding WatchGuard XTMv as an Authentication Node in SAS” on page 9. |
| **Confirm** | Re-enter the shared secret key to confirm it. |

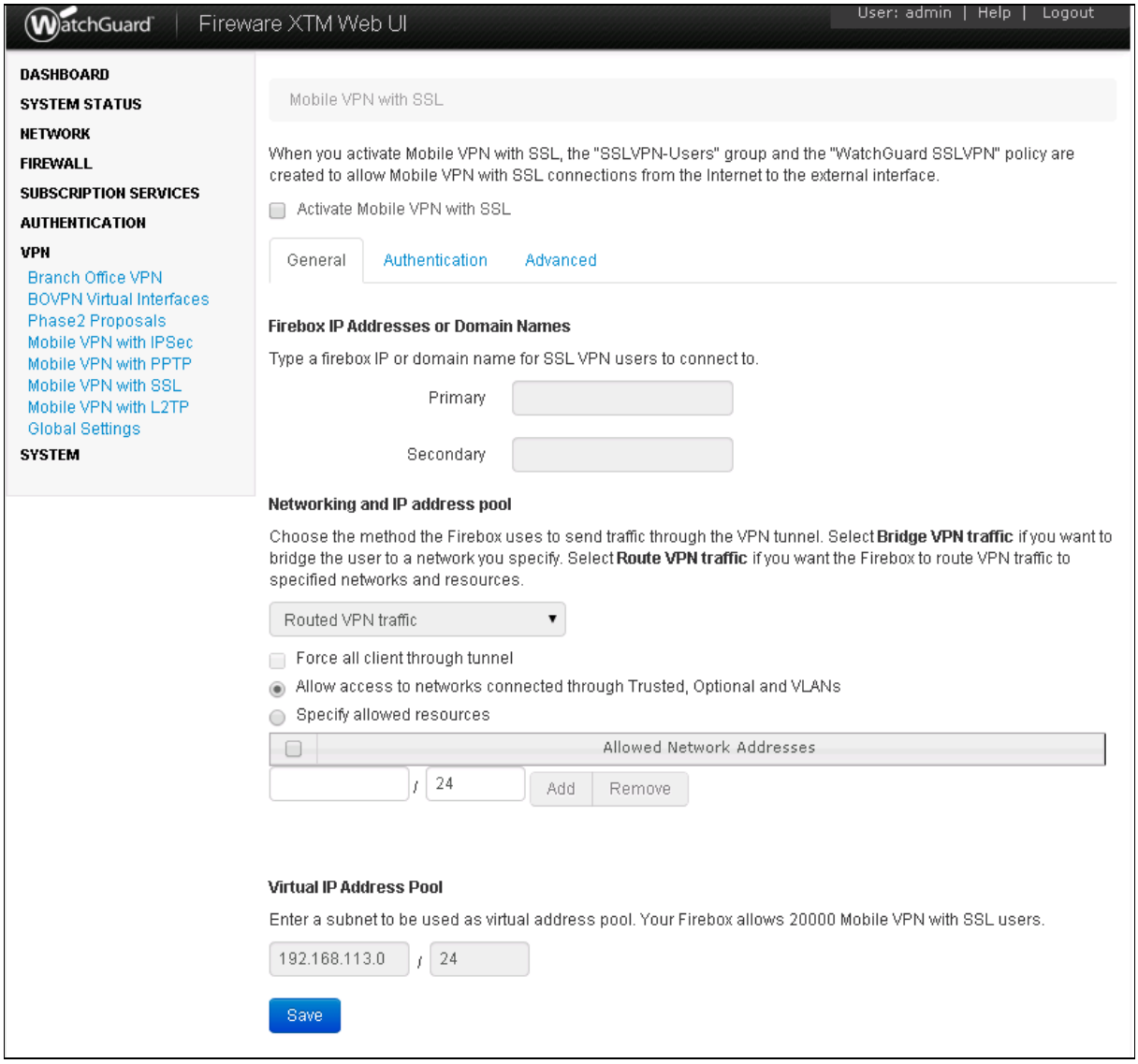



*(The screen image above is from WatchGuard® software. Trademarks are the property of their respective owners.)*

# Activating WatchGuard Mobile VPN with SSL

Activate the WatchGuard Mobile VPN with SSL to ensure that a secure connection is made from the remote computer to the protected network through an unsecured network, such as the Internet.

