SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Workspot Workspace
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012961-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>March 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

- Third-Party Software Acknowledgement ............................................................................................................. 4
- Description ......................................................................................................................................................... 4
  - SafeNet Authentication Service ......................................................................................................................... 4
  - Workspot ........................................................................................................................................................ 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 Users Stores with SAS ............................................................................................................. 7
  - Assigning an Authenticator in SAS ................................................................................................................... 8
  - Adding Workspot Workspace as an Authentication Node in SAS .................................................................... 9
- Checking the SAS RADIUS Server’s IP Address ................................................................................................. 11
- Configuring Workspot Workspace ........................................................................................................................ 12
  - Configuring Cisco ASA for RADIUS Authentication with SAS ...................................................................... 12
  - Configuring Workspot Workspace with Cisco ASA .......................................................................................... 22
- Running the Solution ......................................................................................................................................... 24
- Support Contacts .................................................................................................................................................. 26
Third-Party Software Acknowledgement

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

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 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.

Workspot

Workspot is a provider of enterprise software that can help IT deliver apps and data to mobile devices.

This document describes how to:

- Configure Workspot Workspace to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Workspot Workspace environment is already configured, and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Workspot Workspace 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 (SPE)**—An on-premises version of SafeNet Authentication Service that is 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 that is targeted at organizations interested in hosting SAS in their private cloud environment
Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service – Private Cloud Edition (PCE)**—An on-premises version of SafeNet Authentication Service that is targeted at organizations interested in hosting SAS in their private cloud environment
- **Workspot Workspace**—A provider of enterprise software that can help IT deliver apps and data to mobile devices
- **Cisco ASA**—Version 9.2(2.4)

Audience

This document is intended for system administrators who are familiar with Workspot Workspace 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 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 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 following diagram describes the data flow of a multi-factor authentication transaction for Workspot Workspace.

1. A user attempts to log in to Workspot Workspace using a one-time password (OTP) authenticator.
2. Workspot Workspace sends the authentication request to Cisco ASA.
3. Cisco ASA sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
4. The SAS authentication reply is sent back to the Cisco ASA.
5. Cisco ASA forwards the authentication reply to Workspot Workspace.
6. The user is granted or denied access to the Workspot Workspace based on the OTP value calculation results from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Workspot Workspace, ensure the following:

- End users can authenticate from the Workspot Workspace environment using Cisco ASA with a static password, before configuring the Workspot Workspace to use RADIUS authentication.
- Ports 1812/1813 are open to and from Cisco ASA.
- 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 Workspot Workspace and RADIUS protocol requires the following:

- Synchronizing User Stores with SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding Workspot Workspace as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS IP address, page 11

Synchronizing Users 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 methods that can be used as a second authentication factor for users authenticating through Workspot Workspace.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet Gold
- 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 Workspot Workspace 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 Workspot Workspace. You will need the IP address of Workspot Workspace and the shared secret that will be used by SAS and Workspot Workspace.

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**:

   - **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 (in this case, enter the Cisco ASA IP address).
   - **Configure FreeRADIUS Synchronization**: Select this option.
   - **Shared Secret**: Enter the shared secret key.
   - **Confirm Shared Secret**: Re-enter the shared secret key.

The authentication node is added to the system.
Checking the SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in Workspot Workspace, check its IP address. The IP address will be added to Workspot Workspace 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.
Configuring Workspot Workspace

Configuring Workspot Workspace and Cisco ASA to work with SAS Cloud requires the following:

- Configuring Cisco ASA for RADIUS Authentication with SAS, page 12
- Configuring Workspot Workspace with Cisco ASA, page 22

Configuring Cisco ASA for RADIUS Authentication with SAS

Configuring Cisco ASA for RADIUS authentication with SAS requires the following:

- Creating a AAA Server RADIUS Server Group for SAS, page 12
- Creating a Group Policy, page 16
- Creating a Connection Profile, page 18

Creating a AAA Server RADIUS Server Group for SAS

1. Launch the Cisco Adaptive Security Device Manager (ASDM).
2. Click the Configuration tab.

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
3. Click **Remote Access VPN**.

![Remote Access VPN Screen](image1)

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

4. Click **AAA/Local Users**, and then click **AAA Server Groups**.

![AAA Server Groups Screen](image2)

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

5. Adjacent to the **AAA Server Groups** window, click **Add**.

![Add AAA Server Group](image3)
6. On the **Add AAA Server Group** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>AAA Server Group</th>
<th>Enter a name for the AAA Server Group (for example, SAS).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select <strong>RADIUS</strong>.</td>
</tr>
</tbody>
</table>

