SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for Oracle Access Management R2 PS2
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.

© 2015 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. 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:** 007-012899-001, Rev. B  
**Release Date:** June 2016
# Contents

- Third-Party Software Acknowledgement ................................................................. 4
- Description ................................................................................................................. 4
- Applicability .............................................................................................................. 4
- Environment .............................................................................................................. 4
- Audience .................................................................................................................... 5
- SAML Authentication using SafeNet Authentication Service Cloud .......................... 5
- SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE .............................................................. 5
- SAML Authentication Flow using SafeNet Authentication Service .......................... 5
- SAML Prerequisites ................................................................................................. 6
- Configuring Oracle Access Management R2 ............................................................ 6
  - Creating an Identity Provider Partner .................................................................. 6
  - Creating an Authentication Module ..................................................................... 10
  - Creating an Authentication Scheme ................................................................... 12
  - Creating an Authentication Policy ....................................................................... 14
- Configuring SafeNet Authentication Service ............................................................ 16
  - Synchronizing Users Stores to SafeNet Authentication Service .......................... 16
  - Assigning an Authenticator in SafeNet Authentication Service .......................... 16
  - Adding Oracle Access Management R2 as a Service Provider (SP) in SafeNet Authentication Service ................................................................. 17
  - Enabling SAML Services in SafeNet Authentication Service .............................. 21
- Running the Solution .................................................................................................. 26
- Support Contacts ....................................................................................................... 28
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Oracle Access Management R2.

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 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.

Oracle Access Management delivers risk-aware end-to-end user authentication, single sign-on, and authorization protection, providing enterprises with secure access from mobile devices and seamless integration of social identities with applications.

This document describes how to:

- Configure SAML authentication in Oracle Access Management R2 using SafeNet Authentication Service as an identity provider.

It is assumed that the Oracle Access Management R2 environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Oracle Access Management R2 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

Environment

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

- **SafeNet Authentication Service**—A cloud-based service
- **Oracle Access Management R2**
Audience

This document is targeted to system administrators who are familiar with Oracle Access Management R2, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

SAML Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (SAS) Cloud provides a service for SAML authentication that is already implemented in the SAS Cloud environment and can be used without any installation.

SAML Authentication Flow 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 the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

For more information on how to install and configure the SafeNet Authentication Service Agent for Shibboleth, refer to the SafeNet Support Portal.

SAML Authentication Flow using SafeNet Authentication Service

SafeNet Authentication Service (SAS) communicates with a large number of service providers and cloud-based services solutions using the SAML protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Oracle Access Management R2.
1. A user attempts to log on to Oracle Access Management R2. The user is redirected to SafeNet Authentication Service. SAS collects and evaluates the user’s credentials.

2. SAS returns a response to Oracle Access Management R2, accepting or rejecting the user’s authentication request.

SAML Prerequisites

To enable SafeNet Authentication Service (SAS) to receive SAML authentication requests from Oracle Access Management R2, ensure that the end users can authenticate from the Oracle Access Management R2 environment with a static password.

Configuring Oracle Access Management R2

To add SafeNet Authentication Service as an identity provider in Oracle Access Management R2, perform the following steps:

- Creating an Identity Provider Partner
- Creating an Authentication Module
- Creating an Authentication Scheme
- Creating an Authentication Policy

Creating an Identity Provider Partner

In this section, you will create an identity provider partner, and configure the IDP certificate and URL’s.

1. Log in to the Oracle Access Management administration console.
2. Under Identity Federation, select Service Provider Administration.
3. On the Service Provider Administration window, click Create Identity Provider Partner on the right of the window.

(The screen image above is from Oracle Access Management. Trademarks are the property of their respective owners.)

