Financial Corporate & Compliance

Customer Identity and Access Management (CIAM)

Wiz® SaaS Suite

Content

1. Introduction

1.1 What is the OneID Customer Identity and Access Management (CIAM) Service?

Customer Identity and Access Management (CIAM) is the user interface for OneID. OneID is a gateway to access the Wolters Kluwer products ecosystem, while offering a set of technologies that include a user account self-service platform (My Profile) together with a subscription and user management portal (CIAM).

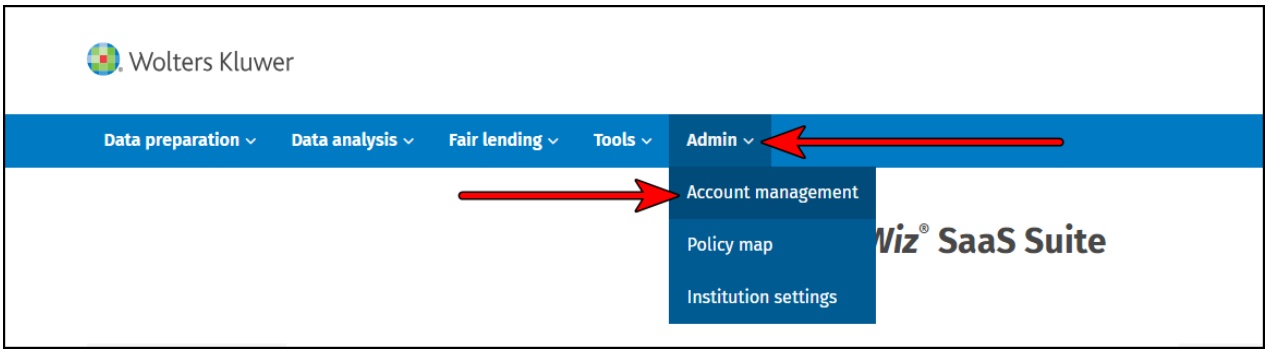
CIAM streamlines the administration of Wiz® SaaS Suite by providing a platform used for authentication, user management, and role assignments.

What browsers are supported with the Customer Identity and Access Management (CIAM) application?

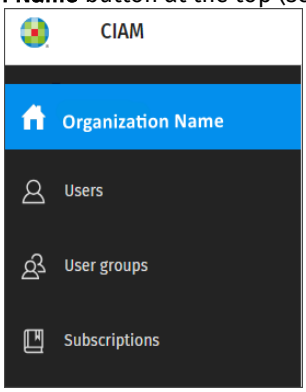
- Chrome (latest version)
- Microsoft Edge (latest version)

1.2 Logging Into CIAM

You can log into CIAM at: https://ciam.wolterskluwer.com
Or within *Wiz*® SaaS Suite, select **Account Management** from the **Admin** menu.



Upon Logging into CIAM, you will see a navigation menu on the left, in which you can perform various functions related to managing your users. Click on the **Organization Name** button at the top (see below).



Users tab

Select **Users** to perform various actions related to managing your organization's users, such as, adding new user(s), viewing and managing user application roles, and viewing user details, groups, and subscriptions.
Note: Email addresses cannot be updated by the User Group Manager (UGM) or the user. A new user will have to be created with the updated email address.

User Groups tab
Select **User Groups** to perform various actions related to managing your organization's User Group(s), such as viewing users and Admins, adding/removing user(s), changing user roles (Standard User/UGM), and viewing subscriptions.
Note: UGMs can remove users from a user group but cannot remove them from the organization.

Subscriptions tab
Select **Subscriptions** to view your licensed products and seats.

2. User Group Manager Permissions

User Group Managers (UGM) have managerial rights to a user group(s) of an organization.

