Recast

Access Policies

Last Modified on 04.16.26

Access policies allow you to restrict or grant access to certain components of Application Workspace.
There are two types of access policies:

- Role – you can grant predefined privileges to it.
- Script – allows for greater control but requires scripting.

Access policies can be assigned per user, user collection, group and context.
For more dynamic customization, access policies can be defined on different levels; while the inheritance flows top-down, a local override has priority. This means for example that an access policy assigned at the group level can be overridden by one defined at the context level.

Access policies list

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

Selecting multiple rows from the table

- To select multiple adjacent rows, click on the first row, then hold down the Shift key and click on the last row in the range; all rows between will be selected.
- To select multiple non-adjacent rows, hold down the Ctrl key (or "Command" on Mac) and click on each row you want to select individually.
- To select multiple adjacent rows using the mouse only, 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.
- Selecting rows using only the keyboard is not possible.

Table toolbar

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

Views gives you control on how the table is displayed.
The default view contains all your access policies in alphabetic ascending order, and only a few columns: **Name**, **Type** and **Built-in**.
You can create your own personalized view of the table, by filtering the access policies or adding/deleting columns and clicking **Save as** in the drop-down menu of **Views**.

Detailed view of an access policy

See below the description of each screen in the detailed view of an access policy, and what actions you can perform in each of them.

Overview screen

Displays the same information as in the **Create access policy** dialog box you used when you created the current access policy.

> Note that the type of an access policy cannot be changed once created.

Recast

Privileges screen

It shows a list of privileges that are available in Application Workspace. By enabling entries in the list, you enable these privileges for the current access policy. For example, if you enable “Create Access Policy” for a specific access policy, the user associated with that access policy will be able to create access policies.

The **Privileges** screen is available only for the *Role* type access policy.

Script screen

Here you can create your scripts to regulate access to Application Workspace components. This option facilitates the creation of more complex access policies, that can’t be solved with the editor.

Below you will find a sample script that grants access to the connector functionality and API.

```
(
 isof(resource, '#recastsoftware.Server.BLL.Zone')
 and
 (
  (action eq 'access_connector')
  or
  (action eq 'access_api')
 )
)
```

The **Script** screen is available only for the *Script* type access policy.

Usage screen

This screen is for information purpose only and it displays the entities associated with the current access policy.
An access policy can be assigned to a user, group or context in **Manage** > **System** > **Permissions** or within the identity's detailed view in the **Access policy** screen.
For a user collection it can be assigned only in **Manage** > **System** > **Permissions**.