SafeNet Authentication Manager Integration Guide

SAM using RADIUS Protocol with Amazon WorkSpaces
SafeNet Authentication Manager: Integration Guide
SAM using RADIUS Protocol with Amazon WorkSpaces

Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012844-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>November 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>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<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>4</td>
</tr>
<tr>
<td>Setting Up the Amazon Virtual Private Cloud</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAM</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SAM</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Manager</td>
<td>7</td>
</tr>
<tr>
<td>Synchronizing User Stores to SafeNet Authentication Manager</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SAM’s Connector for OTP Authentication</td>
<td>8</td>
</tr>
<tr>
<td>Token Assignment in SAM</td>
<td>8</td>
</tr>
<tr>
<td>Adding Amazon WorkSpaces as a RADIUS Client in IAS/NPS</td>
<td>9</td>
</tr>
<tr>
<td>SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration</td>
<td>11</td>
</tr>
<tr>
<td>Configuring Amazon WorkSpaces</td>
<td>11</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>14</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>15</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 Amazon WorkSpaces.

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.

Amazon WorkSpaces is a fully managed desktop computing service in the cloud. Amazon WorkSpaces allows customers to easily provision cloud-based desktops that allow end users to access documents, applications, and resources they need with the device of their choice, including laptops, iPad, Kindle Fire, or Android tablets.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Amazon WorkSpaces using SafeNet OTP tokens managed by SafeNet Authentication Manager.
- Configure Amazon WorkSpaces to work with SafeNet Authentication Manager in RADIUS mode.

It is assumed that the Amazon WorkSpaces 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.

Amazon WorkSpaces 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.
- **Amazon WorkSpaces**
Setting Up the Amazon Virtual Private Cloud

For using multi-factor authentication with Amazon WorkSpaces, the corporate network should be able to communicate with the Amazon Virtual Private Cloud (VPC). There are several methods through which this can be achieved. Some of the methods are:

- Deploying a VPN solution on the corporate network. For the list of supported VPN devices and other information, see Amazon documentation.
- Using the Amazon Direct Connect Service.
- Deploying Active Directory on a machine with a public IP (not recommended as it is not a secure connection).

In the above scenario, the pfSense firewall is deployed on the corporate network. The pfSense firewall is configured to communicate with the Amazon Virtual Private Network (VPN) through an IPsec tunnel.

On the Amazon Virtual Private Cloud (VPC), the Amazon VPN gateway is configured to communicate with the corporate network through the pfSense firewall.

All communications between the corporate network and Amazon VPC occur through the secured IPsec tunnels.

NOTE: The above setup can be configured using the steps provided at the following link:
Audience

This document is targeted to system administrators who are familiar with Amazon WorkSpaces 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 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 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 Amazon WorkSpaces.

1. A user attempts to log on to Amazon WorkSpaces using an OTP authenticator.
2. User enters the AD username and password, and then logs in.
3. User enters the OTP and logs in.
4. Amazon WorkSpaces sends a RADIUS request with the user’s credentials to SafeNet Authentication Manager for validation.
5. The SAM authentication reply is sent back to Amazon WorkSpaces.
6. The user is granted or denied access to Amazon WorkSpaces based on the OTP value calculation results from SAM and is connected to Amazon WorkSpaces.
RADIUS Prerequisites

To enable SafeNet Authentication Manager to receive RADIUS requests from Amazon WorkSpaces, ensure the following:

- End users can authenticate from the Amazon WorkSpaces environment with a static password before configuring Amazon WorkSpaces to use RADIUS authentication.
- Ports 1812/1813 are open to and from Amazon WorkSpaces.
- 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.

NOTE: Currently, multi-factor authentication is only supported with Amazon Connect Directory. It does not work with Amazon Cloud Directory.

Configuring SafeNet Authentication Manager

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

- Synchronizing User Stores to SafeNet Authentication Manager—page 7
- Configuring SAM’s Connector for OTP Authentication—page 8
- Token Assignment in SAM—page 8
- Adding Amazon WorkSpaces as a RADIUS Client in IAS/NPS—page 9
- SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration—page 11

Synchronizing User 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 Amazon WorkSpaces.

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 Amazon WorkSpaces as a RADIUS Client in IAS/NPS

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

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 Amazon WorkSpaces.

Amazon WorkSpaces must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Amazon WorkSpaces 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 the Amazon WorkSpaces subnet.</td>
</tr>
</tbody>
</table>
**Shared secret**
Enter the shared secret for the RADIUS client. The value must be the same when configuring the RADIUS server in Amazon WorkSpaces.

**Confirm shared secret**
Re-enter the shared secret to confirm it.

4. Click OK.
Amazon WorkSpaces is added as a RADIUS client in NPS.

---

**NOTE:** A connected directory has two IP addresses (one for each subnet). Both the subnet IP addresses should be added as separate clients with the same shared secret. The IP addresses can be found in the directory details on the Amazon WorkSpaces console. Repeat the above steps for second subnet.
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 Amazon WorkSpaces

Enable multi-factor authentication for the Amazon WorkSpaces by configuring the RADIUS server. In addition, add the details of the NPS/IAS RADIUS server in Amazon Directory.

1. Log in to the Amazon WorkSpaces Management Console.
2. In the left pane, click Directories.

![Directories](image1)

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

3. To enable MFA for the users under a directory, select the check box for that directory.

![Directories](image2)

(The screen image above is from Amazon®. Trademarks are the property of their respective owners.)
4. Click **Actions > Update Details**.

![Image of Update Details screen](image)

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

5. In the **Update Directory Details** window, click **Multi-Factor Authentication**.

![Image of Multi-Factor Authentication](image)

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

6. Select **Enable Multi-Factor Authentication**, and then complete the following fields. When finished, click **Update and Exit**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS server IP address(es)</td>
<td>Enter the IP Address of RADIUS server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number of RADIUS server.</td>
</tr>
<tr>
<td>Shared secret code</td>
<td>Enter the shared secret key. It should be same as entered in the NPS/IAS RADIUS server.</td>
</tr>
<tr>
<td>Confirm shared secret code</td>
<td>Re-enter the shared secret key.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select an appropriate protocol, such as PAP.</td>
</tr>
<tr>
<td>Server timeout (in seconds)</td>
<td>Enter the timeout period of the server.</td>
</tr>
<tr>
<td>Max retries</td>
<td>Enter the maximum number of retries.</td>
</tr>
</tbody>
</table>
7. Amazon takes few minutes to check the connectivity with the RADIUS server. To check the RADIUS status of a directory, expand the Directory ID. The details are shown below the row. Verify that **Completed** is displayed for the **RADIUS Status**.

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

The Amazon WorkSpaces Client application is used to connect to Amazon Workspaces. The client should be installed on the machine from where the user wishes to access Amazon WorkSpaces.

1. Start the **Amazon Workspaces Client** application.

2. In the login window, enter your username and Active Directory password, and then click **Sign In**.

3. Enter the OTP in the **Passcode** field, and then click **Sign In**.

(The screen image above is from Amazon®. Trademarks are the property of their respective owners.)
On successful authentication, the user will be logged in to Amazon WorkSpaces.

(The screen image above is from Amazon®. 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 Base.</td>
</tr>
</tbody>
</table>