

# SafeNet Authentication Service Integration Guide

Using SafeNet Authentication Service as an Identity Provider for OpenIAM

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 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:** 007-013481-001, Rev. A

**Release Date:** April 2016

# Contents

Third-Party Software Acknowledgement.....	4
Description .....	4
Applicability .....	4
Environment .....	5
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 .....	6
SAML Prerequisites .....	6
Configuring OpenIAM.....	6
Creating a Service Provider.....	7
Downloading the OpenIAM Metadata.....	10
Creating an Identity Provider .....	12
Downloading the SafeNet Authentication Service Metadata .....	15
Configuring SafeNet Authentication Service .....	15
Synchronizing Users Stores to SafeNet Authentication Service .....	15
Assigning an Authenticator in SafeNet Authentication Service .....	15
Adding OpenIAM as a Service Provider (SP) in SafeNet Authentication Service.....	16
Enabling SAML Services in SafeNet Authentication Service .....	19
Running the Solution.....	23
Appendix: Assigning a Service Provider (as the Default Resource) to OpenIAM Users for SSO .....	25
Support Contacts .....	29

# Third-Party Software Acknowledgement

---

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

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.

OpenIAM is a comprehensive Identity and Access Management infrastructure that provides a strong security foundation to provision users and authenticate and authorize access to enterprise systems.

OpenIAM is an integration of OpenIAM Identity Manager and OpenIAM Access Manager.

OpenIAM Identity Manager automates the task of managing identities across the various devices and applications used by the enterprise. OpenIAM Access Manager integrates seamlessly with OpenIAM Identity Manager to provide a comprehensive solution that allows you take control of not only who can access your systems, but what they can do once they are in there.

This document describes how to:

- Deploy multifactor authentication (MFA) options in OpenIAM using SafeNet OTP authenticators managed by SafeNet Authentication Service.
- Configure SAML authentication in OpenIAM using SafeNet Authentication Service as an identity provider.

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

OpenIAM 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 – Private Cloud Edition (SAS-PCE)**
- **OpenIAM**—Version 3.3.3

## Audience

---

This document is targeted to system administrators who are familiar with OpenIAM, 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 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 OpenIAM.



1. A user attempts to log on to OpenIAM. The user is redirected to SafeNet Authentication Service (SAS). SAS collects and evaluates the user's credentials.
2. SAS returns a response to OpenIAM, accepting or rejecting the user's authentication request.

## SAML Prerequisites

---

To enable SafeNet Authentication Service to receive SAML authentication requests from OpenIAM, ensure the following:

- End users can authenticate from the OpenIAM environment with a static password.
- End users must be assigned a service provider as the default resource to achieve SSO (Refer to “Appendix: Assigning a Service Provider (as the Default Resource) to OpenIAM Users for SSO” on page 25).
- OpenIAM must be deployed on either the Jboss application server or Apache Tomcat server.

## Configuring OpenIAM

---

Adding SafeNet Authentication Service (SAS) as an identity provider in OpenIAM requires the following:

- Creating a Service Provider, page 7
- Downloading the OpenIAM Metadata, page 10
- Creating an Identity Provider, page 12

## Creating a Service Provider

A service provider offers services that access protected resources and handles authorization.

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

**http://<FQDN\_of\_client\_machine>:9080/webconsole**

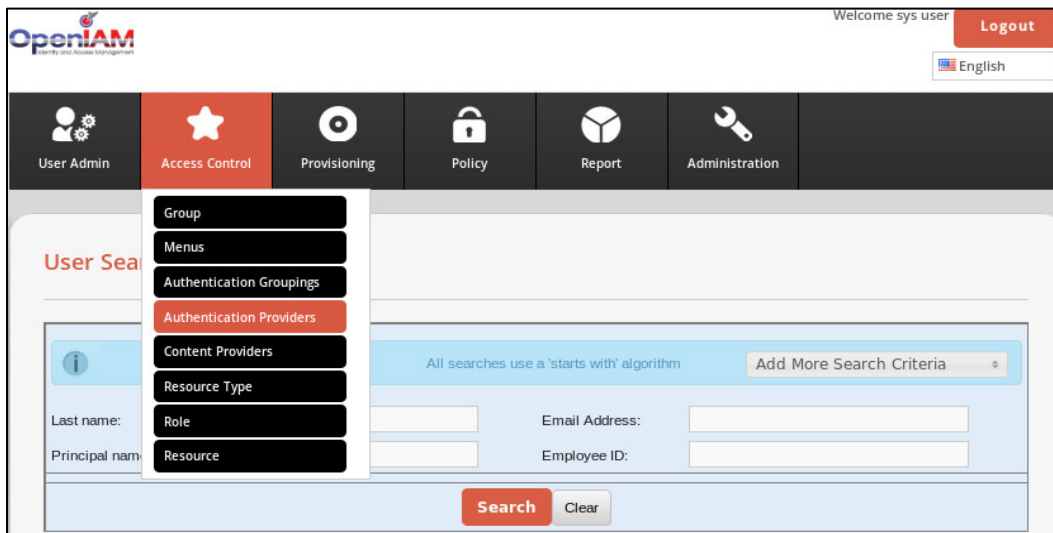
where, **FQDN\_of\_client\_machine** is the domain name of the client machine, and **9080** is the default JBoss server port number.

2. On the OpenIAM login window, enter the administrator login ID and password, and then click **Login**.



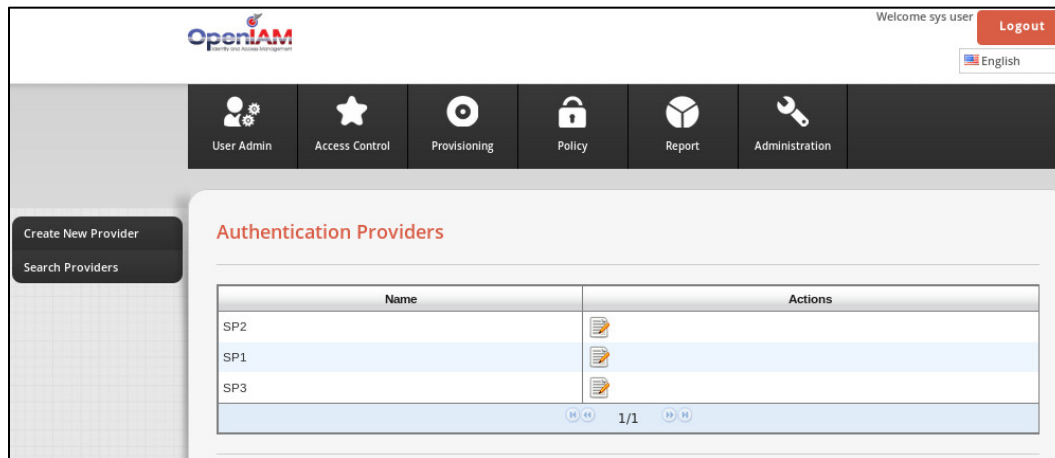
(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)