1. On the **WatchGuard Web UI** console, in the left pane, click **VPN > Mobile VPN with SSL**.



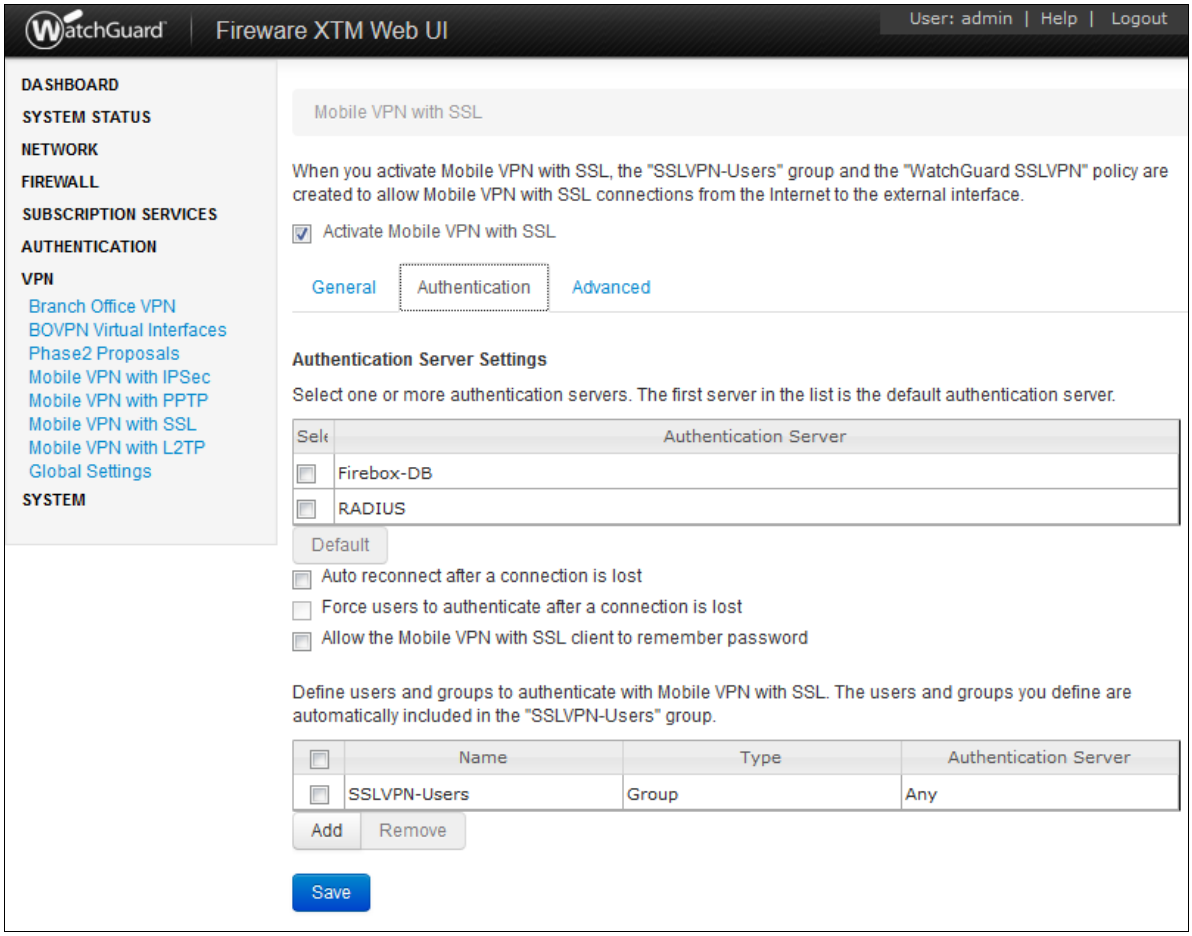

*(The screen image above is from WatchGuard® software. Trademarks are the property of their respective owners.)*

2. In the right pane, select **Activate Mobile with VPN**.
3. In the right pane, on the **General** tab, in the **Primary** field, enter the IP address or domain name of the WatchGuard XTMv appliance.
4. Click **Save**.

