SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for RadiantOne Cloud Federation Service (CFS)
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Document Part Number:** 007-013675-001, Rev. A

**Release Date:** November 2016
## 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>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>SAS Authentication API Authentication using SafeNet Authentication Service Cloud</td>
<td>5</td>
</tr>
<tr>
<td>SAS Authentication API using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE</td>
<td>5</td>
</tr>
<tr>
<td>SafeNet Authentication Service Authentication API Flow using SAS</td>
<td>6</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td>Configuring RadiantOne CFS</td>
<td>6</td>
</tr>
<tr>
<td>Configuring AD FS</td>
<td>6</td>
</tr>
<tr>
<td>- Configuring AD FS Relying Party Trust for the Claims-based Authentication</td>
<td>11</td>
</tr>
<tr>
<td>Configuring Gemalto SafeNet SAS AD FS Agent</td>
<td>17</td>
</tr>
<tr>
<td>- Configuring AD FS Authentication Policy</td>
<td>19</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>20</td>
</tr>
<tr>
<td>- Creating Users Stores in SafeNet Authentication Service</td>
<td>21</td>
</tr>
<tr>
<td>- Assigning an Authenticator in SafeNet Authentication Service</td>
<td>21</td>
</tr>
<tr>
<td>- Configuring the SafeNet Authentication Service Auth Node and Downloading the Encryption Key....</td>
<td>22</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>23</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>25</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 RadiantOne Cloud Federation Service (CFS). Material from the third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from the third-party software will be acknowledged as such.

Description

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.

The RadiantOne Cloud Federation Service (CFS), powered by identity virtualization, is the latest component of the RadiantOne suite. Together with RadiantOne VDS, CFS delegates the task of authenticating against all your identity stores to one common virtual layer, and shields your external and cloud applications from the complexity of your identity systems.

VDS virtualizes the authentication, validating the user against a variety of sources—including multiple Active Directory domains and forests, LDAP, databases, and web services—then CFS acts as a secure token service, (STS), gathering the requested attributes and building an encrypted claim in the form that the application understands. CFS is a Microsoft-certified, third-party SSO provider and can securely deliver claims to many of today’s mission-critical applications, including Office 365, WebEx, SharePoint 2010/2013, Google Apps, Salesforce, and Jive.

CFS enables a secure federated infrastructure, and creates one access and audit point to connect all your internal identity and authentication sources to the growing world of cloud applications.

This document describes how to:

- Deploy multifactor authentication (MFA) options in RadiantOne Cloud Federation Service (CFS) using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure SAML authentication in RadiantOne Cloud Federation Service (CFS) using SafeNet Authentication Service as an identity provider.

It is assumed that the RadiantOne Cloud Federation Service (CFS) environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

The RadiantOne Cloud Federation Service (CFS) 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 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

- **Gemalto SafeNet SAS AD FS Agent**

### 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)**
- **RadiantOne Cloud Federation Service (CFS)**—Version 3.8
- **RadiantOne VDS**—Version 7.2.7
- **AD FS** (in Windows Server® 2012 R2)

### Audience

This document is targeted to system administrators who are familiar with RadiantOne Cloud Federation Service (CFS), and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

### SAS Authentication API Authentication using SafeNet Authentication Service Cloud

SAS Cloud provides a service for SafeNet Authentication Service (SAS) Authentication API that is already implemented in the SAS Cloud environment and can be used using the Gemalto SafeNet SAS AD FS Agent.

### SAS Authentication API using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service (SAS) comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)**—An on-premises version of SafeNet Authentication Service 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 targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, SAS can be integrated with AD FS infrastructure, which uses a special on-premises agent called Gemalto SafeNet SAS AD FS Agent.
SafeNet Authentication Service Authentication API Flow using SAS

AD FS provides extensible multi-factor authentication through the concept of “additional authentication providers” that are invoked during secondary authentication. External providers can be registered in AD FS.

Once a provider is registered with AD FS, it is invoked from the AD FS authentication code via specific interfaces and methods that the provider implements and that AD FS calls. Because it provides a bridge between AD FS and an external authentication provider, the external authentication provider is also called an AD FS MFA “adapter”.

