



Deltek

Deltek Ajera 9

Microsoft Azure Active Directory
Integration for Single Sign-On

August 16, 2021

While Deltek has attempted to verify that the information in this document is accurate and complete, some typographical or technical errors may exist. The recipient of this document is solely responsible for all decisions relating to or use of the information provided herein.

The information contained in this publication is effective as of the publication date below and is subject to change without notice.

This publication contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, or translated into another language, without the prior written consent of Deltek, Inc.

This edition published January 2021.

© Deltek, Inc.

Deltek's software is also protected by copyright law and constitutes valuable confidential and proprietary information of Deltek, Inc. and its licensors. The Deltek software, and all related documentation, is provided for use only in accordance with the terms of the license agreement. Unauthorized reproduction or distribution of the program or any portion thereof could result in severe civil or criminal penalties.

All trademarks are the property of their respective owners.

Overview	1
About Single Sign-On with Microsoft Azure Active Directory	2
Important Considerations Regarding SSO Model	2
Support for Multi-Factor Authentication	2
Configure Single Sign-On using Azure AD	2
Sign Up for a Microsoft Azure AD Account	3
Configure Azure AD Connect	4
Configuration Steps for Azure AD Connect	4
Add and Configure the Deltek Ajera Application	6
Setting up the Azure integration in Ajera	10
Log in Using Windows Authentication (SSO)	11
FAQs for Microsoft Azure Active Directory Integration	12
Is there a fee to use Microsoft Azure Active Directory?	12
Does Single Sign-On (SSO) and Two Factor Authentication (2FA) need to be set up before or after moving to Ajera Cloud?	12
Is SaaS Administrator Access required to set up SSO?	12
Where do I find the Ajera customer URL?	12
Is it possible to use a separate Active Directory vendor and have it connect to Microsoft Azure?	12
Is it possible to do a test run using SSO?	12
Is SSO available using Mobile Timesheets and using the Deltek Mobile Expense app?	13

Overview

Welcome to the Deltek Ajera Microsoft Azure Active Directory Integration for Single Sign-On Guide. This guide provides technical guidance for configuring single sign-on in Microsoft Azure and turning on the integration in Ajera.

About Single Sign-On with Microsoft Azure Active Directory

Microsoft Azure AD's single sign-on feature lets Ajera users log on to Ajera using their Windows usernames and passwords instead of using separate Ajera usernames and passwords. To set up single sign-on, an Ajera administrator must complete the following configuration steps, described in more detail in this guide.

Note :	You will still use your Ajera username and password when logging into the Mobile Time and Mobile Expense apps.
------------------	--

Important Considerations Regarding SSO Model

Currently, the most common single sign-on model used by Ajera customers is to synchronize users and passwords to Windows Azure Active Directory.

An alternative method is to set up Windows Azure Active Directory to federate back to your local Active Directory via ADFS (Active Directory Federation Services) to authenticate users via your on-premises Active Directory. With this model, you do not need to synchronize users and passwords to Windows Azure Active Directory.

Support for Multi-Factor Authentication

Windows Azure Active Directory supports multi-factor authentication.

Configure Single Sign-On using Azure AD

To set up single-sign on, an Ajera administrator must complete the following steps:

1. [Sign up for Microsoft Azure AD account.](#)
2. [Configure Azure AD Connect.](#)
3. [Add and Configure the Deltek Ajera Application.](#)
4. [Set Up the Azure Integration in Ajera.](#)
5. [Log in Using Windows Authentication.](#)

Sign Up for a Microsoft Azure AD Account

If your firm does not already have a Microsoft Azure AD account, you can sign up for a free account at <https://azure.microsoft.com/en-us/free>.

Microsoft also offers an Azure AD Premium account for a cost at <https://azure.microsoft.com/enus/trial/get-started-active-directory>.

The Premium edition is **not** required for using the single sign-on solution for Ajera.

Configure Azure AD Connect

For more background information about Azure AD Connect, see [Microsoft's What is Azure AD Connect](#). This describes what Azure AD Connect is and how it works.

Note :	This part of the set up is managed by you. Ajera Support cannot assist in the steps needed to set up Azure properly.
------------------	--

Prerequisites

Review and complete the prerequisites for Azure AD Connect as outlined by [Microsoft's Prerequisites for Azure Active Directory Connect \(Azure AD Connect\)](#).

This article also lists hardware requirements.



Deltek recommends that you do not install Azure AD Connect on your domain controllers.

