Configuration

Last Modified on 12/11/2021 11:30 am EET

After Carillon solution installation configuration rules for managing local group memberships and local user accounts need to be created. Management rules can be create for different locations providing you a way to target what devices rules are affecting. You can combine different rules to get desired configuration.

Management rule usage

- **Domain or organization unit rules**

  If you are using on-premises AD with Carillon, these rules will affect all devices where AD computer object is at or below target hierarchy level. Domain level rules affect all devices in whole domain where as OU level rules affect devices somewhere below the target OU. Use these rules to create base configuration (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 AD computer object will be placed to correct location.
- **Group rules**

  Group rules are available for both on-premises and Azure AD directories. Groups need to have devices as members and rule 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 Carillon Portal and then target rules to 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 will be created to 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 Administrators group on developers computer).

Example 1: Removing permanent admin permissions

Create management rules that specify members of local Administrators group. Combine different management rule targets (domain, OU, group, category and computer) to get desired configuration for each device. Carillon will enforce these rules by adding missing members and removing existing members that are no longer allowed to be in local Administrators group. If existing admin permissions are removed from user that still needs permanent, no worries, just add new computer management rule to add user back to local Administrators group. Remember to always create management rule for Built-In local administrator account (and don't worry, Carillon will use well known SID's to manage groups and users so you don't need to worry about different localized names) to local

Administrators group as Windows OS will not allow removing this account and Carillon removal attempt for this accounts Administrators group membership will fail.

Example 2: Providing temporary admin access

Create managed user rule that will create (or start to manage if account already exist on device) new local user account (for example named as TempAdmin) using option '**Generate temporary user account that can be activated**' and then create another management rule that will add this local user account to 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, for example so that self-service is available on users primary devices.

Example 3: Creating managed local user account

If domain credentials (on-premises or Azure AD) cannot be used to login (trust broken, AAD connection fails etc.) or IT support needs to connect using some remote administration tool (connect to $-shares, remote registry connection etc.), then it's an good idea to create managed local user account to all devices that can be used in these cases. Create managed user rule that will create (or start to manage if account already exist on device) new local user account (for example named as LocalAdmin) using option '**Generate random password and save to database**' and then create another management rule that will add this local user account to 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 need to be used, go to Carillon management portal and under **ServiceDesk\Retrieve** password to find current password for desired device.