

Users & User Groups

Last Modified on 11/12/2024 4:24 pm EST

Create a New User

Overview

Every individual you want to access your Resolver environment requires a user account. A user with Administrator privileges can add user accounts to Resolver. When a user account is created, an Administrator must assign each user-to-user groups for the user to access the Resolver environment. Only Administrators can add users to the system.

User Account Requirements

The user account you use to log into Resolver must have Administrator or advanced permissions to access the ***User Management*** screen.

Related Information/Setup

For more information regarding Administrative user privileges, please see the [Administrator Overview](#) article.

For more information on adding a user to a user group, please see the [Adding a User to a User Group](#) article.

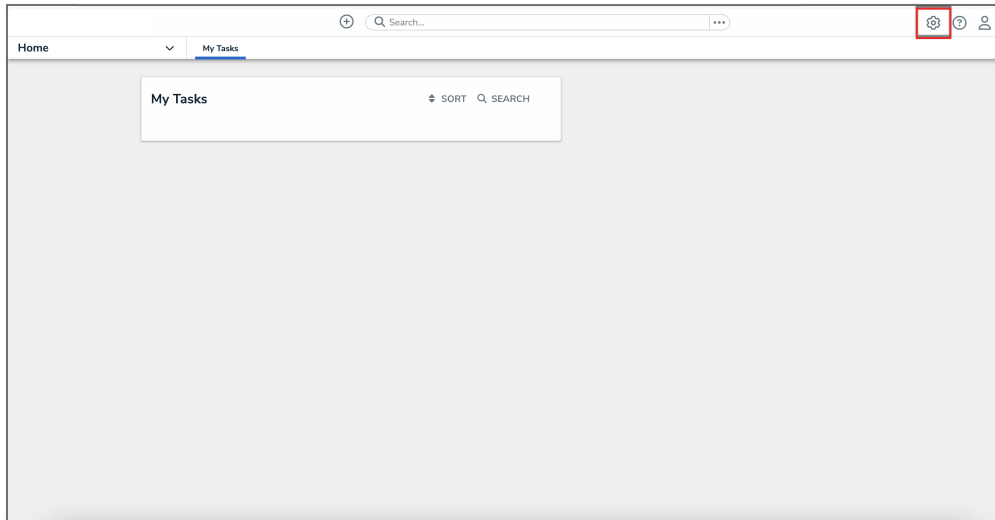
For more information on using an alternate language setting, please see the [Languages Overview](#) article.

For Orgs that have Data Warehouse enabled, please see the [Access Your Data Warehouse Settings](#) article.

For password requirements, please see the [Password Requirements](#) article.

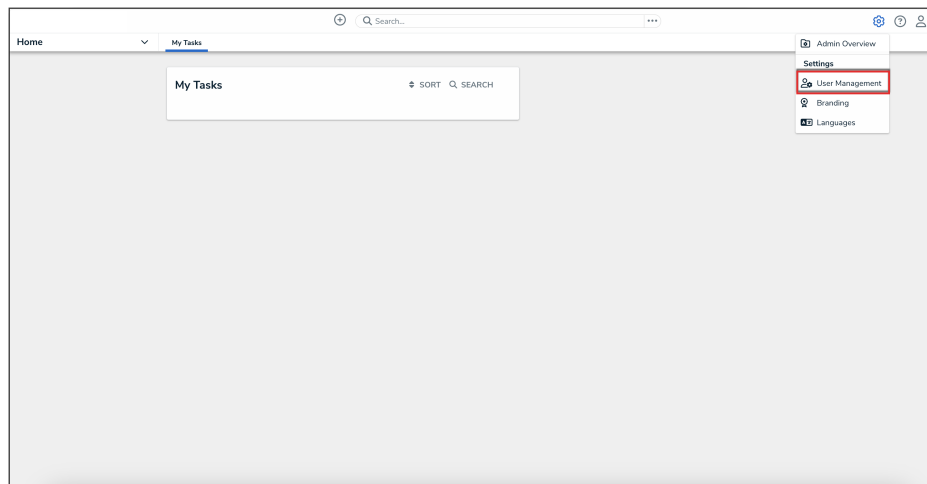
Navigation

1. From the ***Home*** screen, click the ***Administration*** icon.



Administration Icon

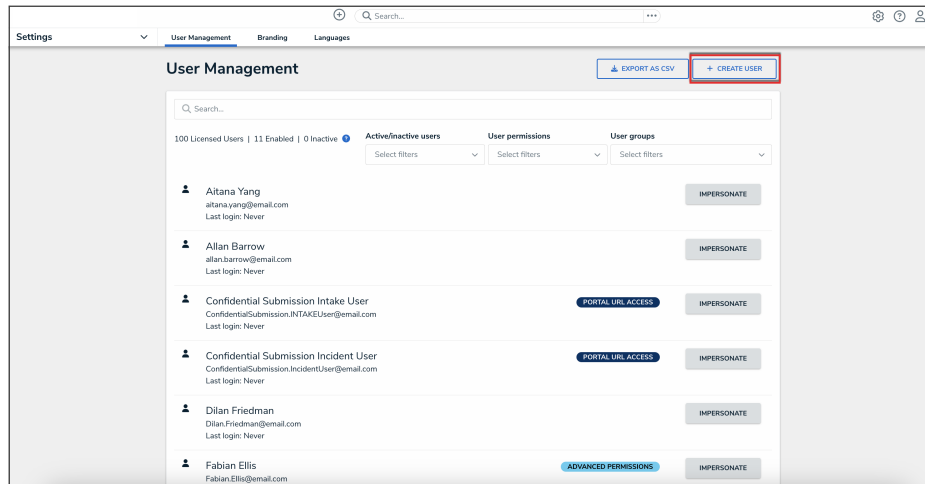
2. From the **Administrator Settings** menu, click **User Management**.



Administrator Settings Menu

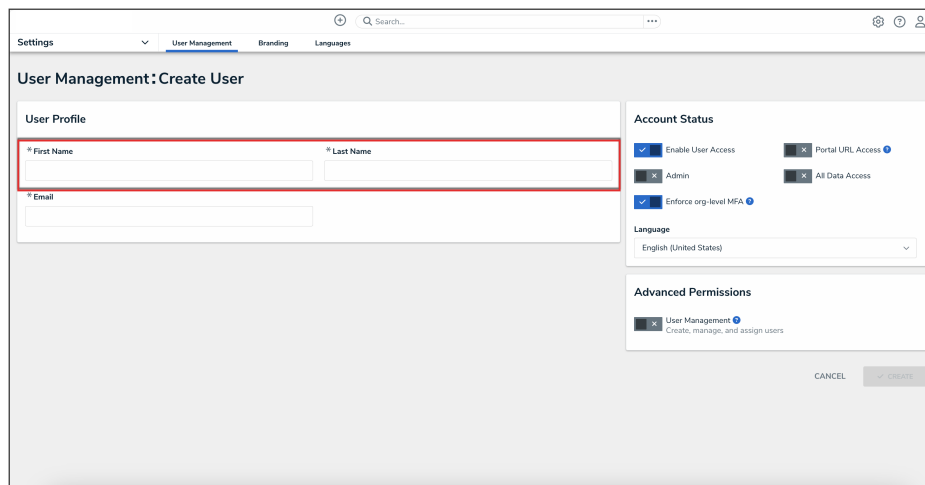
Creating a New User

1. From the **User Management** screen, click the **Create User** button.



Create User Button

2. Enter the user's name in the **First Name** and **Last Name** fields.



First and Last Name Fields

3. Enter the user's email address in the **Email** field. The email address is used to:

- Receive the Resolver sign-up email containing instructions on creating a new password and signing into Resolver.
- Authenticate the user when logging in to Resolver.

The screenshot shows the 'User Management: Create User' interface. It features a 'User Profile' section with input fields for 'First Name', 'Last Name', and 'Email'. The 'Email' field is highlighted with a red border. To the right, there are sections for 'Account Status' and 'Advanced Permissions'. The 'Account Status' section includes toggle switches for 'Enable User Access' (checked), 'Portal URL Access' (unchecked), 'Admin' (unchecked), 'All Data Access' (unchecked), and 'Enforce org-level MFA' (checked). The 'Advanced Permissions' section includes a toggle for 'User Management' (checked). At the bottom right, there are 'CANCEL' and 'CREATE' buttons.

Email Field

4. **(Optional):** The following toggle switches are options settings and can give users absolute access or visibility in the system:

- **Enable User Access:** Click the **Enable User Access** toggle switch to deactivate the user account. By default, the user account is enabled.
- **Portal URL Access:** Click the **Portal URL Access** toggle switch to grant the user account access only to the Portal URL.
 - When you click the **Portal URL Access** toggle switch, the **Admin, All Data Access, Enforce Org Level MFA,** and **Advanced Permission** toggle switches will automatically be disabled.
- **Admin:** The Admin toggle switch gives users Administrative privileges with the potential to cause irreparable system damage.
- **All Data Access:** The All Access toggle switch allows Users to view, edit, and delete Objects and Object Types. The **All Data Access** toggle switch overrides Object Type Workflow permissions.



Warning:

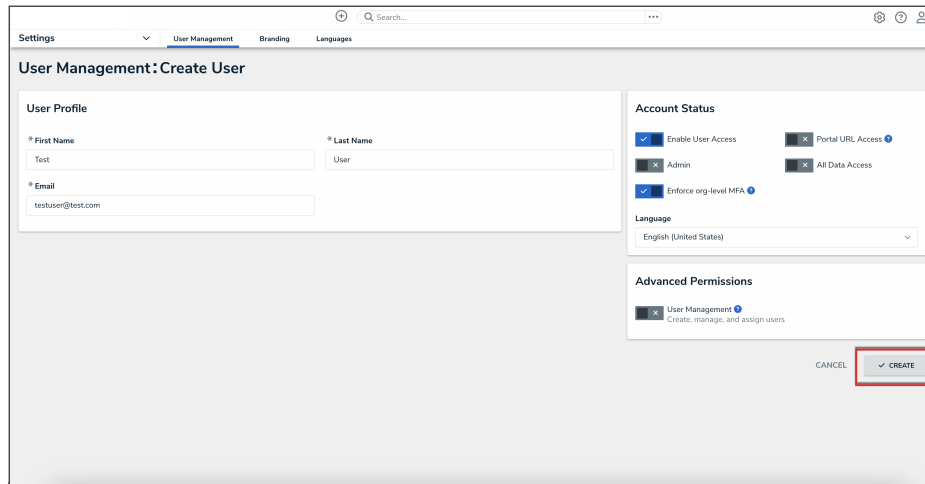
Resolver recommends not enabling the **Admin** or **All Access** toggle switches on for new user accounts.

Optional Toggle Switches

5. **(Optional):** Select a language from the **Language** field dropdown menu to change the system's language setting. Before you can set an alternate language setting, an Administrator needs to download a Languages .csv file from the system, map language translations to the user interface text, and upload the .csv file for use within Resolver.
6. **(Optional):** Click the User **Management** toggle switch under the **Advanced Permissions** section to grant the user advanced permissions. Please see the [Assigning Advanced Permissions to a User](#) article for adding advanced permissions to a user.