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

7. Under **AAA Server Groups**, select the newly created AAA server group.

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

8. Adjacent to the **Servers in the Selected Group** window, click **Add**.
9. On the **Add AAA Server** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Interface Name</strong></th>
<th>Select the interface to use to reach the RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Name or IP Address</strong></td>
<td>Enter a server name or IP address to use to reach the RADIUS server.</td>
</tr>
<tr>
<td><strong>Server Authentication Port</strong></td>
<td>Enter the RADIUS server’s authentication port.</td>
</tr>
<tr>
<td><strong>Server Secret Key</strong></td>
<td>Enter the shared secret. This entry must match the shared secret that you specified for the SAS authentication node (refer to “<strong>Adding Workspot Workspace as an Authentication Node in SAS</strong>”).</td>
</tr>
</tbody>
</table>

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

10. Click **Apply**.

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

1. Launch the Cisco ASDM.
2. Click Remote Access VPN.

   ![Cisco ASDM Configuration Screen](image)

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

3. Click Clientless SSL VPN Access, and then click Group Policies.

   ![Cisco ASDM Group Policies Screen](image)

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

4. Click Add.
5. On the **Add Internal Group Policy** window, in the **Name** field, enter a name for the group policy (for example, **SafeNet**).

![Add Internal Group Policy window](image1)

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

6. Click **More Options**.

7. Adjacent to **Tunneling Protocols**, deselect **Inherit**, select **Clientless SSL VPN**, and then click **OK**.

8. Click **Apply**. The new group policy is created.

![Remote Access VPN configuration](image2)

*(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)*
Creating a Connection Profile

1. Launch the Cisco ASDM.
2. Click **Remote Access VPN**.
3. Click **Clientless SSL VPN Access**, and then click **Connection Profiles**.

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
4. Under **Access Interfaces**, select the appropriate interface(s) (for example, **outside** and **inside**), and then click **Allow Access**.

5. Under **Connection Profiles**, click **Add**.

6. On the **Add Clientless SSL VPN Connection Profile** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the connection profile (for example, <strong>SafeNet Connection</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>Enter an alias for the connection profile (for example, <strong>SafeNet</strong>).</td>
</tr>
<tr>
<td>AAA Server Group</td>
<td>Select the AAA server group that you created in &quot;Creating a AAA Server RADIUS Server Group for SAS&quot; (for example, <strong>SAS</strong>).</td>
</tr>
<tr>
<td>Group Policy</td>
<td>Select the group policy that you created in &quot;Creating a Group Policy&quot; (for example, <strong>SafeNet</strong>).</td>
</tr>
<tr>
<td>Enable clientless SSL VPN protocol</td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

![Add Clientless SSL VPN Connection Profile](image)

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
7. Click **Advanced**, and then click **Clientless SSL VPN**.

![Add Clientless SSL VPN Connection Profile](image)

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

8. Under **Group URLs**, click **Add**.

9. On the **Add Group URL** window, in **URL** field, enter a unique URL for this connection profile, and then click **OK**. (For example, the entry would follow the format: `https://<Public IP>`, or it could be the DNS of Cisco ASA/SafeNet, where SafeNet is a virtual name.)

![Add Group URL](image)

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
10. On the **Add Clientless SSL VPN Connection Profile** window, click OK.

![Add Clientless SSL VPN Connection Profile](image)

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

11. In the center panel, under **Connection Profiles**, select **Enabled** for the connection profile you added, and then click **Apply**.

![Connection Profiles](image)

*The screen image above is from Cisco®. Trademarks are the property of their respective owners.*)
Configuring Workspot Workspace with Cisco ASA

1. Log in to the Workspot Workspace admin console.

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

2. Click the **Network** tab.
3. Click **Add a New Network**.
4. On the **Add a New Network** window, complete the following fields, and then click **Add Network**.

<table>
<thead>
<tr>
<th><strong>Service Name</strong></th>
<th>Enter a name for the service (for example, Cisco).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication URL</strong></td>
<td>Enter the unique authentication URL of the connection profile created in Cisco ASA. (For example, the entry would follow the format: <code>https://&lt;Public IP&gt;</code>, or it could be the DNS of Cisco ASA/SafeNet).</td>
</tr>
<tr>
<td><strong>SSL VPN Type</strong></td>
<td>Select Cisco.</td>
</tr>
<tr>
<td><strong>Select Groups</strong></td>
<td>Select Default User Group.</td>
</tr>
</tbody>
</table>

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

A network is added to Workspot Workspace.
Running the Solution

Check the configured solution of Workspot Workspace and Cisco ASA using SAS.

NOTE: For this solution, an app must be configured for the Workspot Workspace user, and app traffic must be routed through Cisco ASA.

1. Launch the **Workspot** app on the IOS device, and then enter the user passcode.

2. The workspace will display all of the apps that are configured for the user to access.

3. Click the app that is configured through Cisco ASA.
4. If the **Certificate Not Trusted** message is displayed, click **Accept**.

![Certificate Not Trusted](image1)

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

5. On the **VPN Login** page, enter the SAS username in **Username** field.

![VPN Login](image2)

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

6. Generate an OTP, and then enter it in **Password** field.

7. Click **Sign In**. After successful authentication, the user is granted access to the app.

![Sign In](image3)
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 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 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>