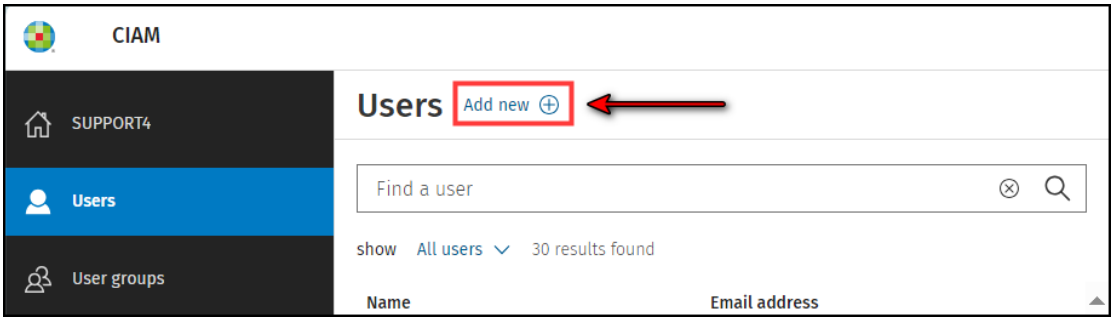
You can:

- View users in the organization
- Manage application user roles
- View organization and user groups details
- View subscriptions
- Invite users to a user group
- Manage user's roles in user groups
- Remove users from user groups
- Manage user access to the products (add/remove to the subscriptions) associated with the user group they belong to

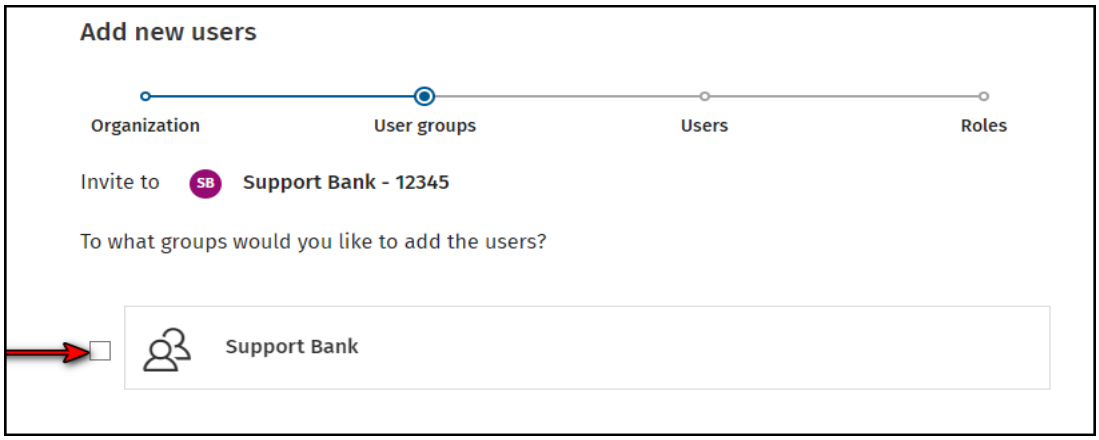
2.1 Setting up a Standard User

A standard user is the most common entity of CIAM. Standard users **DO NOT** have access to CIAM unless they are promoted to the User Group Manager Role. Standard users are managed by the UGM and are associated with a certain subscription and user group. Adding a user must be completed by a UGM at your institution.