Advanced Permissions

7. Click the **Create** button to create the new user account.



Create Button

Create a New User Group

Overview

An Administrator can add new user groups to the system. A user group organizes system users into specific groups based on their organizational role (e.g., Employee, Management, etc.). Adding users to a user group allows an Administrator to assign multiple users within a user group to a role by assigning the user group to a role instead of manually assign a role to each user.

User Account Requirements

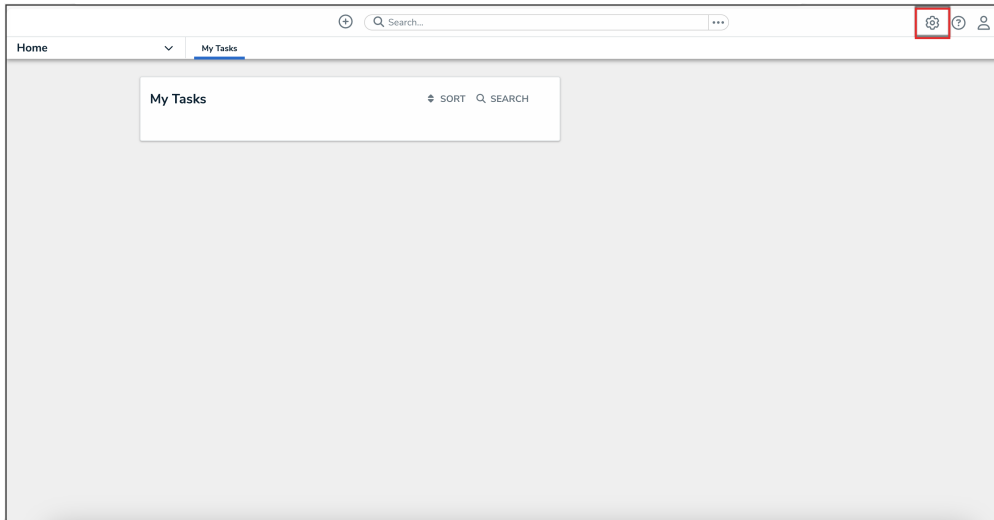
The user account you use to log into Resolver must have Administrator permission to access the **Admin Overview** screen.

Related Information/Setup

Please read the [User Group Overview](#) article for more information regarding user groups.

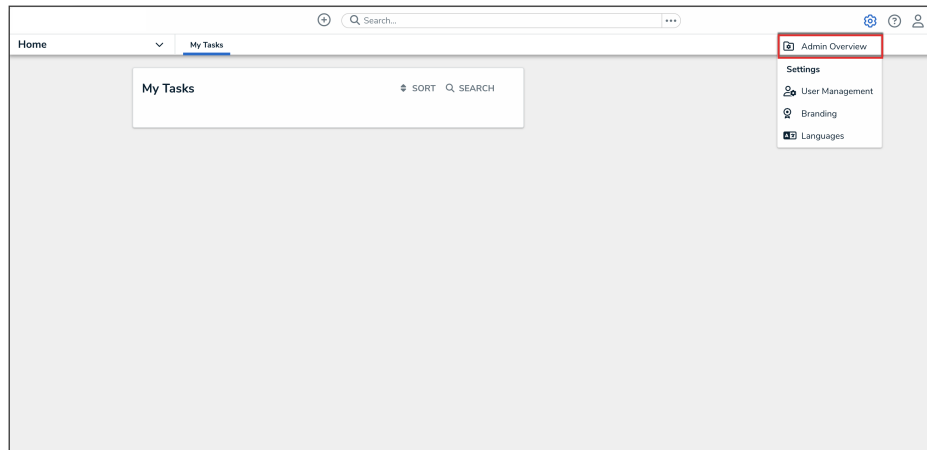
Navigation

1. From the **Home** screen, click the **Administration** icon.



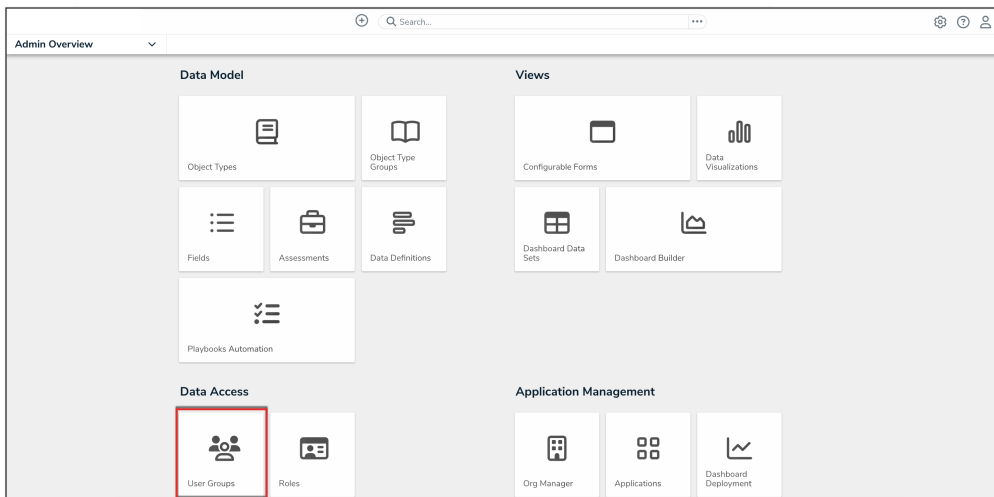
Administration Icon

2. From the **Administrator settings** menu, click **Admin Overview**.



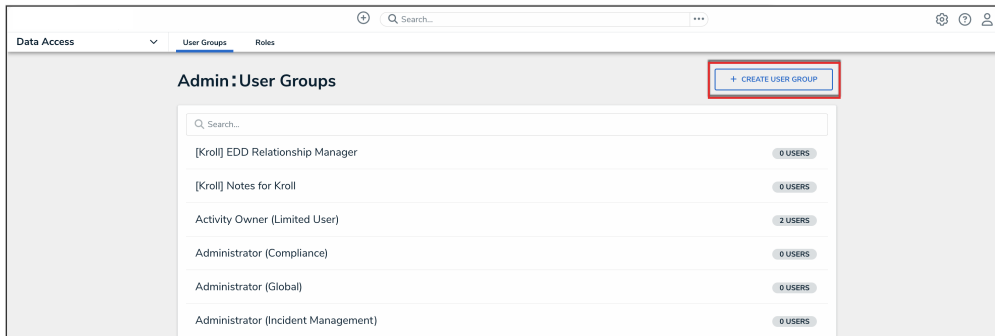
Administrator Settings Menu

3. From the **Admin Overview** screen, click the **User Groups** tile under the **Data Access** section.



User Groups Tile

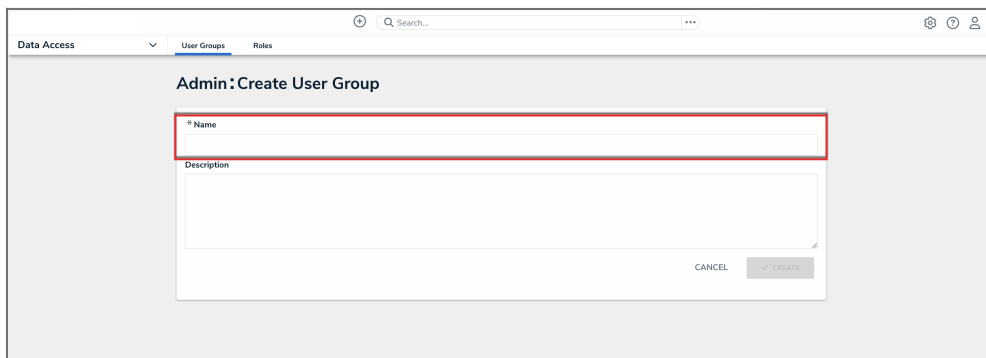
3. From the **Admin: User Groups** screen, click the **Create User Group** button.



Create User Group Button

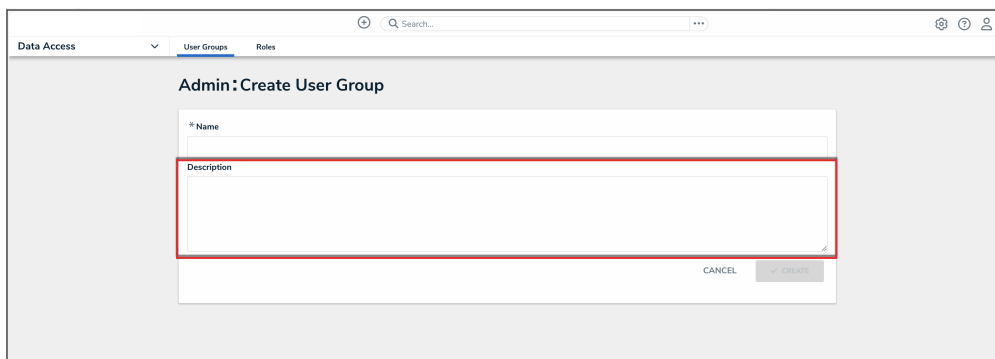
Creating a User Group

1. From the **Create User Group** screen, enter a user group name in the **Name** field.



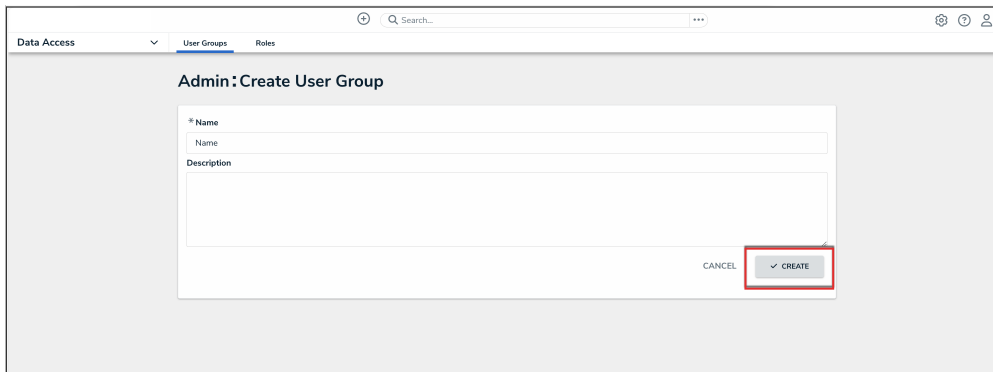
Name Field

2. **(Optional)** Enter a brief description outlining the user group in the **Description** field.



Description Field

3. Click the **Create** button.



Create Button

Create a Confidential Login

Overview

An Administrator must create a Confidential Portal Login before you can allow external and occasional stakeholders access to the **Confidential Portal**.

An Administrator must create a non-administrative user account for the login, and assign it to a [role](#) with access to the appropriate object type(s) and activity before they can create the Confidential Portal Login.

User Account Requirements

The user account you use to log into Resolver must have Administrator permissions.

Required Information/Setup

For more information on Confidential Portal Submissions, please refer to the Confidential Portal Submissions article.

