Configuration Rules

Last Modified on 12.12.22

After installing Privilege Manager, you'll need to create configuration rules for managing local group memberships and local user accounts. Management rules can be created for different locations, provided you have a way to target the devices affected by rules. You can combine different rules for your desired configuration.

Management rule usage

Domain or organization unit rules
If you are using on-premises AD with Privilege Manager, these rules will affect all devices where AD computer objects are at or below target hierarchy level. Domain level rules affect all devices in the whole domain, whereas OU level rules affect devices somewhere below the target OU.

Use these rules to create base configurations (like adding temporary admin, local admin, SCCM service account to local Administrators group) to all devices (existing and new) so that every device will automatically have these rules when the AD computer object is placed in the correct location.

Group rules
Group rules are available for both on-premises and Azure AD directories. Groups need to have devices as members and rules will be applied to all devices that are direct or indirect members of the target group.

Use these rules to handle exceptions (like adding SQL admins to local Administrators group in SQL servers) for group of computers and whenever possible use dynamic groups.

Category rules
If you have standalone WORKGROUP devices (like devices used to control CNC machine or servers in DMZ that are not domain joined), you can create category structure in the Privilege Manager Portal and then target rules for categories. WORKGROUP devices can be placed to single category and rules created to categories will be applied to WORKGROUP devices somewhere below the target category.

Use these rules to create base configuration (like adding temporary admin and local admin to local Administrators group) to all WORKGROUP devices (existing and new) so that every device will automatically have these rules when WORKGROUP computer is created in the correct category.

Computer rules
Computer rules are available for all device types (WORKGROUP, on-premises AD and Azure AD computers).

Use these rules to create specific single computer exceptions (like adding developer user to local the Administrators group on a developer's computer).

Example 1: Removing permanent admin permissions

Create management rules that specify members of a local Administrators group. Combine different management rule targets (domain, OU, group, category and computer) to get the desired configuration for each device. Privilege Manager will enforce these rules by adding missing members and removing existing members that are no longer allowed to be in the local Administrators group. If existing admin permissions are removed from a user that still needs to be permanent, you can add a new computer management rule to add users back to the local Administrators group.

NOTE: Remember to always create management rules for the Built-In local administrator account (Privilege Manager will use well-known SID's to manage groups and users so you don't need to worry about different localized names) to the local Administrators group. Privilege Manager cannot remove the built-in Administrator account from the local Administrators group, as Microsoft Windows prevents this action. To ensure that this account isn't used, you can disable it and randomize its password in Privilege Manager.

Example 2: Providing temporary admin access

Create a managed user rule that will create (or start to manage, if the account already exists on the device) new local user account (for example, named 'TempAdmin') using the **Generate temporary user account that can be activated** option and then create another management rule that will add this local user account to the local Administrators group. Target these rules to all devices where you want to make temporary admin access possible (use OU rules for on-premises AD devices, category rules for WORKGROUP devices and group rules for Azure AD devices).

Then configure which users are allowed to use self-service activation methods (where user is able to get temporary admin access by them selves) and on which devices this is possible. You can use groups (both on-premises AD and Azure AD) and single computers (all) to create the configuration. With on-premises AD you have also possibility to use users primary devices information from AD so that, for example, self-service is available on users' primary devices.

Example 3: Creating a managed local user account

If domain credentials (on-premises or Azure AD) cannot be used to log in (trust broken, AAD connection fails etc.) or IT support needs to connect using some remote administration tool (connect to $-shares, remote registry connection etc.), it's an good idea to create managed local user account to all devices that can be used in these cases. Create a managed user rule that will create (or start to manage, if the account already exists on the device) a new local user account (for example, named 'LocalAdmin') using the **Generate random password and save to database** option and then create another management rule that will add this local user account to the local Administrators group. Target these rules to all devices (use OU rules for on-premises AD devices, category rules for WORKGROUP devices and group rules for Azure AD devices).

When this managed local user account needs to be used, you can find the current password for desired device in your Privilege Manager Portal under **ServiceDesk** > **Retrieve**.