3. On the OpenIAM Administrative console window, click **Access Control > Authentication Providers**.



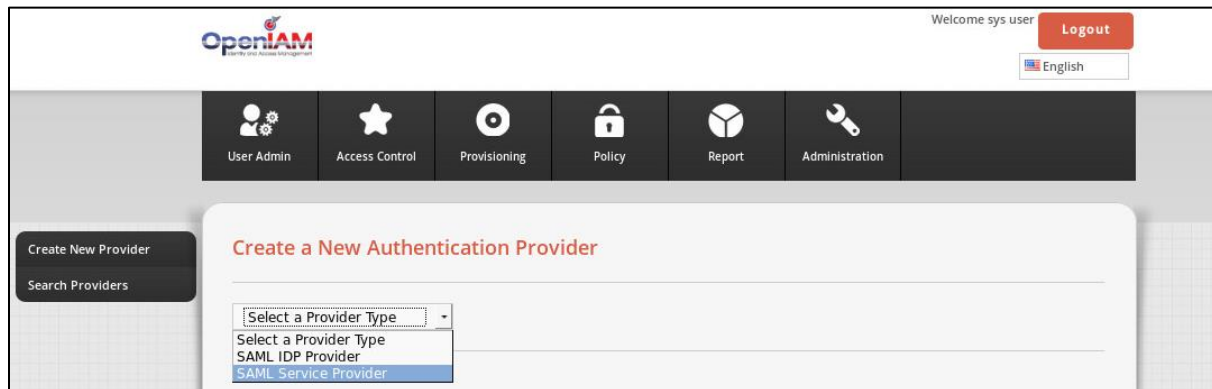
(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)

4. On the **Authentication Providers** window, in the left pane, click **Create New Provider**.



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

5. On the **Create a New Authentication Provider** window, in the right pane, select **SAML Service Provider**.



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



6. On the **Create SAML Service Provider** window, in the right pane, complete the following fields, and then click **Save**.

<b>Provider Name</b>	Enter a name for the service provider (for example, <b>SAS_SP</b> ).
<b>Linked to Managed System</b>	Select a managed system (identity repository) (for example, <b>OPENIAM</b> ).
<b>SAML Issuer Name</b>	Enter a request issuer name (for example, <b>http://&lt;IP address of the OpenIAM machine&gt;/idp/SAMLLogin.html</b> ).
<b>Sign-in page URL</b>	Enter the SAML login page URL (for example, <b>https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO</b> ).
<b>Sign-out page URL</b>	Enter the SAML logout page URL (for example, <b>https://idp1.cryptocard.com/idp/signout.jsp</b> ).

**Create SAML Service Provider**

Provider Name\*

Application URL

Application Icon

Linked to Managed System\* Select a Managed System

Sign Response?\* ☐ Yes ☒ No

Is this provider chained? ☐ Yes ☒ No

Next Authentication Provider in Chain Select a value

NameID Resolver Groovy Script

Issuer Format

SAML Issuer Name\*

Just-in-time provisioning groovy script

Sign-in page URL\*

Sign-out page URL\*

AuthnContextClassRef element value

Destination attribute enabled ☐ Yes ☒ No

AllowCreate on the NameIdPolicy ☐ Yes ☒ No

NameID IN SAML Request

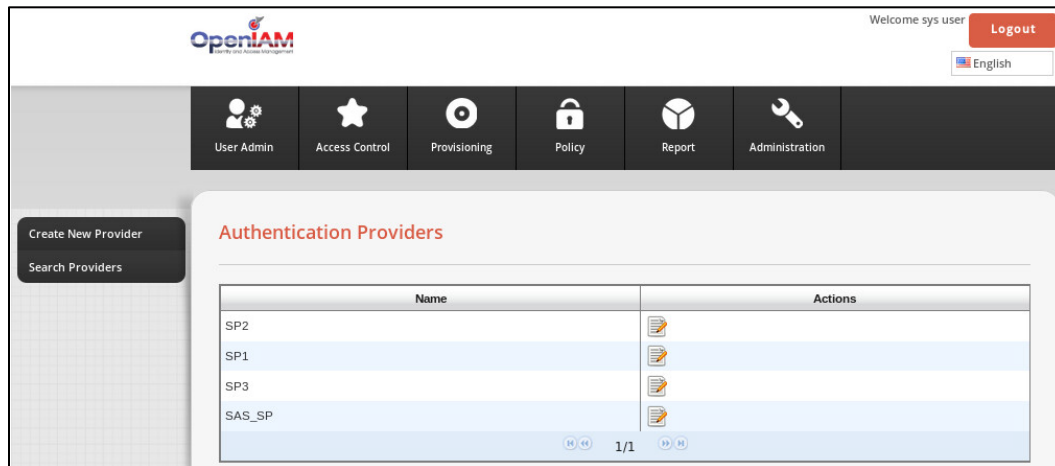
SP Name Qualifier

Description

Save Cancel

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

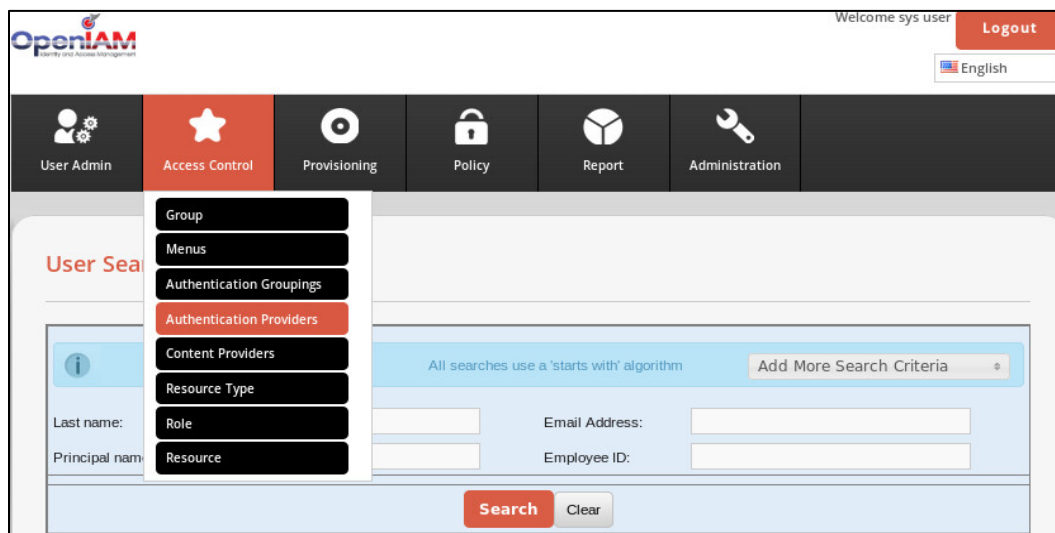
On the **Authentication Providers** window, in the right pane, the newly created service provider (for example, **SAS\_SP**) is listed.



