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>2017-11-21</td>
<td>Initial draft</td>
</tr>
<tr>
<td>1.0</td>
<td>2018-03-09</td>
<td>First draft completed</td>
</tr>
<tr>
<td>1.1</td>
<td>2018-08-06</td>
<td>Updates</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/support)
[https://www.secureauth.com/contact](https://www.secureauth.com/contact)
## Table of Contents

**Introduction** .................................................................................................................. 4  
Prerequisites ......................................................................................................................... 4  

**Integration** ..................................................................................................................... 5  
SecureAuth IdP Configuration ............................................................................................... 5  
PingFederate Configuration ................................................................................................. 10  
Testing the Configuration ................................................................................................. 23
Introduction
This guide details how to integrate PingFederate with SecureAuth IdP using SAML through SP-initiated workflow.

Prerequisites
Before beginning the integration, perform these steps:

+ Have a Ping Federate Administrator Account
+ Create a SecureAuth IdP Realm for the PingFederate Integration
Integration
Integrating SecureAuth IdP to PingFederate is a three-step process:

+ SecureAuth IdP Configuration
+ PingFederate Configuration
+ Testing the Configuration

SecureAuth IdP Configuration
Follow this process to configure SecureAuth IdP for use with PingFederate:

1. Create a realm in SecureAuth IdP to handle PingFederate communications. For more on this, refer to the SecureAuth IdP Realm Guide.
2. Configure the new realm using the following tabs in the Web Admin, before configuring the Post Authentication tab:
   • Overview – the description of the realm and SMTP connections must be defined
   • Data – an enterprise directory must be integrated with SecureAuth IdP
   • Workflow – the way in which users access this application must be defined
   • Registration Methods / Multi-Factor Methods – the Multi-Factor Authentication methods that are used to access this page (if any) must be defined
3. Return to the **Data** tab and ensure the Membership Connection is set correctly by scrolling down to the ‘Profile Fields’ section and map the directory field that contains the user’s email address (‘Email 1’ field, for example) to the correct SecureAuth IdP property.

![Profile Fields Section for Email Mapping](image)

**FIGURE 1.** Profile Fields Section for Email Mapping

You can choose to map additional fields as SAML attributes, if necessary.

4. Click to select the **Post Authentication** tab, then select the **SAML 2.0 (SP Initiated) Assertion** option from the ‘Authenticated User Redirect’ drop-down list as shown in Figure 2.

An unalterable URL auto-populates the ‘Redirect To’ field, which then appends to the domain name and realm number in the address bar (like this example: Authorized/SAML20SPInit.aspx).

![Post Authentication Page Example](image)

**FIGURE 2.** Post Authentication Page Example

5. If required, upload a customized post authentication page using the ‘Upload a Page’ field.
6. Scroll down to the ‘User ID Mapping’ section and make the following field selections.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description/Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID Mapping</td>
<td>Select the SecureAuth IdP property that corresponds to the Profile Field value (see Figure 1). In this case, it is <strong>Email 1</strong>.</td>
</tr>
<tr>
<td>Name ID Format</td>
<td>Select <strong>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</strong>.</td>
</tr>
<tr>
<td>Encode to Base64</td>
<td>Select <strong>False</strong>.</td>
</tr>
</tbody>
</table>

An example of this section is shown in Figure 3.

![User ID Mapping Section](image)

