Aderant

BETTER TOGETHER

Aderant Identity

Azure AD Integration (December 2023)

Version 22.1

This document contains proprietary and confidential information of Aderant Holdings, Inc. (“Aderant”)

Aderant makes no representations or warranties with respect to the contents of this document publication and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

The contents of this manual are believed to be current and accurate as of its date of publication. Changes to this manual between reprintings and other important information about the software product are made or published in release notes, and you are urged to obtain the current release notes for the software product.

We welcome user comments and reserve the right to revise this publication and/or make improvements or changes to the products or programs described in this publication at any time, without notice.

Aderant North America
The Pointe
500 Northridge Road, Suite 800
Atlanta, GA 30350
Tel: +1.404.720.3600
Fax: +1.404.720.3601
info@aderant.com | www.aderant.com

Table of Contents

Overview **1**

Prerequisites **2**

Users 2

Security Layers 2

Identity Integration Methodology **3**

Example Scenario 3

Values Stored in Aderant Identity **4**

Setting Up your Azure AD Integration **5**

Getting Support **7**

Overview

This guide details how to integrate Azure Active Directory (Azure AD) with Aderant Identity.

Prerequisites

Users

We recommend limiting authentication rights in the integration to the users who require access to the Aderant Cloud applications.

Security Layers

Aderant Identity authentication flow has three layers of security that become available after your integration has been set up:

1. Your firm manages the users who can access your Azure AD tenancy.
2. Aderant Identity provides a mechanism for managing user application access rights and permissions within the Aderant cloud applications through the Aderant User Management Portal. .
3. Your firm can limit the users who can authenticate through the integration in your Azure AD tenancy.

For detailed documentation on limiting the access of an application within your Azure infrastructure, see *https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-restrict-your-app-to-a-set-of-users*.

Identity Integration Methodology

Aderant Identity's integration is built on top of Microsoft Azure resources. When a user attempts to sign into an Aderant cloud application, they will be challenged for their username. After submitting this, they will be routed directly to your firm's Azure AD tenancy to complete the authentication process.

After authentication has occurred, Aderant Identity manages which applications and level of access the user is granted within the Aderant cloud infrastructure.

Note: If a user leaves your firm, it is your responsibility to deactivate that user within your Azure AD tenancy. Doing so will disable authentication and deactivate the user within the Aderant User Management Portal.

Example Scenario

A new iTimekeep administrator has joined your firm and has been added to your Azure AD tenancy.

1. The administrator is granted access to the Aderant iTimekeep application within the Azure AD tenancy and signs into the Aderant cloud application.
2. Upon their initial sign-in request, the user is routed to your Azure AD tenancy for authentication. They sign in, as they would for any other application that is within your Azure AD tenancy (including MFA, code challenges, or network restrictions), and when they successfully authenticate, they are passed back to Aderant Identity to continue their first-time setup.
3. Aderant iTimekeep will ask the user for additional information, depending on the set of applications they are licensed to use. In this example, a new iTimekeep user will be requested to supply their Employee ID. The iTimekeep application requires ethical walls to be set up for your firm's safety.
4. Depending on your firm's internal processes for a new user sign-up to an Aderant application, you may be responsible for assigning roles to the user within the Aderant User Management portal. If this is your internal process, your firm can provide access to the iTimekeep application, and only the iTimekeep application for this user. Conversely, if your firm intends to grant access to all Aderant cloud applications, you will need to provide Aderant with a list of users who are granted access to all of your licensed Aderant cloud applications.

Values Stored in Aderant Identity

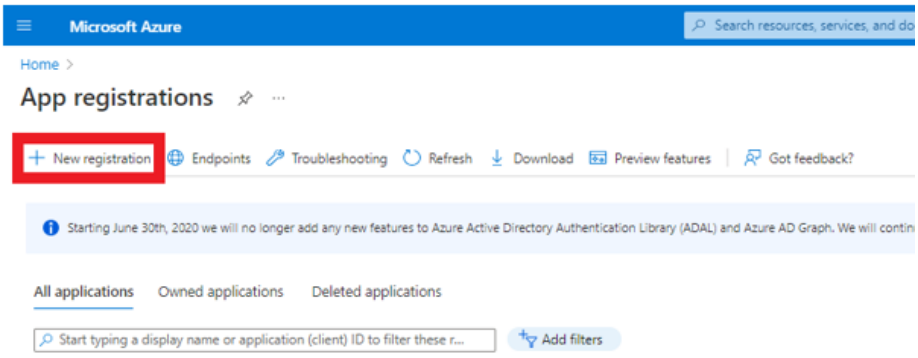
Aderant Identity stores the following user information for user authentication and access to your firm's licensed products:

- Email address
- First and last names
- Employee ID (if required for your firm's licensed applications)
- Any other relevant information associated with the user and their assigned applications

Setting Up your Azure AD Integration

Below are the steps required to integrate your Azure Ad tenancy with Aderant Identity.