## Selecting an Authentication Server and Adding Users

Specify the RADIUS server to be used as the authentication server. Additionally, add users to authenticate with Mobile VPN with SSL.

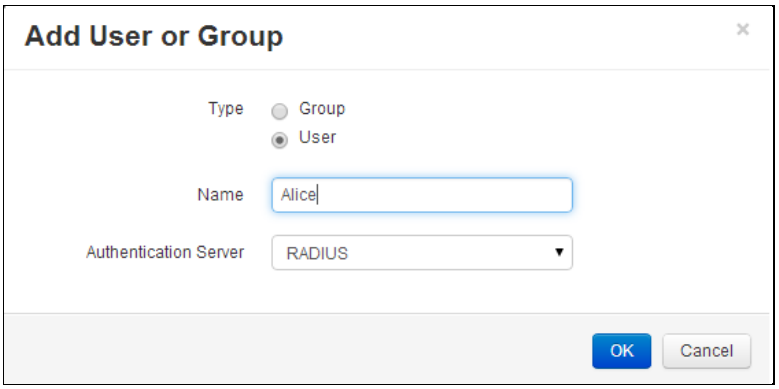
1. On the **WatchGuard Web UI** console, in the left pane, click **VPN > Mobile VPN with SSL**.
2. In the right pane, click the **Authentication** tab.




*(The screen image above is from WatchGuard® software. Trademarks are the property of their respective owners.)*

3. Under **Authentication Server Settings**, in the list of authentication servers, select **RADIUS**.
4. To add a user to authenticate with Mobile VPN with SSL, perform the following steps:
   a. On the **Authentication** tab, under **Authentication Server Settings**, click **Add**.
   b. Complete the following fields, and then click **OK**. The user is added to the **Users and Groups** list.

| | |
|---|---|
| **Type** | Select **User** |
| **Name** | Enter the user name. |
| **Authentication Server** | Select **RADIUS**. |




*(The screen image above is from WatchGuard® software. Trademarks are the property of their respective owners.)*

5. On the **WatchGuard Web UI** console, click **Save**.

# Running the Solution

A user can be assigned several types of SAS-supported tokens. For this integration, the SafeNet e-Token PASS is configured for authentication with the SAS solution.

You can use the following methods to securely connect to WatchGuard XTMv:

- Using the WatchGuard  Mobile VPN client
- Using the OpenVPN Connect application (for Android devices)

## Using the WatchGuard Mobile VPN Client

The WatchGuard Mobile VPN with SSL client is a software application that is installed on a remote computer. This client makes a secure connection from the remote computer to the protected network through an unsecured network, such as the Internet. The Mobile VPN client uses SSL to secure the connection.

1. On your Windows machine, open the **WatchGuard Mobile VPN with SSL Client**.
2. In the login window, complete the following fields, and then click **Connect**.

| | |
|---|---|
| **Server** | Enter or select the IP address of the WatchGuard XTMv device you want to connect to. |
| **User name** | Enter your user name.<br>If Mobile VPN with SSL on the XTMv device is configured to use multiple authentication methods, you might need to specify the authentication server or domain as part of the user name. |
| **Password** | Use the OTP token (for example, SafeNet e-Token PASS) to generate a passcode, and then enter it in this field. |

