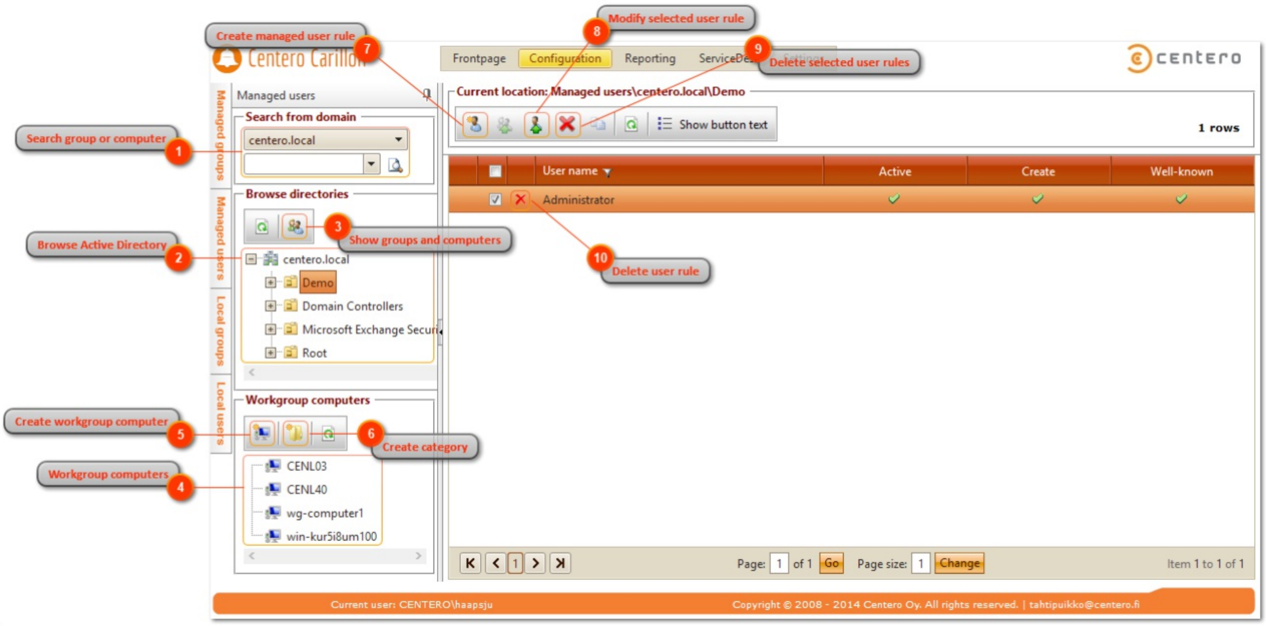
Managed users

Last Modified on 22/09/2020 11:32 am EEST



Managed users allows you to create rules that control local user accounts on target computer(s). Custom local users that you want to manage must be first created to Centero Carillon (see Create local user page) before rules that control the local account can be created. Built-in local users (for example Administrator) can be used in managed user rules immediately.

Managed user rules can be created to set local user account password to desired or to set local user account as Centero Carillon temporary account.

Management rules can be created to any management level using Active Directory existing objects or workgroup computers.

Rules can be created to four different management levels and are processed in this order:

1. Active Directory or workgroup computer account (highest priority)
2. Active Directory groups
3. Active Directory organizational units
4. Active Directory domain (lowest priority)

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

- Rule in domain management level specifies that local Administrator account password is reset. This rule will be applied to all Carillon Clients in this domain.
- Another rule in Active Directory organizational unit named 'Workstations' specifies that local user account TempAdmin will be set as Centero Carillon temporary account. This rule will be applied to all Carillon Clients that are in organizational unit 'Workstations' or in any it's sub organizational units

In this example Carillon Clients that belong to 'Workstations' organizational unit will have two user management rules, one that specifies local Administrator account password and another that set Centero Carillon temporary user account. Carillon Clients that do not belong to 'Workstations' organizational unit will have only one rule (from domain management level) and therefore only local Administrator account password is set but Centero Carillon temporary user account is not available.

Rule collections works quite like GPO's in 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 Active Directory search to manage rules linked to Active Directory groups or computers. See more information in 'Active Directory search' chapter.
2. Browse Active Directory

   Browse 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 Active Directory groups and computers can be also

   managed.
3. Show groups and computers

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

   Select workgroup computers to manage rules linked to workgroup computers.
5. Create workgroup computer

   Create new workgroup computer. See more information in 'Create workgroup computer' chapter.
6. Create category

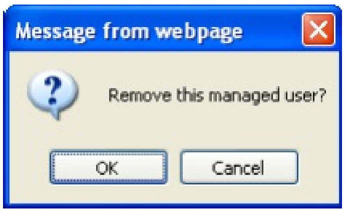
   Create a new category to organize local groups, local users and workgroup computers. See more information in 'Create category' chapter.
7. Create managed user rule

   Create new managed user rule. See more information in 'Create managed user rule' chapter.
8. Modify selected user rule

   Modify selected managed user rule. This is available only if managed user rule is selected. See more information in 'Modify managed user rule' chapter.
9. Delete selected user rules

   Delete selected managed user rules. This is available only if managed user rules are selected.
10. Delete user rule

    Delete managed user rule. You need to verify the delete action before managed user rule is deleted.



Message from webpage

Remove this managed user?

Click **OK** to delete managed user rule and Cancel to cancel the delete operation.