SafeNet Authentication Manager
Integration Guide

SAM using RADIUS Protocol with WatchGuard XTMv
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAM</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SAM</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Manager</td>
<td>7</td>
</tr>
<tr>
<td>Synchronizing Users Stores to SafeNet Authentication Manager</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SAM’s Connector for OTP Authentication</td>
<td>7</td>
</tr>
<tr>
<td>Token Assignment in SAM</td>
<td>8</td>
</tr>
<tr>
<td>Adding WatchGuard XTMv as a RADIUS Client in IAS/NPS</td>
<td>8</td>
</tr>
<tr>
<td>SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration</td>
<td>10</td>
</tr>
<tr>
<td>Configuring WatchGuard XTMv</td>
<td>11</td>
</tr>
<tr>
<td>Configuring WatchGuard XTMv for RADIUS Server Authentication</td>
<td>11</td>
</tr>
<tr>
<td>Activating WatchGuard Mobile VPN with SSL</td>
<td>13</td>
</tr>
<tr>
<td>Selecting Authentication Server and Adding Users</td>
<td>14</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>16</td>
</tr>
<tr>
<td>Using the WatchGuard Mobile VPN with SSL Client</td>
<td>16</td>
</tr>
<tr>
<td>Using the OpenVPN Connect Application</td>
<td>17</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>20</td>
</tr>
</tbody>
</table>
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 Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

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 a per-customer, -department, or -app scenario for your virtual infrastructure.

The WatchGuard® XTMv device delivers:

- 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—that boost 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 tokens managed by SafeNet Authentication Manager.
- Configure WatchGuard XTMv to work with SafeNet Authentication Manager in RADIUS mode.

It is assumed that the WatchGuard XTMv environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager, and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager installation modes, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

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 Manager.

Applicability

The information in this document applies to:

- **SafeNet Authentication Manager** - A server version of SAM 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 Manager 8.2 HF 493** - A server version of SAM that is used to deploy the solution on-premises in the organization.
- **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 Manager.

RADIUS-based Authentication using SAM

SafeNet's OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SafeNet Authentication Manager (SAM).

SAM's OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS, providing strong authentication for remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*. 
RADIUS Authentication Flow using SAM

SafeNet Authentication Manager 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 token.
2. WatchGuard XTMv sends a RADIUS request with the user’s credentials to SafeNet Authentication Manager for validation.
3. The SAM 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 SAM.

RADIUS Prerequisites

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

- End users can authenticate 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 the RADIUS client for encryption, decryption, and digital signature purposes.
Configuring SafeNet Authentication Manager

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

- Synchronizing Users Stores to SafeNet Authentication Manager, page 7
- Configuring SAM’s Connector for OTP Authentication, page 7
- Token Assignment in SAM, page 8
- Adding WatchGuard XTMv as a RADIUS Client in IAS/NPS, page 8
- SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration, page 10

Synchronizing Users Stores to SafeNet Authentication Manager

SAM manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Configuring SAM’s Connector for OTP Authentication

SafeNet Authentication Manager is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications, including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected the Simplified OTP-only configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The Simplified OTP-only configuration is as follows:

- **Connectors** - SAM Connector for OTP Authentication is installed
- **SAM Back-end Service** - Activated on this server; scheduled to operate every 24 hours
In addition, the SAM default policy is set as follows:

- OTP support (required for OTP) is selected in the **Token Initialization** settings.

- The **SAM Connector for OTP Authentication** is set, by default, to enable enrollment of OTP tokens without requiring changes in the TPO settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

### Token Assignment in SAM

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

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- MobilePASS
- SafeNet eToken 3400
- SafeNet eToken 3500

Tokens can be assigned to users as follows:

- **SAM Management Center**: Management site used by SAM administrators and help desk for token enrollment and lifecycle management.

- **SAM Self-Service Center**: Self-service site used by end users for managing their tokens.

