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.

© 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-013149-001, Rev. C
Release Date: September 2017
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-PCE5 
SAML Authentication Flow using SafeNet Authentication Service .............................................................. 6
SAML Prerequisites ................................................................................................................................... 6
Configuring PingFederate .......................................................................................................................... 6
  Deploying PingFederate Quick Start Demo Applications ................................................................. 6
  Downloading the SafeNet Authentication Service Metadata .......................................................... 7
  Downloading the SafeNet Identity Provider Certificate ............................................................... 7
  Configuring SafeNet Authentication Service as an Identity Provider in PingFederate ..................... 7
  Exporting the PingFederate Metadata ............................................................................................... 24
Configuring PingFederate with PingFederate Apache (Windows) Integration Kit .............................. 27
  Installing the OpenToken Adapter and Configuring PingFederate .................................................. 27
  Installing and Configuring the Apache Agent ................................................................................ 35
Configuring SafeNet Authentication Service ........................................................................................... 36
  Synchronizing Users Stores to SafeNet Authentication Service .................................................... 36
  Assigning an Authenticator in SafeNet Authentication Service .................................................... 36
  Adding PingFederate as a Service Provider (SP) in SafeNet Authentication Service ............... 37
  Enabling SAML Services in SafeNet Authentication Service ....................................................... 41
Running the solution ................................................................................................................................ 46
  Using Quick-start Demo Application .............................................................................................. 46
  Using PingFederate Apache (Windows) Integration Kit ................................................................ 48
Appendix: Configuring mod_pf.conf file ............................................................................................... 49
Support Contacts .................................................................................................................................... 51
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 (SSO) 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:

- Deploy multifactor authentication (MFA) options in PingFederate using SafeNet OTP authenticators managed by SafeNet Authentication Service.
- 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**—On Cloud
• PingFederate—Version 8.1.3
• PingFederate Quickstart Demo Apps—Version 1.1
• PingFederate Apache (Windows) Integration Kit—Version 1.2.1
• Apache HTTP Server—Version 2.2.31

**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 (SAS).

**SAML Authentication using SafeNet Authentication Service Cloud**

SafeNet Authentication Service (SAS) Cloud provides a service for SAML authentication that is already implemented in the SafeNet Authentication Service (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, SafeNet Authentication Service 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 Gemalto 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). SAS collects and evaluates the user's credentials.
2. SafeNet Authentication Service (SAS) returns a response to PingFederate, accepting or rejecting the user's authentication request.

SAML Prerequisites

1. To enable SafeNet Authentication Service to receive SAML authentication requests from PingFederate, ensure that the end users can authenticate through from the PingFederate environment with a static password.
2. An Apache server with an application hosted on it must be up and running.

Configuring PingFederate

Adding SafeNet Authentication Service (SAS) as an Identity Provider in PingFederate requires:

- Deploying PingFederate Quick Start Demo Applications, page 6
- Downloading the SafeNet Authentication Service Metadata, page 7
- Downloading the SafeNet Identity Provider Certificate, page 7
- Configuring SafeNet Authentication Service as an Identity Provider in PingFederate, page 7
- Exporting the PingFederate Metadata, page 24

Deploying PingFederate Quick Start Demo Applications

After installing PingFederate, perform the following steps to configure the PingFederate server and deploy the demo applications:

1. In a web browser, open the following URL to download the PingFederate quick-start demo applications:
2. Go to the quick-start distribution directory that you downloaded in the previous step, copy the following files, and then paste them to the <pingfederate installation directory>
/</pingfederate/server/default/deploy directory:

- quickstart-app-idp.war
- quickstart-app-sp.war
- json-simple-1.1.jar
- pf-referenceid-adapter-1.0.jar

3. Go to the quick-start distribution directory, copy the data.zip file, and then paste it to the following directory:

<pingfederate installation directory>/pingfederate/server/default/data/drop-in-deployer

4. Stop and restart the PingFederate server.

**Downloading the SafeNet Authentication Service Metadata**

To download the SafeNet Authentication Service (SAS) metadata, browse to the https://idp1.cryptocard.com/idp/shibboleth URL. It will automatically download the SafeNet Authentication Service metadata. Save it locally on your machine.

