SafeNet Authentication Manager
Integration Guide

SAM using RADIUS Protocol with SonicWALL E-Class
Secure Remote Access
## Contents

Third-Party Software Acknowledgement.............................................................4  
Description........................................................................................................4  
Applicability........................................................................................................4  
Environment.........................................................................................................4  
Audience..............................................................................................................5  
RADIUS-based Authentication using SAM ........................................................5  
RADIUS Authentication Flow using SAM...........................................................5  
RADIUS Prerequisites.........................................................................................6  
Configuring SafeNet Authentication Manager ....................................................7  
  Synchronizing Users Stores to SafeNet Authentication Manager ........................7  
  Configuring SAM’s Connector for OTP Authentication ........................................7  
  Token Assignment in SAM ..............................................................................8  
  Adding SonicWALL E-Class Secure Remote Access as a RADIUS Client in IAS/NPS .......................................................................................................................8  
  SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration .........................10  
Configuring SonicWALL E-Class Secure Remote Access .....................................11  
  Creating a Realm .............................................................................................11  
  Creating a User .................................................................................................15  
  Applying Configuration Changes .....................................................................17  
Running the Solution...........................................................................................18  
  Using a Web Browser .......................................................................................18  
  Using the Connect Tunnel Application .............................................................19  
  Using the SonicWALL Mobile Connect Application ..........................................21  
Support Contacts..................................................................................................25
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as SonicWALL E-Class Secure Remote Access.

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.

SonicWALL E-Class Secure Remote Access (SRA) appliances extend secure remote networking over an SSL VPN to potentially thousands of locations—providing anytime, anywhere access. The encrypted SSL VPN tunnel protects the transmitted data. In addition, as an added layer of protection, granular access controls allow the administrator to delegate access privileges to different individuals or groups so that they can access only specific, defined resources. SonicWALL SRA appliances integrate seamlessly with virtually any firewall.

This document describes how to:

- Configure SonicWALL E-Class Secure Remote Access to work with SafeNet Authentication Manager in RADIUS mode.

It is assumed that the SonicWALL E-Class Secure Remote Access 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.

SonicWALL E-Class Secure Remote Access 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.
- **SonicWALL E-Class Secure Remote Access Virtual Appliance 11.0**
Audience

This document is targeted to system administrators who are familiar with the SonicWALL E-Class Secure Remote Access appliance 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 authenticated 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 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 SonicWALL E-Class Secure Remote Access.

1. A user attempts to log on to SonicWALL E-Class Secure Remote Access using an OTP token.
2. SonicWALL E-Class Secure Remote Access sends a RADIUS request with the user’s credentials to SafeNet Authentication Manager for validation.
3. The SAM authentication reply is sent back to SonicWALL E-Class Secure Remote Access.
4. The user is granted or denied access to SonicWALL E-Class Secure Remote Access based on the OTP value calculation results from SAM and is connected to SonicWALL E-Class Secure Remote Access.

**RADIUS Prerequisites**

To enable SafeNet Authentication Manager to receive RADIUS requests from SonicWALL E-Class Secure Remote Access, ensure the following:

- End users can authenticate from the SonicWALL E-Class Secure Remote Access environment with a static password before configuring SonicWALL E-Class Secure Remote Access to use RADIUS authentication.
- A user with the same *username* as in Active Directory should be in SonicWALL E-Class Secure Remote Access.
- Ports 1812/1813 are open to and from SonicWALL E-Class Secure Remote Access.
- 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 Manager

The deployment of multi-factor authentication using SAM with SonicWALL E-Class Secure Remote Access 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 SonicWALL E-Class Secure Remote Access 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 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 Backend 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 SonicWALL E-Class Secure Remote Access.

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- SafeNet GOLD
- SMS tokens
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)
- 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 SonicWALL E-Class Secure Remote Access 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 SonicWALL E-Class Secure Remote Access.

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 SonicWALL E-Class Secure Remote Access.

SonicWALL E-Class Secure Remote Access must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize SonicWALL E-Class Secure Remote Access for authentication.
NOTE: It is assumed 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.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</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 SonicWALL E-Class Secure Remote Access.</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 SonicWALL E-Class Secure Remote Access.</td>
</tr>
<tr>
<td>Confirm shared secret</td>
<td>Re-enter the shared secret to confirm it.</td>
</tr>
</tbody>
</table>
4. Click **OK**.

SonicWALL E-Class Secure Remote Access 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 IAS or NPS to provide strong, authenticated 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 SonicWALL E-Class Secure Remote Access

For configuring the SonicWALL E-Class Secure Remote Access appliance, complete the following activities:

- Create a realm
- Create users
- Apply configuration changes

To perform these activities, log in to the SonicWALL E-Class Secure Remote Access appliance with administrator credentials.

Creating a Realm

A realm references an authentication server and determines which access agents are provisioned to users and which endpoint control restrictions are imposed.

To create a realm:
1. Open the SonicWALL Management Console.
2. On the Secure Mobile Access Management Console window, in the left pane, under User Access, click Realms.

3. In the upper right corner of the window, click the New realm link.
4. On the **Configure Realm** window, in the **General** tab, complete the following details:
   a. In the **Name** field, enter a name for the realm.
   b. In the **Authentication server** field, click **New**.

   ![Configure Realm Window]

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

   c. Under **Authentication directory**, select **RADIUS**, and then click **Continue**.