- **SAM Remote Service**: Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet’s tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

### Adding WatchGuard XTMv as a RADIUS Client in IAS/NPS

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in WatchGuard XTMv.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in WatchGuard XTMv.

WatchGuard XTMv must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize WatchGuard XTMv for authentication.

---

**NOTE:** This document assumes that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

The details below refer to NPS and are very similar to IAS.
To add a RADIUS client:

2. From the NPS web console, in the left pane, expand RADIUS Clients and Servers, right-click RADIUS Clients, and then click New.

![Network Policy Server](image)

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

3. On the New RADIUS Client window, complete the following fields on the Settings tab:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable this RADIUS client</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Friendly name</td>
<td>Enter a RADIUS client name.</td>
</tr>
<tr>
<td>Address (IP or DNS)</td>
<td>Enter the IP address or DNS of WatchGuard XTMv.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>Enter the shared secret for the RADIUS client. The value must be the same when configuring the RADIUS server in WatchGuard XTMv.</td>
</tr>
<tr>
<td>Confirm shared secret</td>
<td>Re-enter the shared secret to confirm it.</td>
</tr>
</tbody>
</table>
4. Click OK.

WatchGuard XTMv is added as a RADIUS client in NPS.

**SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration**

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) as Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

SAM’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS to provide strong authentication for remote access through the IAS or NPS RADIUS server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.
Configuring WatchGuard XTMv

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

Configuring WatchGuard XTMv requires the following:

- Configuring WatchGuard XTMv for RADIUS Server, page 11
- Activating WatchGuard Mobile VPN with SSL, page 13
- Selecting Authentication Server and Adding User, page 14

Configuring WatchGuard XTMv for RADIUS Server Authentication

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

1. Log in to the WatchGuard Web UI: 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**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable RADIUS server</td>
<td>Select this option.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the RADIUS server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number through which the RADIUS server communicates. The default port number is 1812.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>Enter the shared secret key. This is the same key you specified in the section “Adding WatchGuard XTMv as a RADIUS Client in IAS/NPS” on page 8.</td>
</tr>
<tr>
<td>Confirm</td>
<td>Re-enter the shared secret key entered above to confirm it.</td>
</tr>
</tbody>
</table>

(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.

2. In the right pane, select **Activate Mobile VPN with SSL**.

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 Authentication Server and Adding Users

Specify RADIUS 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.

![WatchGuard Web UI](image)

(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.

<table>
<thead>
<tr>
<th>Type</th>
<th>Select User.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the user name.</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>Select RADIUS.</td>
</tr>
</tbody>
</table>

(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 SAM-supported tokens. For this integration, the SafeNet e-Token PASS is configured for authentication with the SAM solution.

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

- Using the WatchGuard Mobile VPN with SSL Client
- Using the OpenVPN Connect Application (for Android devices)

Using the WatchGuard Mobile VPN with SSL 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 (Secure Sockets Layer) 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.

<table>
<thead>
<tr>
<th>Server</th>
<th>Enter or select the IP address of the WatchGuard XTMv device you want to connect to.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Enter your user name. If Mobile VPN with SSL on the WatchGuard 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.</td>
</tr>
<tr>
<td>Password</td>
<td>Use the one-time passcode (OTP) token (for example, SafeNet e-Token PASS) to generate a passcode, and then enter it in this field.</td>
</tr>
</tbody>
</table>

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

On successful authentication, access to the company’s internal network through the SSL VPN is provided.
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.

![Download button screenshot](image1.png)

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

4. Open the OpenVPN Connect application.

![OpenVPN Connect application](image2.png)

(The screen image above is from OpenVPN® software. Trademarks are the property of their respective owners.)
5. On the right-top corner, tap 📈. In the pop-up menu, tap Import, and then specify the **client.ovpn** file you downloaded earlier.

![OpenVPN Connect](image)

*(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.

![Profile Imported](image)

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

7. Use the one-time passcode (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, access to the company’s internal network through the SSL VPN is provided.

(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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>United States 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>