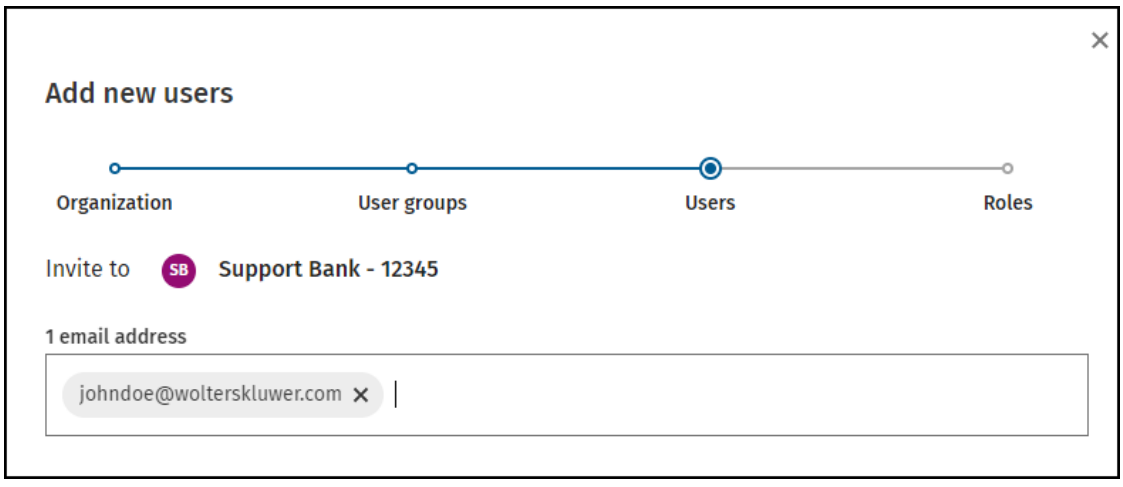
1. Log in to CIAM at https://ciam.wolterskluwer.com.
2. From the **Users** node, select **Add new** + (see below).



3. Select the appropriate **User group(s)** for the new user and click **Next**.

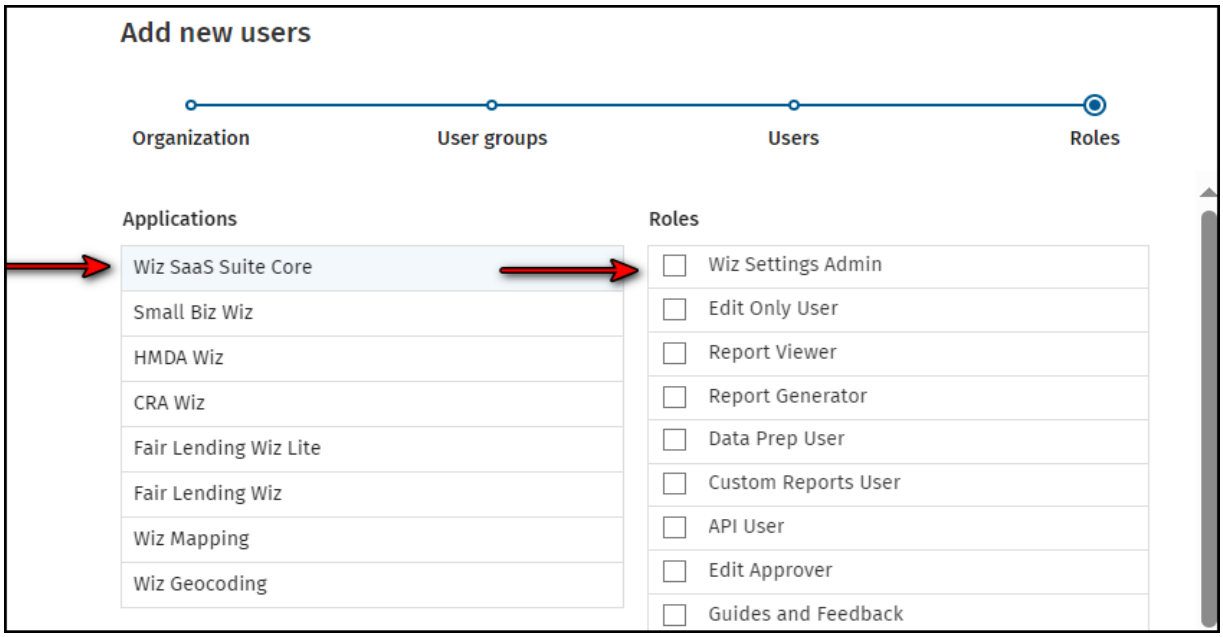


4. Enter the user's email address. If adding multiple users at a time, separate each email address with a comma, space or semicolon. Click **Next.**



5. For each **Application**, assign the appropriate **Roles** for the new user. Refer to the Application Roles and Descriptions section for additional details. After assigning roles for each application, click **Invite**.

