SafeNet Authentication Service
Integration Guide

SAS Using RADIUS Protocol with SonicWALL Secure Remote Access
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012742-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>October 2014</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</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>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
Contents

Third-Party Software Acknowledgement.................................................................4
Description..............................................................................................................4
Applicability...........................................................................................................5
Environment ...........................................................................................................5
Audience................................................................................................................5
RADIUS-based Authentication using SAS Cloud..................................................6
RADIUS-based Authentication using SAS-SPE and SAS-PCE.............................7
RADIUS Authentication Flow using SAS..............................................................8
Prerequisites..........................................................................................................8
Configuring SafeNet Authentication Service.........................................................9
  Synchronizing User Stores to SafeNet Authentication Service............................9
  Authenticator Assignment in SAS..........................................................................9
  Adding FreeRADIUS Server as an Authentication Node in SAS.........................10
  Checking the SAS RADIUS IP Address..............................................................12
Configuring the On-Premises FreeRADIUS Server...............................................14
  Add SonicWALL Secure Remote Access as a RADIUS Client in FreeRADIUS........14
  Edit the Free RADIUS Agent Configuration File................................................14
Configuring SonicWALL Secure Remote Access..................................................16
  Creating a Realm..................................................................................................16
  Creating a User.....................................................................................................20
  Applying Configuration Changes.........................................................................22
Running the Solution.............................................................................................23
  Using a Web Browser............................................................................................23
  Using the Connect Tunnel Application..............................................................24
  Using the SonicWALL Mobile Connect Application.............................................26
Support Contacts..................................................................................................30
Third-Party Software Acknowledgement

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

SonicWALL Secure Remote Access appliances extend secure remote networking over an SSL VPN to potentially thousands of locations, to provide 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 Secure Remote Access appliances integrate seamlessly with virtually any firewall.

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)
This document describes how to:

- Configure SonicWALL Secure Remote Access to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the SonicWALL Secure Remote Access environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

SonicWALL 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 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
- **SonicWALL Secure Remote Access 11.0**

**Audience**

This document is targeted to system administrators who are familiar with SonicWALL Secure Remote Access 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.

  ![Diagram of SAS Cloud RADIUS Protocol](image)

- **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.

  ![Diagram of Local RADIUS Protocol](image)

For more information on how to install and configure SAS Agent for IAS/NPS, refer to:

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 Local RADIUS-hosted on-premises.
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:
  

- **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.

SonicWALL Secure Remote Access does not directly support RADIUS server in the cloud. To overcome this, an intermediate RADIUS server is used, which can connect to both SonicWALL Secure Remote Access and SAS Cloud.

The image below describes the dataflow of a multi-factor authentication transaction for SonicWALL Secure Remote Access.

1. A user attempts to log on to SonicWALL Secure Remote Access using an OTP authenticator.
2. SonicWALL Secure Remote Access sends a RADIUS request with the user’s credentials to the on-premises RADIUS server.
3. The on-premises RADIUS server forwards the credentials to SafeNet Authentication Service for validation.
4. The SAS Authentication reply is sent back to SonicWALL Secure Remote Access via the on-premises RADIUS server.
5. The user is granted or denied access to SonicWALL Secure Remote Access based on the OTP value calculation results from SAS.

Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from SonicWALL Secure Remote Access, ensure the following:

- End users can authenticate through the SonicWALL Secure Remote Access environment with a static password before configuring SonicWALL Secure Remote Access to use RADIUS authentication.
- Ports 1812/1813 are open to and from SonicWALL Secure Remote Access.
- An on-premises FreeRADIUS server that has connectivity to both SonicWALL Secure Remote Access and SAS Cloud. The FreeRADIUS Agent and Updater are already installed on the RADIUS server.
- 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 Service

The deployment of multi-factor authentication using SAS with SonicWALL Secure Remote Access using the RADIUS protocol requires the following:

- Synchronizing user stores to SAS
- Authenticator assignment in SAS
- Adding a FreeRADIUS server 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.


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 SonicWALL Secure Remote Access.

The following authenticators are supported:

- eToken PASS
- KT-4 token
- SMS tokens
- MP-1 software token
- 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.


### Adding FreeRADIUS Server 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 the FreeRADIUS server. You will need the public IP address of FreeRADIUS server and the shared secret to be used by both SAS and the FreeRADIUS server.

**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 SonicWALL Secure Remote Access, check the IP address of the SAS RADIUS server. The IP address will then be added to SonicWALL Secure Remote Access 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 the On-Premises FreeRADIUS Server

Configure the on-premises FreeRADIUS server so that it can communicate with both SonicWALL Secure Remote Access and SAS cloud.

