Link to article: https://discover.claromentis.com/knowledgebase/articles/996

SSO configuration via SimpleSAML 2.0 - Implementation Steps

Introduction

This article outlines the steps that will be undertaken during SSO setup with a supported SimpleSAML 2.0 compliant IDPs

Pre-requisites

One of the following supports IDPs will need to be used for **8.x**:

ADFS / DUO / Google gSuite / Okta / Cetrify / Azure / OneLogin

One of the following supports IDPs will need to be used for **9.x** (please note additional IDPs will be supported in future):

ADFS / Okta / Azure/Entra

Please see below the steps for each IDP, and follow the one for your chosen IDP:

ADFS

Step 1 - Claromentis to perform the initial setup on the server and provide yourselves with the necessary values.

Step 2 - Your team need to provide Claromentis with the following information:

The IDP URL - for example *http://adfs.companyname.com/adfs/services/trust*

ADFS Metadata URL or .XML file

NameID Policy - You will only need to confirm this if you have changed it from the default setting.

ADFS test user - **username** and **password** need to be provided, along with the following 3 attributes populated for this user:

```
1 - Firstname
2 - Lastname
3 - Email
```

IMPORTANT - Please ensure provisioned test users don't have 2FA enabled as this may stop us from testing and completing the work

Step 3 - Your team are to configure Relying Party Trust and Claim rules, using the following details:

Relying Party Trust

Claim rules

Active Directory attributes and additional claim rules dependent on login method (SHA-1 secure hash algorithm):

Username - Email Address:

> LDAP Attribute: E-Mail-Addresses, Outgoing Claim Type: E-mail Address
> LDAP Attribute: Given-Name, Outgoing Claim Type: Given Name
> LDAP Attribute: Surname, Outgoing Claim Type: Surname
> LDAP Attribute: SAMAccountName, Outgoing Claim Type: Windows account name

Username - DOMAIN\username:

This requires an additional claim rule to be set up, in addition to the above.

> Claim Type: 'Pass Through or Filter an Incoming Claim'
> Claim rule name: Windows Account Name
> Incoming claim type: 'Windows account name' & 'Pass through all claim values'

Step 4 - Once the you have confirmed the above has been configured, Claromentis to test the assertion using the provided test account

Step 5 - Troubleshooting with yourselves if needed

Step 6 - Claromentis to configure loginhandler, and pass to yourselves to test

---

Okta

Step 1 - Claromentis to perform the initial setup on the server and provide yourselves with the necessary values:

Single Sign on URL

Recipient URL

Destination URL

Audience Restriction

Attributes

> Firstname - mapped to Okta attribute, or Active Directory attribute
>
> LastName - mapped to Okta attribute, or Active Directory attribute
>
> Email - mapped to Okta attribute, or Active Directory attribute

IMPORTANT - Attribute '**Name format**' needs to be set to '**Unspecified**' otherwise Okta may not pass

attribute values to SAML

Step 2 - Your team needs to provide Claromentis with the following information for Claromentis to finish the SSO configuration:

The IDP URL

Metadata URL or .XML file

NameID Policy - The client will only need to confirm this if they have changed it from the default setting.

Okta test user - **username** and **password** need to be provided, along with the following 3 attributes populated for this user:

```
1 - Firstname
2 - Lastname
3 - Email
```

IMPORTANT - Please ensure provisioned test users don't have 2FA enabled as this may stop us from testing and completing the work

Step 3 - Once you have confirmed the above has been configured, Claromentis will test the assertion using the provided test account

Step 4 - Troubleshooting with yourselves if needed

Step 5 - Claromentis to configure loginhandler, and pass to your team to test

---

Azure

Step 1 - Claromentis Install the login handler and provide the necessary values to your team to configure within the Azure Gallery application (these are output to the LH Admin panel)

Step 2 Your team has to check out the Gallery App and follow the instructions:

https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/claromentis-tutorial

Step 3 Your team must provide Claromentis with the following information prior to the initial setup

The IDP URL

Metadata URL or .XML file

NameID Policy - The client will only need to confirm this if they have changed it from the default setting.