**Downloading the SafeNet Identity Provider Certificate**

To download the SafeNet Identity Provider Certificate, browse to the https://cloud.safenet-inc.com/console/cert/idp.crt URL. It will automatically download the SafeNet IDP certificate. Save it locally on your machine.

**Configuring SafeNet Authentication Service as an Identity Provider in PingFederate**

Perform the following steps to add SafeNet Authentication Service as an Identity Provider in PingFederate:

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

   https://<DNS_NAME or IP Address of PingFederate Server>:9999/pingfederate/app

   Where, DNS_NAME is the fully-qualified name of the machine on which the PingFederate server is running.
2. On the PingFederate Administrative Login window, enter your administrator username and password, and then click Login.

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

NOTE: If you are running the server console for the first time, enter the default username and password.

3. After successful login, the PingFederate dashboard is displayed. In the left pane, click SP Configuration.

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

4. In the right pane, under IDP CONNECTIONS, click Create New.

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
5. Under **IdP Connection**, on the **Connection Type** tab, select **BROWSER SSO PROFILES**, and then click **Next**.

   ![IdP Connection](image1.png)

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

6. On the **Connection Options** tab, ensure that **BROWSER SSO** is selected, and then click **Next**.

   ![IdP Connection](image2.png)

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

7. On the **Import Metadata** tab, perform the following steps:
   a. In the **METADATA** field, select **FILE**.
   b. Click **Choose File** to search for and select the SAS Metadata file to be downloaded.
   c. Click **Next**.

   ![IdP Connection](image3.png)

   *(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
8. On the **Metadata Summary** tab, click **Next**.

![Metadata Summary tab](image)

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

9. On the **General Info** tab, values in the **PARTNERS ENTITY ID (CONNECTION ID)**, **Connection Name**, and **Base URL** fields are populated from the metadata file. In the **Connection Name** field, you can change the connection name (for example, **SAS**) as this is an identifier for this connection. Click **Next**.

![General Info tab](image)

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

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

![Browser SSO tab](image)

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

11. Under **Browser SSO**, on the **SAML Profiles** tab, perform the following steps:
   a. Under **Single Sign-On (SSO) Profiles**, select **IDP-INITIATED SSO** and **SP-INITIATED SSO**.
   b. Under **Single Logout (SLO) Profiles**, select **SP-INITIATED SLO**. It is enabled after selecting SSO profiles.
c. Click **Next**.

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

12. On the **User-Session Creation** tab, click **Configure User-Session Creation** to:

- Choose an identity-mapping method.
- Define the attribute contract that you will use with this partner, if any.
- Configure instances of one or more target sessions and specifying how they are used to fulfill the contract.

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

13. Under **User-Session Creation**, on the **Identity Mapping** tab, select the **ACCOUNT MAPPING** option, and then click **Next**.

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
14. On the **Attribute Contract** tab, a set of user attributes are displayed that 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.)

15. On the **Target Session Mapping** tab, click **Map New Adapter Instance** to map an adapter instance for each target application on your system.

![Target Session Mapping tab](image)

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

16. Under **Adapter Mapping & User Lookup**, on the **Adapter Instance** tab, in the **ADAPTER INSTANCE** field, select **SP Adapter**, and then click **Next**.

![Adapter Instance tab](image)

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
17. On the **Adapter Data Store** tab, select **USE ONLY THE ATTRIBUTES AVAILABLE IN THE SSO ASSERTION** option, and then click **Next**.

![Adapter Data Store Tab](image)

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

18. On the **Adapter Contract Fulfillment** tab, for each attribute, perform the following steps:
   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.*

19. Click **Next**.

20. 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.*
21. On the **Summary** tab, review the configuration, and then click **Done**.

![Adapter Mapping Summary](image)

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

22. Under **User-Session Creation**, on the **Target Session Mapping** tab, click **Next**.

![IdP Connection | Browser SSO | User-Session Creation](image)

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

23. On the **Summary** tab, review the configuration, and then click **Done**.

![Target Session Mapping](image)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
24. Under **Browser SSO**, on the **User-Session Creation** tab, click **Next**.