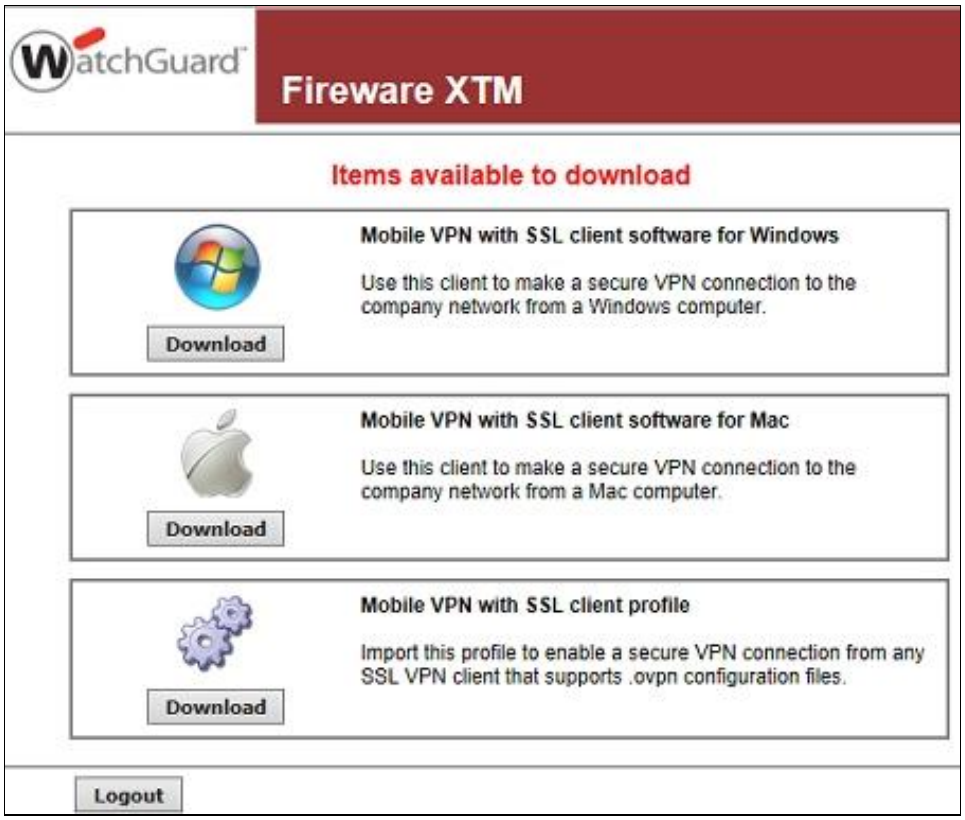

*(The screen image above is from WatchGuard® software. Trademarks are the property of their respective owners.)*

On successful authentication, you will gain access to the company's internal network through the SSL VPN.

## Using the OpenVPN Connect Application

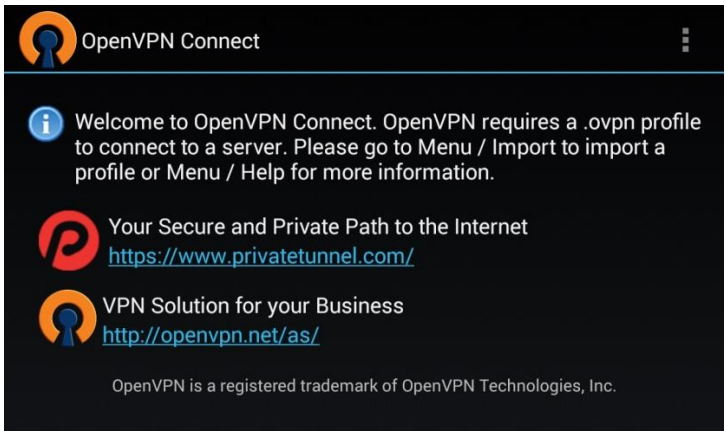
OpenVPN Connect is the official full-featured Android VPN client for the OpenVPN Access Server, Private Tunnel VPN, and OpenVPN Community, developed by OpenVPN Technologies, Inc.

1. On your Android device, open this URL in a web browser: **https://<Firebox IP Address>/sslvpn.html**
2. Log in as an administrator.
3. Click the **Download** button for **Mobile VPN with SSL client profile**. The **client.ovpn** file is downloaded.