- [Confidential Portal Submissions](#)

To Edit or Delete a Confidential Portal login, please refer to the Edit or Delete a Confidential Login article.

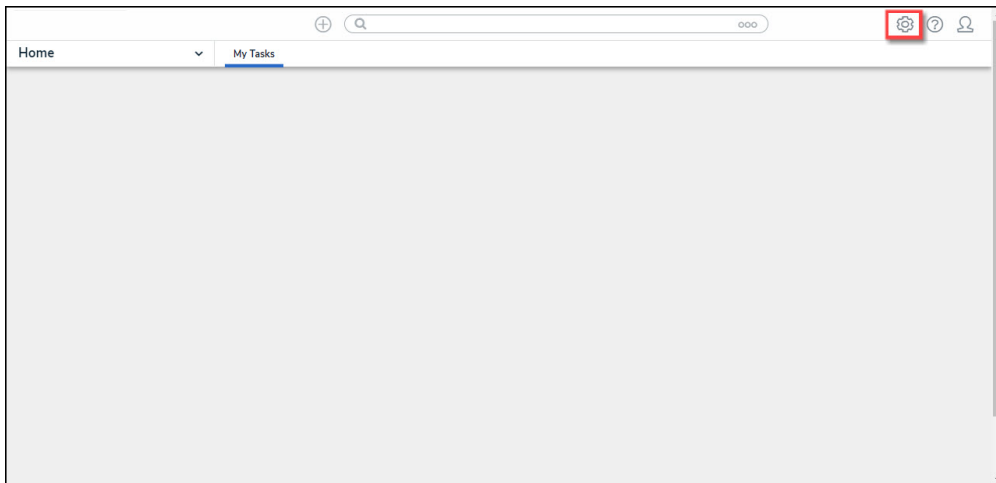
- [Edit or Delete a Confidential Login](#)

An Administrator must create a non-administrative login for use with the Confidential login, please refer to the Create a New User article.

- [Create a New User](#)

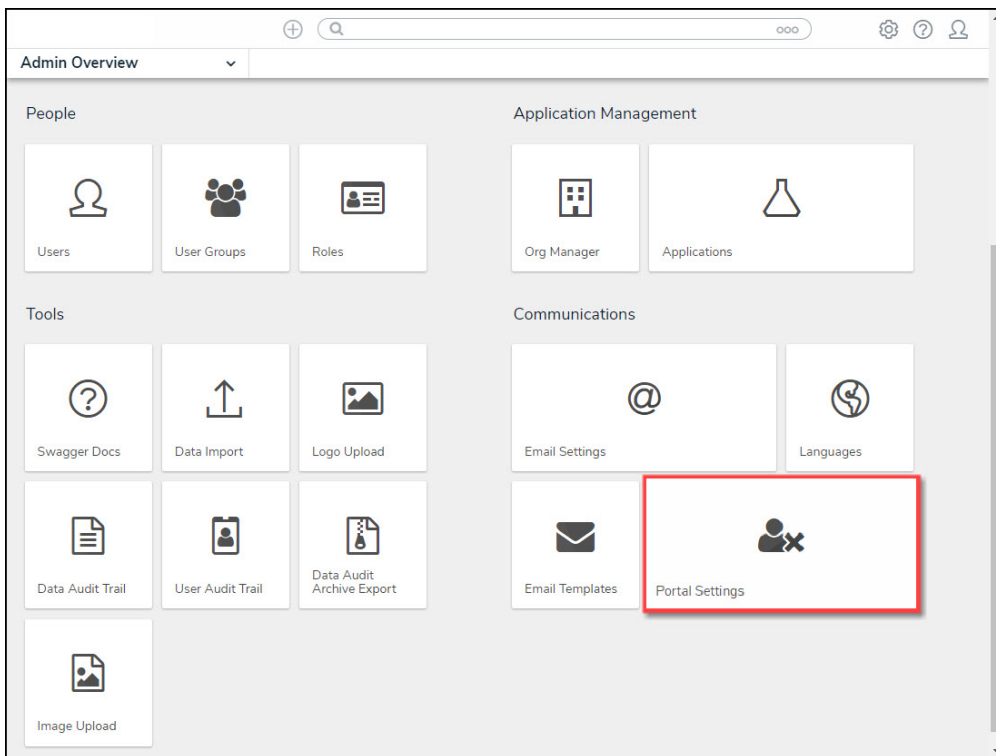
Navigation

1. From the **Home** screen, click on the **System** icon.



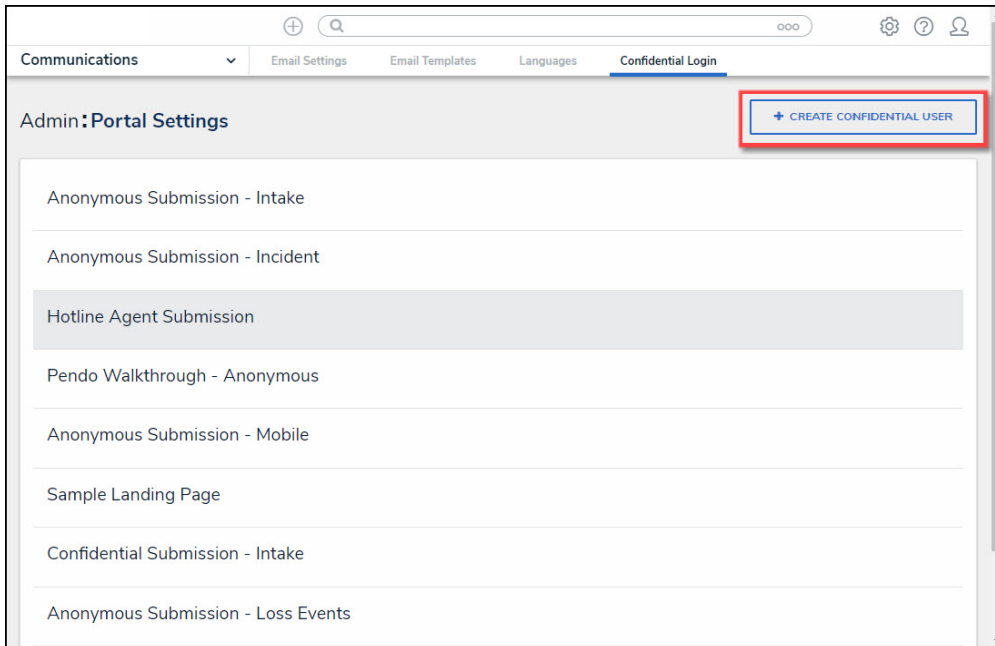
System Icon

2. From the **Admin Overview** screen, click the **Portal Settings** tile on the **Communications** section.



Portal Settings Tile

3. From the **Portal Settings** screen, click the **+ Create Confidential User** button.

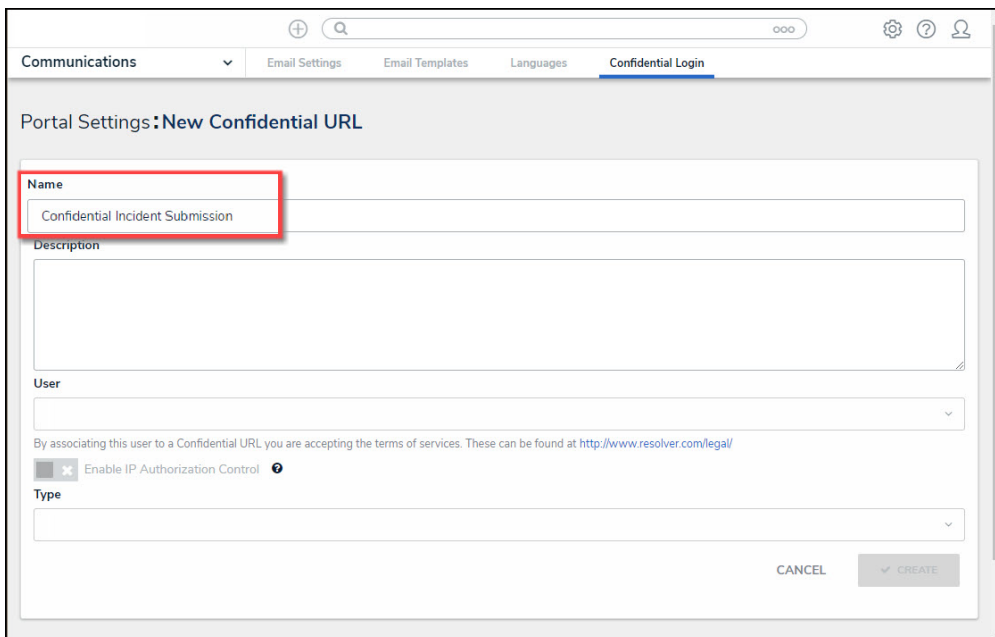


+ Create Confidential User Button

Create a Confidential Login

An Administrator must create a non-administrative user account for the login, and assign it to a [role](#) with access to the appropriate object type(s) and activity before they can create the Confidential Portal Login. For more information, please refer to the [Create a New User](#) article.

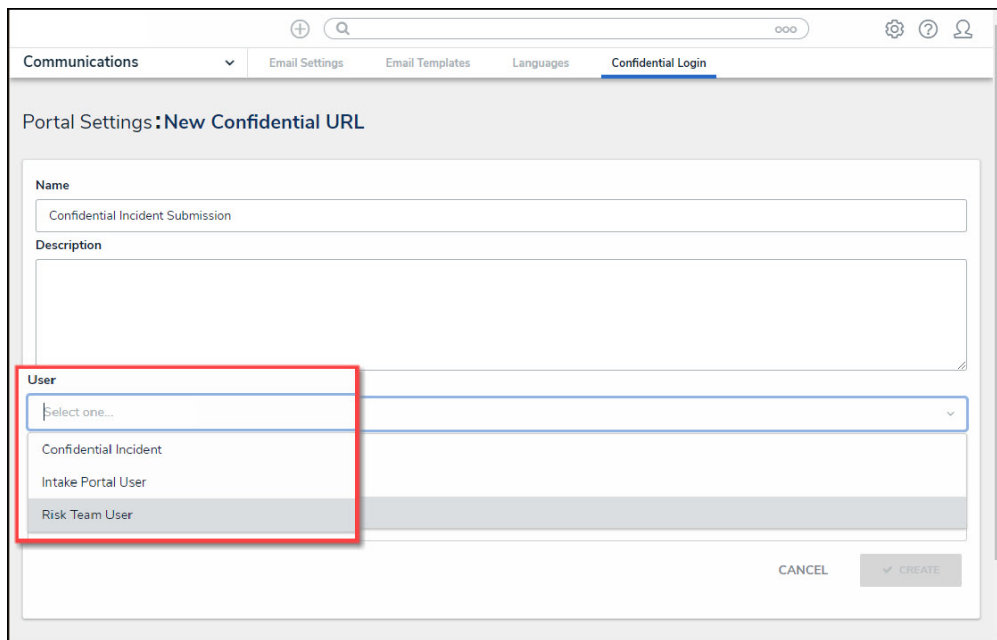
1. From the **New Confidential URL** screen, enter a login name in the **Name** field.



