SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for PingFederate
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: 007-013149-001, Rev. B
Release Date: June 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>4</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>SAML Authentication using SafeNet Authentication Service Cloud</td>
<td>5</td>
</tr>
<tr>
<td>SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE5</td>
<td>5</td>
</tr>
<tr>
<td>SAML Authentication Flow using SafeNet Authentication Service</td>
<td>6</td>
</tr>
<tr>
<td>SAML Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td>Configuring PingFederate</td>
<td>6</td>
</tr>
<tr>
<td>Downloading the SAS Metadata</td>
<td>6</td>
</tr>
<tr>
<td>Configuring SAS as an Identity Provider</td>
<td>7</td>
</tr>
<tr>
<td>Downloading the SafeNet Identity Provider Certificate</td>
<td>22</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>23</td>
</tr>
<tr>
<td>Synchronizing Users Stores to SafeNet Authentication Service</td>
<td>23</td>
</tr>
<tr>
<td>Assigning an Authenticator in SafeNet Authentication Service</td>
<td>23</td>
</tr>
<tr>
<td>Exporting the PingFederate Metadata</td>
<td>24</td>
</tr>
<tr>
<td>Adding PingFederate as a Service Provider (SP) in SafeNet Authentication Service</td>
<td>27</td>
</tr>
<tr>
<td>Enabling SAML Services in SafeNet Authentication Service</td>
<td>30</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>35</td>
</tr>
<tr>
<td>Appendix: Deploying PingFederate Quick-Start Applications</td>
<td>37</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>38</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 PingFederate.

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.

PingFederate is a full-featured federation server that provides identity management, web single sign-on, and API security for customers, partners, and employees. Users can securely access the applications they require with a single identity using any device. Supporting all of the current identity standards including SAML, WS-Federation, WS-Trust, OAuth, and OpenID Connect, PingFederate is recognized as a leading federation product today that also future-proofs your business for tomorrow.

This document describes how to:

- Configure SAML authentication in PingFederate using SafeNet Authentication Service as an identity provider.

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

PingFederate 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 (SAS)**—SafeNet’s cloud-based authentication service
- **PingFederate**—Version 7.3.0
- **PingFederate Quick-Start Demo Apps**—Version 1.1

## Audience

This document is targeted to system administrators who are familiar with PingFederate, 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 Protocol Diagram](image)

## 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 PingFederate.

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

SAML Prerequisites

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

Configuring PingFederate

To add SafeNet Authentication Service as an identity provider in PingFederate requires:

- Downloading the SAS Metadata, page 6
- Configuring SAS as an Identity Provider, page 7
- Downloading the SafeNet Identity Provider Certificate, page 22

Downloading the SAS Metadata

1. Browse to the https://idp1.cryptocard.com/idp/shibboleth URL.
2. The SAS metadata will automatically download. Save it locally on your machine.
Configuring SAS as an Identity Provider

1. Log in to the PingFederate administrative console as an administrator using the following URL:
   https://<DNS_NAME or IP Address of PingFederate Server>:9999/pingfederate/app
   where DNS_NAME is a fully-qualified name of the machine running the PingFederate server.

2. Under IDP CONNECTIONS, click Create New.

3. On the Connection Type tab, select Browser SSO Profiles, and then click Next.

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
4. On the **Connection Options** tab, ensure that **Browser SSO** is selected, and then click **Next**.

![Connection Options Tab](image1)

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

5. On the **Import Metadata** tab, click **Browse**, select the SAS metadata you downloaded in “Downloading the SAS Metadata” on page 6, and then click **Next**.

![Import Metadata Tab](image2)

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

6. On the **Metadata Summary** tab, click **Next**.

![Metadata Summary Tab](image3)

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
7. On the **General Info** tab, the **Partner's Entity ID**, **Connection Name**, and **Base URL** fields are populated from the metadata file. You can change **Connection Name**, as this is an identifier for this connection. Click **Next**.

8. On the **Browser SSO** tab, click **Configure Browser SSO**.

9. On the **SAML Profiles** tab, select **SP-Initiated SSO** and **SP-Initiated SLO** (enabled after selecting SSO profiles), and then click **Next**.
10. On the User-Session Creation tab, click Configure User-Session Creation.

![User-Session Creation Tab](image)

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

11. On the Identity Mapping tab, select the Account Mapping option, and then click Next.

![Identity Mapping Tab](image)

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

12. On the Attribute Contract tab, a set of user attributes is displayed that the IdP will send in the assertion. Click Next.

![Attribute Contract Tab](image)

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
13. On the **Target Session Mapping** tab, map an adapter instance for each target application on your system. Click **Map New Adapter Instance**.

!(image)

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

14. On the **Adapter Instance** tab, in the **ADAPTER INSTANCE** field, select **SP Adapter**, and then click **Next**.

!(image)

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

15. On the **Adapter Data Store** tab, select the **Use only the attribute available in the SSO Assertion** option, and then click **Next**.