The Create Identity Provider Partner window opens.
4. On the **Create Identity Provider Partner** window, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Partner</strong></td>
<td>Enable this option.</td>
</tr>
<tr>
<td><strong>Default Identity</strong></td>
<td>Enable this option.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Enter Rule Name.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>Select <strong>SAML 2.0</strong>.</td>
</tr>
<tr>
<td><strong>Service Details</strong></td>
<td>Select <strong>Enter Manually</strong>.</td>
</tr>
<tr>
<td><strong>Provider ID</strong></td>
<td>Enter the SAS entity ID.</td>
</tr>
<tr>
<td><strong>SSO Service URL</strong></td>
<td>Enter the SAS HTTP-Redirect login URL.</td>
</tr>
<tr>
<td><strong>Logout Request</strong></td>
<td>Enter the SAS logout URL.</td>
</tr>
<tr>
<td><strong>Service URL</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Signing Certificate</strong></td>
<td>Load the SAS certificate file.</td>
</tr>
</tbody>
</table>
5. Click **Save**.

6. After clicking **Save**, an **Advanced** option will be added to the window.

7. Under **Advanced**, select the following options:
   (the **Advanced** section will appear only after saving):
   - Enable global logout
   - HTTP POST SSO Response Binding

8. Click **Save** again.
Creating an Authentication Module

1. Log in to the **Oracle Access Management** administration console.
2. Under **Access Manager**, select **Authentication Modules**.

![Oracle Access Management Console](image1.png)

(The screen image above is from Oracle Access Management. Trademarks are the property of their respective owners.)

The **Search Authentication Modules** window opens.

![Search Authentication Modules](image2.png)

(The screen image above is from Oracle Access Management. Trademarks are the property of their respective owners.)

3. On the **Search Authentication Modules** window, click **Create Authentication Module** and select **Create Custom Authentication Module**.

The **Custom Authentication Module** window opens.

![Custom Authentication Module](image3.png)

(The screen image above is from Oracle Access Management. Trademarks are the property of their respective owners.)
4. On the General tab, enter a module name in the Name field, and then select the Steps tab.

5. On the Steps tab, enter the following:

<table>
<thead>
<tr>
<th>Step Name</th>
<th>Plug-in Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Identification</td>
<td>UserIdentificationPlugin</td>
</tr>
<tr>
<td>LDAP Authentication</td>
<td>UserAuthenticationPlugin</td>
</tr>
<tr>
<td>SAML Auth</td>
<td>FedAuthnRequestPlugin</td>
</tr>
<tr>
<td>SAML FedAuth</td>
<td>FedUserAuthenticationPlugin</td>
</tr>
</tbody>
</table>

6. Click Save and then select the Steps Orchestration tab.
7. On the **Steps Orchestration** tab, add the following steps:

<table>
<thead>
<tr>
<th>Step Name</th>
<th>On Success</th>
<th>On Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Identification</td>
<td>LDAP Identification</td>
<td>Failure</td>
</tr>
<tr>
<td>LDAP Authentication</td>
<td>SAML Auth</td>
<td>Failure</td>
</tr>
<tr>
<td>SAML Auth</td>
<td>SAML FedAuth</td>
<td>SAML FedAuth</td>
</tr>
<tr>
<td>SAML FedAuth</td>
<td>Success</td>
<td>Failure</td>
</tr>
</tbody>
</table>

8. Set **Initial Step** to **LDAP Identification** and then click **Apply**.

**Creating an Authentication Scheme**

After creating the authentication module, create an authentication scheme that will use the module.

1. Log in to the **Oracle Access Management** administration console.
2. Under **Access Manager**, select **Authentication Schemes**.

(The screen image above is from Oracle Access Management. Trademarks are the property of their respective owners.)
The **Search Authentication Schemes** window opens.

![Image of Search Authentication Schemes window](image.png)

*(The screen image above is from Oracle Access Management. Trademarks are the property of their respective owners.)*

3. Click **Create Authentication Scheme**.

   The **Authentication Schemes** window opens.

