

Configuring Single Sign-On (SSO)

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

Prerequisites

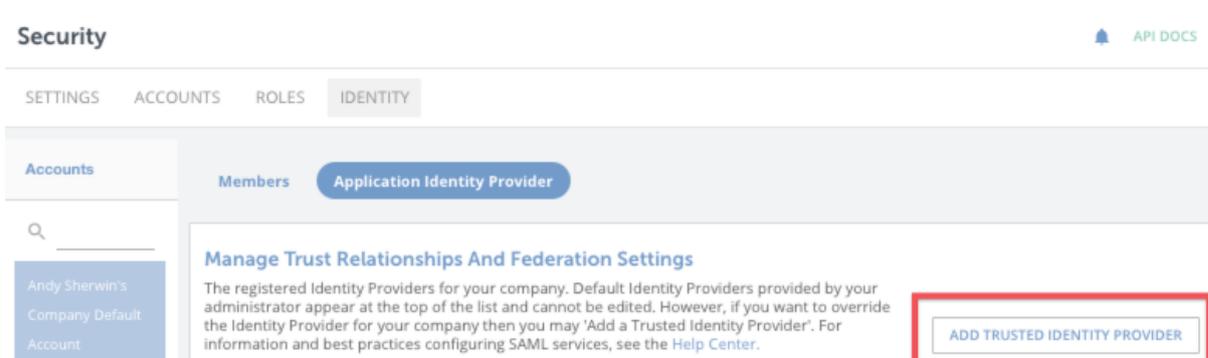
When configuring your SAP Cloud Platform Open Connectors account to use single sign-on (SSO), there are a few things you need to know:

- 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**.



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 Connectors-specific 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`.

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.
