

# Implementing SSO with Login Handler and Ping

### Introduction

This is an overview guide on how to implement SSO (Single-Sign-On) with Claromentis and Ping Identity

## Prerequisite

- Claromentis 9+ with Login Handler Module version 4+
- PingOne SSO Services
- Ping Identity Administrator Access

## **Ping Identity**

□ Ping Documentation:

Step 1: Configure Ping Identity for single sign-on (SSO)

- 1. Navigate to the Ping Administrator Console
- 2. Under Environments, Create Environment > Customer Solution Environment



4. In the Environment Name create a name that you can easily identify the Claromentis system for example

#### Claromentis Intranet SSO

- 5. Add Description and details as required.
- 6. Select "Manage Environments" then navigate to Applications

<ul> <li>PingIdentity.</li> <li>Getting Started</li> </ul>		🔒 tri	ial_claromentis_	> SSO Te	sting POC	Environment SANDBOX	) -	?	🕲 Explore 👻	± more there -
		Ар	Applications 🕂		Ad	dd Application				×
<b>()</b>	Overview	٩	Search		Applica	ation Name *				
*	Directory -	5 Ap	plications by Applicat	tion Name -	Descrip	otion				
	Applications				Clar	romentis SSO Testing				
	Applications Application Catalog	P	PingOne A	Admin Console						
	Resources	P	PingOne /	Application Portal	lcon					
	Application Portal	P	PingOne S	Self-Service - MyAc	Max Siz	ze 1.0 MB				
Ø	Authentication -	í	SSO Testi	ng POC	Applica	ation Type				Show Details
•	Threat Protection				0	Select an option below find what you need in	v or view the A the catalog, co	pplication Catalo	g to use a templated ir OIDC to get started.	tegration. If you can't
(inter)	dentity vertication	-			0	SAML Application		OIDC Web App	6	Native
**	Integrations -				-					
Ģ	User Experience					Single-Page	<>	Worker		Device Authorization
S	Settings -									

- 7. Under Application Type select 'SAML Application"
- 8 Click Configure
- 9. Under SAML Configuration select Import Metadata
- You will need a Metadata file from Claromentis by following these steps:

On the browser navigate to:

Replace {yoursystemurl} with your system address for example companyname.myintranet.com

#### Username: admin

Enter the password by revealing the password in Auth Admin Password (only visible to administrator)

8. Download the Metadata configuration from Ping under Connection Details as this will be required for the Claromentis Login Handler Admin Panel

Connection Details A		
Issuer ID https://auth.pingone.eu/bc76cbee	5a 🖸	
Initiate Single Sign-On URL https://auth.pingone.eu/bc76cbee- =claromentis_t 3b7	a/saml20/idp/startsso?spEntityId	Ō
IDP Metadata URL https://auth.pingone.eu/bc7 b-42 6a	2f71de8cf5a/saml20/metadata/184fdda6-f87	Ū
Single Signon Service https://auth.pingone.eu/bc76	a/saml20/idp/sso	
Single Logout Service https://auth.pingone.eu/bc7	2f71de8cf5a/saml20/idp/slo	
Download Metadata Download Signing Certific	ate	

9. Take a copy of the Issuer ID as this will be used for IDP Identifier under IDP Configuration in Claromentis

#### 10. Attributes Mapping

Here is an example of Attribute Mapping between Claromentis and Ping

	SSO Testing	POC						:	×
		Overview	Configuration	Attribute Mappings	Policies	Access			
Thes Mapp	e mappings asso bing attributes.	ociate PingC	One user attribut	tes to SAML or OIDC	attributes i	in the appli	ication. See	)	0
	If this Applica	ation is acce	essible by users	from more than one	External Id	P, it is reco	mmended t	hat y	bu

SSO Testing POC	PingOne	
saml_subject	User ID	Required
Email	Email Address	Required
Firstname	Given Name	Required
Login	Username	Required
Surname	Family Name	Required

## Claromentis

Step 2: Configure SSO in Claromentis

Navigate to Admin  $\rightarrow$  Custom Login handler  $\rightarrow$  SSO Configuration

- 2. Upload Federation Metadata XML (you will need XML from Ping under Connection Details
- 3. Populate Security Configuration
- 4. IDP Identifier: this should be populated from the XML
- 5. Entity ID you will need to copy this to Ping Configuration
- 7. Name ID Policy: Unspecified
- 6. Save Options

#### **Identity Provider**

Ping ~								
The information in this section will need to be configured by the client in their Claromentis Ping application control panel:								
Audience Restriction:	claromentis_b	WTOM/IN'						
Single Sign On URL:	https://ssotesting.c acs.php/claromenti	laromentis.dev/custom/loginhandler/simplesaml/www/module.ph is	p/saml/sp/saml2-					
Recipient URL:	https://ssotesting.c acs.php/claromenti	laromentis.dev/custom/loginhandler/simplesaml/www/module.ph is	p/saml/sp/saml2-					
Destination URL:	https://ssotesting.c acs.php/claromenti	laromentis.dev/custom/loginhandler/simplesaml/www/module.ph is	p/saml/sp/saml2-					
Attribute	Name	Value						
Statements:	Login	user.login						
	Firstname	user.firstName						
	Surname	user.lastName						
	Email	user.email						
Security Configur	ration							
Technical Contact Name	e							
Administrator								
Technical Contact Email	I							
Auth Admin Password								
•••••	······							
IDP Configuration								
IDP Identifier								
https://auth.pingone.eu/bc 5a								
Entity ID								
claromentis_b:								
Name ID Policy								
Unspecified V								
Federation Metad	lata XML							

# Testing & Troubleshooting