Gemalto SafeNet SAS AD FS Agent is an AD FS MFA adapter that provides users a way to authenticate through AD FS using SAS as a secondary authenticator.

The image below describes the dataflow of a multi-factor authentication transaction for RadiantOne CFS.

1. A user attempts sign in to RadiantOne Cloud Federation Service (CFS). The user is redirected to AD FS login window, then after successful authentication, is forwarded to SafeNet Authentication Service (SAS) for a secondary authentication (AD FS multi-factor authentication).
2. The user uses his or her SAS token for authenticating. SAS collects and evaluates the user's credentials.
3. The SAS authentication reply is sent back to AD FS which returns a response to RadiantOne CFS, accepting or rejecting the user's authentication request.
4. The user is granted or denied access to RadiantOne CFS.

Prerequisites

- RadiantOne VDS is installed and configured.
- RadiantOne CFS is installed and configured.
- AD FS is installed and configured.
- End user should be authenticated by the VDS on the CFS user portal with the static password.
- Gemalto SafeNet SAS agent should be installed on the ADFS machine.

Configuring RadiantOne CFS

Configure AD FS as identity provider in CFS.
1. In a web browser, open the following url:
   https://<CFS_SERVER>/cfs
   For example, https://pradeepcfs/cfs
2. On the RadiantOne Cloud Federation Service login window, in the email and Password fields, enter your tenant administrator login email ID and password, respectively, and then click Sign In.

![RadiantOne Cloud Federation Service login window](image)

(The screen image above is from Radiant Logic, Inc. Trademarks are the property of their respective owners.)

3. On the tenant administrator dashboard, in the left pane, click Administration.

![Tenant administrator dashboard with Administration highlighted](image)

(The screen image above is from Radiant Logic, Inc. Trademarks are the property of their respective owners.)
4. Click **Authentication > Others**.

![Image of RadiantOne dashboard](image1.png)

*(The screen image above is from Radiant Logic, Inc. Trademarks are the property of their respective owners.)*

5. In the right pane, click **New Trusted Identity Provider**.

![Image of RadiantOne dashboard](image2.png)

*(The screen image above is from Radiant Logic, Inc. Trademarks are the property of their respective owners.)*

6. On the **Presentation** tab, perform the steps:
   
   a. **Enable Enable on Master**.
   
   b. In the **Name** field, enter a unique name.
      
      The name is displayed on the tenant web portal login window and helps you to recognize AD FS as an available authentication method.
c. In the **Description** field, enter a description.

d. Click **Metadata file** and then save metadata as a `.xml` file.

7. Click the **Configuration** tab and then perform the following steps:
   a. In the **Metadata URL** field, enter the AD FS metadata URL.
   b. In the **Endpoint** field, enter the endpoint URL.
   c. Click **Choose** to search for and select the AD FS signing certificate to be uploaded.

8. Click the **Mappings** tab and then perform the following steps:
   a. Click **New Mapping**.
      
   b. In the **Attribute** field, enter your attribute name (for example, `mail`, according to the claim rule defined in AD FS) in the newly added mapping.
c. Click **Edit** in the newly added mapping.

d. Click **Save**.

![Map configuration screenshot](image)

9. Under **How do you want to edit this transformation?**, click **Advanced**.

![Advanced transformation window](image)

(The screen image above is from Radiant Logic, Inc. Trademarks are the property of their respective owners.)

10. On the **Advanced Transformation** window, enter the claim rule in the **input(“<claim rule>”)** format.

For example, input(http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress)

![Advanced transformation input area](image)

(The screen image above is from Radiant Logic, Inc. Trademarks are the property of their respective owners.)

11. Click **Save**.
12. Click **Save**.

(Note: The screen image above is from Radiant Logic, Inc. Trademarks are the property of their respective owners.)