**FIGURE 3. User ID Mapping Section**

7. Scroll down to the ‘SAML Assertion/WS Federation’ section and make changes to the following fields.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description/Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSFed/SAML Issuer</td>
<td>Set to any value, typically in the form https://&lt;IssuerName&gt;.com</td>
</tr>
<tr>
<td>SAML Consumer URL</td>
<td>Set to the appropriate value found in PingFederate. Typically, this value is the application’s FQDN with a fixed path extension, such as: https://&lt;FQDN&gt;/sp/ACS/saml2. <strong>NOTE:</strong> This value is located in the <strong>Protocol Endpoints</strong> hyperlink, which is in the ‘Federation Info’ section under the <strong>Server Configuration</strong> tab.</td>
</tr>
<tr>
<td>SAML Recipient</td>
<td>Set to the same value as designated for the ‘SAML Consumer URL’ field.</td>
</tr>
<tr>
<td>SAML Audience</td>
<td>Set to the same value as the <strong>SAML 2.0 Entity ID</strong> on Ping Federate. <strong>NOTE:</strong> This value must differ from the user inputs value for the ‘WSFED/SAML Issuer’ field and is located in the ‘Federation Info’ section under the <strong>Server Configuration</strong> tab.</td>
</tr>
<tr>
<td>Fields</td>
<td>Description/Recommendations</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SP Start URL</td>
<td>This field is not mandatory to enable SSO and to redirect users appropriately to access SecureAuth. In case the user needs to include it, this URL value is the same as the start site for the SP Application. For example: http:&lt;FQDN&gt;:&lt;portNumber&gt;/sp/startSSO.ping?PartnerSpId=SAMLIssuer</td>
</tr>
<tr>
<td>SAML Offset Minutes</td>
<td>Set to 5 minutes to make up for time differences between devices.</td>
</tr>
<tr>
<td>SAML Valid Hours</td>
<td>Set the to 1 hour to limit for how long the SAML assertion is valid.</td>
</tr>
<tr>
<td>WS-Fed Signing Algorithm</td>
<td>Set both to SHA1.</td>
</tr>
<tr>
<td>SAML Signing Algorithm</td>
<td></td>
</tr>
</tbody>
</table>

An example of this section is shown in Figure 4.

![SAML Assertion / WS Federation](image)

**FIGURE 4.** SAML Assertion/WS Federation Section

8. Scroll down to the end of this section and provide these field values.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description/Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign SAML Assertion</td>
<td>Set to <strong>False</strong>.</td>
</tr>
<tr>
<td>Sign SAML Message</td>
<td>Set to <strong>True</strong>.</td>
</tr>
<tr>
<td>Encrypt SAML Assertion</td>
<td>Set to <strong>False</strong>.</td>
</tr>
</tbody>
</table>
An example of these SAML fields is shown in Figure 5.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign SAML Assertion</td>
<td>False</td>
</tr>
<tr>
<td>Sign SAML Message</td>
<td>True</td>
</tr>
<tr>
<td>Encrypted SAML Assertion</td>
<td>False</td>
</tr>
</tbody>
</table>

**FIGURE 5. SAML Fields Examples**

9. Leave the ‘Signing Cert Serial Number’ field as the default value, unless there is a third-party certificate being used for the SAML assertion.

**NOTE:** When using a third-party certificate, click **Select Certificate** and choose the appropriate certificate.

**FIGURE 6. Signing Certificate Section**

10. If required, scroll down to the ‘Forms Auth/SSO Token’ section, then click the **View and Configure FormsAuth keys / SSO token** link to configure the token/cookie settings and to configure this realm for SSO, as shown in Figure 7.

**FIGURE 7. Forms Auth/SSO Token Section**

11. Once the configurations have been completed and before leaving the Post Authentication page, click **Save** to avoid losing changes.
PingFederate Configuration

Follow this process to configure PingFederate for use with SecureAuth IdP:

1. From the left pane of the PingFederate main menu, click on the **SP Configuration** tab. A screen like Figure 8 appears.

   ![PingFederate SP Configuration page](image)

   **FIGURE 8.** PingFederate SP Configuration page

2. Under the IDP CONNECTIONS section, click the **Create New** link to start the IdP Connector wizard and create a new IdP connection.

   ![IdP Connection Wizard](image)

   **FIGURE 9.** IdP Connection Wizard

3. Check the **Browser SSO Profiles** box and the Protocol of SAML 2.0 is auto-selected as shown in Figure 9.

4. Click **Next**.
The Connection Options tab appears.

5. Check the **Browser SSO** box, then click **Next** as shown in Figure 10.

![Connection Options Page](image)

**FIGURE 10.** Connection Options Page

The Metadata URL tab appears.

6. Click **Next** to skip the Metadata URL section.
The General Info page appears as shown in Figure 11.

**FIGURE 11.** General Info Page

7. In the ‘Partners Entity ID’ text box, enter the correct value. This value must be the same as the value entered in the ‘WS-Fed / SAML Issuer’ field on the Post Auth tab in SecureAuth IdP. In Figure 11, this value is **SAMLIssuer**, the same value specified in Step 7 on page 4.

8. At the ‘Connection Name’ text box, enter any name required.

9. Click **Next**.

The Browser SSO tab appears like Figure 12.