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

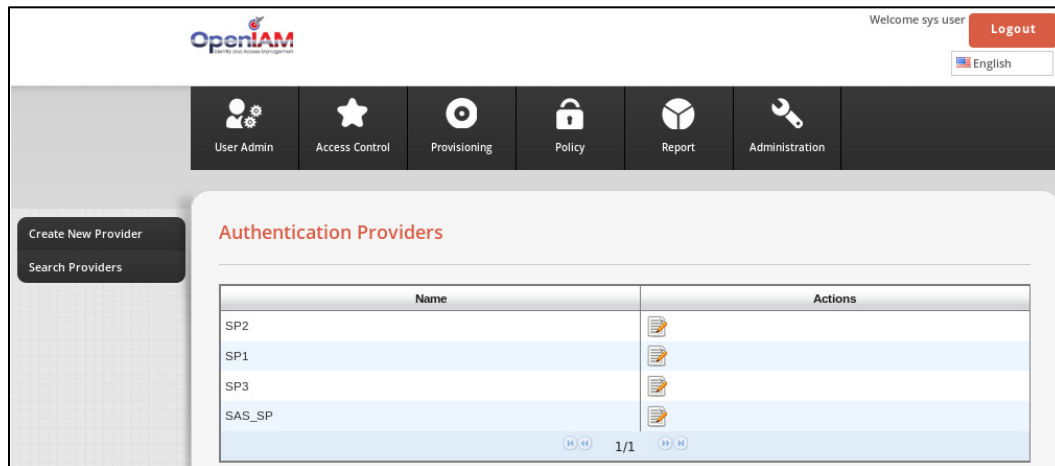
## Downloading the OpenIAM Metadata

1. On the OpenIAM Administrative console window, click **Access Control > Authentication Providers**.



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

- On the **Authentication Providers** window, in the right pane, in the **Name** column, click on the newly created service provider (for example, **SAS\_SP**).



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

- On the **Edit SAML Service Provider** window, at the bottom, click **SAML Metadata**.

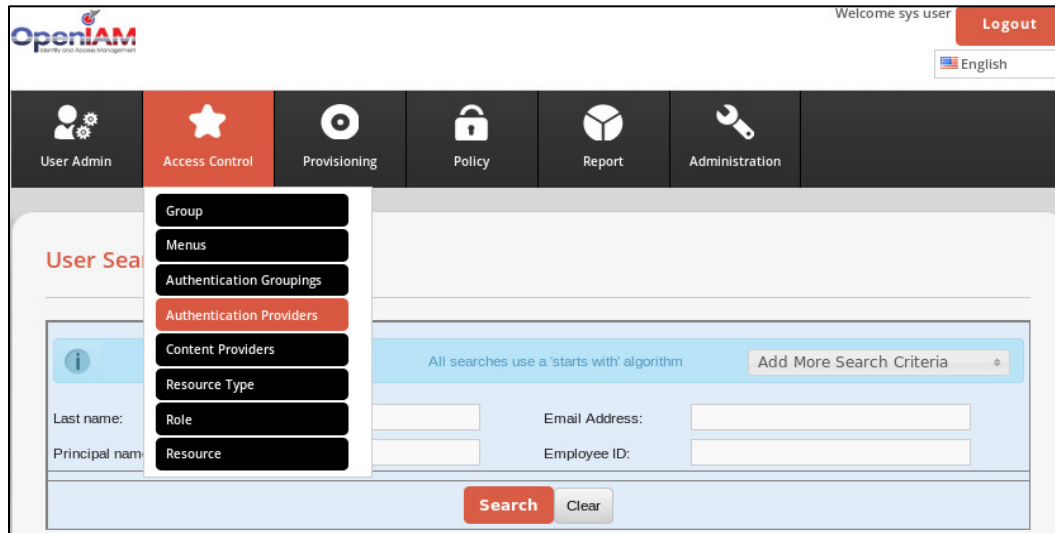
(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)

4. In a web browser, the metadata will be displayed. Copy the metadata and then save it as an XML document in your local drive.

## Creating an Identity Provider

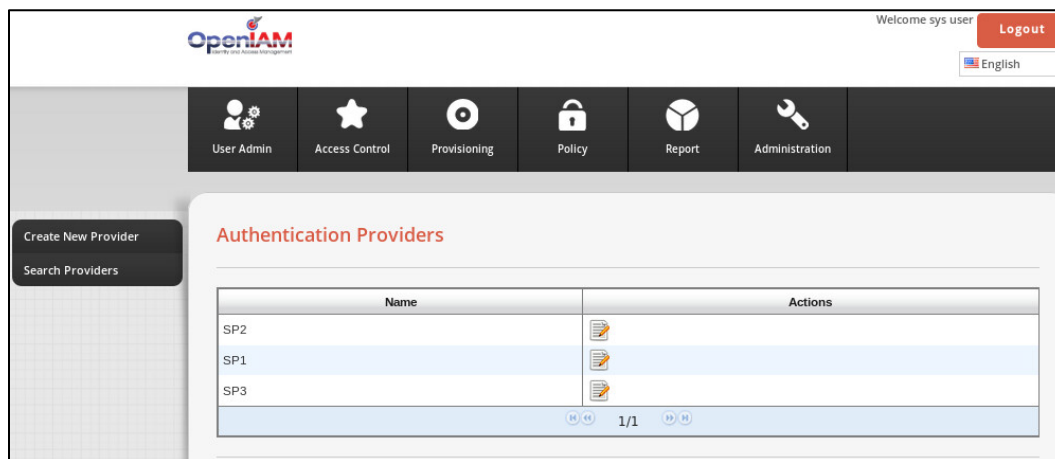
An identity provider stores and serves identity profiles and handles authentication.

1. On the OpenIAM Administrative console window, click **Access Control > Authentication Providers**.



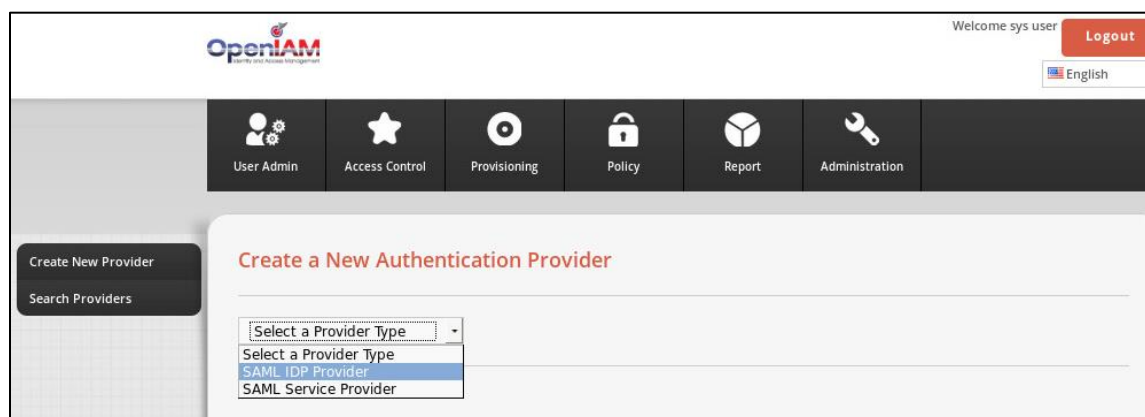
(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)