![Image of Authentication Schemes window](image.png)

4. On the **Authentication Schemes** window, enter the following, and then click **Apply**:

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a rule name.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Level</strong></td>
<td>Set the Authentication Level to 2.</td>
</tr>
<tr>
<td><strong>Challenge Method</strong></td>
<td>Select <strong>Form</strong>.</td>
</tr>
<tr>
<td><strong>Authentication Module</strong></td>
<td>Select the authentication module created in the “Creating an Authentication Module” section on page 10.</td>
</tr>
<tr>
<td><strong>Challenge URL</strong></td>
<td>Enter the credential collector URL.</td>
</tr>
<tr>
<td><strong>Context Type</strong></td>
<td>Select external.</td>
</tr>
</tbody>
</table>
Creating an Authentication Policy

After creating the authentication module and scheme, create an authentication policy and assign the application domain.

1. Login to the Oracle Access Management administration console.
2. Under Access Manager, select Application Domains.

![Oracle Access Management console](image1)

(The screen image above is from Oracle Access Management. Trademarks are the property of their respective owners.)

The Search Application Domains window opens.

![Search Application Domains](image2)

(The screen image above is from Oracle Access Management. Trademarks are the property of their respective owners.)

3. Click Search and select the relevant application domain from the list.
4. Select the **Authentication Policies** tab and then click **Create Authentication Policy**.

![Image of Authentication Policies tab](image)

*(The screen image above is from Oracle Access Management. Trademarks are the property of their respective owners.)*

5. On the **Authentication Policy** window, enter the following, and then click **Apply**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a policy name.</td>
</tr>
<tr>
<td><strong>Authentication Scheme</strong></td>
<td>Select the authentication scheme created in the “Creating an Authentication Scheme” section on page 12.</td>
</tr>
<tr>
<td><strong>Resources Tab</strong></td>
<td>Select the protected resource.</td>
</tr>
</tbody>
</table>
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Oracle Access Management R2 using SAML authentication requires:

- Synchronizing Users Stores to SafeNet Authentication Service, page 16
- Assigning an Authenticator in SafeNet Authentication Service, page 16
- Adding Oracle Access Management R2 as a Service Provider (SP) in SafeNet Authentication Service, page 17
- Enabling SAML Services in SafeNet Authentication Service, page 21

Synchronizing Users Stores to SafeNet Authentication Service

Before SafeNet Authentication Service (SAS) can authenticate any user in your organization, you need to create a user store in 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 further 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 authenticating through Oracle Access Management R2.

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” 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 Oracle Access Management R2 as a Service Provider (SP) in SafeNet Authentication Service

Add a service provider entry in the SafeNet Authentication Service (SAS) **SAML Service Providers** module to prepare it to receive SAML authentication requests from Oracle Access Management R2. The Oracle Access Management R2 metadata will be required.

**To get the metadata from Oracle Access Manager:**

1. Log in to the **Oracle Access Management** administration console.
2. Under **Configurations**, select **Federation Settings**.

   ![Oracle Access Management Federation Settings](image)

   *(The screen image above is from Oracle Access Management. Trademarks are the property of their respective owners.)*

   The **Federation Settings** window opens.
3. Click **Export SAML 2.0 Metadata** and save the file.

**To add Oracle Access Management R2 as a ServiceProvider in SafeNet Authentication Service:**

1. Log in to the SafeNet Authentication Service console with an Operator account.
2. Click the **COMMS** tab, and then click **SAML Service Providers**.

3. In the **SAML Service Providers** module, click the **SAML 2.0 Settings** link.

4. Click **Add**.
5. Under **Add SAML 2.0 Settings**, complete the following fields:

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Enter Oracle Access Management R2 name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML 2.0 Metadata</td>
<td>Select <strong>Create New Metadata File</strong>. Enter the Entity ID and Location.</td>
</tr>
</tbody>
</table>

![Add SAML 2.0 Settings](image)

**NOTE:** The remaining options are used to customize the appearance of the logon page presented to the user. For more information on logon page customization, refer “Configure SAML Service” in the **SAML Configuration Guide**: http://www2.safenet-inc.com/sas/implementation-guides/sas-on-prem/SAS-QS-SAML.pdf

Under **Return Attributes**, add the following attributes, and then click **Apply**:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/claims/EmailAddress">http://schemas.xmlsoap.org/claims/EmailAddress</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/claims/CommonName">http://schemas.xmlsoap.org/claims/CommonName</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
</tbody>
</table>
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier

According to ThirdParty Product Requirements

principal

According to ThirdParty Product Requirements

Oracle Access Management R2 is added as a service provider in the system.