![User-Session Creation Tab](image)

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

25. On the **Protocol Settings** tab, click **Configure Protocol Settings**.

![Configure Protocol Settings](image)

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

26. Under **Protocol Settings**, on the **SSO Service URLs** tab, perform the following steps:

   a. In the **Binding** column, select **POST**.
   c. In the **Action** column, click **Add**.
   d. In the **Binding** column, select **Redirect**.
   e. In the **Endpoint URL** column, enter `https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO`.
f. In the Action column, click Add.

g. Click Next.

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

27. On the SLO Service URLs tab, perform the following steps:

a. In the Binding column, select POST.


c. Leave the Response URL column blank.

d. In the Action column, click Add.

e. Click Next.

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

28. On the Allowable SAML Bindings tab, select POST, and then click Next.

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

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

30. On the **Signature Policy** tab, select **USE SAML-STANDARD SIGNATURE REQUIREMENTS**, and then click **Next**.

![Signature Policy Configuration](image)

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

31. On the **Encryption Policy** tab, select **NONE**, and then click **Next**.

![Encryption Policy Configuration](image)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
32. On the **Summary** tab, click **Done**.

![Summary tab screenshot](image)

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

33. Under **Browser SSO**, on the **Protocol Settings** tab, click **Next**.

![Protocol Settings tab screenshot](image)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
34. On the **Summary** tab, review the configuration, scroll down, and then click **Done**.

![Summary tab](image)

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

35. Under **IdP Connection**, 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.)*

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

![Configure Credentials](image)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
37. Under **Credentials**, on the **Back-Channel Authentication** tab, click **Configure**.

![Configure](image)

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

38. Under **Back-Channel Authentication**, on the **Outbound SOAP Authentication Type** tab, select **DIGITAL SIGNATURE (BROWSER SSO PROFILE ONLY)** to sign the message, and then click **Next**.

![Outbound SOAP Authentication Type](image)

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

39. On the **Summary** tab, click **Done**.

![Summary](image)

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

40. Under **Credentials**, on the **Back Channel Authentication** tab, click **Next**.

![Back Channel Authentication](image)

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

41. On the **Digital Signature Settings** tab, define the private key/certificate that will be used to sign assertions and SLO messages for the service provider. Perform the following steps:

   a. In the **SIGNING CERTIFICATE** field, select your PingFederate server’s signing certificate that you will use to sign SAML requests, responses, and assertions.

   b. In the **SIGNING ALGORITHM** field, select **RSA SHA256**.
c. Click **Next**.

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

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

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

43. Under **Signature Verification**, on the **Trust Model** tab, select the **UNANCHORED** option, and then click **Next**.

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
44. On the **Signature Verification Certificate** tab, in the **PRIMARY** field, select the partner certificate, and then click **Next**.

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

45. On the **Summary** tab, click **Done**.

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

46. Under **Credentials**, on the **Signature Verification Settings** tab, click **Next**.

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
47. On the **Summary** tab, review the configuration, and then click **Done**.

![Summary Tab](image1.png)

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

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

![Credentials Tab](image2.png)

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

49. On the **Activation & Summary** tab, in the **Connection Status** field, select the **ACTIVE** option, scroll down, and then click **Save**.

![Activation & Summary Tab](image3.png)

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

Perform the following steps to export the PingFederate metadata:

1. In web browser, open the following URL to log in to the PingFederate administrator console:
   https://<DNS_NAME or IP of PingFederate Server>:9999/pingfederate/app
   Where DNS_NAME is a fully-qualified name of the machine on which the PingFederate server is running.
2. On the PingFederate administrator console, in the left pane, click Server Configuration.

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

3. In the right pane, under Server Configuration, under ADMINISTRATIVE FUNCTIONS, click Metadata Export.

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

4. On the Export Metadata window, on the Metadata Role tab, select the I AM THE SERVICE PROVIDER (SP) option, and then click Next.

   (The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
5. On the **Metadata Mode** tab, select the **USE A CONNECTION FOR METADATA GENERATION** option, and then click **Next**.