2. On the **Authentication Providers** window, in the left pane, click **Create New Provider**.



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

3. On the **Create a New Authentication Provider** window, in the right pane, select **SAML IDP Provider**.



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

4. On the **Create SAML IDP Provider** window, complete the following fields, and then click **Save**.

<b>Provider Name</b>	Enter a name for the provider (for example, <b>SAS_IDP</b> ).
<b>Linked to Managed System</b>	Select a managed system (identity repository) (for example, <b>OPENIAM</b> ).
<b>Sign Response</b>	Select <b>NO</b> .
<b>Request Issuer</b>	Enter the issuer of SAML requests (for example, <b>http://&lt;IP of OpenIAM machine&gt;/idp/SAMLLlogin.html</b> ).
<b>Response Issuer</b>	Enter the issuer of the SAML responses (entity ID of SAS, for example, <b>https://idp1.cryptocard.com/idp/shibboleth</b> ).
<b>Assertion Consumer URL</b>	Enter the assertion consumer URL of OpenIAM (for example, <b>http://localhost:9080/idp/sp/login</b> ).

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

## Downloading the SafeNet Authentication Service Metadata

---

Browse to the <https://idp1.cryptocard.com/idp/shibboleth> URL. The SafeNet Authentication Service (SAS) metadata will be downloaded automatically. Save it locally on your machine.

## Configuring SafeNet Authentication Service

---

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with OpenIAM using SAML authentication requires:

- Synchronizing Users Stores to SafeNet Authentication Service, page 15
- Assigning an Authenticator in SafeNet Authentication Service, page 15
- Adding OpenIAM as a Service Provider (SP) in SafeNet Authentication Service. page 16
- Enabling SAML Services in SafeNet Authentication Service, page 19

## 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*:

[http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet\\_Authentication\\_Service/Safenet\\_Authentication\\_Service\\_\\_Subscriber\\_Account\\_Operator\\_Guide/](http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/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 OpenIAM.

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.

[http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet\\_Authentication\\_Service/Safenet\\_Authentication\\_Service\\_\\_Subscriber\\_Account\\_Operator\\_Guide/](http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/Safenet_Authentication_Service__Subscriber_Account_Operator_Guide/)

## Adding OpenIAM 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 OpenIAM. You will need the metadata of OpenIAM.

**To add OpenIAM as a Service Provider in SafeNet Authentication Service (SAS):**

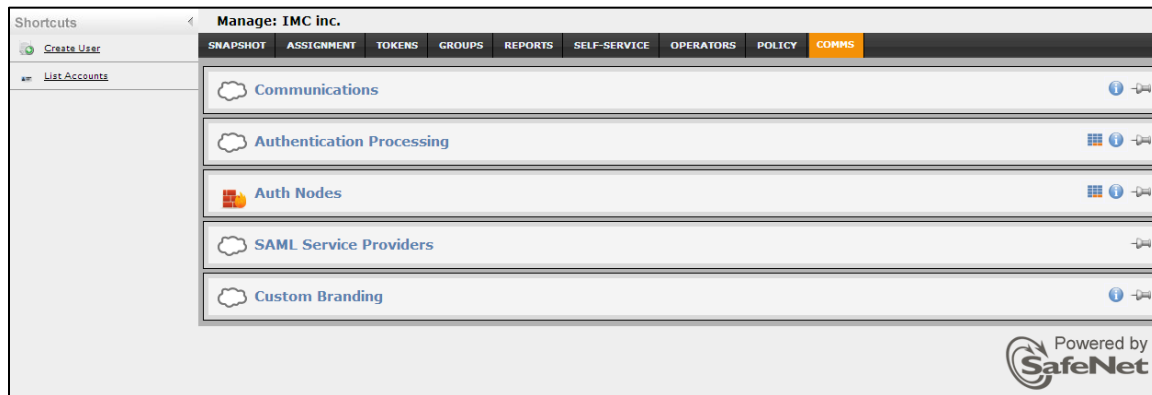
1. Log in to the SafeNet Authentication Service console with an Operator account.

Service Start: 2013-07-17 Service Stop: 2016-02-05

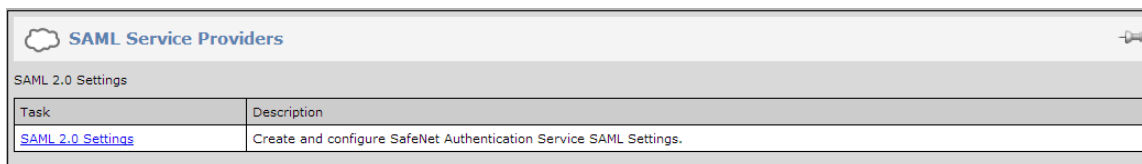
Item	Capacity	KT	RB-1	MP-1/SMS	ICE MP-1/SMS	GRID	SecurID	OATH	SMS Credits	Password	RADIUS	GOLD	eToken	MobilePASS
Maximum	1	0	0	5	0	0	0	0	0	0	0	0	0	0
In Use	1	0	0	0	0	0	0	0	0	1	0	0	0	0



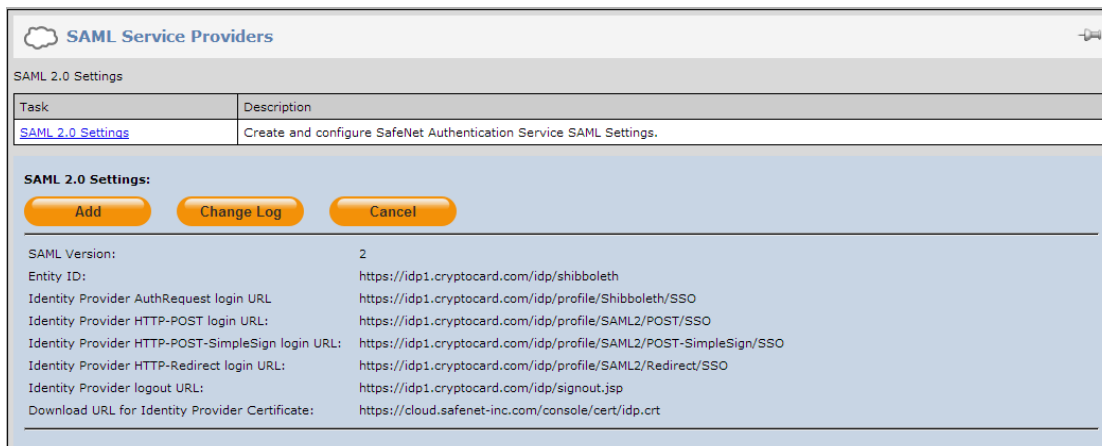
- Click the **COMMS** tab, and then click **SAML Service Providers**.