Note: If multiple users were assigned at the same time (in step 4), the assigned roles will be applied to all users and can be changed after the user set up.

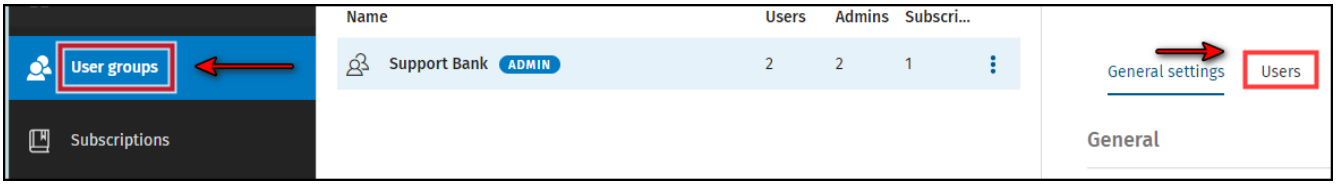


6. An invitation email is sent to the user(s) with a link to create their account(s).

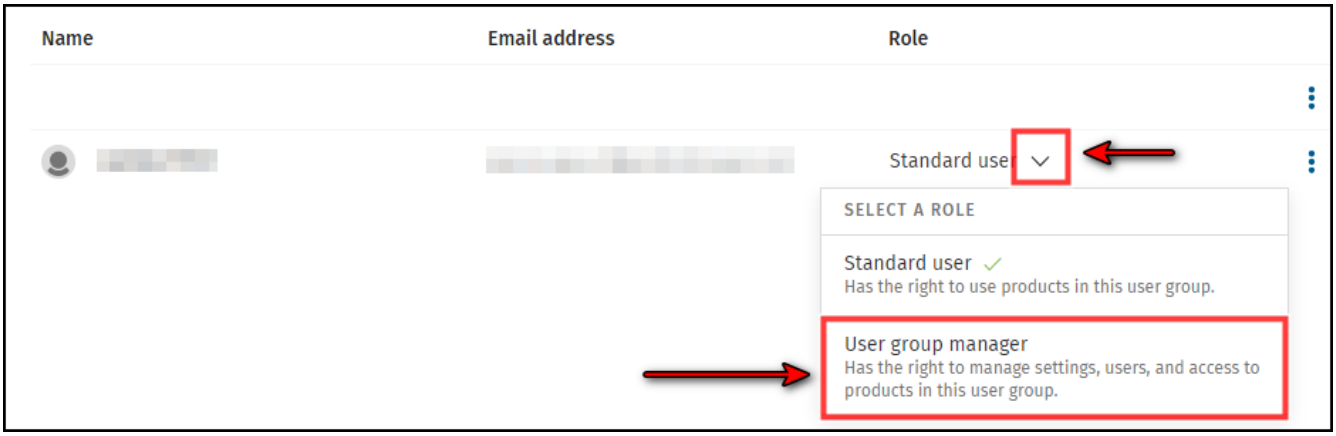
2.2 Setting up a User Group Manager

Note: The user needs to be a registered user before they can be invited as a **User Group Manager**. Please complete the Setting up a Standard User procedure for newly invited user before assigning him as a User Group Manager.

1. Log in to CIAM at https://ciam.wolterskluwer.com.
2. Click on **User Groups** and select the **Users** tab in the selected user group.



3. Locate the user and click on the drop-down arrow under the **Role** column to select **User Group Manager** (see image below).



