SafeNet Authentication Service
Integration Guide
Using RADIUS Protocol for VMware Horizon 6
## Contents

- Third-Party Software Acknowledgement ......................................................... 4
- Description ........................................................................................................... 4
  - SafeNet Authentication Service ........................................................................ 4
  - VMware Horizon™ 6 (with View) ...................................................................... 4
- Applicability ......................................................................................................... 4
- Environment ......................................................................................................... 5
- Audience ............................................................................................................... 5
- RADIUS-based Authentication using SAS Cloud .................................................. 5
- RADIUS-based Authentication using SAS-SPE and SAS-PCE ............................... 6
- RADIUS Authentication Flow using SAS ............................................................... 6
- RADIUS Prerequisites .......................................................................................... 7
- Configuring SafeNet Authentication Service ......................................................... 7
  - Synchronizing User Stores with SAS ............................................................... 7
  - Assigning an Authenticator in SAS ................................................................. 8
  - Adding VMware Horizon 6 as an Authentication Node in SAS ........................... 8
    - Checking the SAS RADIUS Server’s IP Address ............................................ 10
- Configuring VMware Horizon 6 ............................................................................. 11
- Running the Solution ............................................................................................ 17
  - Authenticating Using an SMS Token ............................................................... 17
  - Authenticating Using a Standard OTP Token ................................................... 19
- Support Contacts .................................................................................................. 21
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 Service

SafeNet Authentication Service (SAS) 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.

VMware Horizon™ 6 (with View)

VMware Horizon™ 6 (with View) is 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) authenticators managed by SafeNet Authentication Service.
- Configure VMware Horizon 6 to work with SafeNet Authentication Service 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 Service.

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 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 – Private Cloud Edition (SAS-PCE)**
- **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 Service.

RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS**—A RADIUS service is already implemented in the SAS cloud environment, and can be used without any installation or configuration requirements.

- **Local RADIUS hosted on-premises**—A RADIUS agent is implemented in the customer’s existing 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.

This document demonstrates the solution using the SAS cloud-hosted RADIUS service.

For more information on how to install and configure the SafeNet Authentication Service Agent for IAS/NPS, refer to: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

For more information on how to install and configure FreeRADIUS, refer to the *SafeNet Authentication Service FreeRADIUS Agent Configuration Guide.*
RADIUS-based Authentication using SAS-SPE and SAS-PCE

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: 

- **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.

The image below describes the data flow of a multi-factor authentication transaction for VMware Horizon 6.

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

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

- End users can authenticate through the VMware Horizon 6 environment with a static password, before configuring the 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 between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.

Configuring SafeNet Authentication Service

Deploying multi-factor authentication using SAS with VMware Horizon 6 using RADIUS protocol requires the following:

- Synchronizing User Stores with SAS, page 7
- Assigning an Authenticator in SAS, page Error! Bookmark not defined.
- Adding VMware Horizon 6 as an Authentication Node in SAS, page 8
- Checking the SAS RADIUS Server’s IP Address, page 10

Synchronizing User Stores with SAS

Before SAS can authenticate any user in your organization, you must create a user store in SAS that reflects the users who 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 additional details on importing users to SafeNet Authentication Service, refer to “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.
Assigning an Authenticator in SAS

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

The following authenticators are supported:

- eToken PASS
- SMS Token
- MP-1 Software Token
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users, one at a time.
- **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 VMware Horizon 6 as an Authentication Node in SAS

Add a RADIUS entry in the SAS **Auth Nodes** module to prepare it to receive RADIUS authentication requests from VMware Horizon 6. You will need the IP address of VMware Horizon 6 and the shared secret that will be used by SAS and VMware Horizon 6.

1. Log in to the SAS console with an Operator account.
2. Click the **COMMS** tab, and then select **Auth Nodes**.

3. In the **Auth Nodes** module, click the **Auth Nodes** link.

4. Under **Auth Nodes**, click **Add**.

5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Description</td>
<td>Enter a host description.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the IP address of the host or the lowest IP address in a range of addresses that will authenticate with SAS.</td>
</tr>
<tr>
<td>High IP Address In Range</td>
<td>Enter the highest IP address in a range of IP addresses that will authenticate with SAS.</td>
</tr>
<tr>
<td>Configure FreeRADIUS Synchronization</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td>Confirm Shared Secret</td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>
The authentication node is added to the system.

**Auth Nodes:**

Using the RADIUS protocol over the Internet provides limited security of the traffic between the organization’s data center and the authentication service. For improved security and for alternatives to RADIUS traffic, refer to the recommendations included in the SafeNet Authentication Service Administrator Guide.

<table>
<thead>
<tr>
<th>Primary RADIUS Server IP:</th>
<th>10.73.120.140:1812</th>
<th>Primary SafeNet Authentication Service Agent DNS:</th>
<th>agent1.safenet-inc.com:443</th>
<th>Max. Auth Nodes: 10</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
<th>Host Name</th>
<th>IP Address</th>
<th>FreeRADIUS Synchronization</th>
<th>Log</th>
<th>Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VMware Horizon 6</td>
<td>VMware Horizon 6</td>
<td>10.94.215.66</td>
<td>True</td>
<td>Log</td>
<td>Error</td>
</tr>
</tbody>
</table>

**Displaying:** 1 to 6 of 6

---

**Checking the SAS RADIUS Server’s IP Address**

Before adding SAS as a RADIUS server in VMware Horizon 6, check its IP address. The IP address will be added to VMware Horizon 6 as a RADIUS server later in this document.

1. Log in to the SAS console with an Operator account.
2. Click the **COMMS** tab, and then select **Auth Nodes**.
3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.

![Auth Nodes Module](image)

### Configuring VMware Horizon 6

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

1. **Login to VMware Horizon View Server using the URL** **Invalid Hyperlink reference not valid.**

   ![Login Screen](image)

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

![VMware Horizon View Administrator](image1.png)

(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.

![VMware Horizon View Administrator](image2.png)

(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.

![Advanced Authentication settings](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.

![Create 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>Label</th>
<th>Enter an authenticator name (for example, SAS).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>(Optional) Add a description for the authenticator.</td>
</tr>
<tr>
<td>Hostname/Address</td>
<td>Enter the IAS/NPS server name or IP address to use to reach the RADIUS server.</td>
</tr>
<tr>
<td>Authentication port</td>
<td>Enter the RADIUS server’s IAS/NPS port (for example, 1812).</td>
</tr>
<tr>
<td>Authentication type</td>
<td>Select PAP.</td>
</tr>
<tr>
<td>Shared secret</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. (Skip this step if there is no secondary authentication server to configure.) On the Add RADIUS Authenticator window, under Secondary Authentication Server, complete the following, and then click Next.

<table>
<thead>
<tr>
<th>Hostname/Address</th>
<th>Enter the IAS/NPS secondary server name or IP address to use to reach the RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication port</td>
<td>Enter the RADIUS server’s IAS/NPS port (for example, 1812).</td>
</tr>
<tr>
<td>Authentication type</td>
<td>Select PAP.</td>
</tr>
<tr>
<td>Shared secret</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.)

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

![Image of Edit Connection Server Settings window](image)

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

12. Click OK.
Running the Solution

Authenticating Using an SMS 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**.

![Next Code field](image1.png)

*(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**.

![Password field](image2.png)

*(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.

![VMware Horizon Client](image)

(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.

![VMware Horizon Client](image)

(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**.

![Image of VMware Horizon Client login screen]

*(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**.

![Image of VMware Horizon Client login screen with filled fields]

*(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></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>