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



- Click **Add**.



5. In the **Add SAML 2.0 Settings** section, complete the following fields, and then click **Apply**:

<b>Friendly Name</b>	Enter the OpenIAM name.
<b>SAML 2.0 Metadata</b>	Select <b>Upload Existing Metadata File</b> . Click <b>Choose File</b> , select the service provider's metadata file, and then click <b>Open</b> .

**Add SAML 2.0 Setting:**

Apply Cancel

Friendly Name:

SAML 2.0 Metadata: ☒ Upload Existing Metadata File ☐ Create New Metadata File  
 No file chosen

Entity ID:

Custom Logo:  No file chosen

Custom CSS:  No file chosen

Custom Button Image:  No file chosen

Custom Page Title:

Custom Icon:  No file chosen

Custom Login Header Text:

Custom Login Button Text:

Login Message:

Custom Username Text:

Custom Password Text:



**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 to “Configure SAML Service” in the *SAML Configuration Guide*:

<http://www2.safenet-inc.com/sas/implementation-guides/sas-on-prem/SAS-QS-SAML.pdf>

OpenIAM is added as a service provider in the system.

**SAML Service Providers**

SAML 2.0 Settings

Task	Description
<a href="#">SAML 2.0 Settings</a>	Create and configure SafeNet Authentication Service SAML Settings.

**SAML 2.0 Settings:**

Add Change Log Cancel

SAML Version: 2

Entity ID: <https://idp1.cryptocard.com/idp/shibboleth>

Identity Provider AuthRequest login URL: <https://idp1.cryptocard.com/idp/profile/Shibboleth/SSO>

Identity Provider HTTP-POST login URL: <https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO>

Identity Provider HTTP-POST-SimpleSign login URL: <https://idp1.cryptocard.com/idp/profile/SAML2/POST-SimpleSign/SSO>

Identity Provider HTTP-Redirect login URL: <https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO>

Identity Provider logout URL: <https://idp1.cryptocard.com/idp/signout.jsp>

Download URL for Identity Provider Certificate: <https://cloud.safenet-inc.com/console/cert/idp.crt>

Service Provider	Entity ID	Edit	Remove	Resync
		Edit	Remove	Resync
		Edit	Remove	Resync
		Edit	Remove	Resync
Openiam	<a href="http://10.164.44.187/idp/SAMLLogin.html">http://10.164.44.187/idp/SAMLLogin.html</a>	Edit	Remove	Resync
		Edit	Remove	Resync
		Edit	Remove	Resync
		Edit	Remove	Resync

## Enabling SAML Services in SafeNet Authentication Service

After OpenIAM 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 SAS console with an Operator account.

Shortcuts

Manage: IMC inc.

Create User

SNAPSHOT ASSIGNMENT TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS POLICY COMMS

Authentication Activity

Authentication Metrics

Token States

SMS Credits

Allocation

Transaction Log

Service Start: 2013-07-17 Service Stop: 2016-02-05

Item	Capacity	KT	RB-1	MP-1/SMS	ICE MP-1/SMS	GRID	SecurID	OATH	SMS Credits	Password	RADIUS	GOLD	eToken	MobilePASS
Maximum	1	0	0	5	0	0	0	0	0	0	0	0	0	0
In Use	1	0	0	0	0	0	0	0	0	1	0	0	0	0

References

Powered by SafeNet

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

Search User

Search User:

User ID:  Auth Method:  Container:

Last Name:  E-mail:  Account State:

Search Clear

Provision Delete Account Unlock

No Records

3. Click the appropriate user in the **User ID** column.

**Manage: DA Test**

SNAPSHOT **ASSIGNMENT** TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS POLICY COMMS

**Search User**

Search User:

User ID:  Auth Method:  Container:

Last Name:  Email:  Account State:

	User ID	Last Name	First Name	Custom #1	Auth Method	RADIUS Attr	Auth State	Account State	Container
<input type="checkbox"/>	alice1	al	alice		Token		Active	Unlocked	Default

Displaying: 1 to 1 of 1

4. Click **SAML Services**.

**Manage: DA Test**

SNAPSHOT **ASSIGNMENT** TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS POLICY COMMS

**User Detail : alice1**

First Name:  Address:  Phone:

Last Name:  Extension:  Alias #1:

User ID:  City:  Emergency:  Alias #2:

Email:  State:  Custom #1:

Mobile/SMS:  Country:  Custom #2:

Container:  Postal/Zip:  Custom #3:

**Tokens**

**Authentication Metrics**

**Authentication Activity**

**Access Restrictions**

**Group Membership**

**RADIUS Attributes (user)**

**SAML Services**

5. Click **Add**.

**SAML Services**

6. Under **Add SAML Service**, do the following:
  - a. From the **Service** menu, select the OpenIAM 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 OpenIAM in the response.
  - c. Click **Add**.

**Add SAML Service**

Add
Cancel

Service: Openiam

SAML Login ID: ☒ User ID ☐ Email ☐ Custom

The user can now authenticate to OpenIAM using SAML authentication.

SAML Services					
<div style="float: right;"> <span style="background-color: #ff9900; color: white; padding: 2px 10px; border-radius: 5px;">Add</span> <span style="background-color: #ffcc00; color: white; padding: 2px 10px; border-radius: 5px;">Change Log</span> </div>					
Index	SAML Service	User ID	Status		
1					
2	Openiam	pradeep.nvki@gmail.com	Active	Edit	Remove

## 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 (SAS) console with an Operator account.

Shortcuts

Manage: IMC inc.

Create User
SNAPSHOT
ASSIGNMENT
TOKENS
GROUPS
REPORTS
SELF-SERVICE
OPERATORS
POLICY
COMMS

Authentication Activity

Grid
Info
Refresh

Authentication Metrics

Info
Refresh

Token States

Info
Refresh

SMS Credits

Info
Refresh

Allocation

Grid
Info
Refresh

Transaction Log

Service Start: 2013-07-17
Service Stop: 2016-02-05

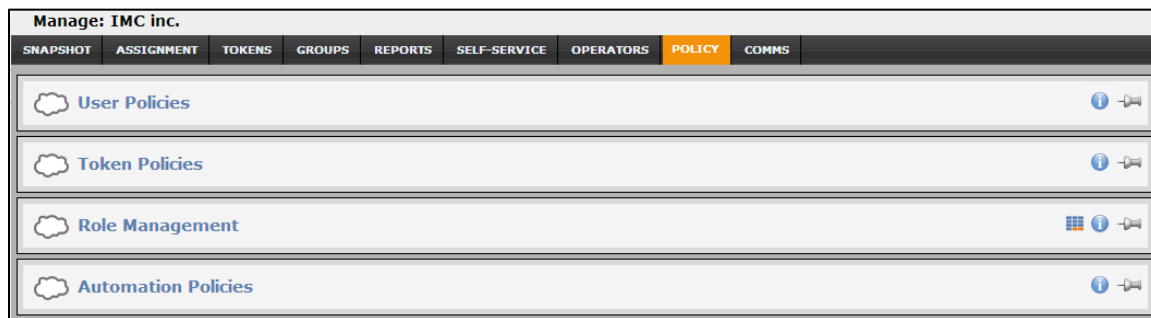
Item	Capacity	KT	RB-1	MP-1/SMS	ICE MP-1/SMS	GRID	SecurID	OATH	SMS Credits	Password	RADIUS	GOLD	eToken	MobilePASS
Maximum	1	0	0	5	0	0	0	0	0	0	0	0	0	0
In Use	1	0	0	0	0	0	0	0	0	1	0	0	0	0

