PingFederate 2FA Value-Added Module (VAM) Deployment Guide
Copyright Information

©2018. SecureAuth® is a registered trademark of SecureAuth Corporation. SecureAuth’s IdP software, appliances, and other products and solutions are copyrighted products of SecureAuth Corporation.

Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>2017-10-12</td>
<td>Initial draft</td>
</tr>
<tr>
<td>1.0</td>
<td>2018-05-24</td>
<td>First draft completed</td>
</tr>
<tr>
<td>1.1</td>
<td>2018-07-31</td>
<td>Redaction of first draft</td>
</tr>
</tbody>
</table>

For information on support for this module, contact your SecureAuth support or sales representative:

Email: support@secureauth.com
inside-sales@secureauth.com

Phone: +1.949.777.6959 or +1-866-859-1526

Website: https://www.secureauth.com/support
https://www.secureauth.com/contact
# Table of Contents

Introduction .................................................................................................................................................. 4  
Configuration ............................................................................................................................................... 5  
  Setting Up the Environment ......................................................................................................................... 5  
  Creating a Password Credential Validator .................................................................................................. 8  
  Creating HTML Form Adapter ................................................................................................................... 11  
  Configuring a SecureAuth Realm for API .................................................................................................... 17  
  Creating a 2FA Adapter ............................................................................................................................... 20  
  Creating the SecureAuth Composite Adapter ............................................................................................ 26  
  Creating SP Connections .............................................................................................................................. 32  
  Configuring the HTML Form Adapter Logout ............................................................................................ 52  
  Testing the Configured SecureAuth 2FA Functionality ................................................................................ 53  
Conclusion .................................................................................................................................................... 58
Introduction
This integration relies upon a SecureAuth PingFederate two-factor authentication (2FA) value-added module (VAM) — a piece of software that allows PingFederate to perform 2FA through the SecureAuth IdP API.

**NOTE:** This VAM guide applies to integrations using PingFederate servers version 8.3 and later.

**NOTE:** This is not the only way SecureAuth IdP can integrate with PingFederate: you can also integrate via SAML SSO. There is a separate guide dealing with this integration, PingFederate SAML Integration Guide.
Configuration

This section outlines the steps needed to configure the SecureAuth PingFederate Two-Factor Authentication (2FA) VAM in PingFederate 8.3. The PingFederate 2FA VAM is a piece of software that enables SecureAuth IdP to talk with a PingFederate server through an exchange of SAML code.

To set up the integration, download the deployment package and take the following steps:

1. Setting Up the Environment
2. Creating a Password Credential Validator
3. Creating HTML Form Adapter
4. Configuring a SecureAuth Realm for API
5. Creating a 2FA Adapter
6. Creating the SecureAuth Composite Adapter
7. Creating SP Connections
8. Configuring the HTML Form Adapter Logout
9. Testing the Configured SecureAuth 2FA Functionality

Setting Up the Environment

To set up the PingFederate environment required to use the 2FA VAM adapter, perform the following procedure:

1. Place the `pf.plugins.secureauth-second-factor-adapter.jar` under the `.../pingfederate-8.3.2/pingfederate/server/default/deploy` directory.

   ![pf.plugins.secureauth-second-factor-adapter.jar](attachment://pf.plugins.secureauth-second-factor-adapter.jar)
2. Place the jars shown under the ...
\`\`\pingfederate-8.3.2\pingfederate\server\default\deploy\`\`
directory as shown in Figure 1.

![FIGURE 1. JARs to Place in the Deploy Folder](image)

You can find these files under “dependency-jars” in the downloaded deployment package.
3. Place the following files in the specified folders. If a folder does not exist for one or more files, create a new folder to accommodate it.