Name Field

2. **(Optional)** Enter a login description in the **Description** field. This description will appear below the login's name on the **Confidential Login** screen.

3. Select a non-administrative account from the **User** dropdown menu.



The screenshot shows a web interface for 'Confidential Login' with a 'New Confidential URL' form. The form includes fields for 'Name' (containing 'Confidential Incident Submission') and 'Description'. A 'User' dropdown menu is highlighted with a red box, showing the following options: 'Confidential Incident', 'Intake Portal User', and 'Risk Team User'. At the bottom right of the form are 'CANCEL' and 'CREATE' buttons.

User Dropdown Menu

4. **(Optional)** Click the Enable IP Authorization Control toggle switch to restrict who can access this URL (based on the entries in the IP allow list). The toggle switch will be greyed out if IP authorization control is not enabled for the Org. For more information, please refer to the [IP Authorization Control](#) article.

5. Select one of the following **Type** options from the dropdown menu:

- **Form:** The **Form** type displays a configurable form only.
 - **Object Type:** Select an **Object Type** from the **Object Type** dropdown list. The **Object Type** dictates which Forms will be available to select on the **Forms** dropdown menu.
 - **Form:** Select a **Form** from the **Form** dropdown menu. The **Form** selected will appear when access the Confidential Portal.

The screenshot shows the 'Confidential Login' configuration page in the Resolver interface. The page title is 'Portal Settings: New Confidential URL'. The form includes the following fields and options:

- Name:** Confidential Incident Submission
- Description:** (Empty text area)
- User:** Confidential Incident
- Terms of Service:** By associating this user to a Confidential URL you are accepting the terms of services. These can be found at <http://www.resolver.com/legal/>
- Enable IP Authorization Control:** (Checked)
- Type:** Form
- ObjectType:** (Empty dropdown menu, highlighted with a red box)
- Form:** (Empty dropdown menu, highlighted with a red box)

At the bottom right of the form, there are two buttons: 'CANCEL' and 'CREATE'.

Form Additional Fields

- **Activity:** The **Activity** type displays the actions and views within an activity.
 - **Application:** Select an **Application** (e.g., IT Risk Management) from the **Application** dropdown list. The **Application** dictates which Activities will be available to select on the **Activity** dropdown menu.
 - **Activity:** Select a **Activity** from the **Activity** dropdown menu. An Activity is the part of an application where users can create, edit, and view data. The **Activity** selected will appear when access the Confidential Portal.
 - **(Optional) Pendo® Guide:**

Communications | Email Settings | Email Templates | Languages | Confidential Login

Portal Settings: New Confidential URL

Name
Confidential Incident Submission

Description

User
Confidential Incident

By associating this user to a Confidential URL you are accepting the terms of services. These can be found at <http://www.resolver.com/legal/>

Enable IP Authorization Control

Type
Activity

Application
Please select an Application

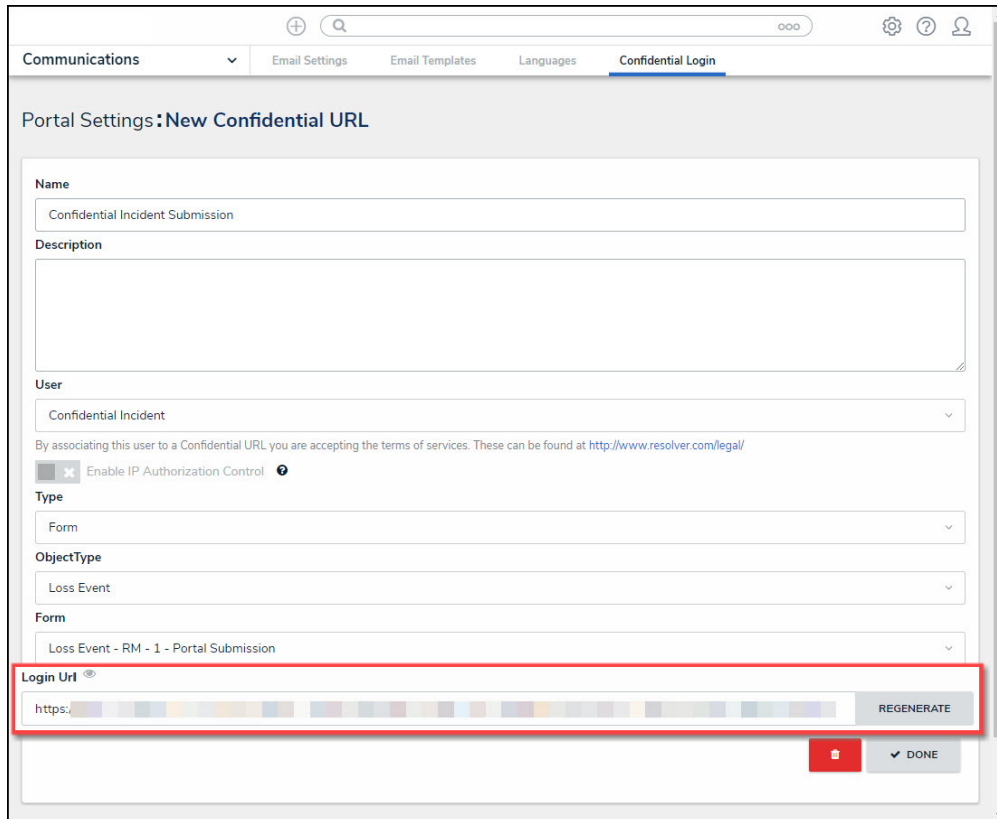
Activity
Please select an Activity

Pendo Guide

CANCEL CREATE

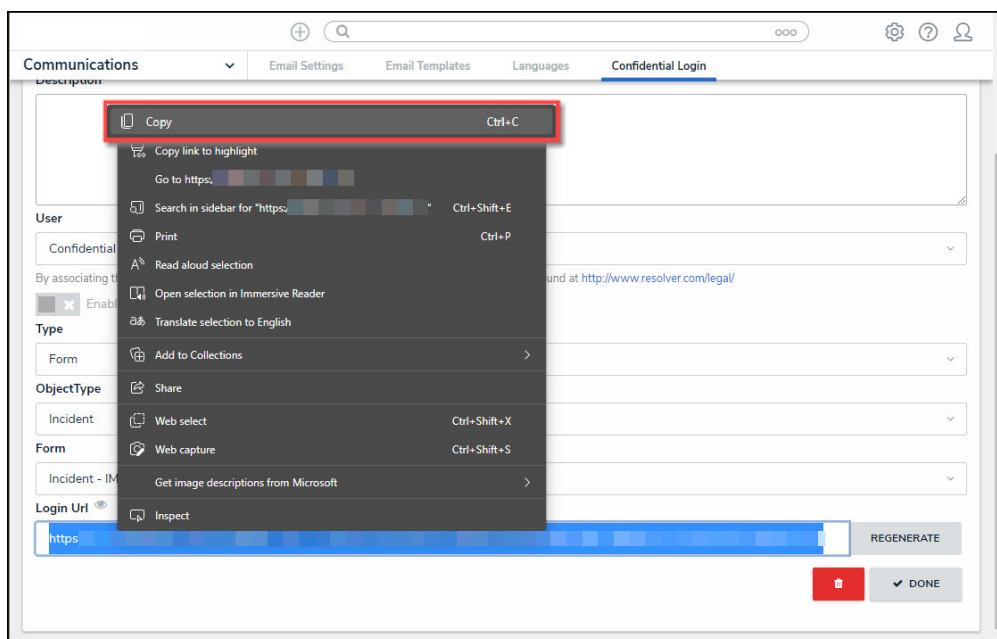
Activity Addition Fields

6. Click the **Create** button to save your changes, the New Confidential URL screen will refresh and the system will generate the confidential **Login URL**. The **Login URL** field is a read-only field.



Login URL Field

7. **(Optional)** Click the **Regenerate** button to create a new Login URL if you have edited any of the field on the **New Confidential URL** screen, or for security reasons.
8. Using your cursor, highlight the **Login URL** and press the **Right** mouse button to select the **Copy** option from the **Context Menu**.



Context Menu

9. Paste the **Login URL** in an email or document to send to a Submitter.

Impersonate Another User

Overview

With the **Impersonation** feature, Administrators can temporarily assume the account of another user to work with objects according to that user's [role](#) and permissions. This feature is useful when Administrators need to test the user's permission levels or to complete a task for users who may otherwise be unable to do so themselves. Administrators can impersonate other Administrators, but they are unable to perform administrative tasks while doing so.

Impersonation Mode can also be used to identify and fix any [standard form](#) conflicts for users in multiple roles. See the [Form Conflicts](#) section for more information.

Any changes made while impersonating another user are captured in the [User Audit Trail](#).

If IP authorization control is enabled on your Org, your IP address will be validated against the IP allow list when activating **Impersonation Mode** and when disabling it. If your IP address cannot be validated, you'll be logged out. See the [IP Authorization Control](#) section for more details.

User Account Requirements

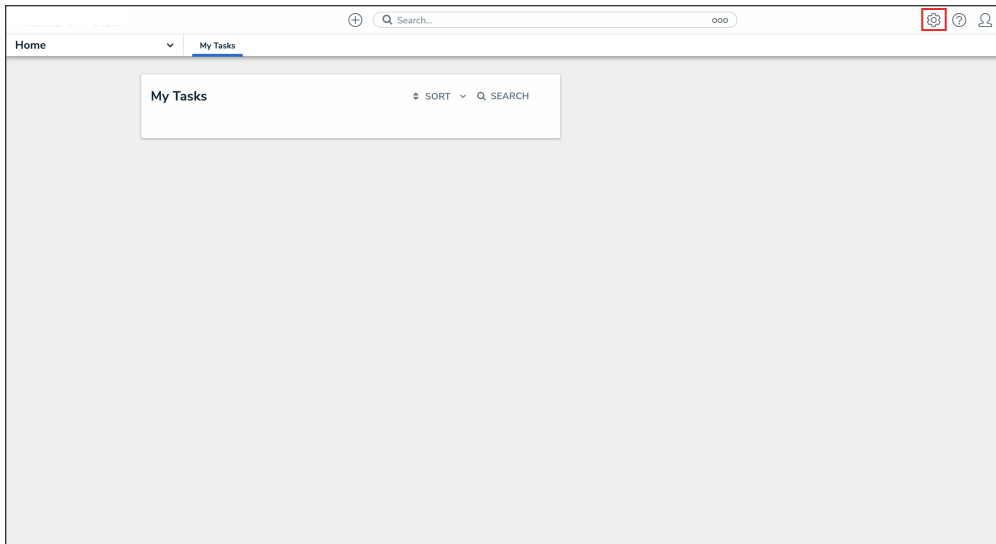
The user account you use to log into Resolver must have Administrator or advanced permissions to access the **User Management** screen.

Related Information/Setup

For more information on the different user types in Resolver, please refer to the [Create a New User](#) article.

