

Overview of Wex External IDP Integration

This document outlines the sequential process for customers integrating their Identity Provider (IDP) with Wex. This integration enables a streamlined and secure authentication experience for users.

Customer interest in connecting via their IDP is typically fielded by Sales and Customer Support teams, who then provide the customer with the IDP enablement requirements document for review by their CTO or technical leadership, before the customer completes and submits it back to Customer Support or Sales.

WEX Internal Process

- **IDP Connection Request:** The completed requirements document is submitted to the OWI team for IDP connection setup. Currently, this involves a manual JIRA ticket.
- **OWI Team Setup:** The OWI team proceeds with setting up the IDP connection based on the provided requirements.

Customer Prerequisite Questionnaire

With our discussions and/or JSM ticket fulfillments, we must confirm the following;

- **Which IDP platform are you using (e.g Okta, Microsoft Entra ID)?**
 - Platforms such as *Okta*, *EntraID*, and *PingIdentity* offer native connections within Auth0, simplifying the process of establishing trust between the Identity Provider (IdP) and Auth0.
- **What Identity provider protocol do you plan to use (e.g SAML, OIDC)?**
- **Which WEX application does the customer desire to access?**
- **What is the experience that the customer wants for their end user?**
 - If using the new email/password login with the Universal Login Screen to kick off the IdP flow, which email domain(s) should be configured to redirect users to your IDP through Home Realm Discovery?
 - Does the user intend to kick off the IdP flow from within your provider?
- **What are the specific deadlines for collaboration and development across the UAT and Production environments?**

Self Service SSO Ticket guide

After initial discussions, the customer should expect to be emailed a link to a Self Service form to complete. This will trigger the creation of the enterprise connection on the Wex Auth0 service provider.

Once you have accessed the link, you will be prompted to complete the form, which guides you through every step.

Set up wex-ent-qa

You are a few simple steps away from setting up access to wex-ent-qa. This setup process involves making some changes to your identity provider. Before you begin, open your identity provider in a separate browser tab or window.

[Get Started](#)

The first decision you must make is to select your identity provider. Here, you will select what has been discussed with the Wex customer support team. Depending on how this ticket was constructed, you should only see one available choice. In this example, we will choose a regular SAML application.

Select Your Identity Provider

Choose the identity provider you plan to integrate with wex-ent-qa to access step-by-step instructions for SSO configuration.

 Okta	 ADFS	 Entra ID
 Google Workspace	 Keycloak	 PingFederate
 Custom SAML	 Custom OIDC	

Next

The next step is to create an application on your identity provider. Here, there are two fields that you must configure;

1. **ACS (Assertion Consumer Service) URL (SSO)** - This is the url that the identity provider will send OIDC tokens / SAML assertions to. This will be in the format of <https://<env>.tch.com/login/callback?connection=<connection-name>&organization=<organization-name>>. Contrary to the self service form, you must include the organization parameter as users on *One Wex Identity* authenticate through the context of an organization.
2. **The service provider entity ID** - This defines the audience that your application expects when receiving requests. This often has the format of [urn:auth0:wex-ent-<env>:<connection-name>](#).

Configure Custom SAML

1. Create Application
2. Configure Connection
3. Test SSO

Create an Application

Create a generic SAML application in your identity provider.

Copy and paste the **Single Sign-On URL** and the **Service Provider Entity ID** in the corresponding field in your identity provider.

Single Sign-On URL

`https://qa.tch.com/login/callback?connection=sampleSaml`



Endpoint users are redirected to for initiating single sign-on, enabling users to access multiple applications. Also known as: Assertion Consumer Service URL, Callback URL.

Service Provider Entity ID

`urn:auth0:wex-ent-qa:sampleSaml`



Unique identifier for service provider. Also known as: Audience URI.

Back

Next

Finally, you will be prompted to test the connection. This is not required, but as the implementation process is not yet complete, you will not be able to fully authenticate to the Wex application.

Configure Custom SAML

1. Create Application
2. Configure Connection
3. Test SSO

Test SSO

Test the connection to ensure SSO setup is successful.

Selecting **Test Connection** will open a new window and redirect you to log in with your SAML Identity Provider. You'll receive a SAML response in return.

Please do not close out this window while testing.

Test Connection 

Back

Done

Below you must enter information about your identity provider such as the Single sign on Url, certificates/credentials and if you are using SAML, you must enable the signing on the SAML assertion requests, preferably using the SHA256 signing algorithm.

Configure Custom SAML

1. Create Application
2. Configure Connection
3. Test SSO

Configure Connection

Establish a connection between your identity provider and wex-ent-qa

Automatic **Manual**

Single Sign-On Login URL

Endpoint for initiating secure authentication in SAML SSO connections.

Signing Certificate

 Upload Signing Certificate



Subject: Microsoft Azure Federated SSO Certificate

1.07 KB



SAML X.509 public key encoded in PEM or CER format.

Advanced Settings

☒ Sign Request

When enabled, the SAML authentication request will be signed. Download the [certificate](#) and provide it to the SAML P that will receive the signed assertion to validate the signature.

Sign Request Algorithm

Sign Request Algorithm Digest

Request Protocol Binding

[Back](#)

Create Connection

Acceptance Testing

The customer should attempt authenticating from their IDP application on lower environments. Due to Wex services being in an internal private network, they will likely fail to access the privacy policy page or the application page after successful authentication.

The lowest environment that is accessible on the public internet is Stage, in which developers from the customer side can authenticate into the Wex application.