<table>
<thead>
<tr>
<th>File</th>
<th>Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>secureauth.second.factor.form.html</code></td>
<td>...\pingfederate\server\default\conf\template</td>
</tr>
<tr>
<td><code>secureauth-logo.jpg</code></td>
<td>...\pingfederate\server\default\conf\template\assets\images</td>
</tr>
<tr>
<td><code>attribute-form-template.properties</code></td>
<td>...\pingfederate\server\default\conf\language-packs</td>
</tr>
</tbody>
</table>

4. Under the `\pingfederate-8.3.2\pingfederate\bin` folder, start the server by executing the `run.bat` command as shown in Figure 2.

![Run the script to start the server](image-url)
Creating a Password Credential Validator

Password credential validators (PCV) allow PingFederate administrators to define a centralized location for username/password validation, enabling validator instances to be referenced by various PingFederate configurations.

To create the password credential validator, follow this procedure.

1. Launch a web browser and enter the URL like this:
   ```
   https://<DNS_NAME>:9999/pingfederate/app
   ```
   where `<DNS_NAME>` is the fully qualified name of the machine running the PingFederate server.

2. The PingFederate administrative console appears. Click Server Configuration in the left panel, and then click Password Credential Validators from the AUTHENTICATION section, as shown in Figure 3.

   ![Server Configuration Panel](image)

   **FIGURE 3.** Go to the Server Configuration panel and click Password Credential Validators
3. The Manage Credential Validator Instances page appears. Click **Add a new row to ‘Users’**, as shown in Figure 4.

![Figure 4. Add a New Row to Users](image)

4. The Create Credential Validator Instance page appears like Figure 5. Enter the username and password for the user being added to the list, then click **Update**.

![Figure 5. Enter a username and password then click Update](image)
5. At the bottom of the same page, click Next.

FIGURE 6. Click Next

6. The summary screen appears like Figure 7. Click Done.

FIGURE 7. Review the first summary and click Done
7. A second summary screen appears like Figure 8. Click Save to return to the PingFederate administrative console.

![Figure 8](image)

**FIGURE 8.** Complete the validator creation by clicking Save.

**Creating HTML Form Adapter**

The HTML Form Adapter enables you to customize a different login page for each configured adapter instance. You can define a logout path and page or a logout redirect page. You can also enable users to change their network passwords and customize a change-password page, or redirect users to a company-hosted password management system.

PingFederate packages an HTML Form Adapter that delegates user authentication to a configured password credential validator. This authentication mechanism validates credentials based on either an LDAP directory or a simple username validator that authenticates credentials maintained by PingFederate. If you are using the packaged adapter, you can skip this step and go to Step 4; otherwise continue with this step.

To create an HTML Form Adapter, do the following:
1. From the main panel on the Administrative Console, click **IdP Configuration**, then click **Adapters**.

![Click this link](image1)

**FIGURE 9.** Go to the **IdP Configuration** panel then click **Adapters**

2. The Manage IdP Adapter Instances screen appears like Figure 10. Click **Create New Instance**.

![Click this link](image2)

**FIGURE 10.** Create a new adapter instance
3. The Create Adapter Instances screen appears like Figure 11. Enter the required values in the INSTANCE NAME and INSTANCE ID fields, select the HTML Form IdP Adapter option from the TYPE field, then click Next.

![Figure 11. Configure the New Adapter Instance](image)

4. The IdP Adapter screen appears like Figure 12. Click the Add a new row to ‘Credential Validators’ link.

![Figure 12. Create HTML Form Adapter Instance – IdP Adapter Page](image)

5. Click the Add a new row to ‘Credential Validators’ link.
A screen like Figure 13 appears.

![Figure 13](image1.png)

**FIGURE 13. Create HTML Form Adapter Instance – IdP Adapter 2**

6. Select the password credential validator you want to use then click Update. A summary screen like Figure 14 appears.

![Figure 14](image2.png)

**FIGURE 14. Create HTML Form Adapter Instance – IdP Adapter 3**

7. Click Next.
A screen like Figure 15 appears.

FIGURE 15. Create HTML Form Adapter Instance – IdP Adapter 4

8. Click Next again.

A screen like Figure 16 appears.

