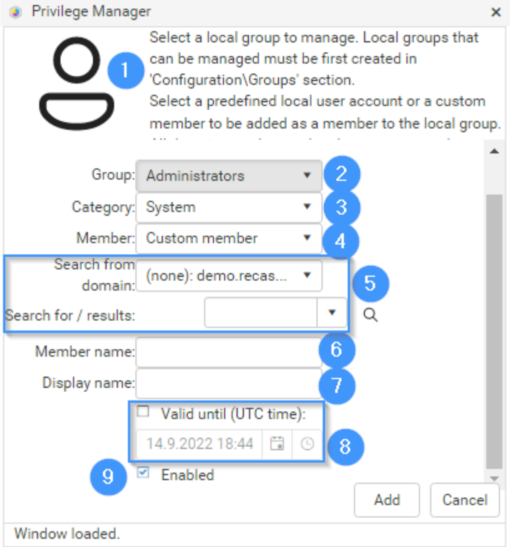
Add Or Modify a Managed Group Rule

Managed group rules allow you to add a member to a selected local group on a target.



Privilege Manager

Select a local group to manage. Local groups that can be managed must be first created in 'Configuration\Groups' section.
Select a predefined local user account or a custom member to be added as a member to the local group.

Group: Administrators

Category: System

Member: Custom member

Search from domain: (none): demo.recas...

Search for / results:

Member name:

Display name:

☐ Valid until (UTC time): 14.9.2022 18:44

☑ Enabled

Window loaded.

To add or modify a managed group rule:

1. Rule target

   You can see what will be the management level (see more information about management levels from Managed groups) and target for the new rule. Verify that you are adding the new rule to a correct management level and target.

2. Select group

   Select the local group from the dropdown list. This will be the local group in target computer(s) where specified member will be added. Selected local groups must exist on the target computer(s) for rules to be applied on target computer(s). If selected local group do not exist on target computer(s) then the rule will not affect these computers but error log events will be written to the Privilege Manager Client log.

3. Select category

   Select the category from dropdown list. Category filters selections on Select predefined or custom member dropdown list. By default there is one built-in System category that filters list to show built-in users (like local Administrator account, everyone, etc.). In addition to System built-in category there is always (none) available on category dropdown list. This filters list to show additional local users that have been created without specifying a category. Other categories can be available in the dropdown list if additional categories have been created (see Create a Category). Selecting other category filters the list to show local users that have been created in this category.

4. Select predefined or custom member

   Select predefined built-in user accounts or local users from the dropdown list. Always use built-in users (shown when System category is selected) when possible because predefined built-in users are detected on computers using the SID of the account. This will make sure that the operating system language or renamed built-in user does not affect applying the management rule on target computer(s). For example when adding local built-in

Administrator accounts to the managed local group, always use System category and the Administrator predefined built-in user as a member. This makes sure that management rule will work on different operating system language versions.

When a predefined member is selected, the search and member name fields are disabled.

There is always Custom member as the first item on the dropdown list. When a custom member is selected you will need to search or specify the member that needs to be added to the local group. This selection makes search and member name fields available for you to specify the member. Use this selection always when you need to add members from the on-premises Active Directory.

5. Search for member from on-premises Active Directory

   You can use search from on-premises Active Directory to populate Custom member name fields. If custom members are local users you do not need to select domain, just specify the custom member to the Custom member name field. You do not need to search custom member from on-premises Active Directory, you can also specify the custom member directly to Custom member name field. Searching custom member from on-premises Active Directory helps you to get the correct member name format for the custom member.

   This field is available only if Custom member is selected. For more information about using search controls see Active Directory Search.

6. Custom member name

   Use Search for member from Active Directory to automatically populate this field or type in the custom member name manually. If you specify the custom member name manually use 'DOMAIN\account name' format for domain based custom members. For local users, custom members use the 'account' format.

   This field is available only if Custom member are selected.

7. Specify the display name

   If you want to show custom members with different names in the Privilege Manager portal, specify a display name for the custom member.

   This field is available only if Custom member is selected.

8. Validity time

   Select if you want managed group rules to be valid only for a specified time. Also specify validity time. Maximum validity time is specified by the Recast Privilege Manager Administrator.

   This field is available only if enabled by the Recast Privilege Manager administrator.

9. Rule status

   Select if the managed local group rule is enabled or disabled. When the rule is enabled it will be applied to target computer(s). When all rules for managed local groups are disabled for target computers then this target computer is in reporting mode. Then only reports of local groups and users will be sent to Recast Privilege Manager database. If any of the disabled managed local group rules are enabled then local group will be changed to managed, even if rest of the managed local group rules are still disabled!