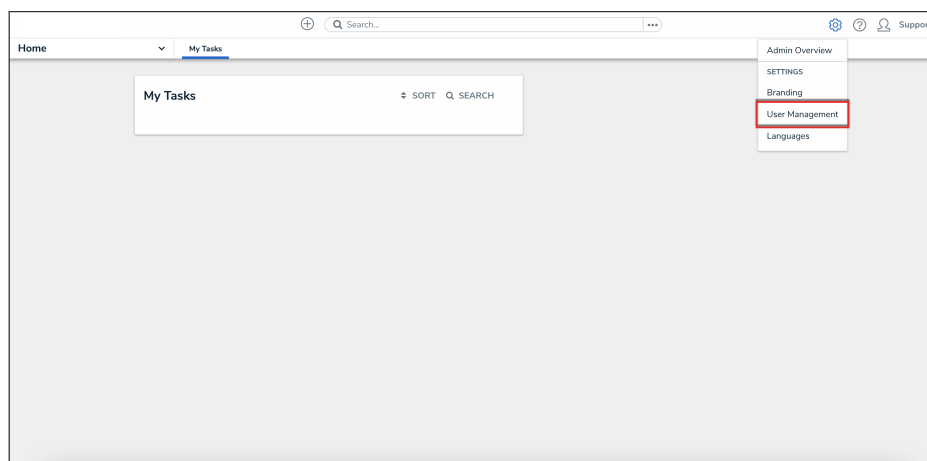
Navigation

1. From the **Home** screen, click the **Administration** icon.



Administration Icon

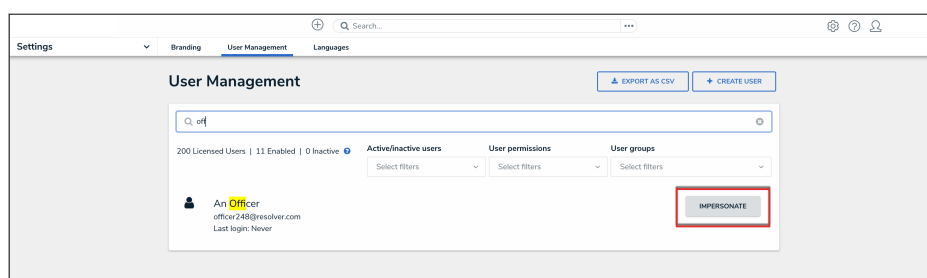
2. From the **Administrator** settings menu, click **User Management**.



Administrator Settings Menu

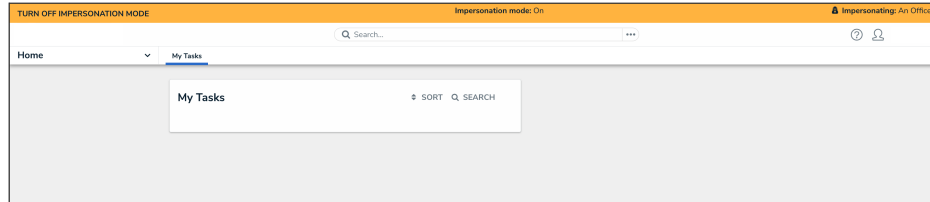
Impersonating Another User

1. From the **User Management** screen, enter a user's name in the **Search** field to narrow the search results.
2. Click the **Impersonate** button next to the user you wish to impersonate.



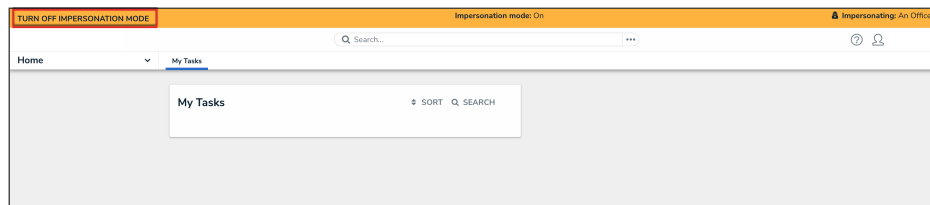
Impersonate Button

3. While in **Impersonation Mode**, the name of the user you're impersonating will appear in a yellow banner at the top of the page.



Impersonation Mode

4. To deactivate Impersonation Mode, click **Turn Off Impersonation Mode** from the yellow banner at the top of the page.



Turn Off Impersonation Mode

Edit or Delete a User

Overview

From the **Edit User** screen, an Administrator can edit a user's information, set the user account status and advanced permissions, and add the user to user groups and roles.

User Account Requirements

The user account you use to log into Resolver must have Administrator or advanced permissions to edit users.

Related Information/Setup

Please see the [Languages Overview](#) article for more information on using an alternate language setting.

Please see the [Access Your Data Warehouse Settings](#) article for Orgs that have Data Warehouse enabled.

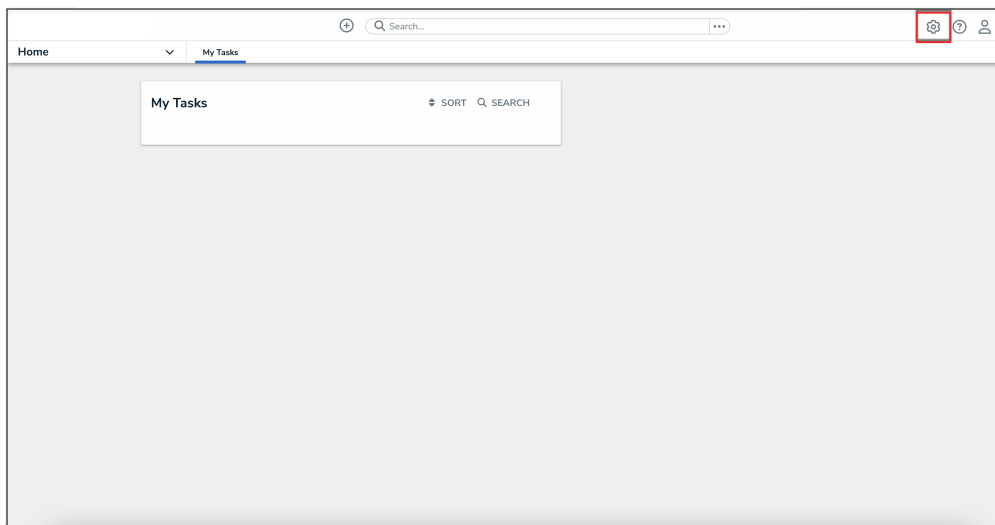
Please see the [Assigning Advanced Permissions to a User](#) article for adding advanced permissions to a user.

Please see the [Managing Portal URL Membership](#) article for more information on managing Portal URL membership for Portal URL Access users.

Please see the [Resetting Multi-Factor Authentication](#) and [Opt-Out Multi-Factor Authentication for a Specific User](#) articles for more information on opting out of and resetting MFA for an individual user.

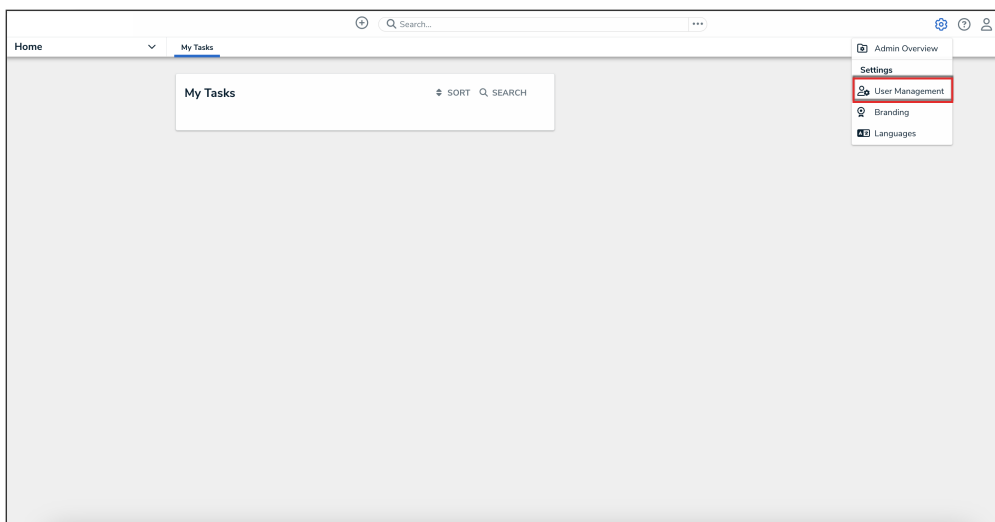
Navigation

1. From the **Home** screen, click the **Administration** icon.



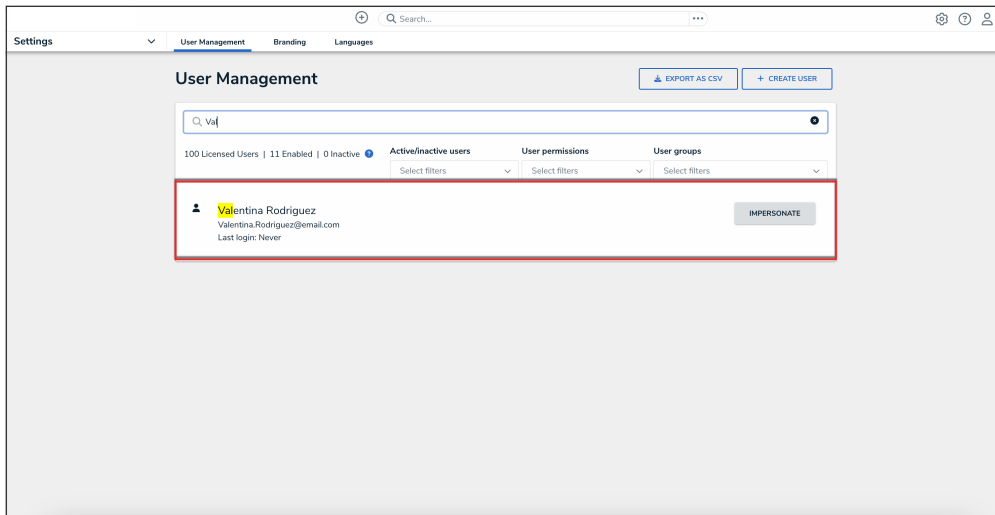
Administration Icon

2. From the **Administrator Settings** menu, click **User Management**.



Administrator Settings Menu

3. Enter a user's name in the **Search** field to narrow the search results.
4. Click the name of the user you want to edit.