**FIGURE 12.** Browser SSO Page
10. Click on the **Configure Browser SSO** button.

11. Under the ‘SAML Profiles’ tab page, check both **IDP Initiated SSO** and **SP Initiated SSO** as shown in Figure 13, then click **Next**.

![FIGURE 13. Browser SSO SAML Profiles Tab Page](image)

The User-Session Creation tab page appears as shown in Figure 14.

![FIGURE 14. Browser SSO User-Session Creation Tab Page](image)

12. Click **Next**.
The Protocol Settings tab page appears as shown in Figure 15.

**FIGURE 15.** Browser SSO Protocol Settings Tab Page

13. Click on the **Configure Protocol Settings** button.

The SSO Service URLs tab page of the Protocol Settings page appears like Figure 16.

**FIGURE 16.** Protocol Settings – SSO Service URLs Page

14. On the SSO Service URLs tab page, ensure that the only two bindings are: **Redirect** and **SOAP** and that the Endpoint URL maps to the correct SecureAuth realm. (In the Figure 16 example, it is realm **SecureAuth39**.)

15. Click **Next** when completed.
The Allowable SAML Bindings tab page appears like Figure 17.

![Figure 17. Protocol Settings – Allowable SAML Bindings Page](image)

16. Check the **POST** box then click **Next** twice.

The Signature Policy tab page appears like Figure 18.

![Figure 18. Protocol Settings – Signature Policy Page](image)

17. Click to select the **Use SAML Standard Requirements** radio button then click **Next**.
The Encryption Policy tab page appears like Figure 19.


18. Click the **None** radio button then click **Next**.

The Summary tab page appears like Figure 20.

**FIGURE 20. Protocol Settings – Summary Page**

19. Verify all the settings on this page then click **Done**.
The Protocol Settings page reappears like Figure 21.

20. Click **Next**.
The Browser SSO Summary page appears as shown in Figure 22.

![Browser SSO Summary Page](image)

**FIGURE 22.** Browser SSO Summary Page

21. Ensure that all the settings are correct then click **Done**.
The Browser SSO tab reappears, like Figure 23.

FIGURE 23. IdP Connection – Browser SSO Subpage

22. Click Next.

The Credentials subpage appears like Figure 24.

FIGURE 24. IdP Connection – Credentials Subpage

23. Click the Configure Credentials button.
The Signature Verification Settings tab appears like Figure 25.

![Signature Verification Settings Tab Page](image)

**FIGURE 25.** Signature Verification Settings Tab Page

24. Click the **Manage Signature Verification Settings** button.

The Trust Model tab page appears like Figure 26.

![Signature Verification – Trust Model Subpage](image)

**FIGURE 26.** Signature Verification – Trust Model Subpage

25. Click to select the **Unanchored** radio button then click **Next**.
26. The Signature Verification Certificate subpage appears like Figure 27.

![Signature Verification Certificate Subpage](image)

**FIGURE 27.** Signature Verification – Signature Verification Certificate Subpage

27. At the ‘Primary’ pick list, select the SecureAuth IdP certificate.

28. Once the thumb print of the certificate appears, click **Next**.

**NOTE:** If no certificate appears in the pick list, click the **Manage Certificates** button and import the appropriate SecureAuth certificate.

The Summary page appears like Figure 28.

![Signature Verification Summary Subpage](image)

**FIGURE 28.** Signature Verification – Summary Subpage

29. When satisfied, click **Done**.
The Signature Verification Settings page reappears like Figure 29.

![Signature Verification Settings Page 2](image)

**FIGURE 29.** Signature Verification Settings Page 2

30. Click **Next**.

The Credentials Page reappears, like Figure 30.

![Credentials Summary Page](image)

**FIGURE 30.** Credentials Summary Page

31. Verify all the settings and make appropriate edits if necessary, then click **Done**.
32. Click **Next** twice to move to the Activation & Summary tab page like Figure 31.

![Activation & Summary Page](image)

**FIGURE 31.** Activation & Summary Page

33. Make sure ‘Connection Status’ is set to ‘Active’ and that all the other configuration values you specified are correctly displayed, then click **Save**.

**Testing the Configuration**

To test this configuration, perform these steps:

1. Open Firefox browser and download SAML Tracer.
2. Enter the SP Start URL.
3. Check to see if the SP Start URL is redirected to SecureAuth.
4. Enter the credentials (username and password) on the SecureAuth page. The user should be authenticated successfully into the application.