Configuration Steps for Azure AD Connect

To configure Azure AD Connect:

1. Download and install the Microsoft Online Services Sign-In Assistant for IT Professionals RTW (msoidcli_64.msi) from the Microsoft web page.
Refer to the installation instructions on the web page.
2. Download and install the Azure Active Directory Module for Windows PowerShell for the 64-bit version (AdministrationConfig-en.msi) from the Microsoft web page.
Download the latest version that is in general availability. Refer to Microsoft documentation for help.
3. Download and install Microsoft Azure Active Directory Connect (AdministrationConfigen.msi) available on the Microsoft web page.
 - Review the account and permissions information on the Microsoft web site.
 - You must set up the following required accounts with a username and password:
 - Windows Azure Active Directory (Global Administrator)
 - On-Premise Active Directory (Enterprise Administrator)



- For more information, see Managing Azure AD Connect.
- Depending on the size of your on-premises Active Directory, the installation of Azure AD Connect can take some time, especially if you select the option to synchronize users at the end of the installation.

4. Log into your Windows Azure portal and verify that users are synchronized with Windows Azure AD.
5. Test a user on the Microsoft Apps portal at: <https://myapps.microsoft.com>.
 - You will not see any applications, but you can test authentication.
 - Use an existing user name and password for the test.



For troubleshooting information, see:

<https://msdn.microsoft.com/library/azure/jj151834.aspx>.

Add and Configure the Deltek Ajera Application

To add and configure the Deltek Ajera application:

1. Go to <https://portal.azure.com> to launch the Azure portal.
2. From Azure services, select **Azure Active Directory**.
3. From the Manage menu, select **App registrations**.
4. From the actions at the top of the menu on the App Registrations screen, Select **+ New registration**.

Microsoft Azure Search resources, services, and docs (G+)

Home > Default Directory >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Deltek Ajera ✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Default Directory only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web https://SERVERNAME/Ajera ✓

[By proceeding, you agree to the Microsoft Platform Policies](#)

Register

5. Perform the following actions on the Register an Application screen:
 - a. In the **Name** field, enter: **Deltek Ajera**.
 - b. Under **Supported account types**, select **Accounts in this organizational directory**

only.


- c. Under **Redirect URI (Optional)**, select **Web** and enter your Ajera customer URL.

For example, enter: **https://ajera.com/V#####** (SaaS clients) or
https://[ServerName]/Ajera (On-Premise clients).


- d. Click **Register** to create and save the application.

The properties of the Deltek Ajera application display.

6. Click on the application that you just registered (Deltek Ajera) from the list, hover over the **Application (client) ID**, and click the clipboard icon to the right to store the ID for future use.

You will enter this ID into the **Application (client) ID** field on the **Azure** tab in  > **Setup** > **Company** > **Preferences** > **Integration** tab.

7. On the same application, hover over the **Directory (tenant) ID** and click the clipboard icon to the right to store the ID for future use.

You will enter this ID into the **Directory (tenant) ID** field on the **Azure** tab in  > **Setup** > **Company** > **Preferences** > **Integration** tab.

Display name : Deltek Ajera

Application (client) ID : ab2fb4e5-e8af-423f-b49d-36b0c41d037c

Directory (tenant) ID : dc4b9e6e-e1ad-4932-a913-b9d87fb6c2d4

Object ID : 91fdf564-926b-4eba-aa07-2a5536204bfa

8. From the Manage menu, select **Certificates & secrets**.
9. On the Certificates and Secrets screen, click **+ New client secret**.
 - a. In the **Description** field, enter: **DeltekAjeraKey**.
 - b. Under **Expires**, we recommend that you select **In 2 years**.
 - c. Click **Add** to generate the secret value.

Add a client secret
Description

Expires
☐ In 1 year
☒ In 2 years
☐ Never

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

- d. Click the clipboard icon to the right of the secret value to save the value for future use.

You will enter this ID into the **Client Secret** field on the **Azure** tab in  > **Setup** > **Company** > **Preferences** > **Integration** tab.



This is the only time the client secret will be visible so it's important to ensure you save it for future use.

DeltekAjeraKey

12/15/2022

HcV7XQD-R~-r3irBeorR19-zT-dAXH4~ja

acf3026d-b8f5-43ff-b59b-5a2c17147c77

9. From the Manage menu, select **Authentication**.

 Save  Discard  Got feedback?

