RECAST SOFTWARE

Managed Groups

Last Modified on 08.08.25

Managed groups allow you to create rules that specify which members should local groups have on target computer(s). Custom local groups that you want to manage must be first created to Privilege Manager before rules that control members on local group can be created. Built-in local groups (for example Administrators) can be used in managed group rules immediately.

When target computer(s) have at least one enabled managed group rule specified for local group then Privilege Manager will start to manage local group. This means that only members that have enabled managed group rules will be members of the local group. Other members will be removed from the local group!

Management rules can be created to any management level using on-premises Active Directory objects (domain, organization unit, group and computer), Azure AD objects (group and computer) or workgroup computers.

Rules can be created to four different management levels and have following priority order:

1. On-premises Active Directory, Azure AD or workgroup computer account (highest priority)
2. On-premises Active Directory or Azure AD groups
3. On-premises Active Directory organizational units
4. On-premises Active Directory domain (lowest priority)

Rules can be created to multiple levels and Privilege Manager creates a collection of rules for Privilege Manager Client when several rules are available for Privilege Manager Client. Example of rule collection could be:

- Rule in domain management level specifies that local Administrator account is member of local Administrators group. This rule will be applied to all Privilege Manager Clients in this domain.
- Another rule in Active Directory organizational unit named 'Workstations' specifies that Active Directory group named 'Workstation Administrators' is member of local Administrators group. This rule will be applied to all Privilege Manager Clients that are in organizational unit 'Workstations' or in any it's sub organizational units

In this example Privilege Manager Clients that belong to 'Workstations' organizational unit will have two group management rules and therefore two members will be in local Administrators group. Privilege Manager Clients that do not belong to 'Workstations' organizational unit will have only one rule (from domain management level) and therefore only one member will be in local Administrators group.

Rule collections works quite like GPO's in on-premises Active Directory. Main difference is that you can also use Active Directory groups and single computers as management level. In computer account, group and organizational unit levels you can also use rule inheritance blocking. When rule inheritance is blocked in some level then rules that has been created in lower priority levels are blocked.

1. Search group or computer

   Use directory search to manage rules linked to on-premises Active Directory and Azure AD groups or computers.
2. Show groups and computers

Select if on-premises Active Directory group and computer objects should be shown on browse directories tree view. By
default group and computer objects are not shown. If group and computer objects are shown, page load time might slow down because large amount of nodes in tree view.

3. Browse directories
   Browse on-premises Active Directory organizational units to manage rules linked to Active Directory domain or organizational
   units. If **Show groups and computers** is selected then rules for on-premises Active Directory groups and computers can be also
   managed.
4. Create workgroup computer
   Create new workgroup computer.
5. Create category
   Create a new category to organize local groups, local users and workgroup computers.
6. Workgroup computers
   Select categories or workgroup computers to manage rules linked to workgroup computers.
7. Create managed group rule
   Create new managed group rule.
8. Modify group settings
   Modify selected managed group settings. This is available only if managed group rule is selected.
9. Modify member rule
   Modify selected managed group rule. This is available only if managed group rule is selected.
10. Delete selected member rule
    Delete selected managed group rule. This is available only if managed group rule is selected.
11. Copy selected member rules
    Copy selected managed group rules. This is available only if managed group rules are selected.
12. Delete member rule
    Delete managed group rule. Confirm the deletion and click **OK.**