User Name

Editing a User



Note:

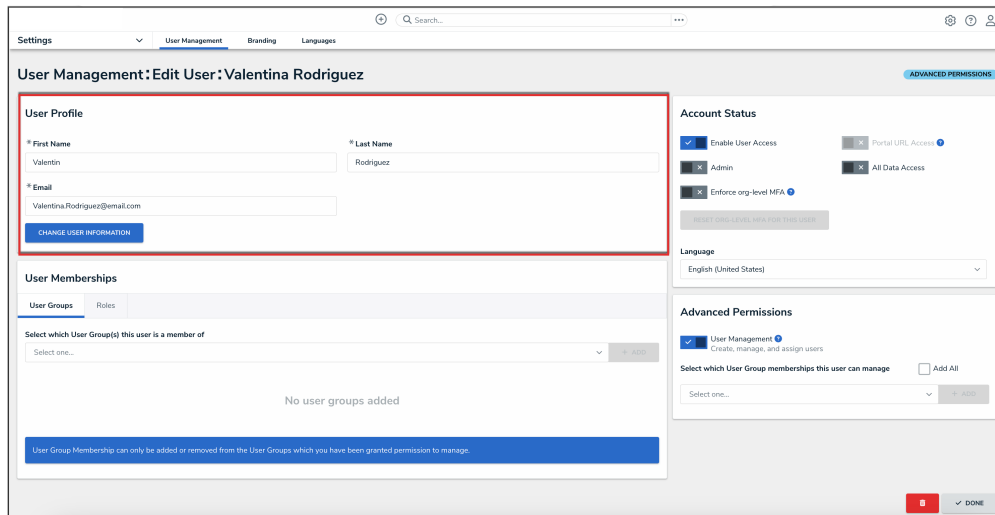
The **Edit User** screen may look different if SSO or MFA is enabled on your Org.

1. From the **Edit User** screen, an Administrator can edit the following fields under the **User Profile** section:

- **First Name:** Click the **First Name** field to change to the user's first name.
- **Last Name:** Click the **Last Name** field to change to the user's last name.
- **Email Address:** Click the **Email Address** field to change to the user's email address.
 - The following are different situation that can occur when change a user's email address:
 - If the Administrator who changes the email address is a member of all the same Orgs as the user. The email address change will take effect immediately.
 - If the Administrator who changes the email address is not a member of all the same Orgs as the user. The user is moved to a Pending state and must click a **Verification** link for the changes to take effect. The Administrator can also **Resend Email Confirmation** or **Cancel Changes**.
 - If the user is logged in to the system. The user will see a system notification at the top of their screen, indicating Email Updated.
 - If the user is not logged in to the system. The user will be redirected the next time they log in. The user must log in on the redirected screen using their original email address. On successful login, the user will see an

Email Updated confirmation message.

- In the **User Profile** section, an Administrator can edit the user's **First Name**, **Last Name**, or **Email Address** fields. Once you make a edit to one of these fields, click the **Change User Information** button to save the changes.



User Profile Section

- An Administrator can edit the following toggle switches and fields under the **Account Status** section:

- **Enable User Access:** Select the **Enable User Access** toggle switch to enable (blue) or disable (grey) a user profile.
- **Portal URL Access:** Click the **Portal URL Access** toggle switch to grant the user account access only to the Portal URL.



Note:

When you click the **Portal URL Access** toggle switch, the **Admin**, **All Data Access**, **Enforce Org Level MFA**, and **Advanced Permission** toggle switches will automatically be disabled.

- **Admin:** Select the **Admin** toggle switch to enable (blue) or disable (grey) Administration permissions.
- **All Data Access:** Select the **All Data Access** toggle switch to enable (blue) or disable (grey) all access, granting the user access to all object types and objects within an organization.
- *For Orgs that have multi-factor authentication (MFA) enforced:* An **Enforce Org Level MFA** toggle switch will be visible which allows Administrators to opt that user out of MFA for that Org. Please see the [Opt-Out Multi-Factor Authentication for a](#)

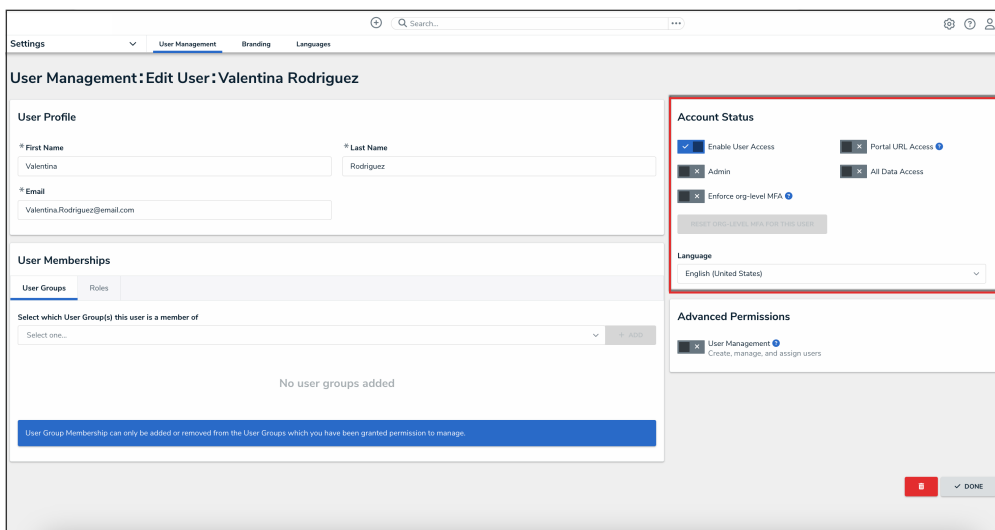
[Specific User](#) article for more information.

- **Language:** Select a **Language** preference from the dropdown menu to change the system's language setting. Before you can set an alternate language setting, an Administrator needs to download a language .csv file from the system, map language translations to the user interface text, and upload the .csv file for use within Resolver.



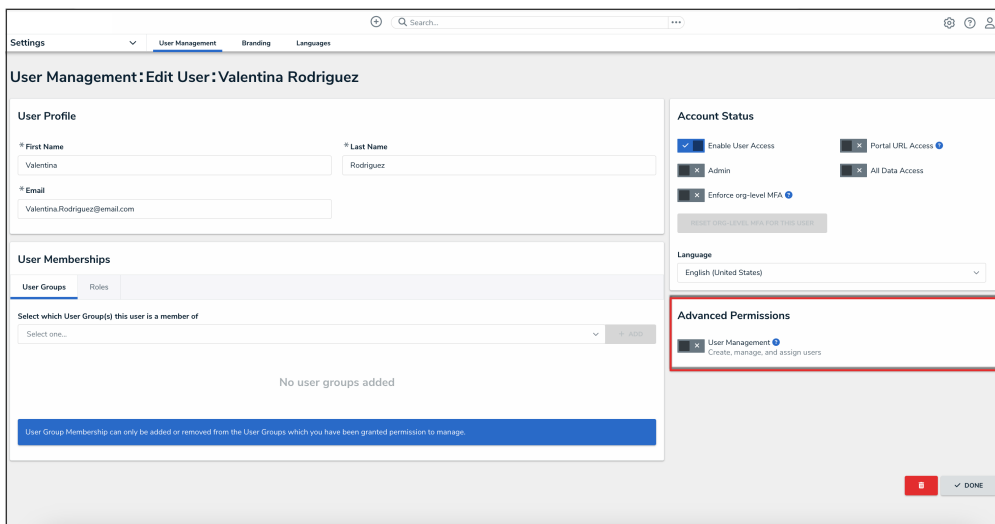
Note:

The default language setting in the user's browser will take precedence over Resolver for language translations.



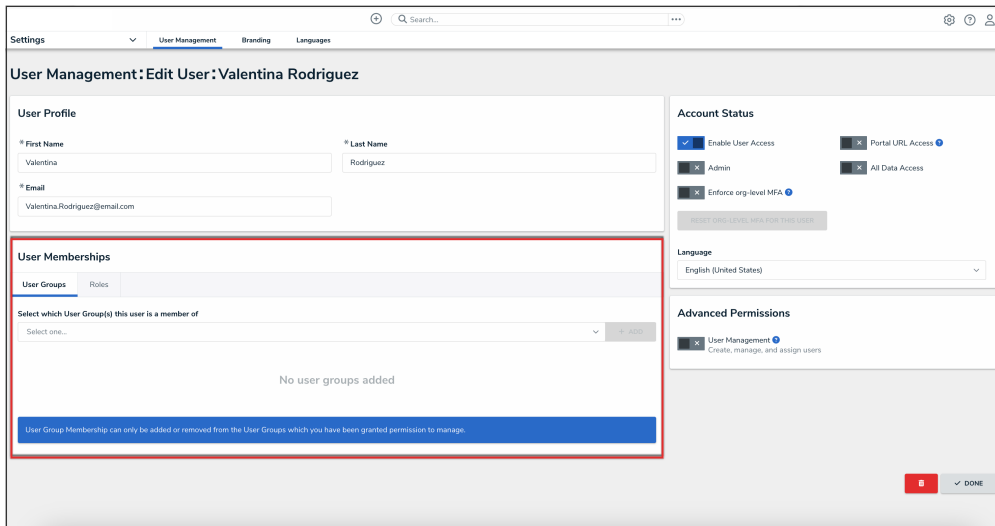
Account Status Section

4. Click the **User Management** toggle switch under the **Advanced Permissions** section to grant the user advanced permissions. Please see the [Assigning Advanced Permissions to a User](#) article for adding advanced permissions to a user.



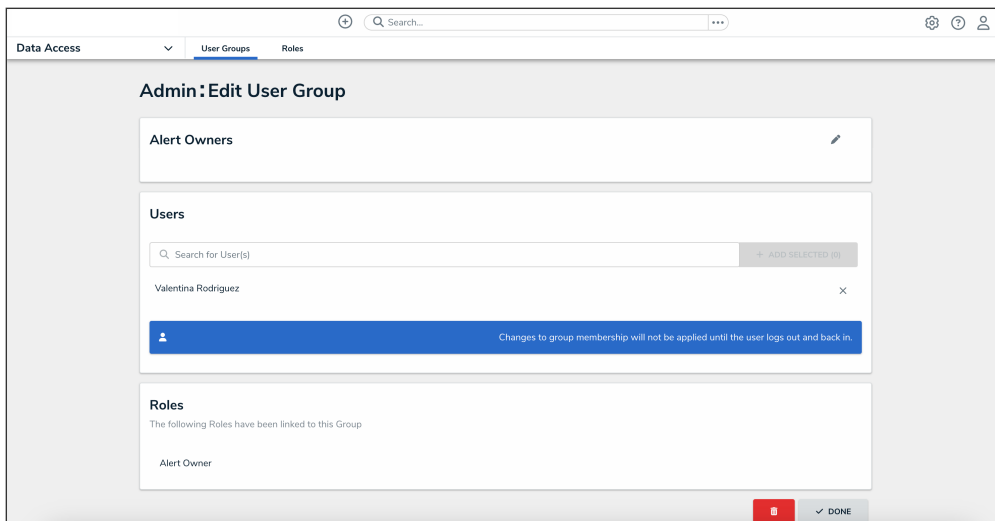
User Management Toggle Switch

5. For **Portal URL Access** users: In the **User Group Membership** section, the **Portal URLs** tab shows which Portal URL a Portal URL Access user is assigned to. Please see the [Managing Portal URL Membership](#) article for more information.
6. In the **User Group Membership** section, the **User Groups** tab shows the user groups the user is enrolled in. To add a user to a user group, select the user group from the **Select which User Groups(s) this user is a member of** dropdown and click the **Add** button.