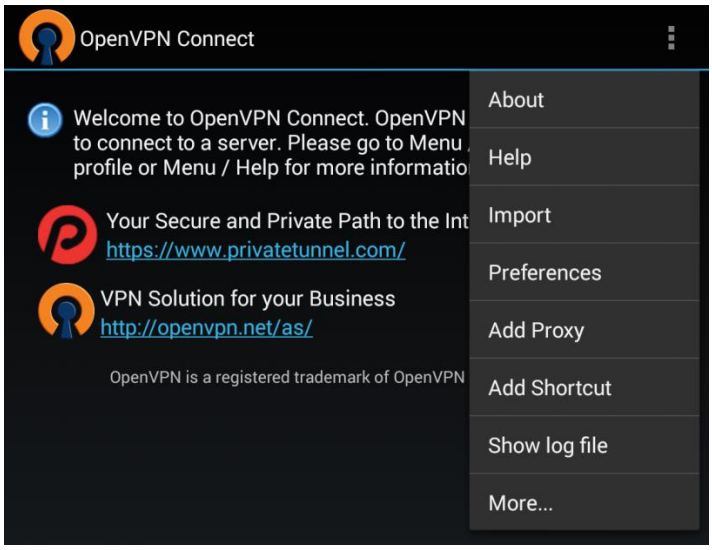

*(The screen image above is from WatchGuard® software. Trademarks are the property of their respective owners.)*

4. Open the **OpenVPN Connect** application.



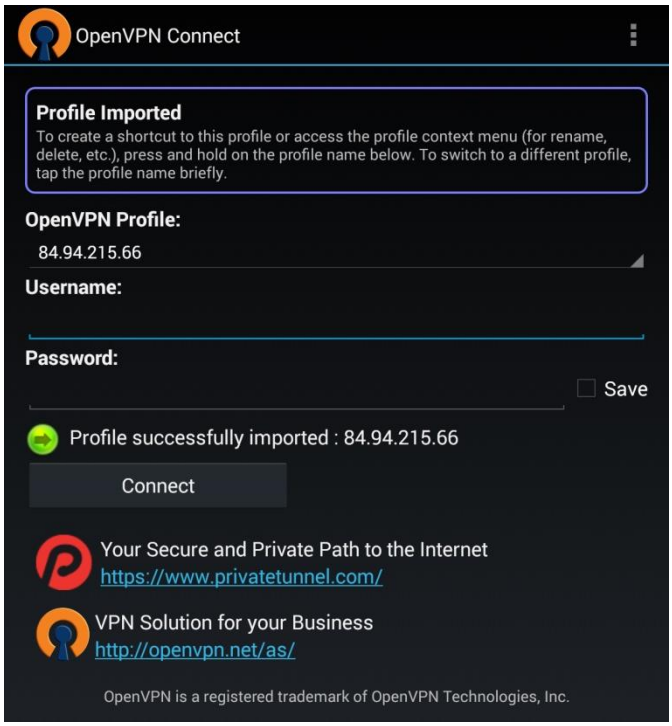

*(The screen image above is from OpenVPN® software. Trademarks are the property of their respective owners.)*

5. In the top right corner, tap ⋮. On the menu, tap **Import** and then select the **client.ovpn** file you downloaded earlier.




*(The screen image above is from OpenVPN® software. Trademarks are the property of their respective owners.)*

6. In the **Username** field, enter your user name.




*(The screen image above is from OpenVPN® software. Trademarks are the property of their respective owners.)*

7. Use the OTP token (for example, SafeNet e-Token PASS) to generate a passcode, and then enter it in the **Password** field.

8. Tap **Connect**.

   On successful authentication, you will gain access to the company's internal network through the SSL VPN.


*(The screen image above is from OpenVPN® software. Trademarks are the property of their respective owners.)*

# Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

| Contact Method | Contact Information | |
|---|---|---|
| **Address** | SafeNet, Inc.<br>4690 Millennium Drive<br>Belcamp, Maryland 21017 USA | |
| **Phone** | United States | 1-800-545-6608 |
| | International | 1-410-931-7520 |
| **Technical Support Customer Portal** | https://serviceportal.safenet-inc.com<br>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base. | |