Configure an On-Premise User Store for API Cloud Authentication

WSO2 Cloud services are offered to users who are registered in the Cloud's user store. Admins of the organization can invite and register their corporate users to the Cloud's user store, after signing up to WSO2 Cloud. Instead of explicitly inviting each and every user, some organizations might want to directly connect their internal user stores to the API Cloud. In such cases, organizations can connect their local LDAP user stores to the API/Identity Cloud through the WSO2 Outbound Agent. This allows the organization to provide authentication for users in the LDAP, without sharing the credentials of the LDAP with WSO2 Cloud.

For information on authenticating users who are not in the WSO2 Cloud's user store, see Authenticate External Users for API Invocation.

As WSO2 Cloud only supports email addresses as the user IDs to connect with WSO2 Cloud, your user stores should use the email address as the user ID.

The diagram below shows how authentication happens with an on-premise user store in WSO2 API Cloud:

1. The user visits the API Cloud.
2. A SAML authentication request is sent to WSO2 Identity Cloud.
3. The Identity Cloud sends an authentication request (HTTPS) to the outbound agent that is configured in the customer’s environment.
4. The agent completes the authentication and sends the response back to the Identity Cloud.
5. The Identity Cloud sends the SAML Auth response to the API Cloud and the user is logged in to the requested application after authorizing.
6. The API Cloud directly calls the outbound agent for authentication requirements that are not related to SSO.

In this tutorial, you configure an on-premise (secondary) user store for WSO2 API Cloud authentication.

Let's get started.
1. Log in to WSO2 API Cloud. Click **Configure > External Users**.

2. In the **API Cloud Web UI Access** tab, select **Connect Your LDAP User Store** and submit the requested details.
   Role permission mappings are as follows:
   - Create APIs: Roles allowed to create APIs
   - Publish APIs: Roles allowed to publish APIs
   - Subscribe to APIs: Roles allowed to subscribe to APIs
   - Access Admin App: Roles allowed to access the Admin app

3. Configure custom URLs for SSO login.

   WSO2 API Cloud applications identify the organizations that have secondary user stores configured, based on a specific custom header. When the header is available in the request, the application executes the secondary user store-based authentication flow. If the header 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. But, `api.customdomain.organization.com/publisher` has a custom header. This is executed with the secondary user-store based authentication flow.

   For details on how to configure a custom URL for the API Store, see **Customize Cloud URLs**.
Configuring a custom URL for API Publisher and Admin Apps

To configure custom URLs for API Publisher and Admin apps, submit a support request as described in step 2. (WSO2 will support this through UIs 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 account for administrative tasks.

4. Note that WSO2 informs you once the configurations are completed. You can create, publish, subscribe, and invoke APIs after completion.