FIGURE 16. Create HTML Form Adapter Instance – Adapter Attributes Page

9. Check the box under ‘Pseudonym’ then click Next. A screen like Figure 17 appears.

FIGURE 17. Create HTML Form Adapter Instance – Adapter Contract Mapping Page

10. Click Done.
A screen like Figure 18 appears.

FIGURE 18. Create HTML Form Adapter Instance – Summary
The Manage IdP Adapter Instances screen reappears with the new HTML Form adapter instance included like Figure 19.

![Manage IdP Adapter Instances](image)

**FIGURE 19.** Manage IdP Adapter Instances Summary

11. Click **Save**.

You are returned to the main PingFederate Administrative Console screen.

**Configuring a SecureAuth Realm for API**

If you have already created a SecureAuth IdP realm for this purpose, skip to “Creating a 2FA Adapter” starting on page 20.

If you have NOT already created a SecureAuth IdP realm for use with the PingFederate server, do the following:

1. Install a SecureAuth appliance.
   For more information on installing an appliance, refer to [https://docs.secureauth.com/display/91docs/Install+Part+I+-+Install+the+Appliance](https://docs.secureauth.com/display/91docs/Install+Part+I+-+Install+the+Appliance).
   Use the host name/address of this appliance when configuring the PingFederate second-factor adapter (**API-HOST** field).
2. Select/create a realm for your second-factor API.
   For more information on creating a realm, refer to [https://docs.secureauth.com/display/91docs/SecureAuth+IdP+Realm+Guide](https://docs.secureauth.com/display/91docs/SecureAuth+IdP+Realm+Guide).
   Use the realm number created here when configuring the PingFederate second-factor adapter (**API_REALM** field).
3. Go to the **Data** tab page on the new realm and supply the following values.
a. Scroll down to the Membership Connection Settings section as shown in Figure 20.

![Membership Connection Settings](image)

**FIGURE 20. Membership Connection Settings**

b. Select a value for the ‘Data Store’ field from the drop-down list and provide connection settings for the data store. Figure 20 shows example settings for an Active Directory data store.

c. Click Save.

For more on Data tab page field settings, refer to: [https://docs.secureauth.com/display/91docs/Data+Tab+Configuration](https://docs.secureauth.com/display/91docs/Data+Tab+Configuration)
4. Go to the API tab page and configure SecureAuth API settings for Java SAML Consumer Login authentication as shown in Figure 21.

![API Key Section](image)

**FIGURE 21. API Key Section**

a. Check the **Enable API for this realm** box.
b. Click on **Generate Credentials**.
c. Copy the generated Application ID and Application Key to another program, such as Notepad or Word. You will need these values when configuring the ‘API-App-Key’ and ‘API-App-ID’ fields for the PingFederate second-factor adapter as explained in “Creating a 2FA Adapter” starting on page 17.
d. Check the **Enable Authentication API** box.
e. Click **Save**.

For more on the API tab page field settings, refer to: [https://docs.secureauth.com/pages/viewpage.action?pageId=44833616](https://docs.secureauth.com/pages/viewpage.action?pageId=44833616)
Creating a 2FA Adapter
Once you have configured a SecureAuth realm with API service, create a second-factor adapter by following these steps:

1. At the PingFederate Administrative Console screen, select **IdP Configuration** then **Adapters**.

   ![IdP Configuration](image1)

   The Manage IdP Adapter Instances screen reappears.

   ![Manage IdP Adapter Instances](image2)

   2. Click **Create New Instance**.

   ![Create New Instance](image3)
The Create Adapter Instance screen appears like Figure 22.

![Create Adapter Instance Screen](image)

**FIGURE 22. Create Adapter Instance 1**

3. Enter an Instance Name and Instance ID.
4. At the Type field, select **SecureAuth Second Factor Adapter** as a type.

![Create Adapter Instance Screen](image)

**FIGURE 23. Create Adapter Instance 2**

5. Click **Next**.
The IdP Adapter screen appears showing the SecureAuth Second Factor Adapter settings as shown in Figure 24 appears.