Step 4 Optional: Test the configuration and SSO - joint work between Claro and client. For Claromentis to perform this your team will need to configure a test user, configured like the below:

Azure test user - **username** and **password** need to be provided, along with the following 3 attributes populated for this user:

```
1 - Firstname
2 - Lastname
3 - Email
```

IMPORTANT - Please ensure provisioned test users don't have 2FA enabled as this may stop us from testing and completing the work

Step 5 Troubleshooting with your team if needed.

Loginhandler 1.x - backend installation directly on the server

DUO

Step 1 - Claromentis to perform the initial setup on the server and provide your team with the necessary values:

Service Provider Name

Entity ID

Assertion Consumer Service

Attributes:

> Firstname - mapped to DUO attribute, or Active Directory attribute
>
> LastName - mapped to DUO attribute, or Active Directory attribute
>
> Email - mapped to DUO attribute, or Active Directory attribute

Step 2 - Your team then must provide Claromentis with the following information:

The IDP URL - for example https://duodag.clientname.com/dag/saml2/idp/metadata.php

Metadata URL or .XML file

NameID Policy - You will only need to confirm this if they have changed it from the default setting.

DUO test user - **username** and **password** need to be provided, along with the following 3 attributes populated for this user:

> 1 - Firstname
> 2 - Lastname
> 3 - Email

IMPORTANT - Please ensure provisioned test users don't have 2FA enabled as this may stop us from testing and completing the work

Step 3 - Once your team have confirmed the above has been configured, Claromentis to test the assertion using the provided test account

Step 4 - Troubleshooting with your team if needed

Step 5 - Claromentis to configure loginhandler, and pass to your team to test

---

Centrify

Step 1 - Claromentis to perform the initial setup on the server and provide your team with the necessary values:

Service Provider Configuration - Manual configuration

SP Entity ID / Issuer / Audience

Assertion Consumer Service (ACS) URL

Account Mapping (this may only be needed if your team wants to use 'DOMAIN\username'. Please see section 6 of the following guide which contains information and screenshots of how your team may need to configure this. You can copy/paste and send the screenshots if needed.

Attributes:

> Firstname - mapped to Centrify attribute, or Active Directory attribute
>
> LastName - mapped to Centrify attribute, or Active Directory attribute
>
> Email - mapped to Centrify attribute, or Active Directory attribute

Step 2 - Your team must then provide Claromentis with the following information prior to the initial setup:

The IDP URL

Metadata URL or .XML file

NameID Policy - Your team will only need to confirm this if they have changed it from the default setting.

Centrify test user - username and **password** need to be provided, along with the following 3 attributes populated for this user:

> 1 - Firstname
> 2 - Lastname
> 3 - Email

IMPORTANT - Please ensure provisioned test users don't have 2FA enabled as this may stop us from testing and completing the work

Step 3 - Once you have confirmed the above has been configured, Claromentis will test the assertion using the provided test account

Step 4 - Troubleshooting with your team if needed

Step 5 - Claromentis to configure loginhandler, and pass to your team to test

---

OneLogin

Step 1 - Claromentis to perform the initial setup on the server and provide your team with the necessary

values:

Login URL

Recipient

Consumer URL

Audience

Attributes:

> Firstname - mapped to OneLogin attribute
>
> LastName - mapped to OneLogin attribute
>
> Email - mapped to OneLogin attribute

Step 2 - Your team must then provide Claromentis with the following information prior to the initial setup:

The IDP URL

Metadata URL or .XML file

NameID Policy - You will only need to confirm this if you have changed it from the default setting.

Azure test user - **username** and **password** need to be provided, along with the following 3 attributes populated for this user:

> 1 - Firstname
> 2 - Lastname
> 3 - Email

IMPORTANT - Please ensure provisioned test users don't have 2FA enabled as this may stop us from testing and completing the work

Step 3 - Once your team has confirmed the above has been configured, Claromentis will test the assertion using the provided test account

Step 4 - Troubleshooting with your team if needed

Step 5 - Claromentis to configure loginhandler, and pass to yourselves to test

---

Windows NTLM Single Sign-On

NTLM is only available to **Windows On-Premise** clients and *not* SaaS. The setup is very simple, the steps are:

Step 1 - Claromentis to configure IIS, the configuration file or .env and PHP session folder

Step 2 - You will need to configure browser settings which Claromentis will send over in a block of instructions.

Created on 26 September 2024 by Jack Lord