Advanced Permission Types

Last Modified on 07/23/2025 2:01 pm EDT

Overview

Administrators can grant Standard users limited access to use some Administrator features by assigning them advanced permissions.

The five types of advanced permissions are:

- **Data Import Management**
- **Data Management**
- **Settings Management**
- **User Impersonation**
- **User Management**

Please scroll through this article to read the list of permissions that each advanced permissions type grants the user.

> ***Note:***
> *One or more advanced permission can be added to the same user and each permission is additive. If one permission gives access to something and another permission doesn't have this access, the user will be granted access.*

Related Information/Setup

For more information on granting a user advanced permissions, please refer to the Assigning Advanced Permissions to a User article.

User Account Requirements

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

Data Management Advanced Permissions

Users with the **Data Management** advanced permission will have access to the following:

- See and access the ***Admin Overview*** screen from the **Administrator Settings** menu
- See and access the **Data Visualizations**, **Dashboard Data Sets**, and **Dashboard**

Builder tiles
- Create and edit data analytics exports, data grids, and reports
- Duplicate existing data visualizations
- Create, edit, and publish dashboard datasets and dashboards
- Create and delete data transformations
- View counts of created, published, and unpublished dashboard datasets and dashboards
- Unpublish dashboards

Users with the **Data Management** advanced permission cannot access the following:

- Adding data visualizations or dashboards to activities, activity actions, views, forms, and form actions
- Creating new config elements to use in data visualizations, dashboard datasets, or dashboards
- Deleting data analytics exports, data grids, and reports
- Deleting and unpublishing dashboard datasets
- Unlinking preselected properties like object name and workflow state
- Deleting dashboards

Settings Management Advanced Permissions

Users with the **Settings Management** advanced permission will have access to the following:

- See and access the ***User Management***, ***Branding***, and ***Languages*** screens from the **Administrator Settings** menu
- Create and edit users
- Enable and disable users
- Add and remove user group and role membership for users
    - Administrators will assign which user groups and roles the **Settings Management** advanced permission user has permission to manage. Only these users groups and roles can be assigned to other users. If the **Settings Management** advanced permission is removed, all users groups and roles they have permission to manage will be permanently removed.
    - If the user has both the **Settings Management** and **User Management** advanced permission, the user groups and roles they have permission to manage will be shared. If one of the advanced permissions is removed, the user groups and roles the user has permission to manage won’t change.
- Add and edit the Org name and logo
- Enable and deactivate the Org name display in header
- Add and edit languages

- Download and import the language file

Users with the **Settings Management** advanced permission cannot access the following:

- Exporting users as a CSV
- Impersonating users
- Creating Portal URL or Administrator users
- Editing user type for existing users
- Viewing Portal URL users
- Adding and editing Portal URL or advanced permission memberships
- Managing **All Data Access**, **SSO Access**, **Enforce Org-Level MFA**, **Reset MFA**, or **Data Warehouse Setting** on the ***User Management*** screen
- Deleting users
- Accessing the ***User Groups*** and ***Roles*** screen by selecting an added user group and role

---

User Management Advanced Permissions

Users with the **User Management** advanced permission will have access to the following:

- See and access the ***User Management*** screen from the **Administrator Settings** menu
- Create and edit users
- Enable and disable users
- Add and remove user group and role membership for users
    - Administrators will assign which user groups and roles the **User Management** advanced permission user has permission to manage. Only these users groups and roles can be assigned to other users. If the **User Management** advanced permission is removed, all users groups and roles they have permission to manage will be permanently removed.
    - If the user has the **Settings Management** and **User Management** advanced permission, the user groups and roles they have permission to manage will be shared. If one of the advanced permissions is removed, the user groups and roles the user has permission to manage won’t change.

Users with the **User Management** advanced permission cannot access the following:

- Exporting users as a CSV
- Impersonating users
- Creating Portal URL or Administrator users
- Editing user type for existing users
- Viewing Portal URL users

- Adding and editing Portal URL or Advanced Permission memberships
- Managing **All Data Access**, **SSO Access**, **Enforce Org-Level MFA**, **Reset MFA**, or **Data Warehouse Setting** on the ***User Management*** screen
- Deleting users
- Accessing the ***User Groups*** or ***Roles*** screens by selecting an added user group or role

---

Data Import Management Advanced Permissions

Users with the **Data Import Management** advanced permission will have access to the following:

- Managing data imports
- Reassigning data

User Impersonation Advanced Permissions

Users with the **User Impersonation** advanced permission will have access to the following:

- View and access the ***User Management*** screen from the Administrator Settings menu.
- View users in the user list they have permission to impersonate.
    - Can see users in user groups/roles they have permission to impersonate.
    - If a user has the **Settings Management** or **User Management** advanced permission, along with the **User Impersonation** advanced permission, they will see both users they have permission to manage and impersonate. Users they only have permission to manage will have a deactivated **Impersonate** button.
- Impersonate active, Standard users with no advanced permissions from specified user groups and/or roles using the **Impersonate** button.
- View and use the user search and filter (active/inactive users and user groups) features.
- View user profiles in read-only for users they have permission to impersonate.
    - Can see **First Name**, **Last Name**, **Email**, **User Type**, **Enabled User Access**, **Language** fields and **User Groups** and **Roles** tabs.
- Turn off the Impersonation feature.
- Have any data changes made while impersonating another user captured in the Data Audit Trail.

Users with the **User Impersonation** advanced permission cannot access the following:

- Impersonate Administrators, inactive users, Portal URL users, or Standard users with advanced permissions (including themselves).
- See Administrators, Portal URL users, or Standard users with advanced permissions

(including themselves) in the user list.

- Create, edit, or delete users.
- Export the user list.
- Access the ***Roles*** or ***User Groups*** pages via the ***Edit User*** page.
- See the **All Data Access**, **SSO Access**, and **Enforce Org-Level MFA** fields, **Data Warehouse Settings,** and **Portal URL** and **Advanced Permission** tabs.