**FIGURE 24. SecureAuth IdP Second Factor Adapter Page**

6. Enter the following values for the specified fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Required Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML Form Template Name</td>
<td>Enter secureauth.second.factor.form.html</td>
</tr>
<tr>
<td>API-App-ID</td>
<td>Configure according to the value entered to create the SecureAuth realm. See “Configuring a SecureAuth Realm for API” on page 14.</td>
</tr>
<tr>
<td>API-App-Key</td>
<td>Configure according to the value entered to create the SecureAuth realm. See “Configuring a SecureAuth Realm for API” on page 14.</td>
</tr>
<tr>
<td>API_REALM</td>
<td>Configure according to the value entered to create the API service for the SecureAuth realm.</td>
</tr>
<tr>
<td>API-HOST</td>
<td>Configure according to the value entered to create the API service for the SecureAuth realm.</td>
</tr>
<tr>
<td>API-PORT</td>
<td>Configure according to the value entered to create the API service for the SecureAuth realm.</td>
</tr>
<tr>
<td>API-SSL</td>
<td>Configure according to the value entered to create the API service for the SecureAuth realm.</td>
</tr>
</tbody>
</table>
7. Click **Next**.
   The Extended Contract page like Figure 25 appears.

![FIGURE 25. Create Adapter Instance – Extended Contract Page](image)

8. Click **Next** again.
   The Adapter Attributes page appears like Figure 26.

![FIGURE 26. Create Adapter Instance – Adapter Attributes](image)

9. Check the box under ‘Pseudonym’ then click **Next**.
The Adapter Contract Mapping page like Figure 27 appears.

![Adapter Contract Mapping Page](image)

**FIGURE 27. Adapter Contract Mapping Page**

10. Click Next again.
A summary information screen like Figure 28 appears.

**FIGURE 28.** IdP Adapter Instance Summary Information

11. Click **Done**.
The Manage IdP Adapter Instances page reappears like Figure 29.

![Manage IdP Adapter Instances Page](image)

**FIGURE 29. Manage IdP Adapter Instances Page**

12. Click **Save**.

**Creating the SecureAuth Composite Adapter**

In order for SecureAuth IdP to communicate with the PingFederate server, you must set up a SecureAuth composite adapter.

Follow these steps to create the required composite adapter:

1. From the PingFederate Administrative Console, select **IdP Configuration** from the main panel.
2. Click on **Adapters** then press the **Create New Instance** button as shown in Figure 30.

![Click this button](image)

**FIGURE 30. Manage IdP Adapter Instances**

The Create Adapter Instance page appears like Figure 31.

![Create Composite Adapter Instance – Type Page](image)

**FIGURE 31. Create Composite Adapter Instance – Type Page**

3. Select the required values on the **INSTANCE NAME** and **INSTANCE ID** fields.
4. At the **TYPE** field, select **Composite Adapter** as shown in Figure 31, then click **Next**.
The IdP Adapter page for this composite adapter appears like Figure 32.

5. Click the **Add a new row to ‘Adapters’** link and add your HTML form and SecureAuth2FA adapter as shown in Figure 33.

**FIGURE 32. Create Composite Adapter Instance – IdP Adapter Page**

**FIGURE 33. Create Composite Adapter Instance – IdP Adapter Page 2**
For a target adapter, select the SecureAuth 2FA adapter. Under the USER ID SELECTION field, select **username** and click **Next**.

6. Make sure the order of the adapter instance is as shown in Figure 33: **HTML Form IDP Adapter** should be above **SecureAuth 2FA adapter**. Then click **Next**.

The Extended Contract page appears like Figure 34.

![Figure 34. Create Composite Adapter Instance – Extended Contract Page](image)

7. Add the username under the Extend the Contract field then click **Next**.

The Adapter Attributes page for this Composite Adapter Instance appears like Figure 35.