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

6. On the **Connection Metadata** tab, perform the following steps:
   a. In the dropdown list, select the connection we created (for example, **SAS**) in step 9 of “Configuring SafeNet Authentication Service as an Identity Provider in PingFederate” on page 7, for which you want to create metadata.
   b. Click **Next**.

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

7. On the **Metadata Signing** tab, in the **SIGNING CERTIFICATE** field, select a certificate, and then click **Next**.

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

8. On the **Export & Summary** tab, scroll down, and then click **Export**.
9. Save the PingFederate metadata file.

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
Configuring PingFederate with PingFederate Apache (Windows) Integration Kit

Configuring PingFederate with PingFederate Apache (Windows) Integration Kit requires:

- Installing the OpenToken Adapter and Configuring PingFederate, page 27
- Installing and Configuring the Apache Agent, page 35

NOTE:
- The Apache http server must be installed and configured with a virtual host file hosted on it.
- Download the PingFederate Apache (Windows) Integration Kit from the following link.
- Run Microsoft Visual C++ 2005 Redistributable Package (x86). The package is available at the following URL:

Installing the OpenToken Adapter and Configuring PingFederate

1. Stop the PingFederate server.
2. Open the following directory, and then remove any existing OpenToken Adapter files (for example, opentoken*.jar).
   ```
   <PF_install>/pingfederate/server/default/deploy
   ```
   Where, `<PF_install>` is the PingFederate installation directory.
3. Unzip the integration-kit distribution file that you downloaded from the PingFederate site.
4. In the integration-kit, from the `/dist` directory, copy the `opentoken-adapter-2.5.1.jar` file, and then paste it to the following PingFederate directory:
   ```
   <PF_install>/pingfederate/server/default/deploy
   ```
5. Start the PingFederate server.
6. In web browser, open the following URL to log in to the PingFederate administrator console:
   ```
   https://<DNS_NAME or IP of PingFederate Server>:9999/pingfederate/app
   ```
   Where `DNS_NAME` is a fully-qualified name of the machine on which the PingFederate server is running.
7. On the PingFederate administrator console, in the left pane, click SP Configuration.
8. In the right pane, under **APPLICATION INTEGRATION**, click **Adapters**.

![Image](image1.png)

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

9. On the **Manage SP Adapter Instances** window, click **Create New Instance**.

![Image](image2.png)

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

10. Under **Create Adapter Instance**, on the **Type** tab, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th><strong>INSTANCE NAME</strong></th>
<th>Enter a name for the instance (for example, <strong>apache</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INSTANCE ID</strong></td>
<td>Enter a unique ID for the instance (for example, <strong>apache</strong>).</td>
</tr>
<tr>
<td><strong>TYPE</strong></td>
<td>Select <strong>opentoken adapter</strong>.</td>
</tr>
</tbody>
</table>

![Image](image3.png)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.*)
11. On the Instance Configuration tab, perform the following steps:
   a. In the PASSWORD field, enter a password.
   b. In the CONFIRM PASSWORD field, re-enter the password.
   c. Click Next.

12. On the Actions tab, in the Action Invocation Link column, click Download to download the agent configuration file.

13. On Actions tab, click Export to export the agent configuration file, save the file on the local machine, and then click Reset.

14. Click Next.
15. On the **Extended Contract** tab, click **Next**.

16. On the **Summary** tab, review the configuration information of SP adapter instance, and then click **Done**.

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
17. On the Manage SP Adapter Instances window, click **Save** to save the configured SP adapter instance.

![Manage SP Adapter Instances](image1.png)

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

18. If you have more than one adapter, you need to configure the Target URL mapping. To configure the target URL mapping, on the PingFederate administrator console, in the left pane, click **SP Configuration**.

19. In the right pane, under APPLICATION INTEGRATION, click **Target URL Mapping**.

![Target URL Mapping](image2.png)

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

20. Under **Target URL Mapping**, perform the following steps:

   a. In the **URL** column, enter your target URL.