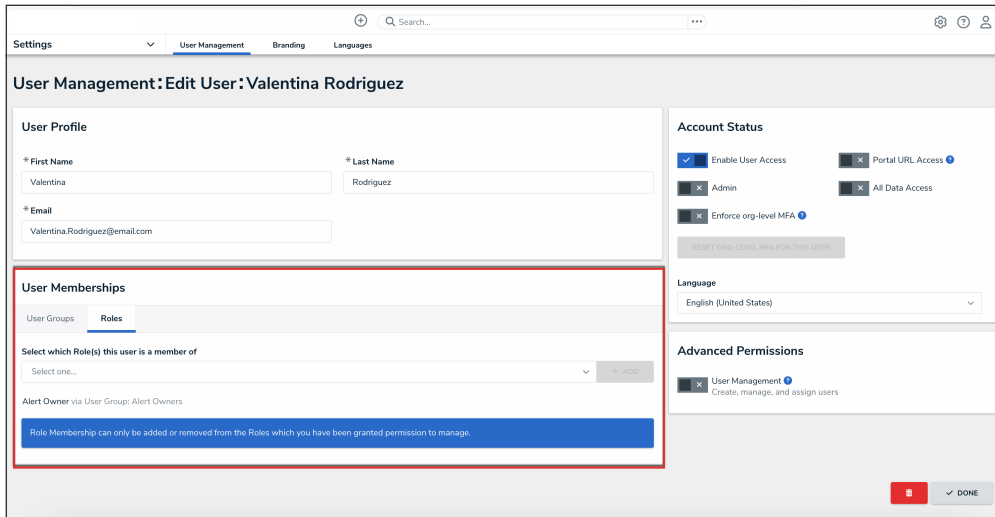
User Groups Tab

7. Click a **User Group** to open the **Admin: Edit User Group** screen to view further details, remove, and add a user to the user group.



Edit User Groups Screen

8. In the **User Group Membership** section, the **Roles** tab shows the roles the user is enrolled in. To add a user to an individual role, select the role from the **Select which Role(s) this user is a member of** dropdown and click the **Add** button.



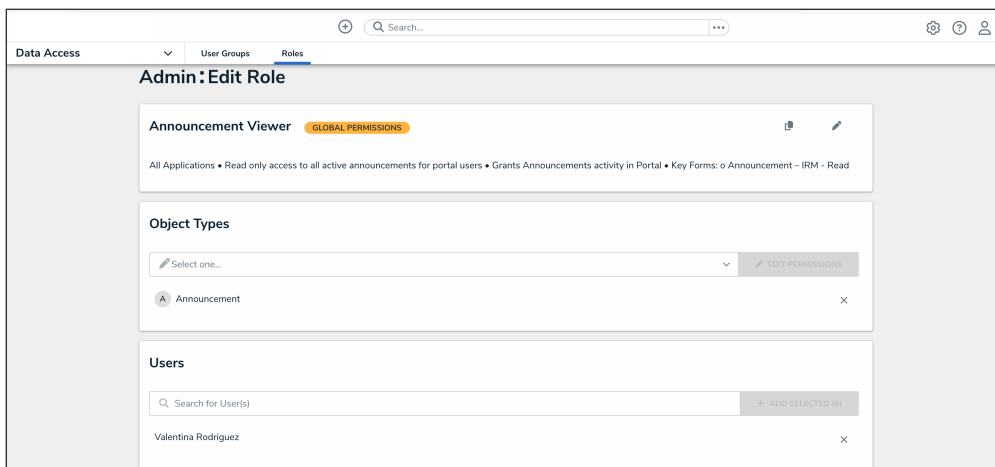
Roles Tab



Best Practice:

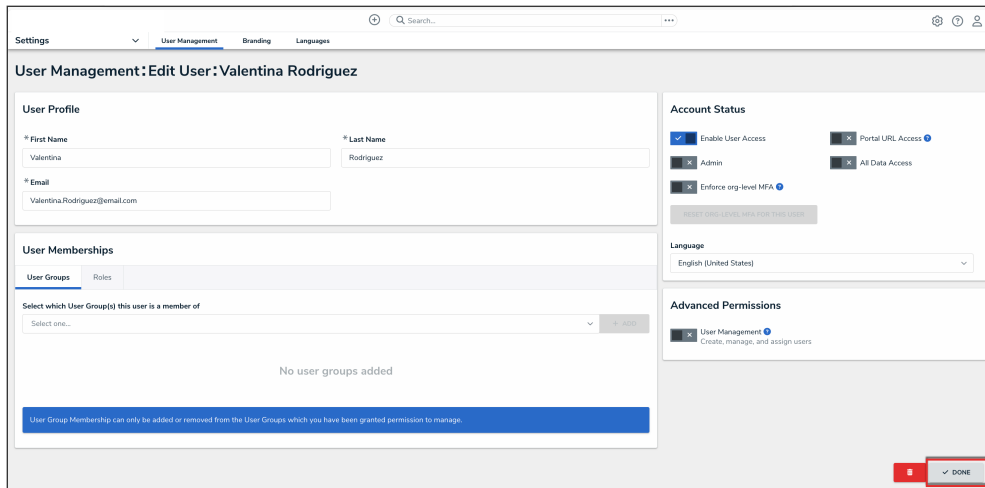
We recommend adding users to a user group via the **User Memberships** section to more accurately manage permissions for all the users in the same group.

9. Click a **Role** to open the **Admin: Edit Role** screen to view further details, remove, and add a user to a role.



Edit Role Screen

10. Click the **Done** button to save your changes.



Done Button

Edit or Delete a User Group

Overview

An Administrator can make changes to a user group or delete a user group. A user group organizes users into specific groups based on their organizational role (e.g., Employee, Management, etc.). Adding users to a user group allows an Administrator to assign multiple users within a user group to a role by assigning the user group to a role instead of manually assigning a role to each user.

If your organization uses LDAP, adding or removing users on a user group will need to be done from LDAP. If changes are made in Resolver, any changes will revert during the next LDAP sync.

User Account Requirements

The user account you use to log into Resolver must have Administrator permission to access the **Admin Overview** screen.

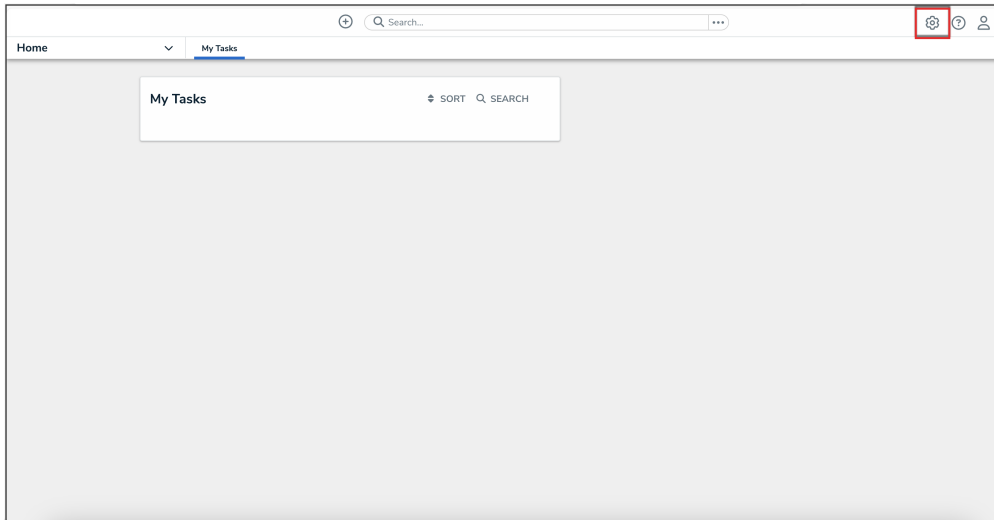
Related Information/Setup

Please read the [User Group Overview](#) article for more information regarding user groups.

Please read the [Configure & Run the LDAP Sync Tool](#) article for more information regarding LPAD.