![Figure 35. Create Composite Adapter Instance – Adapter Attributes Page](image)

8. Check the box under ‘Pseudonym’ then click **Next**.
9. Click **Next** again to go to the Summary page.

![FIGURE 36. Create Composite Adapter Instance – Summary Page](image)

10. Click **Done**.
The Manage IdP Adapter Instances page appears with the new composite adapter listed as shown in Figure 37.

![Manage IdP Adapter Instances](image)

**FIGURE 37.** Manage IdP Adapter Instances

11. Click **Save**.

You are returned to the main menu of the PingFederate Administrative Module.
Creating SP Connections

Once you have created the required composite adapter, you must connect the existing SP instances. To do this, follow these steps.

1. From the PingFederate administrative module, click on the **IdP Configuration** tab then click on the **Create New** button under the SP CONNECTIONS section as shown in Figure 38.

![FIGURE 38. PingFederate Administrative Module Main Menu](image)

The SP Connection page appears like Figure 39.

![FIGURE 39. SP Connection – Connection Type Page](image)

2. Check the **BROWSER SSO PROFILES** box, then click **Next**.
The Connection Options page appears like Figure 40.

![Figure 40. SP Connection – Connect Options Page](image)

3. Check the **BROWSER SSO** box, then click **Next**.

        The Metadata URL page appears like Figure 41.

![Figure 41. SP Connection – Metadata Page](image)

4. Click **Next**.
The General Info page appears like Figure 42.

![SP Connection – General Info Page](image)

**FIGURE 42. SP Connection – General Info Page**

5. Enter the following values in the required fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner’s Entity ID (Connection ID)</td>
<td>Enter an ID for this SP connection</td>
</tr>
<tr>
<td>Connection Name</td>
<td>Enter a name for this SP connection</td>
</tr>
<tr>
<td>Base URL</td>
<td>Enter the base URL for this SP connection</td>
</tr>
<tr>
<td>Company</td>
<td>Enter the name of the company to which this SP connection goes</td>
</tr>
<tr>
<td>Contact Name</td>
<td>Enter the contact name for this SP connection</td>
</tr>
<tr>
<td>Application Name</td>
<td>Enter the name of the application this connection accesses</td>
</tr>
<tr>
<td>Logging Mode</td>
<td>Select STANDARD</td>
</tr>
</tbody>
</table>

6. Click **Next**.
The Browser SSO page appears like Figure 43.

![Image of SP Connection – Browser SSO Page]

**FIGURE 43.** SP Connection – Browser SSO Page

7. Click the **Configure Browser SSO** button.

   The Browser SSO SAML Properties page appears like Figure 44.

![Image of Browser SSO – SAML Profiles Page]

**FIGURE 44.** Browser SSO – SAML Profiles Page

8. Under Single Sign-On (SSO) Profiles column, check the **IDP-INITIATED SSO** box, then click **Next**.

9. Click **Next** to bypass the Assertion Lifetime page.

   The Assertion Creation page appears like Figure 45.

![Image of Browser SSO – Assertion Creation Page]

**FIGURE 45.** Browser SSO – Assertion Creation Page

10. Click the **Configure Assertion Creation** button.
The Assertion Creation page appears like Figure 46.

![Assertion Creation Page](image1)

**FIGURE 46. Assertion Creation Page**

11. Make sure the **STANDARD** radio button is selected then click **Next**.

   The Attribute Contract page appears as shown in Figure 47.

![Attribute Contract Page](image2)

**FIGURE 47. Assertion Creation – Attribute Contract Page**

12. Select the format required for the SAML subject name format as shown in Figure 47 then click **Next**.
The Authentication Source Mapping page appears as shown in Figure 48.

![Authentication Source Mapping Page](image)

**FIGURE 48.** Assertion Creation – Authentication Source Mapping Page

13. Click the **Map New Adapter Instance** button. The IdP Adapter Mapping page appears like Figure 49.

![IdP Adapter Source Mapping](image)

**FIGURE 49.** IdP Adapter Source Mapping – Adapter Instance Page

14. In the ADAPTER INSTANCE section, choose the SecureAuth2FAComp option as shown above then click Next.
The Mapping Method page appears like Figure 50.

