Recast

Permissions

Last Modified on 2026-09-28

Permissions allow you to assign access policies to identities like users, user collections, groups or contexts that do not have one assigned. And for those who have one assigned, you can overwrite it here.

Permissions list

This list displays all permissions currently available in the Application Workspace System.

Selecting multiple table rows

- Adjacent rows: Click on the first row, hold down the Shift key, click on the last row in the range
- Non-adjacent rows: Hold the Ctrl or Cmd key and click on each row you want to select
- Adjacent rows, using only the mouse: Click and hold the left mouse button on the first row, then drag the cursor up or down across the rows to highlight the desired ones

Table toolbar

To create a new permission, click on the **Create** button; to view the details of a permission or edit it, double-click its entry or select the permission and click the **Edit** button.

Views gives you control on how the table is displayed.
The default view contains all your permissions in alphabetic ascending order, and the following columns: **Identity**, **Identity source**, **Access policy** and **Entity**.
You can create your own personalized view of the table, by filtering the permissions or adding/deleting columns and clicking **Save as** in the drop-down menu of **Views**.

Add permissions/Edit permissions dialog box

The **Entity** field is optional and adds an extra level of permissions, on top of the access policy you select in this dialog box. It applies only to the *Administrator* predefined access policy and to newly created access policies. In other words, if you select the *Catalog Maintainer*, *Connector* or *User* access policy, the zone/system level permission will have no effect.

The level permissions are:

- *Zone* – The user can make changes only to his zone.
  - In **Manage** > **System** > **Servers** he has read-only permission regarding the information about the Application Workspace Satellite Servers associated with his zone.
  - In **Manage** > **System** > **System updates** he has read-only permission regarding the updates applied to his zone and Application Workspace Satellite Servers associated with his zone.
- *System* – The user can make changes to his zone and the Application Workspace System but not to other zones. His main capabilities are to:
  - create non-primary zones, Application Workspace Servers and Application Workspace Satellite Servers
  - manage and apply system updates to all servers related to his zone
  - view all the zones within his Application Workspace System and choose which one to be primary
  - recover administrator access within a zone
  - configure settings for Azure blob/local storage
  - configure system level permissions for other users

System level
You can assign *System* level permissions only when you are logged on a primary zone with an account that has system level permissions and rights to create new permissions.

> If you have *System* level permissions and want to make changes to other zones inside your Application Workspace System, you must log in to those zones.

For more information about what privileges each access policy has, go to **System** > **Access policies** > open an access policy > **Privileges** screen.