---

**NOTE:**

- Trusted Identity Provider Authentication Systems are pre-configured with the default mappings. You only need to configure claims rules if the default mappings do not match your requirements.
- The default mappings indicate the claim that contain the user’s unique identifier. This claim value is used to identify the user who is authenticated through AD FS in the CFS identity store.

---

### Configuring AD FS

Configuring AD FS requires:

- Configuring AD FS Relying Party Trust for the Claims-based Authentication, page 11
- Configuring AD FS Authentication Policy, page 19

### Configuring AD FS Relying Party Trust for the Claims-based Authentication

Configure RadiantOne CFS as a relying party to consume claims from AD FS 3.0 for authenticating internal claims access.

1. On the AD FS machine, open the **Server Manager**.
2. On the Server Manager dashboard, click **Tools** > **AD FS Management**.

(Note: The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
3. On the AD FS management console, in the left pane, click **AD FS > Trust Relationships**, right-click **Relying Party Trusts**, and then click **Add Relying Party Trust**.

![AD FS management console screenshot](image1)

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

4. On **Add Relying Party Trust Wizard**, under **Welcome**, click **Start**.

![Add Relying Party Trust Wizard screenshot](image2)

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

5. Under **Select Data Source**, perform the following steps:
   a. Select **Import data about the relying party from a file** option.
   b. Under **Federation metadata file location**, click **Browse** to search for and select the CFS metadata that you downloaded earlier in step 6 (d) of “Configuring RadiantOne CFS” on page 6.
c. Click **Next**.

---

6. Under **Specify Display Name**, in the **Display name** field, enter a name for the relying party (for example, **cfs**), and then click **Next**.

---

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
7. Under **Configure Multi-factor Authentication Now?**, click **Next**.

![Configure Multi-factor Authentication Now?](image1.png)

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

8. Under **Choose Issuance Authorization Rules**, select the **Permit all users to access this relying party** option, and then click **Next**.

![Choose Issuance Authorization Rules](image2.png)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
9. Under **Ready to Add Trust**, click **Next**.

![Add Relying Party Trust Wizard](image)

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

10. Under **Finish**, click **Close**.

![Add Relying Party Trust Wizard](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
11. On the **Edit Claim Rules for cfs** window, click **Add Rule**.

![Edit Claim Rules for cfs window](image1)

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

12. On **Add Transform Claim Rule Wizard**, under **Select Rule Template**, in the **Claim rule template** field, select **Send LDAP Attributes as Claims**, and then click **Next**.

![Add Transform Claim Rule Wizard](image2)

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

13. Under **Configure Rule**, complete the following steps:

   a. Under **Claim rule name**, enter a name for the claim rule (for example, **UID**).

   b. In the **Attribute store** field, select **Active Directory**.
c. Under Mapping of LDAP attributes to outgoing claim types, perform the following steps:
   - Under **LDAP Attribute**, select **SAM-Account-Name**.
   - Under **Outgoing Claim Type**, select **Name ID**.

d. Click **Finish**.

14. On the **Edit Claim Rules for cfs** window, click **OK**.

---

**Configuring Gemalto SafeNet SAS AD FS Agent**

1. Run the Gemalto SafeNet Authentication Service (SAS) Agent for AD FS.
2. On the SFA MFA Plug-In Manager window, on the Policy tab, ensure that the following are selected:

- Enable agent
- Push Challenge

![SFA MFA Plug-In Manager](image1)

3. On the Communications tab, in the Primary Server IP field, enter the SAS server IP address or name (and port if non-causal is used). Also, ensure that under User ID Format, Strip realm ("username is sent as SAS User ID") is checked.

In case your SAS server is not installed on the same machine as AD and AD FS, the encryption key file needs to be loaded (as explained in step 3 of “Configuring the SafeNet Authentication Service Auth Node and Downloading the Encryption Key” on page 22).

![SFA MFA Plug-In Manager](image2)

4. Click Apply. Enabling the agent registers the SafeNet multi-factor authentication (MFA) adapter with AD FS and enables it at a global policy level.
5. You can verify your settings by testing authentication from the agent to the authentication server. To do so, under **Authentication Test**, enter your user name and passcode, and then click **Test**. The result of the test will be displayed in the **Authentication Test Result** field.