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web

Quickstart Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

Add URI

Logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

Implicit grant

Allows an application to request a token directly from the authorization endpoint. Checking Access tokens and ID tokens is recommended only if the application has a single-page architecture (SPA), has no back-end components, does not use the latest version of MSAL.js with auth code flow, or it invokes a web API via JavaScript. ID Token is needed for ASP.NET Core Web Apps. [Learn more about the implicit grant flow](#)

To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

- ☐ Access tokens
- ☒ ID tokens

10. On the Authentication screen, under **Redirect URIs**, perform the following actions.

Points to remember:


- Press TAB after you enter each URL.
- The URL entries are case-sensitive.
 - a. In the **Type** field, select **Web** for each URL.
The first URL must be what users use to launch Ajera.
 - b. In the Advanced settings section, under **Implicit grant**, select the **ID Tokens** option.
 - c. In the Default client type section, select **No** in the **Treat application as a public client** field.
 - d. In the Supported account types section, select the **Accounts in this organizational**

- directory only** option.
 - e. Click **Save** at the top.
- 11. From the Manage menu, select **API permissions**.
 - a. On the API Permissions screen, click **Grant admin consent for your domain** at the bottom, to make it available for end-users.
 - b. Click **Yes** to grant consent for the requested permissions.

Setting up the Azure integration in Ajera

You must enable the Azure integration to use Single Sign-on (SSO) and Two Factor Authentication.

To set up the Azure integration

1. From  > **Setup** menu, click **Company > Preferences > Integration** tab.
2. Click the **Azure** tab.
3. Select the **Enable Windows Authentication** check box.
Enabling this check box turn on Windows Authentication for all active employees.
4. Enter the following information:

Tenant Domain Name (optional)	The domain name for the tenant
Application (Client) ID	The application ID for the Azure client account. This was the ID generated in Step 6 of Add and Configure the Deltek Ajera Client Application .
Client Secret	This is the client secret that was generated in Step 8 of Add and Configure the Deltek Ajera Application .
Directory (Tenant) ID	The directory ID for the Azure tenant account This was the ID generated in Step 7 of Add and Configure the Deltek Ajera Client Application .

5. Click **Save**.

Log in Using Windows Authentication (SSO)

To log in using Windows Authentication

1. Launch your company's Ajera URL.
2. On the log on screen, select the **Windows Authentication** check box.
3. Click **Login**.
4. Enter your Windows credentials.
5. Click **Login**.

FAQs for Microsoft Azure Active Directory Integration

Is there a fee to use Microsoft Azure Active Directory?

No. There is no fee for Microsoft Azure Active Directory. There may be fees associated with multi-factor authorization or if you choose to connect a local active directory setup to Azure AD.

Does Single Sign-On (SSO) and Two Factor Authentication (2FA) need to be set up before or after moving to Ajera Cloud?

SSO/2FA can be setup before or after migrating to Ajera Cloud. The connection from Ajera to Azure will be the same as it is from on-premise.

Is SaaS Administrator Access required to set up SSO?

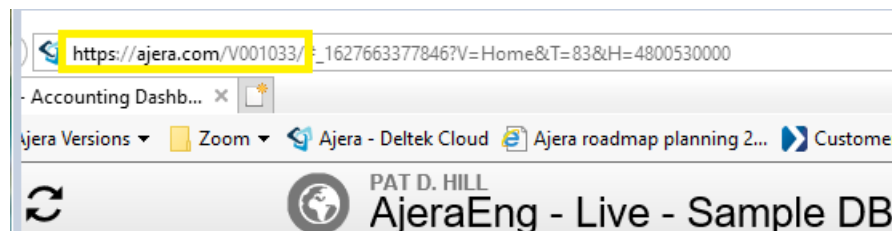
Access to **Company** > **Preferences** in Ajera is needed. SaaS Administrator access is not required.

Where do I find the Ajera customer URL?

On-premise users: Ask your IT professional to provide you with the URL used for Ajera.

Ajera Cloud: When you log in to Ajera, the URL can be found in your browsers URL bar.

For example: The URL in the image below is: **<https://ajera.com/V001033/>**



Is it possible to use a separate Active Directory vendor and have it connect to Microsoft Azure?

You can use a separate tool for Active Directory and connect that tool to Microsoft Azure and then configure the setup between Ajera and Microsoft Azure.

Is it possible to do a test run using SSO?

Yes. You are able to setup a sample database to test SSO.

Is SSO available using Mobile Timesheets and using the Deltek Mobile Expense app?

No, SSO is not available for Mobile Timesheets or the Deltek Mobile Expense app.



About Deltek

Better software means better projects. Deltek delivers software and information solutions that enable superior levels of project intelligence, management and collaboration. Our industry-focused expertise makes your projects successful and helps you achieve performance that maximizes productivity and revenue.

www.deltek.com