   ![Authentication Directory]

   *(The screen image above is from Dell®. Trademarks are the property of their respective owners).*
d. On the **Configure Authentication Server** window, complete the details as specified below:

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary RADIUS Server</strong></td>
<td>Enter the IP address of the RADIUS server (used by SAM), followed by the port number. The format is <code>&lt;IP address&gt;:&lt;port number&gt;</code>. The port number should be either 1812 or 1645.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret value.</td>
</tr>
</tbody>
</table>

![Configure Authentication Server](image)

*(The screen image above is from Dell®. Trademarks are the property of their respective owners).*
e. Click **Save**.

On the **Configure Realm** window, the newly created authentication server is populated in the **Authentication Server** field.

![Configure Realm - SAM RADIUS](image1.png)

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

5. Click **Next > Finish**.

A realm is created and its details are displayed.

![Realms](image2.png)

*(The screen image above is from Dell®. Trademarks are the property of their respective owners).*
Creating a User

A user is an individual who needs access to resources on your network. After creating users on the appliance, you can reference them in an Access Control Rule to permit or deny access to resources.

To create a user:

1. Open the SonicWALL Management Console.
2. On the Secure Mobile Access Management Console window, in the left pane, under Security Administration, click Users & Groups.


(The screen image above is from Dell®. Trademarks are the property of their respective owners.)
4. On the **Add Mapped Account** window, complete the details as specified below, and then click **Save**.

<table>
<thead>
<tr>
<th>Select realm</th>
<th>Select the realm that was created previously.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User type</td>
<td>Select <strong>User</strong>.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the name of the user. The user name must be same as specified in Active Directory.</td>
</tr>
<tr>
<td>Display name</td>
<td>Enter the name of the user for display.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of this mapped account.</td>
</tr>
</tbody>
</table>

![Add Mapped Account](image)  
*(The screen image above is from Dell®. Trademarks are the property of their respective owners).*
Applying Configuration Changes

After you have made the configuration changes, you need to apply them in the system.

To apply configuration changes:

1. Open the SonicWALL Management Console.
2. On the Secure Mobile Access Management Console window, in the upper right corner, click the Pending changes link.

3. On the Apply Pending Changes window, click Apply Changes.

The changes are applied and a message is displayed.

4. Click Close.
Running the Solution

You can use the following methods to securely connect to SonicWALL:

- Using a web browser
- Using the Connect Tunnel application
- Using the SonicWALL Mobile Connect application (for Android and iOS devices)

Using a Web Browser

The WorkPlace portal provides users with dynamically personalized access to web-based (HTTP) resources. It also gives users access from their web browsers to files and folders on Windows file servers, and to TCP/IP resources through Secure Mobile Access agents that can be provisioned from WorkPlace.

1. In a web browser, enter the SonicWALL Secure Mobile Access Workspace URL:
   

2. In the Log in to field, select the configured realm, and then click Next.

   ![Please log in](image1)

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

3. Enter your username and generated OTP password, and then click Log In.

   ![Please log in](image2)

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

**NOTE:** Allow any Java or security warning that is displayed.
If the login credentials entered are correct, the user will be successfully logged in to WorkPlace.

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

NOTE: If you are using SonicWALL for the first time, install Secure Endpoint Manager. When you are logged in to WorkPlace, you will see an option to install Secure Endpoint Manager. For more information, refer to the SonicWALL documentation.

Using the Connect Tunnel Application

The Connect Tunnel application allows you to create a VPN connection between your computer and the corporate network for secure data transmission.

1. Start the Connect Tunnel application.
2. On the Dell VPN Connection window, click Properties.

(The screen image above is from Dell®. Trademarks are the property of their respective owners).
3. On the **Dell VPN Connection Properties** window, on the **Connections** tab, complete the following details, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Host name</strong></th>
<th>Enter the public IP address of the SonicWALL SRA.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login group (Realm)</strong></td>
<td>Click <strong>Change</strong> and then select the realm.</td>
</tr>
</tbody>
</table>

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)
4. On the **Dell VPN Connection** window, enter your username and generated OTP password, and then click **Connect**. If the login credentials are validated, a connection will be established.

![Dell VPN Connection](image)

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

**Using the SonicWALL Mobile Connect Application**

The SonicWALL Mobile Connect application, in combination with SonicWALL Secure Remote Access or next-gen firewall appliances, provides safe and easy access to the data and resources users need to be productive on a range of mobile platforms.

For using this method, the SonicWALL Mobile Connect application should be installed on the Android or iOS device, and a SonicWALL Mobile Connect license should be present.

1. Launch the SonicWALL Mobile Connect application on the device.
2. Tap **Add connection**.

![SonicWALL Mobile Connect](image)

*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*
3. On the **Add Connection** screen, complete the following details, and then tap **Enter**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Enter the public IP address of the SonicWALL appliance.</td>
</tr>
</tbody>
</table>

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

4. Next to **VPN**, tap the **OFF** button to set the connection to **ON**.

(The screen image above is from Dell®. Trademarks are the property of their respective owners).
5. On the **Log in to** screen, tap the realm you have configured to select it.

![Log in to screen](image)

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

6. On the log in screen, enter your username and generate OTP password, and then tap **OK**.

![Login screen](image)

(The screen image above is from Dell®. Trademarks are the property of their respective owners).
7. On the **Attention** message, tap **I trust this application** to select it, and then tap **OK**.

*The screen image above is from Dell®. Trademarks are the property of their respective owners.*

If the login credentials are valid, the user will be successfully logged in.

*The screen image above is from Dell®. 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><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to</td>
</tr>
<tr>
<td></td>
<td>manage incidents, get the latest software upgrades, and access the SafeNet Knowledge</td>
</tr>
<tr>
<td></td>
<td>Base.</td>
</tr>
</tbody>
</table>