Enabling SAML Services in SafeNet Authentication Service

After Oracle Access Management R2 has been added to SafeNet Authentication Service (SAS) as a service provider, the users should be granted permission to use this service provider with SAML authentication.

There are two methods to enable the user to use the service provider:

- Manually, one user at a time, using SAML Services module
- Automatically, by defining groups of users, using SAML Provisioning Rules
Using the SAML Services Module

Manually enable a single user to authenticate against one or more configured SAML Service providers.

1. Log in to the SafeNet Authentication Service console with an Operator account.

2. Click the **ASSIGNMENT** tab, and then search for the required user.

3. Click the appropriate user in the **User ID** column.
4. Click **SAML Services**.

5. Click **Add**.

6. Under **Add SAML Service**, do the following:
   a. From the **Service** menu, select the Oracle Access Management R2 service provider.
   b. In **SAML Login ID** field, select the type of login ID (User ID, E-mail, or Custom) to be sent as a UserID to Oracle Access Management R2 in the response.
   c. Click **Add**.
The user can now authenticate to Oracle Access Management R2 using SAML authentication.

### Using SAML Provisioning Rules

Use this module to enable groups of users to authenticate to SAML service providers.

1. Log in to the SafeNet Authentication Service console with an Operator account.

2. Click the POLICY tab, and then click Automation Policies.
3. Click the **SAML Provisioning Rules** link.

4. Click **New Rule**.

5. Configure the following fields, and then click **Add**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rule Name</strong></td>
<td>Enter a name for the rule.</td>
</tr>
<tr>
<td><strong>User is in container</strong></td>
<td>Users affected by this rule must be in the selected container.</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td>The <strong>Virtual Server groups</strong> box lists all groups. Click the user groups that will be affected by the rule, and then click the right arrow to move it to the <strong>Used by rule</strong> box.</td>
</tr>
<tr>
<td><strong>Parties</strong></td>
<td>The <strong>Relying Parties</strong> box lists all service providers. Click the service providers that the groups of users will authenticate to, and then click the right arrow to move it to <strong>Rule Parties</strong> box.</td>
</tr>
<tr>
<td><strong>SAML Login ID</strong></td>
<td>This is the User ID that will be returned to the Service Provider in the SAML assertion. Select &lt;User ID&gt;</td>
</tr>
</tbody>
</table>
Running the Solution

Once the configurations are done, log in to the protected resource and test the solution.

1. Open a browser and go to the protected resource.

   The LDAP Login window opens.

   (The screen image above is from Oracle Access Management. Trademarks are the property of their respective owners.)
2. Enter the **LDAP credentials**, and click **Login**.

![Login page](image)

(The screen image above is from Oracle Access Management. Trademarks are the property of their respective owners.)

3. After successful LDAP authentication, you will be redirected to the SAS login page.

4. Generate an OTP value in your authenticator and enter your **User Name** and **OTP** value in the appropriate fields.

5. After successful authentication, you will be redirected to the protected resource.
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>Address</td>
<td>Gemalto, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td>Phone</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>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</td>
<td>Existing customers with a Technical Support</td>
</tr>
<tr>
<td></td>
<td>Customer Portal account can log in to manage</td>
</tr>
<tr>
<td></td>
<td>incidents, get the latest software upgrades, and</td>
</tr>
<tr>
<td></td>
<td>access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>