SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol 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: 007-013259-001, Rev. A
Release Date: September 2015
## Contents

Third-Party Software Acknowledgement ........................................................................................................... 4
Description ......................................................................................................................................................... 4
Applicability ....................................................................................................................................................... 4
Environment ....................................................................................................................................................... 5
Audience ............................................................................................................................................................... 5
RADIUS-based Authentication using SAS Cloud ............................................................................................... 5
RADIUS-based Authentication using SAS-SPE and SAS-PCE ....................................................................... 6
RADIUS Authentication Flow using SAS ........................................................................................................... 6
RADIUS Prerequisites ....................................................................................................................................... 7
Configuring SafeNet Authentication Service ..................................................................................................... 7
  Creating Users Stores in SAS ........................................................................................................................... 7
  Assigning an Authenticator in SAS .................................................................................................................... 8
  Adding PingFederate as an Authentication Node in SAS .................................................................................. 9
  Checking the SAS RADIUS Server’s IP Address ............................................................................................. 11
Configuring PingFederate .................................................................................................................................. 12
  Creating a RADIUS Password Credential Validator ....................................................................................... 12
  Creating an HTML Form Identity Provider Adapter ......................................................................................... 16
  Creating a Composite Adapter ......................................................................................................................... 19
    Updating an Identity Provider Adapter in the Demo Service Provider (SP) Connection ................................. 24
Running the Solution ........................................................................................................................................... 28
Appendix: Deploying PingFederate Quick-Start Applications ........................................................................... 31
Troubleshooting ................................................................................................................................................ 31
Support Contacts ............................................................................................................................................... 32
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto 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:

- Deploy multi-factor authentication (MFA) options in PingFederate using SafeNet one-time (OTP) authenticators managed by SafeNet Authentication Service.
- Configure PingFederate to work with SafeNet Authentication Service in RADIUS mode.

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 RADIUS protocol 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 7.3.0.5
- **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.

RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.

- **Local RADIUS hosted on-premises**—A RADIUS agent that is implemented in the existing customer’s RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.

This document demonstrates the solution using the SAS cloud hosted RADIUS service.


For more details on how to install and configure FreeRADIUS, refer to the *SafeNet Authentication Service FreeRADIUS Agent Configuration Guide*. 
RADIUS-based Authentication using SAS-SPE and SAS-PCE

For both on-premises versions, SAS can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS)** or the legacy **Microsoft Internet Authentication Service (MS-IAS)**—SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.

  For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to the following document:


- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

### RADIUS Authentication Flow using SAS

SafeNet Authentication Service communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

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

1. A user attempts to log on to the web application deployed on the PingFederate service provider.
2. The user is redirected to PingFederate IDP for the first level of authentication.
3. After successful user authentication, PingFederate sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for the second level of validation.
4. The SAS authentication reply is sent back to PingFederate.
5. After successful user authentication on SAS, PingFederate IDP sends a SAML response to the service provider, and then the user is granted or denied access to the PingFederate web applications.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from PingFederate, ensure the following:

- End users can authenticate from the PingFederate environment with a static password before configuring PingFederate to use RADIUS authentication.
- Ports 1812/1813 are open to and from PingFederate.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.
- PingFederate Quick-Start demo applications should be deployed.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with PingFederate using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding PingFederate as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS Server’s IP Address, page 11

Creating Users Stores in SAS

Before SAS can authenticate any user in your organization, you must 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 additional details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.
Assigning an Authenticator in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through PingFederate.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet GOLD
- SMS Token
- MP-1 Software Token
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to "Provisioning Rules" in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.

Adding PingFederate as an Authentication Node in SAS

Add a RADIUS entry in the SAS Auth Nodes module to prepare it to receive RADIUS authentication requests from PingFederate. You will need the IP address of PingFederate and the shared secret to be used by both SAS and PingFederate.

1. Log in to the SAS console with an Operator account.

2. Click the COMMS tab, and then select Auth Nodes.

3. In the Auth Nodes module, click the Auth Nodes link.
4. Under **Auth Nodes**, click **Add**.

5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Description</td>
<td>Enter a host description.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the IP address of the host or the lowest IP address in a range of addresses that will authenticate with SAS.</td>
</tr>
<tr>
<td>Configure FreeRADIUS Synchronization</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td>Confirm Shared Secret</td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>

The authentication node is added to the system.
Checking the SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in PingFederate, check its IP address. The IP address will then be added to PingFederate as a RADIUS server at a later stage.

