



HR Learn Azure AD/O365 Integration Guide

Table of Contents

HR LEARN AZURE AD/O365 INTEGRATION GUIDE	1
OVERVIEW	2
INTEGRATION SETUP	2
ADDITIONAL INFORMATION	4

Overview

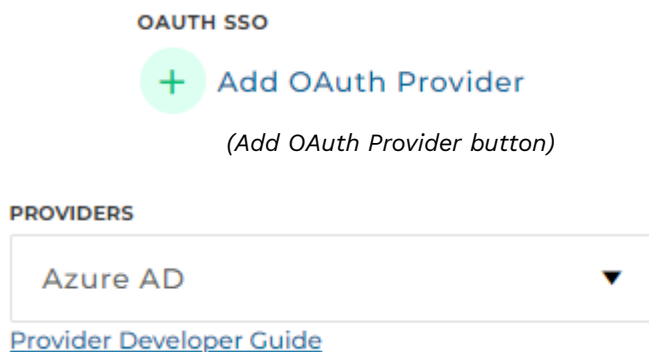
This guide is targeted at LMS and IT administrators who would like their LMS users to authenticate via OAuth to their company's Azure AD or O365 directory service.

This guide will walk you through the process of setting up OAuth SSO integration with your company's Azure AD or O365 directory services. Parts of this process are technical in nature and will require you to consult with your IT administrator or person responsible for administering your company's Azure AD or O365.

Integration Setup

If you are setting the Azure AD/O365 OAuth integration up on a portal that currently has users who are logging in via the built-in LMS sign-in, or via an existing SAML integration, please be sure to review the "Additional Information" section of this guide before setting up the integration as there may be some nuances related to existing users.

- To begin, you will need to set up your OAuth client in Azure AD/O365. For guidance on this, go to the System > Configuration > Login Setup screen and click the "Add OAuth Provider" button under "OAuth SSO." Then, select "Azure AD" under the "Providers" drop-down and click the "Product Developer Guide" button.



(Product Developer Guide link for Azure AD)

- The link will take you to the Microsoft developer guide for setting up an OAuth client in Azure AD/O365. You will need to work with your company's IT administrator or person responsible for administering your company's Azure AD or O365 to set up the OAuth client.
- Once the OAuth client has been set up and you have your OAuth Client ID, Client Secret, and Tenant ID (if OAuth client is for single tenant), you will need to go back to the LMS System > Configuration > Login Setup screen and click "Add OAuth Provider" again to complete the setup.

(New OAuth Provider modal screen)

- On the “New OAuth Provider” screen, select Azure AD and enter the Client ID, Client Secret, and Tenant ID (if the Account Type is single tenant) from your OAuth client setup.
- Then, select any user field mappings you wish to create from Azure AD/O365 to LMS user profile by clicking the (+) button and selecting the field mapping from the drop-downs. By default, the OAuth client will synchronize the following Azure AD/O365 fields to LMS user profile fields. These are required for the integration to function properly and are unchangeable.
 - givenName -> First Name
 - surname -> Last Name
 - userPrincipalName -> Username

(Field mapping drop-downs)

- Once you have entered all OAuth client information and created your field mappings, click “Save Changes” to finish setting up your Azure AD/O365 OAuth client.
- After the set up is finished, users will now see an option to Sign in with Azure AD on the LMS sign-in form.



(Sign in with Azure AD button on login form)



Sign in

Email, phone, or Skype

[Can't access your account?](#)

Next

 Sign-in options

[Terms of use](#) [Privacy & cookies](#) ...

(Microsoft account login form)

Additional Information

- If you have an existing Azure AD integration to the LMS using SAML and wish to replace it with the new OAuth workflow, be sure that the current SAML integration's user identifier key is the same as the Azure AD [userPrincipalName] field. The initial synchronization of a user keys on the value in the LMS username field against the [userPrincipalName] field in Azure AD. If these values do not match, a new user will be created.
 - You can work with LMS support to ensure these fields are in agreement prior to moving away from your SAML integration.
- If you have existing users in the LMS that you wish to have authenticated via Azure AD/O365, you must ensure their usernames agree with the [userPrincipalName] field values in your Azure AD/O365, similarly to SAML integration described above.
- You may allow for a "hybrid" set up that allows users to both authenticate to the LMS using the standard LMS login form and any combination of OAuth options including Azure AD/O365. However, if a user's username field agrees with the synchronization key of an OAuth SSO integration (in the Azure AD case, [userPrincipalName]) the user will be signed in with that LMS user account.
- You can force users to login using only the Azure AD/O365 OAuth integration (or any other OAuth integration) by turning on the "Require users to sign in using only the SSO options configured below." option from the System > Configuration > Login Setup page.

- If you have additional questions or would like consultation about the various identity management/SSO/sign-in options available in the LMS, please contact support.