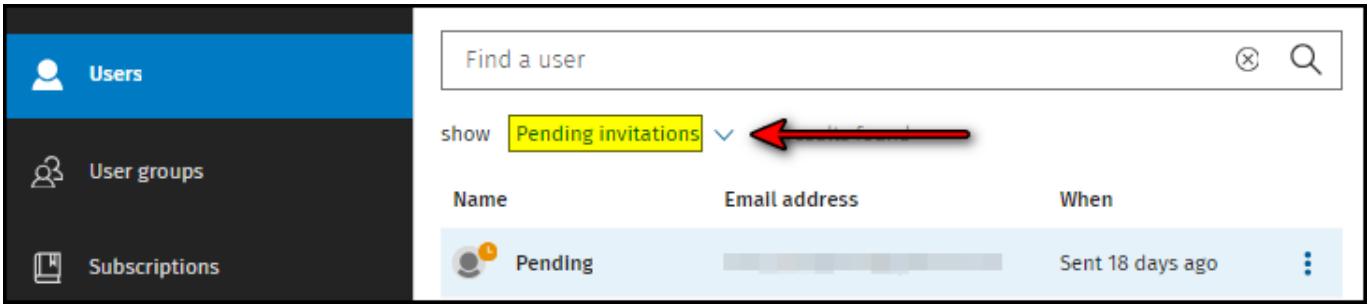
4. Click the **Change** button to confirm.

2.3 Resending or Cancelling an Invitation

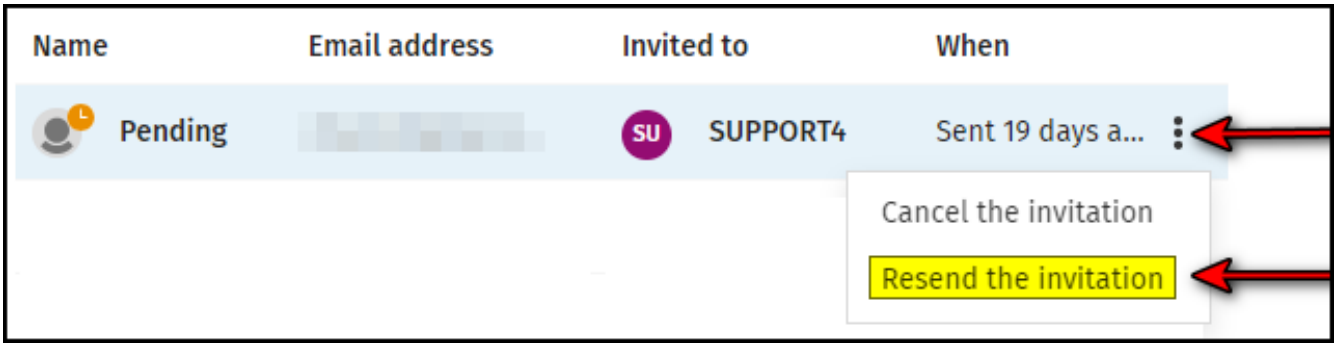
After you set up a new user, an invitation is sent and the user status in CIAM shows as pending until the user creates their account.

In case the mail invitation has not reached the desired user/s or it has expired, you can resend the invitation by following the steps below:

1. Click on the **User**s navigation item on the main navigation menu on the left.
2. Select the dropdown arrow to display users with **Pending invites**.



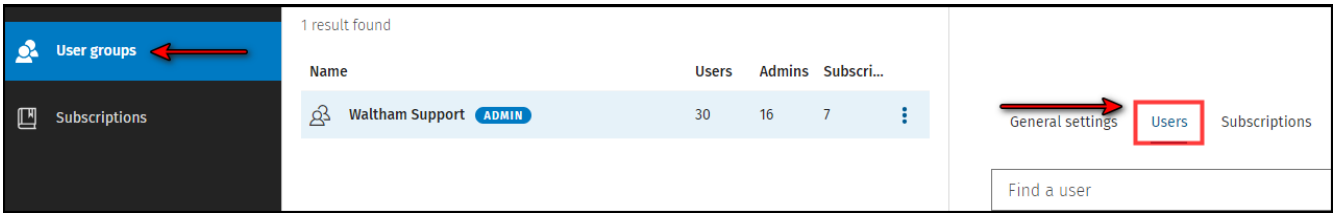
3. Go to the user in question, and click the kebab menu button, and click **Resend invitation**. If you wish to revoke an invitation, you can simply select **Cancel the invitation**.