![Mapping Method Page](image)

**FIGURE 50.** IdP Adapter Mapping – Mapping Method Page

15. Select the **USE ONLY THE ADAPTER CONTRACT VALUES IN THE SAML ASSERTION** radio button, then click **Next**.

![Attribute Contract Fulfillment Page](image)

The Attribute Contract Fulfillment page appears like Figure 51.

**FIGURE 51.** IdP Adapter Mapping – Attribute Contract Fulfillment Page
16. Do this:
   - From the drop-down option list in the ‘Source’ column, select **Adapter**.
   - From the drop-down option list in the ‘Value’ column, select **username**.

17. Click **Next**.

   The Issuance Criteria page appears like Figure 52.

![Figure 52. IdP Adapter Mapping – Issuance Criteria Page](image)

18. Click **Next**.
The Summary page appears.

![Diagram of the Summary page]

**FIGURE 53.** IdP Adapter Mapping – Summary Page

19. **Click Done.**

The Assertion Creation Authentication Source Mapping page appears.

![Diagram of the Assertion Creation page]

**FIGURE 54.** Assertion Creation – Authentication Source Mapping Page

20. **Click Next.**
The Assertion Creation Summary Page appears.

![Assertion Creation Summary Page](image)

**FIGURE 55.** Assertion Creation – Summary Page

21. Click **Done**.

The Browser SSO Protocol Settings page appears.

![Browser SSO Protocol Settings Page](image)

**FIGURE 56.** Browser SSO – Protocol Settings Page
22. Click the **Configure Protocol Settings** button. The Protocol Settings page appears.

![FIGURE 57. Protocol Settings – Assertion Consumer Service URL Page](image1)

23. Check the ‘Default’ box, select **POST** from the ‘Binding’ option list, enter the appropriate endpoint URL, then click **Add**.

![FIGURE 58. Protocol Settings – Assertion Consumer Service URL Page 2](image2)

24. Click **Next**.
The Signature Policy page appears like Figure 59.

![Figure 59. Protocol Settings – Signature Policy Page](image)

25. Check the **ALWAYS SIGN THE SAML ASSERTION** box, then click **Next**.

26. At the Encryption Policy page, click **Next**.

The Summary page appears like Figure 60.

![Figure 60. Protocol Settings – Summary Page](image)

27. Click **Done**.
The Browser SSO Protocol Settings Summary page appears like Figure 61.

![Browser SSO Protocol Settings Summary Page](image)

**FIGURE 61.** Browser SSO Protocol Settings Summary Page

28. Click **Next**.
The full Browser SSO summary page appears like Figure 62.

![Browser SSO Summary Page](image)

**FIGURE 62.** Browser SSO Summary Page

29. Click **Done** after verifying the values.
The SP Connection Browser SSO screen like Figure 63 appears with the new entry displayed.

![SP Connection Browser SSO Page](image)

**FIGURE 63.** SP Connection Browser SSO Page

30. Click **Next**.

A screen like this appears.

![Configure Credentials](image)

31. Click the **Configure Credentials** button.
The SP Connection Credentials page appears like Figure 64.

![Figure 64. SP Connection Credentials Page](image)

32. Click the **Manage Certificates** button.

The Certificate Management page appears like Figure 65.

![Figure 65. SP Connection Certificate Management Page](image)

33. Do one of these:
   - If you want to create an unsigned certificate, click the **Create New** button
   - To use an existing certificate, click the **Import** button
The Create Certificate page appears like Figure 66.