Add SonicWALL Secure Remote Access as a RADIUS Client in FreeRADIUS

1. Go to the following directory: /opt/freeradius/freeradius-server-2.2.0/etc/raddb/
2. Open the clients.conf file.
3. Add the following at the end of the clients.conf file:
   
   ```
   client "Client Name"
   {
   ipaddr = 10.10.11.3
   secret = '1111'
   }
   ```

   where:
   
   Client Name is the user-defined name to identify the client.
   
ipaddr is the IP address of SonicWALL SRA.
   
secret is the shared secret between SonicWALL SRA and the RADIUS server.
4. Save the clients.conf file.

Edit the Free RADIUS Agent Configuration File

1. Go to the following directory: /usr/local/cryptocard/freeradius/
2. Open the CryptocardFreeRadiusConfig file.
3. Make the following changes to the file:
   
a. Under Section 7, change the default value from 0 to 1.
   The radius authentication request will pass with the original IP of the client. It enables the FreeRADIUS server to accept requests from clients on different SAS accounts.
   The value 0 indicates that the IP address passing is OFF.
   The value 1 indicates that the IP address passing is ON.
   
b. Under Section 16, enter the Primary SAS Agent DNS. To get the Primary SAS Agent DNS, refer to “Checking the SAS RADIUS IP Address” on page 12.
   
c. Under Section 17, enter 443.
   
d. Under Section 18, change the value to 30000.
   
e. Under Section 20, change the value to 1, as SAS cloud validates on HTTPS.
The sample content of the **CryptocardFreeRadiusConfig** file is shown below.

```plaintext
### Primary Token Validator START
#
### Section 16: Primary TokenValidator IP Address
agent1.safenet-inc.com
###
#
### Section 17: Primary TokenValidator Port
443
#
###
#
### Section 18: Primary TokenValidator Timeout in milli seconds
30000
#
###
#
### Section 19: Path to Primary TokenValidator
/TokenValidator/TokenValidator.asmx
#
#
### Section 20: Primary TokenValidator connection is HTTPS or HTTP
# 1 - HTTPS
# 0 - HTTP
1
```

4. Save the **CryptocardFreeRadiusConfig** file and exit the editor.

5. Restart the FreeRADIUS server.
Configuring SonicWALL Secure Remote Access

To configure SonicWALL Secure Remote Access for RADIUS authentication requires:

- Creating a Realm, page 16
- Creating a User, page 20
- Applying Configuration Changes, page 22

To perform these configuration settings, log in to the SonicWALL 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](image)

   *(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](image)

   *(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, and then click **Save**.

<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 FreeRADIUS server (on-premises RADIUS server) followed by the port number. The format is <code>&lt;IP address&gt;</code>:&lt;port number&gt;. The port number should be either 1812 or 1645.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret value. The shared secret must be same as on the FreeRADIUS server.</td>
</tr>
</tbody>
</table>

(The screen image above is from Dell®. Trademarks are the property of their respective owners).
On the **Configure Realm** window, the newly created authentication server is populated in the **Authentication Server** field.

![Configure Realm Window](image)

*(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.

![Realm Creation](image)

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

(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.

![SonicWALL Management Console](image)

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

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

![Apply Pending Changes](image)

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

The changes are applied and a message is displayed.

![Apply Pending Changes](image)

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

4. Click Close.
Running the Solution

You can use the following methods to securely connect to SonicWALL Secure Remote Access:

- Using a Web Browser, page 23
- Using the Connect Tunnel Application, page 24
- Using the SonicWALL Mobile Connect Application (for Android and iOS devices), page 26

Using a Web Browser

The WorkPlace portal provides users with dynamically personalized access to the web-based (HTTP) resources. It also gives users access to files and folders from their web browsers 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, open the SonicWALL Secure Mobile Access Workspace:
   ```markdown
   https://<SonicWALL SRA Appliance Public IP>
   ```

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

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

3. In the Username field, enter your username.

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

4. Use the OTP token (for example, SafeNet e-Token PASS) to generate a passcode. In the Password field, enter the generated passcode and then click Log In.

   **NOTE:** Allow any Java or security warning that is displayed.

If authentication is successful, the user will be successfully logged in to WorkPlace.
NOTE: If you are using SonicWALL for the first time with the web browser, 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.

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 Secure Remote Access appliance.</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 authentication is successful, 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-generation 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 mobile 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><strong>Name</strong></th>
<th>Enter a name for the connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server</strong></td>
<td>Enter the public IP address of the SonicWALL Secure Remote Access 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 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; for example, SAS Cloud RADIUS.

6. On the log in window, enter your username and generated OTP password, and then tap **OK**.
7. On the **Attention** message, tap the **I trust this application** option to select it, and then tap **OK**.

![Attention message](image1.png)

*(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.

![Connected](image2.png)

*(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</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>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>