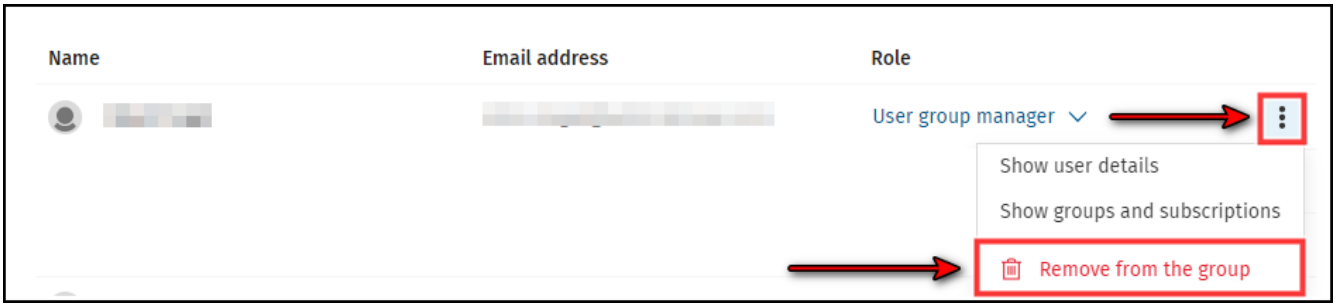
4. In the upper-right corner of the screen, a notification confirming that the mail notification has been resent is displayed.

2.4 Removing a User

1. Log in to CIAM at https://ciam.wolterskluwer.com.
2. Click on **User Groups** and select the **Users** tab in the selected user group.



3. Locate the user and click on the action menu on the right to select Remove from the group.



4. Click the **Remove** button to confirm.

3. Application Roles and Descriptions

In the Wiz® SaaS Suite, roles determine what users are allowed to do. There are two main types of roles: **functional roles** and **data access roles**. Functional roles define what system features a user can utilize, while data access roles specify which types of data the user can view or manipulate within those features. Users can have multiple roles to ensure they have all the necessary permissions.

For example, if a user has both the Data Prep User and HMDA Wiz User roles, they can import data into HMDA DF type files. However, they won't be able to import data into Small Business DF files unless they also have the SB Wiz User role.

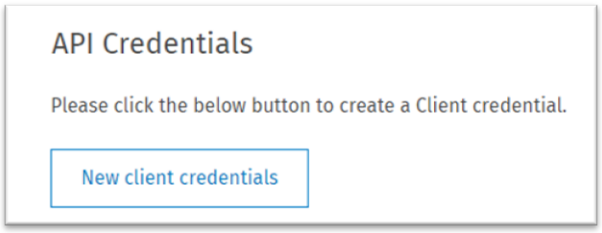
Applications	Role Name	Description
Wiz SaaS Suite Core	Wiz Settings Admin	Allows the user to access Institution Settings for exemptions, self identification, and other application settings. When combined with the FL Wiz User, it also gives access to control groups and proxy settings. When combined with the Edit Approver role, it allows users to disable quality edits and warnings that for the file types they have data access roles for
	Edit Only User	Allows the user to select a current file, filter, and use all functionality within the Edit module for file type that the user has data access roles for
	Report Viewer	Allows the user to access Generated Reports and view reports that were generated by other users in the organization, but no ability to generate the reports themselves.
	Report Generator	Allows the user to access and generate reports for any areas that they have access to based on the data access roles they have. Also grants the user access to Generated reports so that they can view reports that they have generated or that other users in the organization have generated.
	Data Prep User	Allows the user access to File management, Import, Create areas, and User defined edits.
	Custom Reports User	Allows the user to access and generate Custom reports (columnar reports and custom tables) and access to the OData links page.
	Edit Approver	Allows the user to approve quality edits and warnings at the record level or at the file level.
	Guides and Feedback	Enables the feedback button and FAQs, guides, etc
HMDA Wiz	HMDA Wiz User	*Data Access Role
	HMDA Submission User	Allows the user to access Submission and Submission Packages for HMDA DF files.
Small Biz Wiz	SB Wiz Uer	*Data Access Role
	SB Submission User	Allows the user to access Submission and Submission Packages for Small Business DF files.
CRA Wiz	CRA Wiz User	*Data Access Role
	CRA Submission User	Allows the user to access Submission and Submission Packages for Small Business and Farm files.
	CRA Tables User	Allows the user to access and generate CRA Tables.
Fair Lending Lite	FL Lite User	Allows the user to access the Redlining scoping tool, all Fair Lending analytics reports, and the Regression and Comparative File Review.
Fair Lending Wiz	FL Wiz User	Allows the user to access the Redlining scoping tool as well as the Risk scorecard.
Wiz Mapping	Mapping User	Allows user to access the Mapping tool and the Synchronized map items page.