![Create Certificate Page](image)

**FIGURE 66.** SP Connection Create Certificate Page

34. Enter values as required then click **Next**.
A summary page like Figure 67 appears.

FIGURE 67. SP Connection Create Certificate – Summary Page

35. Click Done.
A screen like Figure 68 appears.

![Image of SP Connection Certificate Management](image)

**FIGURE 68. SP Connection Certificate Management**

36. Click **Save**.

**NOTE:** Unless you click the Save button here, you may lose all configuration information you have entered so far.

You should notice that the ‘Signing Certificate’ field is now populated with the correct digital signature data as shown in Figure 69.

![Image of SP Connection Credentials Digital Signature Settings](image)

**FIGURE 69. SP Connection Credentials Digital Signature Settings**
37. Click **Next**.

The summary screen appears like Figure 70.

![Figure 70. SP Connection Credential Digital Signature Settings Summary](image)

38. Click **Done**.

The SP Connection Credentials page appears like Figure 71.

![Figure 71. SP Connection Credentials Page](image)

39. Click **Next**.
The SP Connection Activate & Summary page appears like Figure 72.

![SP Connection Activate & Summary Page](image.png)

**FIGURE 72. SP Connection Activate & Summary Page**

40. Click to select the **ACTIVE** radio button then click **Save**.

**Configuring the HTML Form Adapter Logout**

The next to last configuration step is to set up the HTML Form Adapter logout. To configure the HTML form adapter logout:

1. Edit the HTML form adapter configuration.
2. Enter a path into the Logout Path field.
   
   You can enter any valid path string into this field. Use alphanumerical string to minimize the risk of using an invalid value) into this field. This value must start with a `/` character. For example, if you enter `/mylogoutpath` into this field, the actual logout path will be `/ext/mylogoutpath.`
3. If you want PingFederate to redirect the user to a URL after logout, enter the URL into the ‘Logout Redirect’ field, such as https://myapp.example.com/loggedout.html.

![Logout Redirect Example]

4. In the HTML script, add a `restart login` link to “idp.sso.error.page.template.html” under the `\pingfederate\8.3.2\pingfederate\server\default\conf\template` as shown below:

```html
<div>
    <a href="https://localhost:9031/ext/mylogoutpath">restart login</a>
</div>
```

The result should be a message and restart login link like this example:

![Sign On Error Example]

**Testing the Configured SecureAuth 2FA Functionality**
To test the functionality of the configured SecureAuth 2FA, perform these steps:

1. To obtain the test URL, go to **IdP Configuration** in the PingFederate Administrative Module then click on the appropriate SP connection as shown in Figure 73.
In this example, the name of the connection is **TestSAMLConnection**.

![Figure 73. IdP Configuration Test](image)

When the link is clicked, a page like Figure 74 appears.

![Figure 74. SP Connection Test](image)

2. Make sure the Connection Status is set to **ACTIVE**, then copy the URL displayed to the right of the ‘SSO Application Endpoint’ field.

   In this example, the URL is:
   
   https://localhost:9031/idp/startSSO.ping?PartnerSpId=TestSAMLConnection

3. Open a new browser tab and paste this URL into the URL field.
A screen like this example should appear:

![Sign On form](image)

**FIGURE 75.** URL Browser Test Example

4. Enter a user name in the ‘USERNAME’ field and a password in the ‘PASSWORD’ field. Then click **Sign On**.

A screen like Figure 76 should appear.

![Passcode Delivery Method Selection](image)

**FIGURE 76.** Passcode Delivery Method Selection
5. Select the delivery technique. 
   First test with SMS then click Deliver OTP. 
   If the account has the correct associated phone number, you should receive an SMS with 
   the OTP code.

6. Enter the received OTP in the text box under Step 2, then click Submit as shown in 
   Figure 77.

   ![Figure 77. OTP Entry](image)

If you get a security warning like the one shown in Figure 78, click Continue.

   ![Figure 78. Security Warning](image)
After a successful authentication, the destination page appears like Figure 79.

**FIGURE 79.** Sample Destination Page

7. Repeat the test with both the Voice and Email method.
Conclusion

Once deployed and configured, a PingFederate server can take advantage of all the advanced security features SecureAuth IdP provides.