



Aderant Identity

Okta 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.



Copyright © 2024, Aderant North America, Inc. All rights reserved.

Aderant, Aderant Identity, and the Aderant logo are registered trademarks or trademarks of Aderant Holdings, Inc. Other brand and product names are trademarks or registered trademarks of their respective owners, and may include trademarks owned by subsidiaries and affiliated entities of Aderant Holdings, Inc.

Printed in the United States of America. No part of this publication may be reproduced in any form without the prior written consent of Aderant North America, Inc.

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	2
Prerequisites	3
Users	3
Security Layers	3
Identity Integration Methodology	4
Example Scenario	4
Values Stored in Aderant Identity	5
Setting up your Okta Integration	6
Getting Support	9

Overview

This guide details how to integrate Okta 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 Okta 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 Okta tenancy.

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 Okta 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 Okta 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 Okta tenancy.

1. The administrator is granted access to the Aderant iTimekeep application within the Okta tenancy and signs into the Aderant cloud application.
2. Upon their initial sign-in request, the user is routed to your Okta tenancy for authentication. They sign in, as they would for any other application that is within your Okta 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 Identity 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

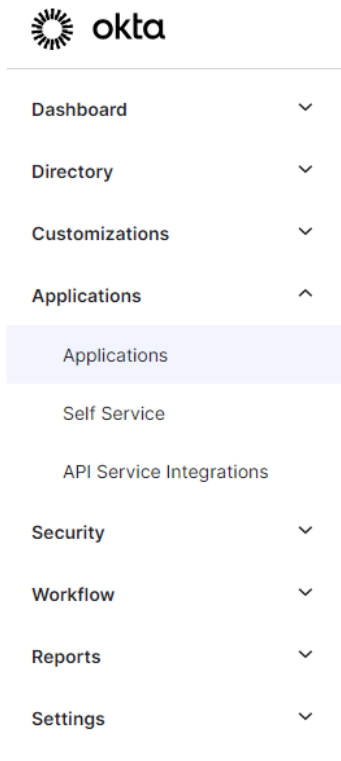
Aderant Identity stores the following user information for user authentication and access to your firm's licensed products:

- 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 Okta Integration

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

1. Launch the administration portal of your Okta tenancy and navigate to **Applications > Applications**.



2. On the *Applications* screen, select **Create App Integration**.
3. On the *Create a new app integration* screen, select **OIDC – OpenID Connect** for the sign-in method. Upon selection, the *Application Type* panel will open below.
4. In the *Application Type* panel, select **Web Application**.
5. Click **Next**, and the *New Web App Integration* screen will open.
6. On the *New Web App Integration* screen, in the *General Settings* section, enter "Aderant Identity Integration" into the **App integration name** text box.



7. *Logo (Optional)* - add your firm's logo by clicking the upload button and selecting an image file from your computer.
 8. In the *Grant Type* section, under *Client Acting on behalf of itself*, select **Client Credentials**, if required.
 9. In the *Grant Type* section, under *Client acting on behalf of a user*, ensure the following are selected:
 - Authorization Code
 - Refresh Token
 - Implicit (hybrid)
 10. In the *Sign-in redirect URIs* section, enter:
https://aderantidentity.b2clogin.com/aderantidentity.onmicrosoft.com/oauth2/authresp
 11. In the *Sign-out redirect URIs* section, enter:
https://aderantidentity.b2clogin.com/aderantidentity.onmicrosoft.com/oauth2/authresp
 12. Leave **Trusted Origins** blank.
 13. In the *Assignments* section, under *Controlled Access*, choose the option that best suits your needs. We suggest you select **Limit access to selected groups**. Choosing this enables you to select your desired groups (see next step).
- Note:** For more information on users and groups, see <https://help.okta.com/oie/en-us/Content/Topics/Provisioning/lcm/lcm-assign-app-groups.htm>.
14. In the *Assignments* section, under *Selected group(s)*, if you selected **Limit access to selected groups** above, select the groups you wish to give access to.
 15. Click **Save** to create the app integration.
 16. Click **Edit** on the new app integration.

General Settings **Edit**

APPLICATION

App integration name	Aderant Identity Integration
Application type	Web
Grant type	Client acting on behalf of itself
	<input checked="" type="checkbox"/> Client Credentials

17. Scroll down to the *LOGIN* section and, under *Login initiated by*, select **Either Okta or App** in the drop-down options.
18. In the *LOGIN* section, under *Login flow*, select *Redirect to app to initiate login (OIDC Compliant)*.
19. In the *LOGIN* section, under *Initiate login URI*, enter:
https://aderantidentity.b2clogin.com/aderantidentity.onmicrosoft.com/oauth2/authresp.
20. Click **Save**.

21. Source and provide the following information to Aderant staff:

Note: We recommend sending this information through secure means.

- The name of your tenancy in Okta
- Your Okta tenancy's sign-in redirect URL

Example: <https://your-okta-org.okta.com/.well-known/openid-configuration>

- The Client ID - listed in the app integration at the top of the *Web App Integration* page
- The Client Secret from within your app integration

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