References

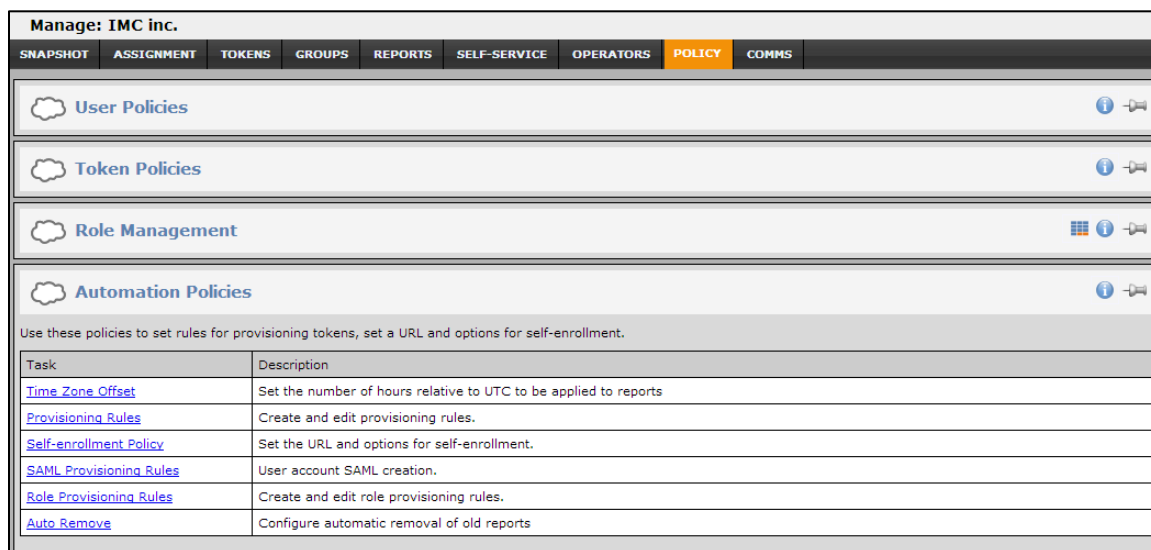
Info
Refresh

Powered by  
SafeNet

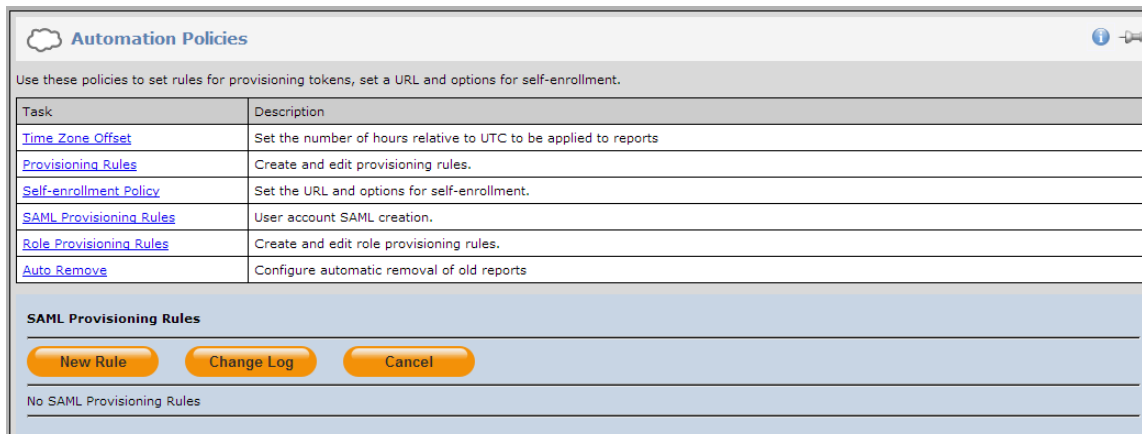
- Click the **POLICY** tab, and then click **Automation Policies**.



- Click the **SAML Provisioning Rules** link.



- Click **New Rule**.



- Configure the following fields, and then click **Add**:

<b>Rule Name</b>	Enter a name for the rule.
<b>User is in container</b>	Users affected by this rule must be in the selected container.
<b>Groups</b>	The <b>Virtual Server groups</b> 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 <b>Used by rule</b> box.
<b>Parties</b>	The <b>Relying Parties</b> 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 <b>Rule Parties</b> box.
<b>SAML Login ID</b>	Select <b>User ID</b> . The <b>User ID</b> will be returned to the service provider in the SAML assertion.

The screenshot displays the 'SAML Provisioning Rules' configuration window. At the top, there are buttons for 'New Rule', 'Change Log', and 'Cancel'. Below this is a table with one rule named 'OpenIAM'. Under the table, there are buttons for 'Apply' and 'Cancel'. The main configuration area includes fields for 'Rule Name' (OpenIAM), 'User is in container' (Default), and 'Groups Filter'. There are also buttons for 'Search' and 'Add'. The 'Groups' section shows 'Virtual Server groups' and 'Used by rule' boxes. The 'Parties' section shows 'Relying Parties' and 'Rule Parties' boxes. At the bottom, there is a 'SAML Login ID' section with radio buttons for 'User ID' and 'Email'.