      For example, if you map the virtual host on the apache server with the **www.example.com** URL and the .html file of the virtual host is **hello.html**, then the target URL mapping will be, **http://www.example.com/hello.html**.

   b. In the **Target Type** column, select **SP Adapter**.

   c. In the **Target Session** column, select the **Instance ID** (for example, **apache**) of the adapter that you configured in step 10.

   d. In the **Action** column, click **Add Mapping**.

   e. Click **Save**.

![Target URL Mapping](image3.png)

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

21. On the PingFederate administrator console, in the left pane, click **SP Configuration**.
22. In the right pane, click **Default URLs**.

23. Under **SP Default URLs**, for successful **SSO** and **SLO**, enter the **URL** that you entered in step 20, and then click **Save**.

24. In the left pane, click **SP Configuration**.

25. In the right pane, under **IDP CONNECTIONS**, click the identity provider name (for example, **SAS**) that you entered in step 9 of "Configuring SafeNet Authentication Service as an Identity Provider in PingFederate" on page 7.

26. On the **summary** tab, under **User Session Creation**, click **Target Session Mapping**.
27. On the **Target Session Mapping** tab, click **Map New Adapter Instance**.

![Target Session Mapping](image)

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

28. Under **Adapter Mapping & Use Lookup**, on the **Adapter Instance** tab, in the **ADAPTER INSTANCE** field, select the **Instance ID** (for example, *apache*) of the adapter that you configured in step 10, and then click **Next**.

![Adapter Instance](image)

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

29. On the **Adapter Data Store** tab, Select **USE ONLY THE ATTRIBUTES AVAILABLE IN THE SSO ASSERTION**, and then click **Next**.

![Adapter Data Store](image)

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

30. On the **Adapter Contract Fulfilment** tab, perform the following steps:
   a. In the **Source** column, select **Assertion**.
   b. In the **Value** column, select **SAML_SUBJECT**.
c. **Click Next.**

![Screen Image](image_url)

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

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

![Screen Image](image_url)

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

32. **On the Summary tab, review the adapter mapping summary, and then click Save.**

![Screen Image](image_url)

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

33. **On the PingFederate administrator console, in the left pane, click SP Configuration.**
34. In the right pane, under **IDP CONNECTIONS**, click the identity provider name (for example, **SAS**) that you entered in step 9 of “Configuring SafeNet Authentication Service as an Identity Provider in PingFederate” on page 7.

35. On the **Summary** tab, under **Target Session Mapping**, ensure that the new adapter (for example, **apache**) is listed.

### Installing and Configuring the Apache Agent

1. Open the integration-kit distribution folder.
2. Copy the content of the `/dist/apache-agent/lib` directory to the `/modules` directory of the Apache server.
3. In the integration-kit, in the `/dist` directory, copy the `zlib1.dll` and `libeay32.dll` files, and then paste the files to the folder in your system PATH.

   **NOTE:** The recommended deployment is to place these files in the Apache modules directory, along with the shared object files, and then add the directory to the system PATH.

   The PingFederate Apache agent is represented by the **mod_pf.so** Apache module and an auxiliary OpenToken library. The behavior of the agent is controlled by the properties present in the **mod_pf.conf** file.

4. Open the `/dist/apache-agent/config` directory, copy the **mod_pf.conf**, **start_page_template.html**, and **error_page_template.html** files, and then paste the files in the `/conf` directory of your Apache server installation directory.

   **NOTE:** The **mod_pf.conf** file must be configured (Refer Appendix: Configuring mod_pf.conf file, page 49).
5. Copy the `config` file (that you downloaded while configuring the PingFederate adapter in step 12 of “Installing the OpenToken Adapter and Configuring PingFederate” on page 27), and then paste it to the `/conf` directory of the Apache installation directory.

