Configure an External Identity Provider for API Cloud Authentication

Single Sign-On (SSO) allows users, who are authenticated against one application, to gain access to multiple other related applications without having to repeatedly authenticate themselves. It also allows web applications to gain access to a set of backend services with the logged-in user’s access rights. The backend services can authorize the user based on different claims like the user role. An Identity Provider (IdP) is responsible for issuing identification information and authenticating users by using security tokens. WSO2 API Cloud uses WSO2 Identity Server as the default Identity provider (IdP). An organization can have its own IdP that provides authentication for internal users. In such scenarios, the organization can link their IdP to WSO2 Identity Cloud to provide SSO based authentication for API Cloud apps.

The diagram below shows how an external IdP-based SSO is configured.

1. The user visits the API Cloud application.
2. A SAML authentication request is sent to the Identity Cloud.
3. Identity Cloud is configured to forward the authentication requests received for a particular organization to an external IdP.
4. The organization’s IdP prompts the login window and the user submits the credentials.
5. An authentication success response is sent back to the Identity Cloud.
6. Identity Cloud sends a SAML response to the corresponding API Cloud application. Before sending the response, Identity Cloud stores (provisions) the permission information of the authenticated user in an internal user store. The API Cloud applications refer to this user store for authorization.

In this tutorial, you learn how to configure an external identity provider for API Cloud authentication.
1. Log in to WSO2 API Cloud. Click **Configure > External Users**.

2. In the **API Cloud Web UI Access** tab, select **Connect Your Identity Provider** and submit the identity provider details.

   ![Connect External Users To API Cloud](image)

   **Connect External Users To API Cloud**

   To connect your users to WSO2 API Cloud, provide us with the information below so that the necessary configurations can be made on your behalf.

   - **API Cloud Web UI Access**
   - **API Consumer Authentication**
   - **Connect Your User Store**
   - **Connect Your Identity Provider**

   Not sure what you need? Click here to contact us and we will get back to you.

   To connect your identity provider to provide Single Sign-On (SSO) to the web interface of WSO2 Cloud, please provide the following information:

   - **Identity Provider**: Select Your Identity Provider
   - **Auth Mechanism**: Select the Authentication Mechanism

   **Submit Request** | **Cancel**

   ![Connect External Users To API Cloud](image)

   **Connect External Users To API Cloud**

   To connect your users to WSO2 API Cloud, provide us with the information below so that the necessary configurations can be made on your behalf.

   - **API Cloud Web UI Access**
   - **API Consumer Authentication**
   - **Connect Your User Store**
   - **Connect Your Identity Provider**

   Not sure what you need? Click here to contact us and we will get back to you.

   To connect your identity provider to provide Single Sign-On (SSO) to the web interface of WSO2 Cloud, please provide the following information:

   - **Identity Provider**: Select Your Identity Provider
   - **Auth Mechanism**: Select the Authentication Mechanism

   **Submit Request** | **Cancel**

3. The WSO2 team will contact you, get the required information, and configure your IdP in the Identity Cloud.

   Users in your user store can have different roles. You may want to restrict access to the API Cloud applications for the users in your user store. In such cases, you can send a `roles` attribute with the IdP authentication response and this attribute will be mapped to the cloud-related roles. This capability depends on your IdP.

   When the role information is not present in the response (e.g. Google OpenID-Connect), Identity Cloud maps the authenticated user to the organization’s default internal role. We can assign subscribe/create/publish/admin permissions to this role. All the authenticated users will have the same role and the same set of permissions. Permissions should be determined based on your organization's needs.

   **WSO2 supports only the email address as the user ID. Therefore, your IdP will have to send the email address in the response.**

4. Configure custom URLs for SSO login.
API Cloud applications identify organizations with an external IdP configured, based on a specific custom header. When the header is available in the request, the application executes the external IdP-based authentication flow. If the header is unavailable, the default authentication flow is executed. This custom header is sent through custom URL configurations. Let's say we have configured a load balancer to send the custom header with `api.customdomain.organization.com/publisher`. Then, `api.cloud.wso2.com/publisher`, which does not have a custom header, is executed with the default authentication flow. However, `api.customdomain.organization.com/publisher`, which includes a custom header, is executed with the external IdP-based authentication flow.

For details on how to configure a custom URL for the API Cloud Store, see Customize Cloud URLs.

To configure custom URLs for the API Cloud Publisher and Admin apps, you have to submit a support request as described in step 2 (this will be supported through a UI in the future).

Provide the following information to configure custom URLs:

- Custom Domain
- SSL Certificates
- SSL Key and Chain Files

You can always use the default cloud URLs and log in to your Cloud account for administrative tasks.

5. WSO2 will inform you once the configurations are completed. You will be able to create, publish, subscribe and invoke APIs after completion.

Token API: You will not be able to use the password grant to generate access tokens because your credentials are unavailable in our user store.