SafeNet Authentication Manager
Integration Guide

Using RADIUS Protocol for VMware Horizon 6
SafeNet Authentication Manager: Integration Guide
Using RADIUS Protocol for VMware Horizon 6

Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012966-001, Rev. B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>September 2015</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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>SafeNet Authentication Manager</td>
<td>4</td>
</tr>
<tr>
<td>VMware Horizon™ 6 (with View)</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>5</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAM</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SAM</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Manager</td>
<td>7</td>
</tr>
<tr>
<td>Synchronizing Users Stores with SAM</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SAM’s Connector for OTP Authentication</td>
<td>8</td>
</tr>
<tr>
<td>Assigning a Token in SAM</td>
<td>8</td>
</tr>
<tr>
<td>Adding VMware Horizon 6 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 VMware Horizon 6</td>
<td>11</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>16</td>
</tr>
<tr>
<td>Authenticating Using a MobilePASS Messaging Token</td>
<td>16</td>
</tr>
<tr>
<td>Authenticating Using a Standard OTP Token</td>
<td>18</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>20</td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as VMware Horizon 6.

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

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.

VMware Horizon™ 6 (with View)

VMware Horizon™ 6 (with View) is a virtual desktop infrastructure (VDI) platform that delivers virtualized and remote desktops and applications through a single platform, giving end users access to all of their Windows and online resources through one unified workspace.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in VMware Horizon 6 using SafeNet one-time password (OTP) tokens managed by SafeNet Authentication Manager.
- Configure VMware Horizon 6 to work with SafeNet Authentication Manager in RADIUS mode.

It is assumed that the VMware Horizon 6 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 additional information on SafeNet Authentication Manager installation modes, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

VMware Horizon 6 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**—Version 8.2 (HF 493)
- VMware Horizon 6

Audience

This document is targeted to system administrators who are familiar with VMware Horizon 6, 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 either Microsoft’s IAS or NPS, and provides 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 VMware Horizon 6.

1. A user attempts to log on to VMware Horizon 6 using an OTP token.
2. VMware Horizon 6 sends a RADIUS request with the user’s credentials to SAM for validation.
3. The SAM authentication reply is sent back to VMware Horizon 6.
4. The user is granted or denied access to VMware Horizon 6 based on the OTP value calculation results from SAM.

RADIUS Prerequisites

To enable SafeNet Authentication Manager to receive RADIUS requests from VMware Horizon 6, ensure the following:

- End users can authenticate from the VMware Horizon 6 environment with a static password before configuring VMware Horizon 6 to use RADIUS authentication.
- Ports 1812/1813 are open to and from VMware Horizon 6.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and the RADIUS client for encryption, decryption, and digital signature purposes.
Configuring SafeNet Authentication Manager

The deployment of multi-factor authentication using SAM with VMware Horizon 6 using the RADIUS protocol requires:

- Synchronizing Users Stores with SAM, page 7
- Configuring SAM’s Connector for OTP Authentication, page 8
- Assigning a Token in SAM, page 8
- Adding VMware Horizon 6 as a RADIUS Client in IAS/NPS, page 9
- SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration, page 11

Synchronizing Users Stores with SAM

SAM manages and maintains OTP token information in its data store, including the token’s status and user assignment, and the OTP algorithm used to generate the OTP. 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 (Token Policy Object) 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.

Assigning a Token in SAM

SAM supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through VMware Horizon 6.

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- MobilePASS
- MobilePASS Messaging

Tokens can be assigned to users through:

- **SAM Management Center**—Management site used by SAM administrators and help desk personnel 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 VMware Horizon 6 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 VMware Horizon 6.

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 VMware Horizon 6.

VMware Horizon 6 must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize VMware Horizon 6 for authentication.

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

The details below refer to NPS, and are very similar to IAS.

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

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
3. On the **New RADIUS Client** window, complete the following fields on the **Settings** tab.