6. Restart the Apache server.

7. Go to `/conf` directory and then open the `httpd.conf` file in the notepad.

8. In the `httpd.conf` file, at the end of the `LoadModule` lines, copy the following lines:

   ```
   PingFederateConfigurationFile conf/mod_pf.conf
   LoadFile modules/libopentoken.so
   LoadModule pf_module modules/mod_pf.so
   ```

9. Save the file.

10. Restart the Apache server.

### Configuring SafeNet Authentication Service

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

- Synchronizing Users Stores to SafeNet Authentication Service, page 36
- Assigning an Authenticator in SafeNet Authentication Service, page 36
- Adding PingFederate as a Service Provider (SP) in SafeNet Authentication Service, page 37
- Enabling SAML Services in SafeNet Authentication Service, page 41

### 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:

- **Manually provision** – 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 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 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.

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

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>Enter the PingFederate name.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SAML 2.0 Metadata</strong></td>
<td>Select <strong>Upload Existing Metadata File</strong>. Click <strong>Choose File</strong> to search for and select the Service Provider’s metadata file, and then click <strong>Open</strong>.</td>
</tr>
</tbody>
</table>

**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 Providers” in the SAML Authentication Quick Start Guide:

6. 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>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td>principal</td>
<td>According to ThirdParty Product Requirements</td>
</tr>
</tbody>
</table>
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 the 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**, perform the following steps:
   a. In the **Service** menu, select the PingFederate 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 User ID to PingFederate in the response.
   c. Click **Add**.

   ![SafeNet Authentication Service console](image)

   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.

![SafeNet Authentication Service console](image)
2. Click the **POLICY** tab, and then click **Automation Policies**.

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

4. Click **New Rule**.
5. Complete 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 <em>Virtual Server Groups</em> 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 <em>Used by rule</em> box.</td>
</tr>
<tr>
<td><strong>Parties</strong></td>
<td>The <em>Relying Parties</em> 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 <em>Rule Parties</em> box.</td>
</tr>
<tr>
<td><strong>SAML Login ID</strong></td>
<td>Select User ID. The User ID will be returned to the service provider in the SAML assertion.</td>
</tr>
</tbody>
</table>
Running the solution

For this integration, the SafeNet GrIDsure token is configured for authentication with SafeNet Authentication Service (SAS).

Using Quick-start Demo Application

In the PingFederate quick-start demo application, the quick-start application of the service provider 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.

1. In a web browser, open the following URL:
   
   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 on which the PingFederate server is running.

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

   (The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
3. You will be redirected to the SafeNet Authentication Service login page. In the **User Name** field, enter your user name, and then click **Login**.

![Login page](image)

4. In the **Password** field, enter your preferred grid pattern, and then click **Login**.

![Password grid](image)
After successful authentication, you are logged in and the following window is displayed that represents the protected “target” resource of the SSO transaction.

Using PingFederate Apache (Windows) Integration Kit

1. In a web browser, open the following URL which is given under Target URL Mapping in step 20 of “Installing the OpenToken Adapter and Configuring PingFederate” on page 27.
   For example, www.example.com/hello.html

2. You will be redirected to the SafeNet Authentication Service login window. In the User Name field, enter your user name, and then click Login.
3. In the **Password** field, enter your preferred grid pattern, and then click **Login**.

![Login](image)

After successful authentication, the virtual host page is displayed that was hosted on the Apache http server.

**Appendix: Configuring mod_pf.conf file**

Perform the following steps to configure the **mod_pf.conf** file:

1. In the Apache installation directory, in the `/conf` directory, open the **mod_pf.conf** file.
2. In the **mod_pf.conf** file, search for `pingfederatefileter`, and then replace `(\?i).*/*example_app/.` with `(\?i).*/`
3. Search for `pingfederateloginpageurl` and then replace

   ```
   http://pfhost.example.com:9031/sp/startSSO.ping?partnerSpId=example
   ```

   with

   ```
   http://<ipaddress of pingfederate>:9031/sp/startSSO.ping?PartnerIdpID=<entity id of our IDP>
   ```

   Where,
   - `<ipaddress of pingfederate>` is the IP address PingFederate server.
   - `<entity id of our IDP>` is the SAS entity ID.

**NOTE:** In a web browser, open the following link to access the Configuring Apache Integration Kit guide.

https://documentation.pingidentity.com/display/apachewin121/User+Guide

4. Search for the line, **PingFederateCookieDomain**, and then comment it out.
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</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></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>