!(image)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
16. On the **Adapter Contract Fulfillment** tab, for each of the attributes, complete the following steps, and then click **Next**.

   a. In the **SOURCE** column, select **Assertion**.

   b. In the **VALUE** column, select the required value.

   ![Adapter Contract Fulfillment Tab](image)

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

17. On the **Issuance Criteria** tab, click **Next**.

   ![Issuance Criteria Tab](image)

   *(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
18. On the **Summary** tab, click **Done**. You are returned to the **Target Session Mapping** tab.

19. On the **Target Session Mapping** tab, click **Next**.

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
20. On the **Summary** tab, review the configured session settings, and then click **Done**. You are returned to the **User-Session Creation** tab.

21. On the **User-Session Creation** tab, click **Next**.

23. On the SSO Service URLs tab, perform the following steps, and then click Next:
   c. In the BINDING column, select POST.
   d. In the ENDPOINT URL column, enter https://idp1.cryptocard.com/idp/profile/SAML2/POST/SSO.
   e. In the ACTION column, click Add.

24. On the SLO Service URLs tab, perform the following steps, and then click Next:
   f. In the BINDING column, select POST.
   g. In the ENDPOINT URL column, enter https://idp1.cryptocard.com/idp/signout.jsp.
   h. In the RESPONSE URL column, do not enter anything.
   i. In the ACTION column, click Add.
25. On the **Allowable SAML Bindings** tab, select **POST**, and then click **Next**.

![Allowable SAML Bindings](image1)

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

26. On the **Default Target URL** tab, in the **Default Target URL** field, enter `https://<PingFederate IP Address>:9031/quickstart-app-sp/go`, and then click **Next**.

![Default Target URL](image2)

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

27. On the **Signature Policy** tab, select **Use SAML-standard signature requirements**, and then click **Next**.

![Signature Policy](image3)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
28. On the **Encryption Policy** tab, select **None**, and then click **Next**.

![Encryption Policy](image1)

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

29. On the **Summary** tab, click **Done**. You are returned to the **Protocol Settings** tab.

![Summary](image2)

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

30. On the **Protocol Settings** tab, click **Next**.

![Protocol Settings](image3)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
31. On the **Summary** tab, click **Done**. You are returned to the **Browser SSO** tab.

![Summary Tab](Image)

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

32. On the **Browser SSO** tab, click **Next**.

![Browser SSO Tab](Image)

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

33. On the **Credentials** tab, click **Configure Credentials**.

![Credentials Tab](Image)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
34. On the **Digital Signature Settings** tab, define the private key/certificate that will be used to sign assertions and SLO messages for this SP. Perform the following steps, and then click **Next**:

j. In the **Signing Certificate** field, select your PingFederate server’s signing certificates that you will use to sign SAML requests, responses, and assertions.

k. In the **Signing Algorithm** field, select **RSA SHA256**.

35. On the **Signature Verification Settings** tab, click **Manage Signature Verification Settings**.

36. On the **Trust Model** tab, select **Unanchored**, and then click **Next**.
37. On the **Signature Verification Certificate** tab, in the **Primary** field, select the partner certificate, and then click **Next**.

![Signature Verification Certificate tab](image)

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

38. On the **Summary** tab, click **Done**. You are returned to the **Signature Verification Settings** tab.

![Summary tab](image)

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

39. On the **Signature Verification Settings** tab, click **Next**.

![Signature Verification Settings tab](image)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
40. On the **Summary** tab, review the credentials configurations, and then click **Done**. You are returned to the **Credentials** tab.

![Summary tab](image)

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

41. On the **Credentials** tab, click **Next**.

![Credentials tab](image)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
42. On the Activation & Summary tab, in the Connection Status field, select Active, and then click Save.

![Activation & Summary Tab](image)

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

**Downloading the SafeNet Identity Provider Certificate**

1. Browse to the https://cloud.safenet-inc.com/console/cert/idp.crt URL.
2. The SafeNet IDP Certificate will automatically download. Save it locally on your machine.
Configuring SafeNet Authentication Service

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

- Synchronizing Users Stores to SafeNet Authentication Service, page 23
- Assigning an Authenticator in SafeNet Authentication Service, page 23
- Exporting the PingFederate Metadata, page 24
- Adding PingFederate as a Service Provider (SP) in SafeNet Authentication Service, page 27
- Enabling SAML Services in SafeNet Authentication Service, page 30

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 PingFederate.

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.


### Exporting the PingFederate Metadata

1. Open the PingFederate administrative console using the following URL:
   
   https://<DNS_NAME or IP of PingFederate Server>:9999/pingfederate/app
   
   where DNS_NAME is a fully-qualified name of the machine running the PingFederate server.

2. Under ADMINISTRATIVE FUNCTIONS, click Metadata Export.

   ![Metadata Export](image)

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

3. On the Metadata Role tab, select I am the Service Provider (SP), and then click Next.
4. On the Metadata Mode tab, select Use a connection for metadata generation, and then click Next.

