SafeNet Authentication Manager

Integration Guide

Using SAM as an Identity Provider for SonicWALL Secure Remote Access
# Contents

Third-Party Software Acknowledgement........................................................................................................ 4
Description......................................................................................................................................................... 4
Applicability....................................................................................................................................................... 4
Environment ..................................................................................................................................................... 4
Audience.............................................................................................................................................................. 5
SAML Authentication using SAM ...................................................................................................................... 5
Authentication Flow using SAM .......................................................................................................................... 5
SAML Prerequisites ........................................................................................................................................... 5
Configuring SafeNet Authentication Manager ................................................................................................. 6
    Synchronizing User Stores to SafeNet Authentication Manager ................................................................. 6
    Assigning a Token in SAM ............................................................................................................................ 6
    Configuring SAM as an Identity Provider .................................................................................................... 7
    Exporting the SAM Certificate .................................................................................................................... 8
    Configuring SAM for SAML-based User Federation ............................................................................... 10
Configuring SonicWALL Secure Remote Access ........................................................................................... 13
    Importing a SAM Certificate ....................................................................................................................... 13
    Creating a Realm ....................................................................................................................................... 16
    Creating a User ....................................................................................................................................... 20
    Applying the Configuration Changes ...................................................................................................... 22
Running the Solution ...................................................................................................................................... 23
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 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 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 SAML authentication in SonicWALL Secure Remote Access using SafeNet Authentication Manager as an identity provider.

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 Manager.

SonicWALL Secure Remote Access can be configured to support multi-factor authentication in several modes. The SAML authentication 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 468**
- **SonicWALL Secure Remote Access 10.7.1 (HF clt-hotfix-10.7.1-449, pform-hotfix-10.7.1-474)**
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 Manager.

SAML Authentication using SAM

SAM provides a SAML authentication option that is already implemented in the SAM environment and can be used without any installation.

Authentication Flow using SAM

SafeNet Authentication Manager communicates with a large number of service providers and cloud-based services solutions using the SAML protocol.

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. The user is redirected to SafeNet Authentication Manager (SAM). SAM collects and evaluates the user’s credentials.
2. SAM returns a response to SonicWALL Secure Remote Access, accepting or rejecting the user’s authentication request.

SAML Prerequisites

To enable SafeNet Authentication Manager to receive SAML authentication requests from SonicWALL Secure Remote Access, ensure that end users can authenticate through the SonicWALL Secure Remote Access environment with a static password.
Configuring SafeNet Authentication Manager

Using SAM as an identity provider for SonicWALL Secure Remote Access requires the following:

- Synchronizing User Stores to SafeNet Authentication Manager, page 6
- Assigning a Token in SAM, page 6
- Configuring SAM as an Identity Provider, page 7
- Exporting the SAM Certificate, page 8
- Configuring SAM for SAML-based User Federation, page 10

Synchronizing User Stores to SafeNet Authentication Manager

SAM manages and maintains tokens information in its data store, including the tokens status 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

Assigning a Token in SAM

SAM supports a number of OTP authenticators that can be used as a second authentication factor for users authenticating through SonicWALL Secure Remote Access.

The following tokens are supported:

- eToken PASS
- SafeNet GOLD
- SafeNet eToken 3400
- SafeNet eToken 3500
- eToken NG-OTP
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
• SafeNet Mobile Authentication (iOS)

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*.

**Configuring SAM as an Identity Provider**

To use SonicWALL Secure Remote Access as a service provider and SAM as an identity provider, SAM must be set as an identity provider.

1. From the Windows **Start** menu, click **All Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager**.

2. On the **SafeNet Authentication Manager – Configuration Manager** window, from the menu bar, click **Action > Cloud Configuration**.
3. On the Cloud Settings window, click the Info for Service Provider tab. In the Domain URL field, enter the web address of the SAM portal server.

The system fills in the rest of the fields according to the Domain URL entered.