## Running the Solution

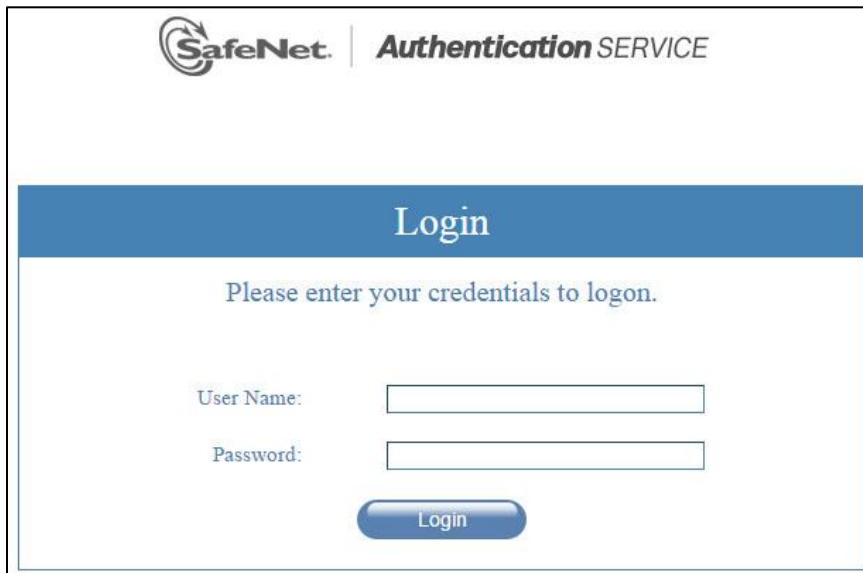
For this integration, the SafeNet GrIDsure token is configured for authentication with the SAS solution. Before running the solution, ensure that the JBoss server is running on the client machine.

- In a web browser, open the following URL:

**`http://<domain or localhost or ip of OpenIAM Machine>/idp/sp/login?issuer=SAMLIssuerNameFromAbove`**

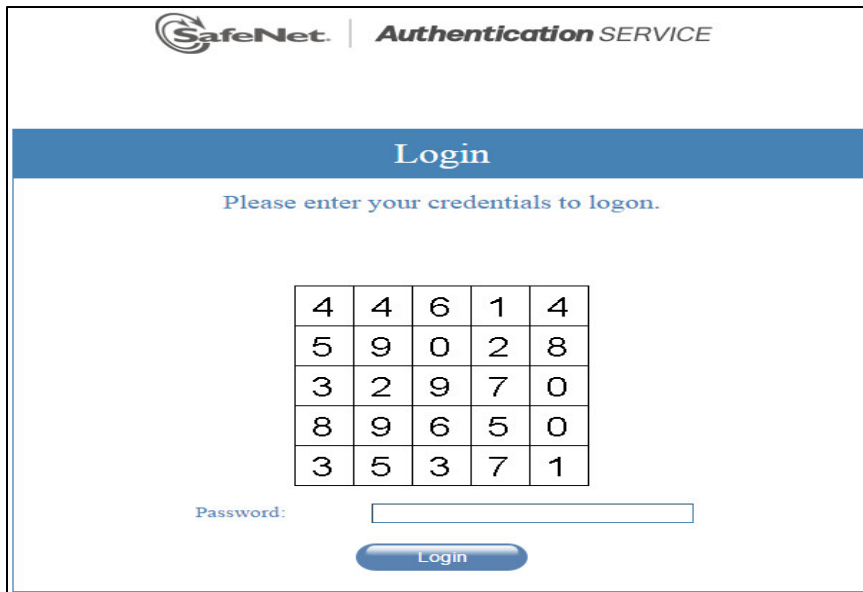
For example, **`http://localhost:9080/idp/sp/login?issuer=http://10.164.44.187/idp/SAMLLLogin.html`**

2. You will be redirected to the SAS login page. In the **User Name** field, enter your user name, and then click **Login**.



The image shows the SafeNet Authentication Service login page. At the top, there is a header with the SafeNet logo and the text "Authentication SERVICE". Below this is a blue bar with the word "Login" in white. Underneath the bar, the text "Please enter your credentials to logon." is displayed. There are two input fields: "User Name:" and "Password:". Below the "Password:" field is a blue "Login" button.

3. In the **Password** field, enter your Personal Identification Pattern (PIP), and then click **Login**.

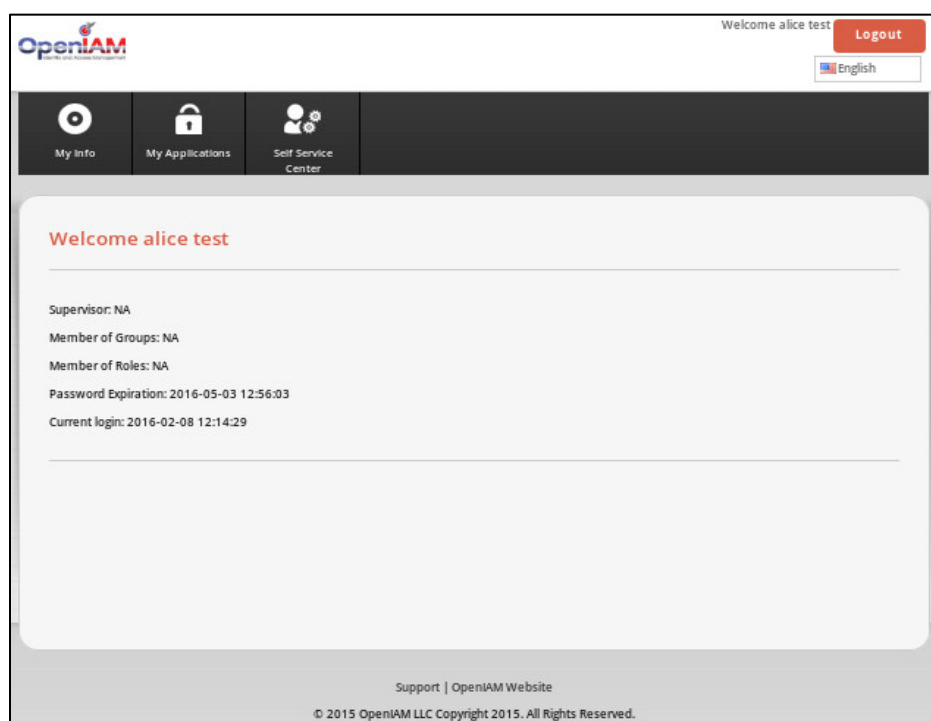


The image shows the SafeNet Authentication Service login page, similar to the one above, but with a Personal Identification Pattern (PIP) grid. The grid is a 5x5 table of numbers. Below the grid is a "Password:" label and an input field. At the bottom is a blue "Login" button.

