Enabling Single Sign-On Using OneLogin in Axon Data Governance 5.4
Abstract

This document describes the steps to enable Single Sign-On (SSO) in a cloud or on-premises deployment of Axon Data Governance 5.4 using the OneLogin identity management tool.

Supported Versions

- Informatica Axon 5.4

Table of Contents

Overview ................................................. 2
Create a New Application in OneLogin ........................................................................ 3
Configure Axon Details in OneLogin. ............................................................................. 3
Generate SAML Metadata Assertion. .............................................................................. 6
Configure Axon to Use OneLogin. .................................................................................. 8
Clear the Axon Cache and Restart Services. ................................................................. 8

Overview

When you enable SSO, users with an account in the Identity Provider (IDP) of your organization can log in to the Axon web interface without entering a username and password. Axon uses Security Assertion Markup Language (SAML) 2.0 to authenticate users based on the IDP credentials.

OneLogin is an enterprise IDP tool. If your organization uses OneLogin, you can set up Axon as the service provider and enable SSO using SAML. SAML is an XML-based open-standard data format for authorization and authentication between the IDP and the service provider.

To enable SSO, you must configure Axon as an application in OneLogin. Axon supports any IDP that uses SAML 2.0 authentication.
The following image shows the steps to configure SSO for Axon:

### Create a New Application in OneLogin

Perform the following steps to set up Axon as an application in OneLogin:

1. Log in to OneLogin, and add a new application.
2. Select the **SAML Test Connector (IdP)** application type.
3. Click on the **Info** tab, and type in the application name as **Axon**.
4. Enter other basic information for the Axon application.

### Configure Axon Details in OneLogin

To configure Axon as a SAML application, perform the following tasks in OneLogin:

1. Click on the **Configuration** tab, and enter the following values:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audience</td>
<td>http(s)://&lt;Axon_URL&gt;/saml/metadata</td>
</tr>
<tr>
<td>Recipient</td>
<td>http(s)://&lt;Axon_URL&gt;/saml/acs</td>
</tr>
<tr>
<td>ACS (Consumer) URL Validator</td>
<td>http(s)://&lt;Axon_URL&gt;/saml/acs</td>
</tr>
<tr>
<td>ACS (Consumer) URL</td>
<td>http(s)://&lt;Axon_URL&gt;/saml/acs</td>
</tr>
</tbody>
</table>
2. In the **Users** menu of the Admin Page, go to the **Custom User Fields** section and add the following mandatory custom fields:

- orgunit
- firstName
- lastName
- orgunitTitle
- email
The following image shows sample entries for the **Custom User Fields** section:

**Note:** The **statusID** and **orgunitDescription** fields are optional.

- If you do not select the **statusID** property, or if you select the **statusID** property and do not assign a default value, Axon assigns the *Active* value to all the users.

- If you do not select the **orgunitDescription** property, or if you select the **orgunitDescription** property and do not assign a default value, Axon assigns a blank value to all organization units.

3. Open the Axon application in OneLogin, click on the **Parameters** tab, and select the **Configured by admin** option.

4. Click **Add parameter** to add the parameters that must be included in the SAML assertion. For each parameter that you add, select the **Include in SAML assertion** check box. Map the values for the following custom parameters that you have created:

- orgunit
- status
- firstName
- lastName
- orgunitDescription
- orgunitTitle
- email
5. Click the **Access** tab, and define the role-based policies as required by your organization.

6. Click the **Users** tab, and add the users and user groups that will login to Axon using SSO.

**Generate SAML Metadata Assertion**

After you configure Axon in OneLogin, perform the following steps in OneLogin to obtain the SAML metadata assertion:

1. Open the Axon application that you created in OneLogin and click the **SSO** tab.
2. For the **Issuer URL** field, click the **Copy to clipboard** icon. Paste the contents of the clipboard to another document to record the value.
3. For the **SAML 2.0 Endpoint (HTTP)** field, click the **Copy to clipboard** icon. Paste the contents of the clipboard to another document to record the value.
The following image shows sample values for the **Issuer URL** and **SAML 2.0 Endpoint (HTTP)** fields:

4. For the X.509 certificate, click the **View details** link. The certificate opens in a new window.
5. Copy the value of the **X.509 Certificate** field. Paste the contents of the clipboard to another document to record the value.

The following image shows a sample value for the **X.509 Certificate** field:

You must enter the values of the **Issuer URL**, **SAML 2.0 Endpoint (HTTP)**, and **X.509 Certificate** fields when you configure Axon.
Note: The SAML metadata is based on the configuration parameters that you have entered in OneLogin. If you modify any of the parameters in OneLogin, you must perform the above steps again to get the new SAML metadata values.

**Configure Axon to Use OneLogin**

After you create Axon as an application in OneLogin, you must configure Axon to authorize and authenticate the data that is exchanged with OneLogin. You must have the Super Admin profile to perform this task.

Perform the following configuration steps in Axon to use SSO:

1. From the Axon toolbar, click the **Admin Panel** menu item under your user name.
2. In the menu on the left, under the **Customize & Configure** category, click **Configure Axon**.
3. In the **Group** dropdown, select **SAML Configuration**.
4. Click **Edit**.
5. Enter the following values:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSO URL</td>
<td>http(s)://&lt;Axon_URL&gt;:&lt;port_number&gt;/saml/login</td>
</tr>
<tr>
<td>IDP Endpoint</td>
<td>SAML 2.0 Endpoint (HTTP) value that you recorded.</td>
</tr>
<tr>
<td>IDP Entity ID</td>
<td>Issuer URL that you recorded.</td>
</tr>
<tr>
<td>IDP X.509 Certificate</td>
<td>X.509 Certificate that you recorded.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Enter this value in a single line without line breaks.</td>
</tr>
</tbody>
</table>

6. Click **Save**.

**Clear the Axon Cache and Restart Services**

After you have configured Axon in the IDP and configured the Axon SAML files, you must update the Axon cache with the new configuration values.

1. In the Linux environment, run the following command to clear the contents of the cache directory:
   
   ```bash
   rm -rf <INSTALLATION_DIRECTORY>/axonhome/axon/app/cache/*
   ```

2. Run the following commands to restart the Memcached and HTTPD services:

   ```bash
   <INSTALLATION_DIR>/axonhome/third-party-app/scripts/memcached restart
   <INSTALLATION_DIR>/axonhome/third-party-app/scripts/httpd restart
   ```

**Author**

Abhilash Scariya
Lead Technical Writer

**Acknowledgements**

Pradeep G.N.
Lead QA Engineer