Exporting the SAM Certificate

The SAM certificate is shared between SAM and SonicWALL Secure Remote Access. The certificate will be used to sign the authentication requests.
1. From the Windows Start menu, click All Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager.

![SafeNet Authentication Manager - Configuration Manager](image)

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

2. On the SafeNet Authentication Manager – Configuration Manager window, click Action > Cloud Configuration.

![SafeNet Authentication Manager Server 6.2](image)

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

3. On the Cloud Settings window, click the Info for Service Provider tab. Click Export Certificate and save the certificate file. Later, this certificate file needs to be imported into SonicWALL Secure Remote Access.
Configuring SAM for SAML-based User Federation

SafeNet Authentication Manager’s Token Policy Object (TPO) policies include Application Authentication Settings for SAML service providers. These settings are used by SAM’s portal to communicate with service providers.

For general portal configuration, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

To edit the Token Policy Object for SAM’s portal configuration:

1. Open the Token Policy Object Editor for the appropriate group. Refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide for more information.

2. On the Token Policy Object Editor window, expand Protected Application Settings, and then click User Authentication.

4. On the **Application Authentication Settings Properties** window, perform the following steps:
   a. Select **Define this policy setting**.
   b. Select **Enabled**.
   c. Click **Definitions**.

   ![Application Authentication Settings Properties](image1)

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

5. On the **Application Authentication Settings** window, right-click **Application Authentication Settings**, and then click **Create a new profile**.

   ![Application Authentication Settings](image2)

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

6. Right-click the new profile and rename it to a friendly name (for example, **SonicWall**).
7. Click the new profile (for example, **SonicWall**).
8. Double-click on each of the following policies, and then enter the appropriate information:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application issuer</td>
<td>Enter the SonicWall EntityID, which will be used while configuring SonicWall.</td>
</tr>
<tr>
<td>SAM issuer</td>
<td>Enter a unique SAM ID to be identified in SAML authentication.</td>
</tr>
<tr>
<td>Application’s login URL</td>
<td>Enter the SonicWall login URL. For example: <code>https://&lt;Public IP of SonicWALL SRA Appliance&gt;/saml2ssoconsumer</code></td>
</tr>
<tr>
<td>Audience URI</td>
<td>Enter the same SonicWall EntityID that you entered in the Application issuer field.</td>
</tr>
<tr>
<td>User mapping</td>
<td>Select the field name in your user repository that identifies your SonicWALL Secure Remote Access login name.</td>
</tr>
</tbody>
</table>


The following is an example of the completed fields in the Application Authentication Settings window:

10. Click OK until all of the Token Policy Object Editor windows are closed.
Configuring SonicWALL Secure Remote Access

To add SafeNet Authentication Manager as an identity provider in SonicWALL Secure Remote Access, perform the following procedures:

- Importing a SAM Certificate, page 13
- Creating a Realm, page 16
- Creating a User, page 20
- Applying the Configuration Changes, page 22

Importing a SAM Certificate

The SAM certificate is imported on the SonicWALL SRA appliance so that a trust can be established between SAM and the SonicWALL appliance. Before performing this activity, a SAM certificate should be downloaded. To download a SAM certificate, refer to “Exporting the SAM Certificate” on page 8.

1. Open the SonicWALL Management Console and log in as an administrator.
2. On the Aventail Management Console window, under System Configuration, click SSL Settings.

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)
3. On the **SSL Settings** tab, under **CA certificates**, click the first **Edit** link (designated by the red box in the image below).

4. Under **Filters**, click **New**.

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)
5. On the **Import CA Certificate** window, select the **Certificate file** option.

![Import CA Certificate Window]

5. On the **Import CA Certificate** window, select the **Certificate file** option.

   - **Certificate file:**
     - Choose File | No file chosen
   
   - **Certificate text:**

5. **Usage**

   - Specify the connection types the certificate is used to secure.
   - **Authentication server connections (LDAPs)**
   - **Web server connections (HTTPS)**
   - **Device profiling (End Point Control)**
   - **OCSP response verification**

   ![Import button and Cancel button]

5. **Import**

   - Click **Import**.