6. Click **OK** when finished.

**Configuring AD FS Authentication Policy**

1. On the **AD FS Management Console**, in the left pane, under **AD FS**, click **Authentication Policies**, and then, in the right pane, click **Edit Global Primary Authentication**.

   ![AD FS Management Console](image1.png)

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

2. On the **Edit Global Authentication Policy** window, on the **Primary** tab, ensure that **Forms Authentication** is selected for both **Extranet** and **Intranet**.

   ![Edit Global Authentication Policy](image2.png)

   (The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
3. Click the **Multi-factor** tab, and then perform the following steps:
   a. Under **Users/Groups**, add the users and/or groups for which MFA will be required.
   b. Under **Locations**, select **Extranet** and/or **Intranet**, according to your preferred configuration.
   c. Ensure that **SafeNet Multi Factor Authentication (SMFA)** is selected as an additional authentication method.
   d. Click **OK**.

![Edit Global Authentication Policy](image.png)

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

### Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with RadiantOne Cloud Federation Service (CFS) using SAML authentication requires:

- Creating Users Stores in SafeNet Authentication Service, page 21
- Assigning an Authenticator in SafeNet Authentication Service, page 21
- Configuring the SafeNet Authentication Service Auth Node and Downloading the Encryption Key, page 21
Creating Users Stores in SafeNet Authentication Service

Before SafeNet Authentication Service can authenticate any user in your organization, you need to create a user store in SafeNet Authentication Service (SAS) that reflects the users that would 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 SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through RadiantOne Cloud Federation Service (CFS).

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS tokens
- MP-1 software token
- GrIDsure
- 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.

Configuring the SafeNet Authentication Service Auth Node and Downloading the Encryption Key

In the event that the SafeNet Authentication Service server is not installed on the same machine as AD and AD FS, the following steps must be performed:

1. Log in to the SafeNet Authentication Service console as the account operator.
2. Click **Virtual Servers > Comms > Authentication Processing**.
   - Click the **Authentication Agent Settings** link, and then select **Download** to download the encryption key file. This file will be needed in step 3 of

4. Click **Virtual Servers > Comms > Auth Nodes**.
5. Click the **Auth Nodes** link and select **Add**. Complete the **Auth Notes** tab as follows:

<table>
<thead>
<tr>
<th><strong>Agent Description</strong></th>
<th>Type a description for this node (for example, DC).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Name</strong></td>
<td>Type a host name.</td>
</tr>
<tr>
<td><strong>Low IP Address In Range</strong></td>
<td>Type the low IP address.</td>
</tr>
<tr>
<td><strong>High IP Address In Range</strong></td>
<td>Type the high IP address. (The low and high IP addresses may be the same since the node is referencing a single machine.)</td>
</tr>
<tr>
<td><strong>Exclude from PIN change requests</strong></td>
<td>Do not select this check box.</td>
</tr>
</tbody>
</table>

![Auth Nodes](image)

### Running the Solution

For this integration, PASSWORD token is configured for authentication with the SAS solution.

1. In a web browser, open the following user portal URL:

   **https://<CFS_SERVER>/cfs**

   For example, **https://pradeepcfs/cfs**

2. On the RadiantOne Cloud Federation Service user login window, click **microsoft adfs**.

   ![RadiantOne Cloud Federation Service](image)

   *(The screen image above is from Radiant Logic, Inc. Trademarks are the property of their respective owners.)*
3. You are redirected to your organization’s login window. Enter your AD user ID and password, and then click **Sign in**.

![Login Window](image1.png)

4. After your credentials are authenticated by your organization’s AD FS, you are redirected to the SAS login window. In the **Passcode** field, enter the token passcode, and then click **Submit**.

![Login Window](image2.png)

After successful authentication, you will be redirected to the CFS user portal.

![CFS User Portal](image3.png)

*(The screen image above is from Radiant Logic, Inc. 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 Gemalto Customer Support. Gemalto 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 Gemalto 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>Gemalto</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 Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>