5. On the Connection Metadata tab, perform the following steps:
   a. Select the connection (for example, SAS) for which you want to create metadata. (You created a connection in “Configuring SAS as an Identity Provider” on page 7.) After selecting the connection, the remaining fields are automatically populated.
   b. Click Next.

6. On the Metadata Signing tab, in the Signing Certificate field, select a certificate, and then click Next.
7. On the Export & Summary tab, click Export, and then save the PingFederate metadata file. Click Done.
Adding PingFederate 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 PingFederate. You will need the <metadata/Issuer ID and assertion consumer URL location of PingFederate>.

To add PingFederate as a Service Provider 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML 2.0 Settings</td>
<td>Create and configure SafeNet Authentication Service SAML Settings.</td>
</tr>
</tbody>
</table>

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

   **Friendly Name**
   - Enter the PingFederate name.

   **SAML 2.0 Metadata**
   - a. Select **Upload Existing Metadata File**.
   - b. Click **Choose File**, and then browse to select the PingFederate metadata file that you downloaded in step 7 on page 26. Click **Open**.

   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>
</tbody>
</table>
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

http://schemas.xmlsoap.org/claims/CommonName

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier

principal

According to Third Party Product Requirements

PingFederate is added as a service provider in the system.
Enabling SAML Services in SafeNet Authentication Service

After PingFederate 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.

![User ID search](image)

4. Click **SAML Services**.

![SAML Services](image)

5. Click **Add**.
6. Under **Add SAML Service**, do the following:
   
c. From the **Service** menu, select the **PingFederate** service provider.

d. In **SAML Login ID** field, select the type of login ID (User ID, E-mail, or Custom) to be sent as a UserID to PingFederate in the response.

e. Click **Add**.

The user can now authenticate to PingFederate 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>Groups</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>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Parties</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>SAML Login ID</td>
<td>Select <strong>User ID</strong>. The User ID will be returned to the service provider in the SAML assertion.</td>
</tr>
</tbody>
</table>

The diagram shows the SAML Provisioning Rules interface with options for adding a new rule, changing the log, and canceling. It includes sections for rule name, user container search, and group and party selection. The SAML Login ID is highlighted as a feature to select the User ID.
Running the Solution

In the PingFederate quick-start demo application, the service provider quick-start application provides a service provider web page to access the SP-initiated SSO. Ensure that you have deployed the quick-start components and started the PingFederate server.

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

1. Open the following URL in a web browser: https://<DNS_NAME or IP>:9031/quickstart-app-sp/go
   where DNS_NAME or IP is the fully-qualified name or IP address of the machine running the PingFederate server.

2. In the IdP Partner field, select the identity provider that you have already configured (for example, SAS), and then click Single Sign-On.

3. You are redirected to the SAS Login page. In the User Name field, enter your user name, and then click Login.
4. The challenge grid is displayed. In the **Password** field, enter the characters from the grid that correspond to your PIP (personal identification pattern), and then click **Login**.

![Login Screen](image)

After successful authentication, you are logged in. The page that displays represents the protected “target” resource of the SSO transaction.

**My Service Provider**
**Quick-Start Application**

![User Attributes Screen](image)

Welcome, Alice.

You have successfully signed on to this Service Provider (SP) site using SSO — your identity has been verified by the Identity Provider (IdP) who maintains your login credentials.

The IdP has also sent along some information about you ("User Attributes" at left), which a real partner SP would use to enhance and streamline your experience at its site.

You can now either log out of this SP session locally (using the link in the navigation bar above) or log out globally (using the Single Logout links below, which exercise different SAML bindings). If you log out locally, you will not have to sign on at the IdP site again to reach this domain via SSO, since your IdP session is still active. Single logout ends both your IdP and SP sessions, and you will be asked to log on again at the IdP.

**Note**: The "Terminate Account Link" hyperlink (at left) causes an error unless you modify the SP configuration to enable account linking, which establishes a persistent association between two accounts for the same user in different domains.

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
Appendix: Deploying PingFederate Quick-Start Applications

This section describes how to deploy the PingFederate quick-start components. After installing PingFederate, configure the PingFederate server and deploy the demo applications.

1. Download the PingFederate Quick-Start Demo application from:

2. If you have not already done so, install the PingFederate server.

3. From the quick-start distribution directory, copy the following files into the
   
   `<pf_install_dir>/pingfederate/server/default/deploy` directory in your PingFederate installation:
   - `quickstart-app-idp.war`
   - `quickstart-app-sp.war`
   - `json-simple-1.1.jar`
   - `pf-referenceid-adapter-1.0.jar`

4. From the quick-start distribution directory, copy the `data.zip` file into:
   
   `<pf_install_dir>/pingfederate/server/default/data/drop-in-deployer`

5. Stop and restart the PingFederate server if it is running.
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</td>
</tr>
<tr>
<td></td>
<td>manage incidents, get the latest software</td>
</tr>
<tr>
<td></td>
<td>upgrades, and access the Gemalto Knowledge</td>
</tr>
<tr>
<td></td>
<td>Base.</td>
</tr>
</tbody>
</table>