1. Launch the administration portal of your Azure AD tenancy and navigate to the *App registrations* screen.
2. On the *App registrations* screen, click **New Registration**.



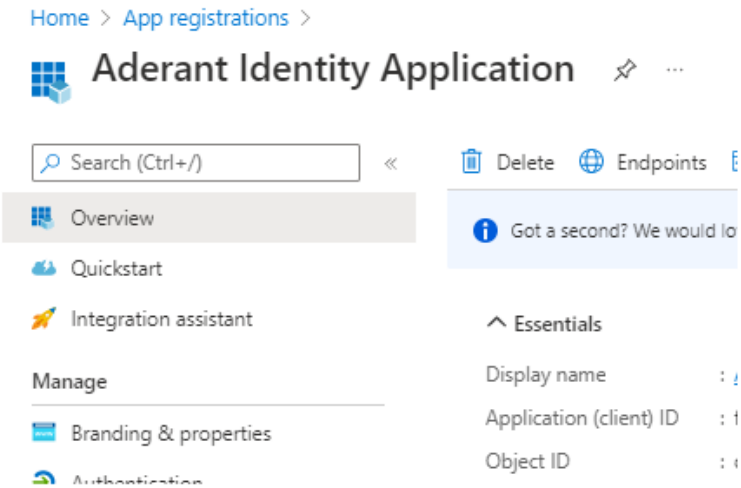
3. In the *Register an application* form, create an application for the Aderant Identity integration:
   a. Enter a **Name** for your application.

      Example: Aderant Identity Application

   b. Under *Supported account types*, select **Accounts in this organization directory only**.
   c. Under *Redirect URL (optional)*, from the *Select a platform* drop-down options, select **Web**.
      i. Enter this URL:
      https://aderantidentity.b2clogin.com/aderantidentity.onmicrosoft.com/oauth2/authresp.
4. Click **Register**.

   Note: Aderant will need to be provided with the information gathered in the following steps to successfully complete authentication.

5. Navigate to the application you have created in the above steps:



6. Record the following information:
    - Application (client) ID
    - Directory (tenant) ID
7. Create a Secret:
    a. Under the *Manage* heading, click **Certificates & Secrets.**
    b. Click **+ New client secret**.
    c. Enter a name for the secret and set the expiry time to match the requirements of your IT team.

    Note: This secret will need to be cycled based upon the requirements of your security and compliance team. This secret is not used for user authentication, but to provide a trust relationship between Aderant Identity and your Azure AD tenancy.

    d. Record the expiration date and the client secret for use in the setup of the tenancy.
8. Within the Aderant User Management Portal, provide the following information to complete your registration:
    a. Your Application (client) ID from your Azure tenancy.
    b. Your Azure Tenant ID.
    c. Your Client Secret and expiration date.
    d. The email address of the administrator responsible for setting up users within your firm to use Aderant Identity.
    e. Your email domains for home realm discovery.
9. When prompted, log into your Aderant Identity test application to confirm that your integration is working correctly.

Getting Support

If you have any difficulty, we recommend that you obtain assistance from the following sources.

Client Support Portal

The Client Support Portal, myAderant, contains the following information:

- Release documents (Release Notes and Installation Guides)
- Product documentation (User, Administration, Customization, and Application Setup Guides)
- Knowledge Base articles relating to the installation, customization, and use of the product
- Salesforce Case details
- Discussions

To access this information:

1. Access the Client Support Portal at *www.myaderant.com*.

   Note: If you do not have login details for the Client Support Portal, contact your firm's portal administrator to create your portal login, or email *myaderant@aderant.com*.

2. Click in the Search bar and enter relevant keywords.
3. Click **Search** or press **Enter**. The search results will span all products and cases available to you.
4. Use the left pane to filter your results further.

   Tip: Click **View More** at the top-right of each section to expand the limited search results into the full list.

Telephone Support

If the online help or our Client Support Portal do not answer your questions, Aderant support representatives are available by phone.

Americas Region:	+1 850 224 2004
Australia (within Australia):	1800 236 285
New Zealand (within NZ):	0800 849 000
Europe & Middle East:	UK +44 (0) 20 7038 9696
	Netherlands +31 88 400 0300