4	4	6	1	4
5	9	0	2	8
3	2	9	7	0
8	9	6	5	0
3	5	3	7	1



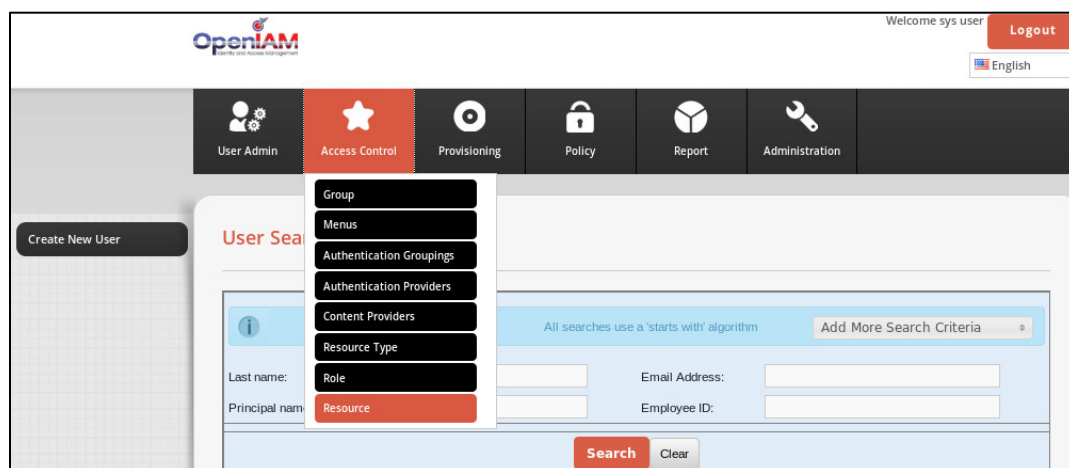
After successful authentication, you will be able to access the OpenIAM console.



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

## Appendix: Assigning a Service Provider (as the Default Resource) to OpenIAM Users for SSO








1. On the OpenIAM Administrative console window, click **Access Control > Resource**.



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

- On the **Search Resources** window, in the **Resource Name** column, click on the service provider (for example, **SAS\_SP**) that you created earlier in step 6 of “Creating a Service Provider” on page 7.

Search Resources

Select a Resource Type		Type a Resource Name	Search	
Resource Name	Type	Description	Risk	Actions
SAS_SP	Authentication Provider			
SAS_IDP	Authentication Provider			
salesforce	Authentication Provider			
ACTIVE DIRECTORY	Managed Systems			
AppTableMSys	Managed Systems			
AUDIT_REPORT	Report			
jira	Content Provider			

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

- On the **Edit Resource** window, in the **URL** field, enter the self-service URL (for example, **http://localhost:9080/selfservice**), and then click **Save**.

**Edit Resource: 1454044868328\_SAS\_SP**

Resource Type: Authentication Provider

Name: 1454044868328\_SAS\_SP

Coorelated Name: SAS\_SP

Description:

Metadata Type: [Click to select a Metadata Type](#)

Risk: Select a Risk

Protected by admin resource: RES\_ADMIN\_1454044868328\_SAS\_SP\_Ow

URL: http://localhost:9080/selfservice

**Attributes**

Attributes

Create New Attribute

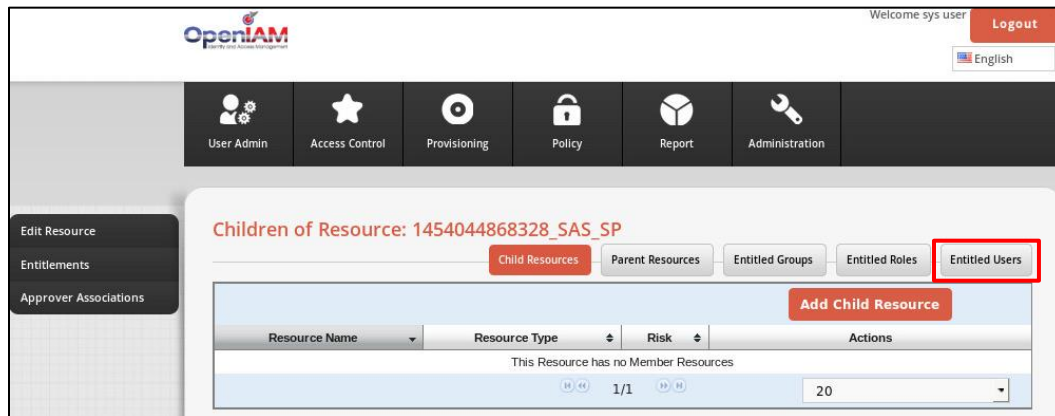
Attribute Name	MetaData Element	Attribute Value	Actions
There are no attributes attached to this Resource			

Save Cancel Delete

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

- In the left pane, click **Entitlements**.

5. On the **Children of Resource** window, in the right pane, click **Entitled Users**.



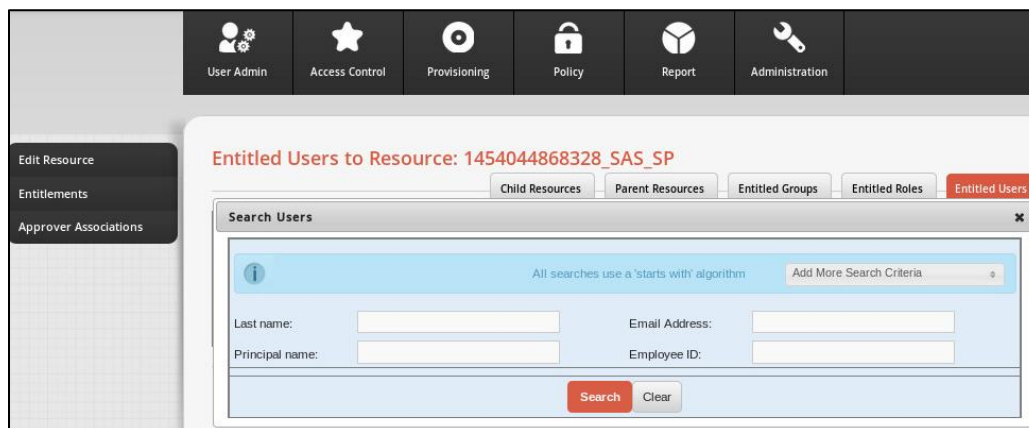
(The screen image above is from OpenIAM. Trademarks are the property of their respective owners.)

6. On the **Entitled Users to Resource** window, in the right pane, click **Add User**.



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

7. Under **Search Users**, in the **Last name** or **Email Address** field, enter the last name or email address of the user, respectively, and then click **Search**.



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

- In the second table, in the **Name** column, click on the OpenIAM user name (for example, **alice al**).

Entitled Users to Resource: 1454044868328\_SAS\_SP

Child Resources Parent Resources Entitled Groups Entitled Roles Entitled Users

Add User

Name	Phone Number	Email Address	User status	Account status	Actions
There are no Users entitled to this Resource					
1/1 20					

Name	Phone Number	Email Address	User status	Account status	Actions
alice al		pradeep.nwk@gmail.com	ACTIVE		
1/1 20					

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

The user is listed in the first table with **User status** as **ACTIVE**.

Entitled Users to Resource: 1454044868328\_SAS\_SP

Child Resources Parent Resources Entitled Groups Entitled Roles Entitled Users

Add User

Name	Phone Number	Email Address	User status	Account status	Actions
alice al		pradeep.nwk@gmail.com	ACTIVE		
1/1 20					

Name	Phone Number	Email Address	User status	Account status	Actions
alice al		pradeep.nwk@gmail.com	ACTIVE		
1/1 20					

(The screen image above is from OpenIAM. 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.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	<a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a> 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.	