1. Log in to the SAS console with an Operator account.

2. Click the COMMS tab, and then select Auth Nodes.

3. In the Auth Nodes module, click the Auth Nodes link. The SAS RADIUS server details are displayed.
Configuring PingFederate

Before configuring PingFederate, ensure that the PingFederate quick-start demo applications are deployed and configured (refer to "..."
Appendix: Deploying PingFederate Quick-Start Applications* on page 31.

Configuring PingFederate requires the following:

- Creating a RADIUS Password Credential Validator, page 12
- Creating an HTML Form Identity Provider Adapter, page 16
- Creating a Composite Adapter, page 19
- Updating an Identity Provider Adapter in the Demo Service Provider (SP) Connection, page 24

Creating a RADIUS Password Credential Validator

The RADIUS Username/Password Credential Validator verifies credentials using the RADIUS protocol.

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 AUTHENTICATION, click Password Credential Validators.

   (The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
3. On the **Manage Credential Validators** tab, click **Create New Instance**.

   ![Create New Instance](image1)

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

4. On the **Type** tab, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instance Name</strong></td>
<td>Enter the name of the instance (for example, <strong>Radius</strong>).</td>
</tr>
<tr>
<td><strong>Instance Id</strong></td>
<td>Enter the instance identifier.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Select <strong>RADIUS Username Password Credential Validator</strong>.</td>
</tr>
<tr>
<td><strong>Parent Instance</strong></td>
<td>Select <strong>None</strong>.</td>
</tr>
</tbody>
</table>

   ![Type Tab](image2)

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

5. On the **Instance Configuration** tab, click **Add a new row to ‘RADIUS Servers’**.

   ![Instance Configuration](image3)

   *(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
6. Complete the following fields, click **Update**, and then click **Next**.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HOSTNAME</strong></td>
<td>Enter the IP address of the RADIUS server (SAS).</td>
</tr>
<tr>
<td><strong>AUTHENTICATION PORT</strong></td>
<td>Enter the User Datagram Protocol (UDP) port used to authenticate to the RADIUS server. The default value is 1812.</td>
</tr>
<tr>
<td><strong>AUTHENTICATION PROTOCOL</strong></td>
<td>Select the protocol used to authenticate to the RADIUS server.</td>
</tr>
<tr>
<td><strong>SHARED SECRET</strong></td>
<td>Enter the text shared between PingFederate and the RADIUS server (SAS) used to encrypt passwords. It should be same as mentioned in step 5 of “Adding PingFederate as an Authentication Node in SAS” on page 9.</td>
</tr>
</tbody>
</table>

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

7. On the **Extended Contract** tab, click **Next**.

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

   ![Summary Tab](image1.png)

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

9. On the **Manage Credential Validator Instances** tab, click **Save**.

   ![Manage Credential Validator Instances](image2.png)

   *(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
Creating an HTML Form Identity Provider Adapter

The RADIUS Password Credential Validator (RADIUS PCV)-backed HTML adapter is deployed in a composite adapter to achieve multi-level authentication. PingFederate packages an HTML Form Adapter that delegates user authentication to a configured RADIUS PCV.

Ensure that you have configured the RADIUS PCV.

1. On the PingFederate Administrative Console window, under APPLICATION INTEGRATION SETTINGS, click Adapters.

2. On the Manage IdP Adapter Instances tab, click Create New Instance.
3. On the **Type** tab, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Name</td>
<td>Enter the name of the instance.</td>
</tr>
<tr>
<td>Instance Id</td>
<td>Enter the instance identifier. The value must not contain spaces or underscores.</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>HTML Form IdP Adapter</strong>.</td>
</tr>
<tr>
<td>Parent Instance</td>
<td>Select <strong>None</strong>.</td>
</tr>
</tbody>
</table>

4. On the **IdP Adapter** tab, click **Add a new row to ‘Credential Validators’**.

5. From the list, select the Password Credential Validator created in “Creating a RADIUS Password Credential Validator” on page 12, and then click **Update**.
6. Click Next.

7. On the **Extended Contract** tab, click Next.

8. On the **Adapter Attributes** tab, select the checkbox in the **PEUSDONYM** column (optionally select other attributes, if available), and then click Next.
9. On the **Summary** tab, review the configuration details, and then click **Done**.

![Configuration Details](image)

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

10. On the **Manage IdP Adapter Instances** tab, click **Save**.

![Manage IdP Adapter Instances](image)

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

### Creating a Composite Adapter

For an identity provider, PingFederate includes a Composite Adapter, which allows an administrator to *chain* the selection of available adapter instances for a connection. At runtime, adapter chaining means that SSO requests are passed sequentially through each adapter instance specified until one or more authentication results are found for the user.

