Configuring Single Sign-On (SSO)

Last Modified on 02/08/2021 9:42 pm EST

Prerequisites

When configuring your SAP Cloud Platform Open Connectors account to use single sign-on (SSO), there are a few things you need to know:

- If your SAP Cloud Platform Open Connectors account was created prior to January 2017, it may not have a customer id by default; this can result in an error if you try to add members after setting up SSO. If this is the case, please talk to your account manager prior to getting started.
- You will need your SSO provider's SAML metadata.

Configuring SSO in SAP Cloud Platform Open Connectors

Please note that code references provided in this article are just examples; your metadata might be structured slightly differently.

- 1. Select the Security tab on the left-side toolbar, and then select Identity.
- 2. Select Application Identity Provider, and then click Add Trusted Identity Provider.

Security		API DOCS
SETTINGS ACCOU	NTS ROLES IDENTITY	
Accounts	Members Application Identity Provider	
م	Manage Trust Relationships And Federation Settings	
Andy Sherwin's Company Default Account	The registered Identity Providers for your company. Default Identity Providers provided by your administrator appear at the top of the list and cannot be edited. However, if you want to override the Identity Provider for your company then you may 'Add a Trusted Identity Provider'. For information and best practices configuring SAML services, see the Help Center.	NTITY PROVIDER

The Trusted Identity Provider configuration page appears.

- 3. In the Level field, select the SAP Cloud Platform Open Connectors level at which you want this trusted SSO to exist. The options are organization and account. This is the only real SAP Cloud Platform Open Connectorsspecific information you will need to provide; the rest of the configuration information is based on the identity provider.
- 4. In the Entity ID field, enter the entity ID. In the metadata, this should appear in a field related to the Entity Descriptor; for example:

entityID="http://localhost:5555/auth/realms/parent">

- 5. In the Description field, enter a unique way to identify the entity provider.
- 6. In the SSO URL field, insert the redirect URL. In the metadata, this should appear in a field related to single sign-on; for example:

Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://localhost:5555
/auth/realms/parent/protocol/saml"/>

7. In the Name ID Format field, select the appropriate option; we recommend selecting persistent.

8. In the optional Logout URL field, enter the redirect URL. In the metadata, this should appear in a field related to logout; for example:

Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="http://localhost:5555 /auth/realms/parent/protocol/saml"/>

- 9. If you enter a value for the Logout URL, you should also enter a value for the Logout Redirect URL. This URL is where users will be redirected after they are logged out.
- 10. In the Signing Certificate field, enter the certificate's content. In the metadata, this should appear in a field with a name similar to "x509 certificate"; for example:

MIICmzCCAYMCBgFujBpE7jANBgkqhkiG9w0BAQsFADARMQ8wDQYDVQQDDAZtYXN0ZXIwHhcNMTkxMTIxMDM1NDIyOcyFPM 2Ed4vWRw5bug6cD21HMcQpbKMTeVV/m2zotETaoZGDZFt3txe3H5M9NqHplf7GivOXfclBd4wA3azDshpvnWCMAwCIxiCO EF6flTY38f7H182Ryeutc9hKJ/6+96Azj00P9uULngQ4GThtClGPia0ui+S0k+ot0dzojXu2HY1raUIvgi8xg45f0MTnMr eUf9Shwlak/iUDw++7Nhg3sAeZsdfsdfsdfcoz4LB2kryaXEX16B+PMQgCRqebtoGHnSBAgMBAAEwDQYJKoZIhvcNAQELB QADggEBAJ7Cna0zgXYbA5iXJpOVBDsuJPauLi7yMOxUP7OMwwfB2+14tvIC50Yxhw96/AM6gkbZCXCSvlEFDucpVv3w8on L8oW+gVxobN7J6vScELXz3sGFfSDq9Z0iVKjXbsWIqFfkMQ1koxUqoU8+xoYAqpp0Fudo71YnwrNafIwkMAJfsxf4meAbX 9MuhVv/1/Yo/4H9sYE9IqM0TAPPtnvNDokNBm0huJ+F0BP6ahkaOWhKQ83S1FN7IuQuihPd14uPCubpAj11/8JUNUquNAb mpmCFTXX3VZw6pYAFEPyqKkegZnN01H8tHj/akMFLrJhuLYgehQfRYSXe5RN6IfhaLnI=

- 11. From the Signature Algorithm menu, select the algorithm to use in the signing process.
- 12. Click Save.

The Manage Trust Relationships and Federation Settings page appears, listing the available trusted providers. 13. Click the download button for your provider to generate and download the provider XML file.

Member	Application Ide	entity Provider						
Manage The registe administrat the Identity information	Manage Trust Relationships And Federation Settings The registered Identity Providers for your company. Default Identity Providers provided by your administrator appear at the top of the list and cannot be edited. However, if you want to override the Identity Provider for your company then you may 'Add a Trusted Identity Provider'. For information and best practices configuring SAML services, see the Help Center. ADD TRUSTED IDENTITY PROVIDER							
Default	Name	Description	Level	Edit	Download			
	http://test.entityid.url	MyCoolProvier	account		B			

- 14. Upload the provider XML file to the SSO provider's side in order to establish the connection.
- 15. Add members who will sign in using SSO. Do this on the Members page of the Identity tab.

Security					API DOCS
SETTINGS ACCC	DUNTS ROLES ID	ENTITY			
Accounts	Members Ap	plication Identity Provider			
Andy Sherwin's Company Default	Access Control	List All Members	Ŧ		BULK ADD ADD MEMBER
Account	Member	Roles	Created	Acti	User Edit
		No	data found		

Note: as a best practice, name the list of members with the corresponding external ID from the service provider's system.

16. After completing these steps, the user should be able to sign in using SSO.

Currently, SAP Cloud Platform Open Connectors does not have a way to force SSO sign-in, but we may develop it in the future.