<table>
<thead>
<tr>
<th><strong>Enable this RADIUS client</strong></th>
<th>Select this option.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Friendly name</strong></td>
<td>Enter a name for the RADIUS client.</td>
</tr>
<tr>
<td><strong>Address (IP or DNS)</strong></td>
<td>Enter the VMware Horizon 6 IP address or DNS.</td>
</tr>
<tr>
<td><strong>Manual/Generate</strong></td>
<td>Select <strong>Manual</strong>.</td>
</tr>
<tr>
<td><strong>Shared secret</strong></td>
<td>Enter the shared secret for the RADIUS client. This entry must match the shared secret that was used when the RADIUS server was configured in VMware Horizon 6.</td>
</tr>
<tr>
<td><strong>Confirm shared secret</strong></td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>

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

4. Click **OK**. VMware Horizon 6 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 either Microsoft’s 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 VMware Horizon 6

Configure the VMware Horizon 6 environment through the VMware Horizon View Server to work with RADIUS protocol.

1. Log in to the VMware Horizon View Server using the URL http://<ViewServer>/admin.

(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners.)
2. Under Inventory, click View Configuration > Servers.

![Screen capture of VMware Horizon View Administrator showing inventory and View Configuration](image1)

(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners.)

3. In the Servers window, click the Connection Servers tab.

![Screen capture of VMware Horizon View Administrator showing connection servers](image2)

(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners.)

4. Click the Connection Server, and then click Edit.

5. On the Edit Connection Server Settings window, click the Authentication tab.
6. Under **Advanced Authentication**, select **RADIUS** from the **2-factor authentication** menu.

![Screenshot of RADIUS configuration](image)

*(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners.)*

7. Under **Advanced Authentication**, select **Create New Authenticator** from the **Authenticator** menu.

![Screenshot of creating new authenticator](image)

*(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners.)*
8. On the Add RADIUS Authenticator window, under Primary Authentication Server, complete the following, and then click Next.

<table>
<thead>
<tr>
<th><strong>Label</strong></th>
<th>Enter an authenticator name (for example, SAM).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>(Optional ) Add a description for the authenticator.</td>
</tr>
<tr>
<td><strong>Hostname/Address</strong></td>
<td>Enter the IAS/NPS server name or IP address to use to reach the RADIUS server.</td>
</tr>
<tr>
<td><strong>Authentication port</strong></td>
<td>Enter the RADIUS server’s IAS/NPS port (for example, 1812).</td>
</tr>
<tr>
<td><strong>Authentication type</strong></td>
<td>Select PAP.</td>
</tr>
<tr>
<td><strong>Shared secret</strong></td>
<td>Enter the shared secret that will be used between the RADIUS client and the RADIUS server.</td>
</tr>
</tbody>
</table>

(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners.)

9. Click Finish.
10. Click OK. The new RADIUS authenticator is displayed in the Authenticator menu.

![Edit Connection Server Settings](image)

(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners.)

11. Click OK.
Running the Solution

Authenticating Using a MobilePASS Messaging Token

1. Open a VMware Horizon View Client.

2. Insert the token and connect to the VMware Horizon 6 environment.

3. Enter your token passcode in the **Passcode** field, and then click **Login**.
4. Enter the SMS response in the **Next Code** field, and then click **Login**.

![Login screen](image1)

*(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners.)*

5. On successful authentication, enter your password in the **Password** field, and then click **Login**.

![Login screen](image2)

*(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners.)*
6. If the credentials are successfully authenticated, the client machine is connected to VMware Horizon 6, and you can access a VM in your assigned virtual machine pool.

(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners.)

Authenticating Using a Standard OTP Token

1. Open a VMware Horizon View Client.

(The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners.)
2. Generate an OTP on your token, enter it in the **Passcode** field, and then click **Login**.

![Login screen](image1.png)

*The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners.*

3. On successful authentication, enter your password in the **Password** field, and then click **Login**.

![Login screen](image2.png)

*The screen image above is from VMware® Horizon View™. Trademarks are the property of their respective owners.*

4. If the credentials are successfully authenticated, the client machine is connected to VMware Horizon 6, and you can access a VM in your assigned virtual machine pool.
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</td>
</tr>
<tr>
<td></td>
<td>Support Customer Portal account can</td>
</tr>
<tr>
<td></td>
<td>log in to manage incidents, get the</td>
</tr>
<tr>
<td></td>
<td>latest software upgrades, and access</td>
</tr>
<tr>
<td></td>
<td>the SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>