6. **Choose File**, and then select the downloaded SAM certificate.

7. Click **Import**.

   - The SAM certificate is imported successfully.

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

A realm refers to an authentication server. It determines which access agents are provisioned to users, and the end point control restrictions that are imposed.

1. Open the SonicWALL Management Console.
2. On the Aventail Management Console window, under User Access, click Realms.

![SonicWALL Management Console](image)

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

3. On the Realms tab, click the New realm link (designated by the red box in the image below).

![Realms tab](image)

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)
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**.
   c. Under **Authentication directory**, select **CA SiteMinder**, and then click **Continue**.

   CA SiteMinder is the name given for SAML authentication by SonicWall.

   *(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 authentication server (for example, <strong>SAM SAML</strong>).</th>
</tr>
</thead>
</table>
| **Appliance ID** | Enter a unique **Entity ID** of the SonicWALL Secure Remote Access appliance.  
Note that this **Entity ID** will be same as configured in SAM. |
| **Server ID** | Enter the SAM **Entity ID**. It should match the entry in the **SAM Issuer** field, in “Configuring SAM for SAML-based User Federation” on page 10. |
| **Authentication service URL** | Enter the SAM **Sign-in page URL**.  
To obtain the URL, refer to step 3 in “Configuring SAM as an Identity Provider” on page 7. |
| **Logout service URL** | Enter the SAM **Sign-out page URL**.  
To obtain the URL, refer to step 3 in “Configuring SAM as an Identity Provider” on page 7. |
| **Trust the following certificate** | Select the SAM certificate that was imported in “Importing a SAM Certificate” on page 13. |

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

![Configure Realm](image)

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

A realm is created and its details are displayed.

![Realm Details](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 the corporate 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.

1. Open the **SonicWALL Management Console**.

2. On the **Aventail Management Console** window, under **Security Administration**, click **Users & Groups**.

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

3. On the **Mapped Accounts** tab, click **New > Manual entry**.

   (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 you created in “Creating a Realm” on page 16.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User type</td>
<td>Select User.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the name of the user. The user name must be the same as specified in SAM.</td>
</tr>
<tr>
<td>Display name</td>
<td>Enter the name of the user to display.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the 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 the Configuration Changes

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

1. Open the **SonicWALL Management Console**.
2. On the **Aventail 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 the following message is displayed:

5. Click **Close**.
Running the Solution

The SonicWALL Aventail WorkPlace portal is used to verify this integration solution. The Aventail WorkPlace portal provides dynamically personalized access to the 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 Aventail WorkPlace.

For this integration, the SafeNet NG-OTP token is configured for authentication with the SAM solution.

---

**NOTE:** While running the solution, if any Java or Security warning is shown, click Allow.

1. In a web browser, open the SonicWALL Aventail Workspace URL (for example, https://<Appliance public IP>).
2. In the Log in to field, select an appropriate realm, and then click Next.
   
   The user will be redirected to the SAM login page.

   ![SonicWALL Aventail WorkPlace login screen](image)

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

3. In the Username field, enter your user name, and then click OK.

   ![SafeNet User Identification screen](image)
4. Generate an OTP using the SafeNet token. On the **OTP Authentication** window, enter the OTP in the **OTP Authentication Code** field, and then click **OK**.

![OTP Authentication](image)

On successful authentication, you will be redirected to the **SonicWall Aventail WorkPlace** home page.

![SonicWall Aventail WorkPlace](image)

*NOTE:* If you are using SonicWALL for the first time, you will need to install the **Secure Endpoint Manager**. When you log in to Aventail WorkPlace, you will see an option to install the **Secure Endpoint Manager**. For more information, refer to the SonicWALL documentation.
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 manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>