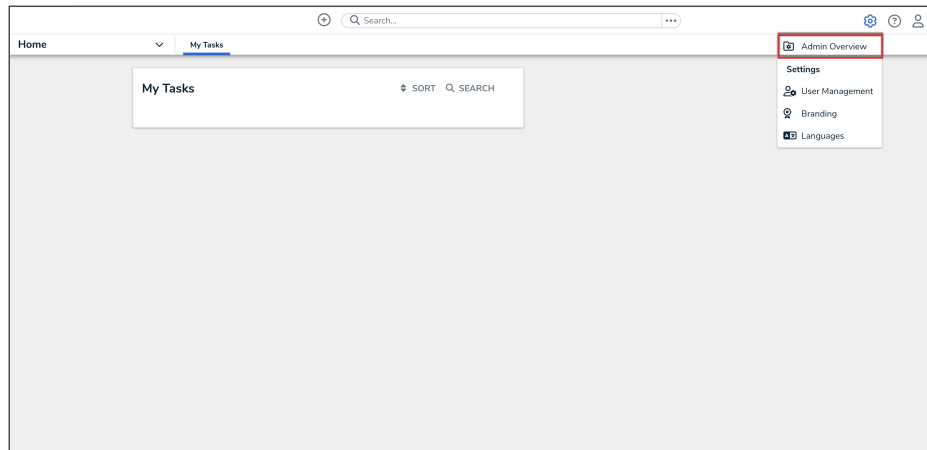
Navigation

1. From the **Home** screen, click the **Administration** icon.



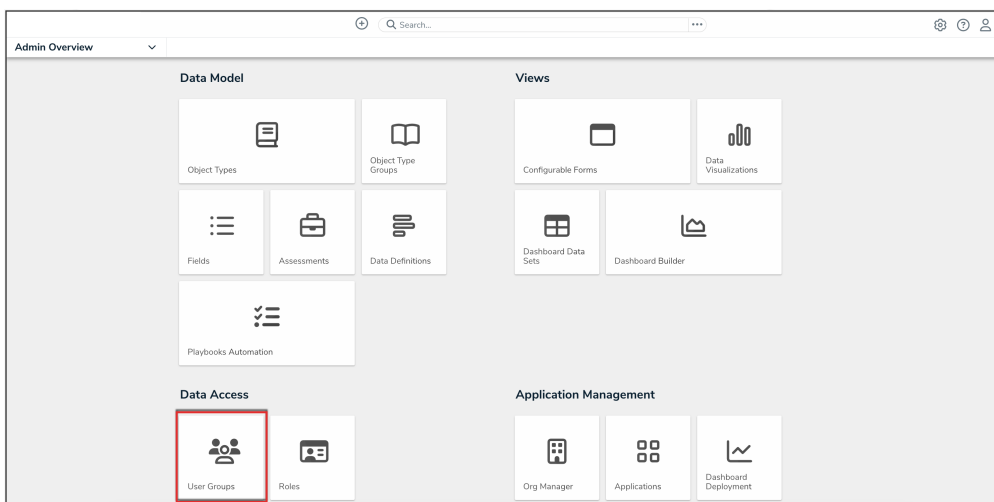
Administration Icon

2. From the **Administrator settings** menu, click **Admin Overview**.



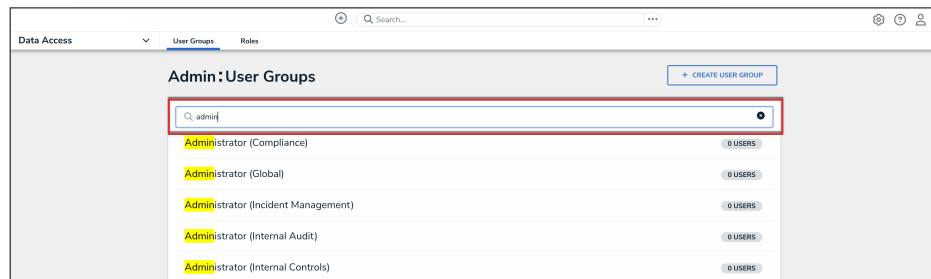
Administrator Settings Menu

3. From the **Admin Overview** screen, click the **User Groups** tile under the **People** section.



User Groups Tile

3. From the **User Groups** screen, enter a user group name or keyword in the **Search** field.

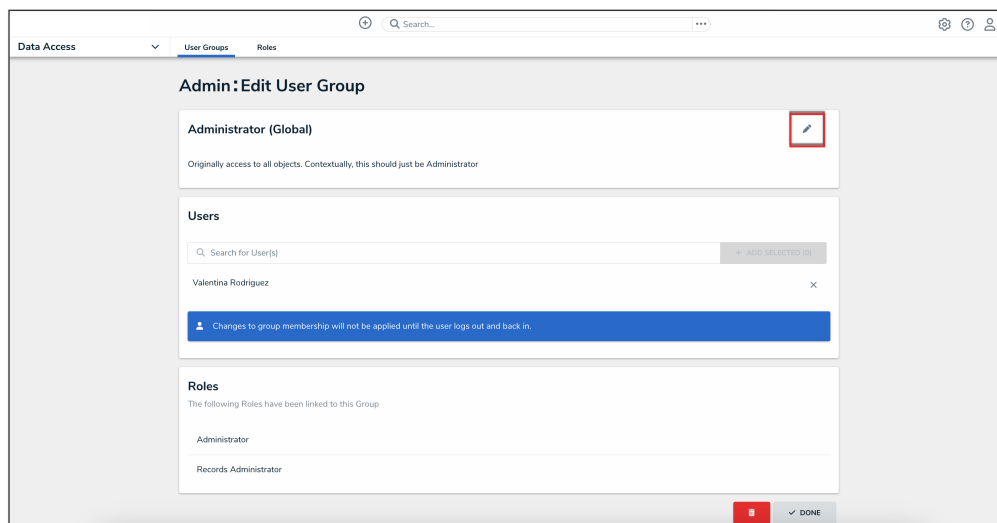


User Groups Screen

4. Click the name of the user group that you want to edit or delete.

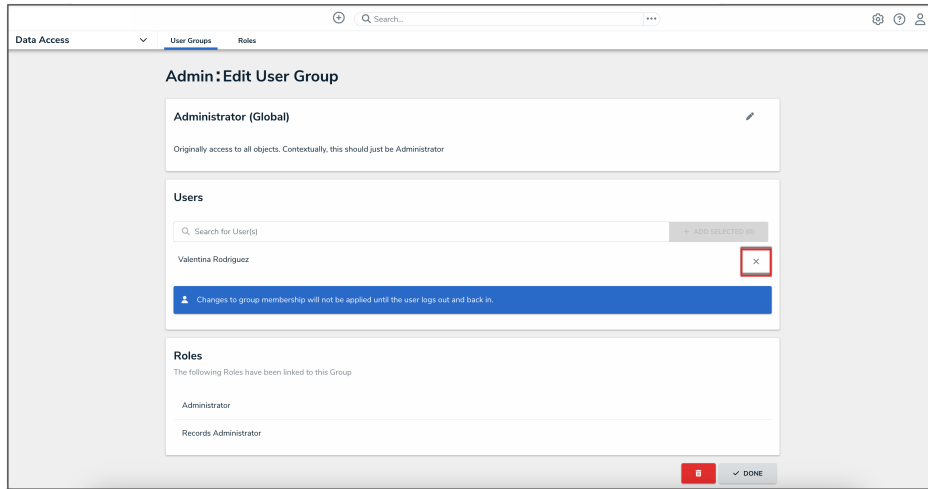
Editing a User Group

1. From the **Edit User Groups** screen, click the **Edit** icon to edit the user group's **Name** and **Description** fields.



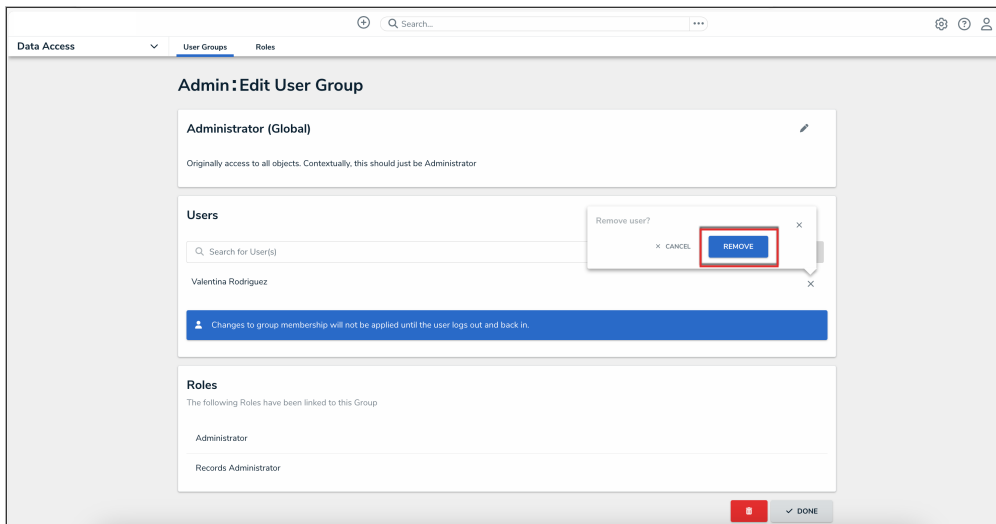
Edit Icon

2. From the **Users** section, you can add users to the user group. Please read the [Add a User to a User Group](#) article for more information.
3. To remove a user from the user group, click the **Remove** icon beside the user's name.



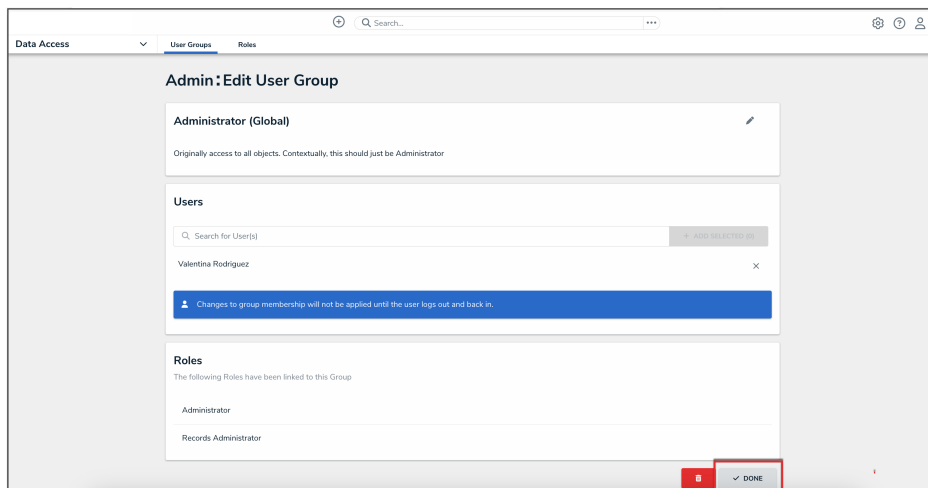
Remove Icon

4. Click the **Remove** button from the **Remove user?** pop-up.



Remove Button

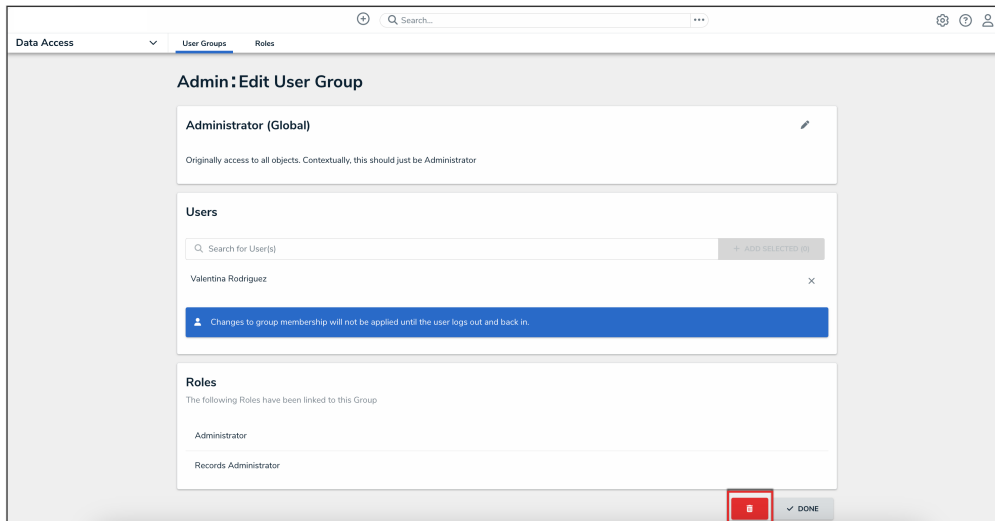
5. Click the **Done** button to save your changes.



Done Button

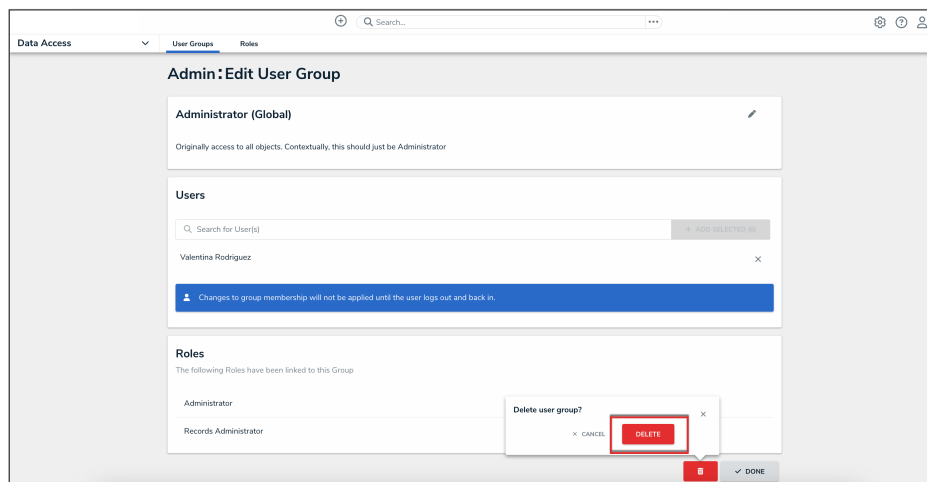
Deleting a User Group

1. From the **Edit User Group** screen, scroll to the bottom of the screen and select the **Delete** icon.



Delete Icon

2. Click the **Delete** button from the **Delete user group?** pop-up.



Delete Button