3.1 Service / Integration Accounts

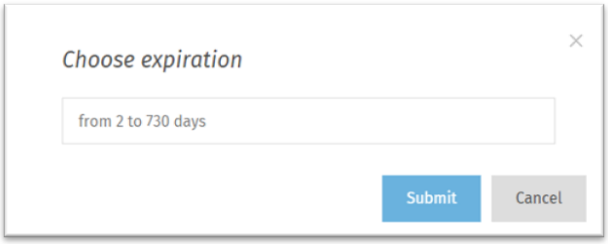
Beginning with August 23rd and the Version 6.3 release, service accounts are no longer supported with Wiz® SaaS Suite. As a Wiz® User Group Manager you will need to create API Credentials and enter these into your Loan Origination System. Refer to this guide for assistance with entering credentials into your WK LOS. For non-WK integrations, you will need to provide the API credentials to your vendor administrator.

Below are the steps that Administrators can take to create new credentials:

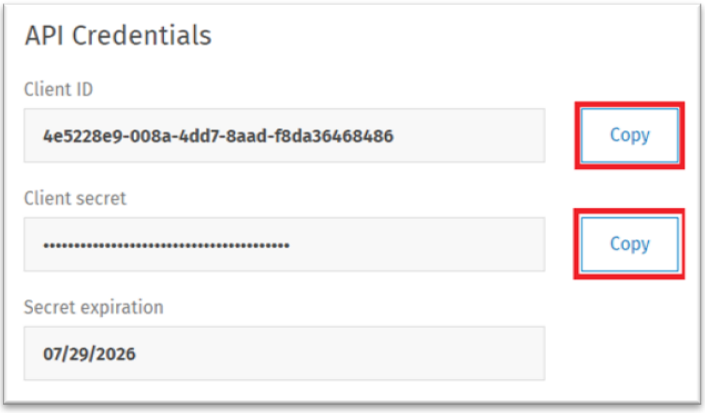
1. Log into the application.
2. Go to **Admin > API Credentials**.
3. Click on **New client credentials**.



4. Choose an expiration date between 2-730 days then click **Submit**.



5. Copy the new Client ID (username) & Client secret (password) and input these new credentials in the system(s) you integrate our services with.



3.2 Multifactor Authentication and IP Whitelisting Configurations

MFA and IP whitelisting will need to be configured by the Wolters Kluwer Team. Please reach out to Wiz SaaS Suite Product Team and our team can assist with reconfiguring your account accordingly.

Support Contact Information

Phone#: 800-261-3111, Ext 1123078
Email: SaaSWizsupport@wolterskluwer.com
Hours are 7am-7pm Central

Wolters Kluwer