Adapter chaining may be used to choose an adapter instance based on the method by which a user authenticated, or to integrate an organization’s multi-factor authentication policy.
1. On the PingFederate administrative console window, under APPLICATION INTEGRATION SETTINGS, click Adapters.

![Adapters screen](image1.png)

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

2. On the Manage IdP Adapter Instances tab, click Create New Instance.

![Create New Instance](image2.png)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
3. On the **Type** tab, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th>Instance Name</th>
<th>Enter the name of the instance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Id</td>
<td>Enter the instance identifier. The value must not contain spaces or underscores.</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>Composite Adapter</strong>.</td>
</tr>
<tr>
<td>Parent Instance</td>
<td>Select <strong>None</strong>.</td>
</tr>
</tbody>
</table>

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

4. On the **IdP Adapter** tab, click **Add a new row to ‘Adapters’**.

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
5. In the **ADAPTER INSTANCE** field, select **IdP Adapter**, and then click **Update**. Similarly, add **htmlform** as an adapter instance, in order of authentication.

You have created the adapter instance with the name **htmlform** in “Creating an HTML Form Identity Provider Adapter” on page 16. **IdP Adapter** is already configured when you deploy PingFederate quick-start demo applications (refer to “
Appendix: Deploying PingFederate Quick-Start Applications* on page 31).

6. Click Next.

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
7. On the **Extended Contract** tab, add attributes (such as email, subject, first_name, last_name, and username) to be returned from each adapter instance configured.

![Image of Extended Contract tab with attributes](image1.png)

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

8. Click **Next**.

![Image of Adapter Attributes tab](image2.png)

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

9. On the **Adapter Attributes** tab, in the **PSEUDONYM** column, select the checkbox for at least one of the attributes, and then click **Next**.

![Image of Pseudonym column selection](image3.png)

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

![Configuration details](image1)

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

### Updating an Identity Provider Adapter in the Demo Service Provider (SP) Connection

Before you proceed with the steps below, ensure that OGNL expressions are enabled. To enable OGNL expressions, refer to the following URL:

https://documentation.pingidentity.com/display/PF73/Enabling+and+Disabling+Expressions

1. On the PingFederate administrative console window, under **SP CONNECTIONS**, click **Demo SP**.

![Console window](image2)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
2. On the **Summary** tab, click the **AUTHENTICATION SOURCE MAPPING** link to modify existing authentication source.

![Authentication Source Mapping](image)

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

3. On the **Authentication Source Mapping** tab, click **Map New Adapter Instance**.

![Map New Adapter Instance](image)

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

4. On the **Adapter Instance** tab, in the **Adapter Instance** field, select a composite adapter (created in “Creating a Composite Adapter” on page 19), and then click **Next**.

![Adapter Instance](image)

*The screen image above is from PingFederate®. Trademarks are the property of their respective owners.*
5. On the **Assertion Mapping** tab, select **Use only the Adapter Contract values in the SAML assertion**, and then click **Next**.

![Assertion Mapping](image1)

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

6. 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 **Adapter**.
   b. In the **VALUE** column, select the required value (example shown in the screen below).

![Adapter Contract Fulfillment](image2)

*The screen image above is from PingFederate®. Trademarks are the property of their respective owners.*
7. On the Issuance Criteria tab, define issuance criteria that compare usernames from adapters to ensure that the end user does not authenticate through the two adapters with different usernames, and then click Show Advanced Criteria.

8. In the EXPRESSION field, define the expression as shown below, and then click Add.

```
!(#this.get("username").toString().contains(" "))
```

9. Click Save.
Running the Solution

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

For this integration, the SafeNet eToken PASS 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. To access the protected resource at the SP site, click **Single Sign-On**.

3. You are redirected to the IdP SSO login page. In the **Select authentication system** field, select the configured composite adapter, and then click **Continue**.

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
4. Select your **User Id**, enter your **Password**, and then click **Login**.

![Login Screen](image)

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

5. You are redirected for second-level of authentication from SAS RADIUS.

Enter your **Username**, generate an OTP and enter it in the **Password** field, and then click **Sign On**.

![Sign On Screen](image)
After successful authentication, you are logged in. The page that displays represents the protected “target” resource of the SSO transaction.

(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.

Troubleshooting

To customize the PingFederate user-facing screens, refer to:
https://documentation.pingidentity.com/display/PF73/Customizing+User-Facing+Screens

The template page you have to edit for the HTML form is:
<pf_install>/pingfederate/server/default/conf/template/html.form.login.template.html
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 Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>