Managed Users Overview

Last Modified on 11.09.23

On the portal's **Managed Users** page you can create rules that control local user accounts on target computer(s). Custom local users that you want to manage must be first created in Recast Privilege Manager (see Create a Local User) 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 passwords as desired or to set local user account as Recast Privilege Manager temporary accounts.

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

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

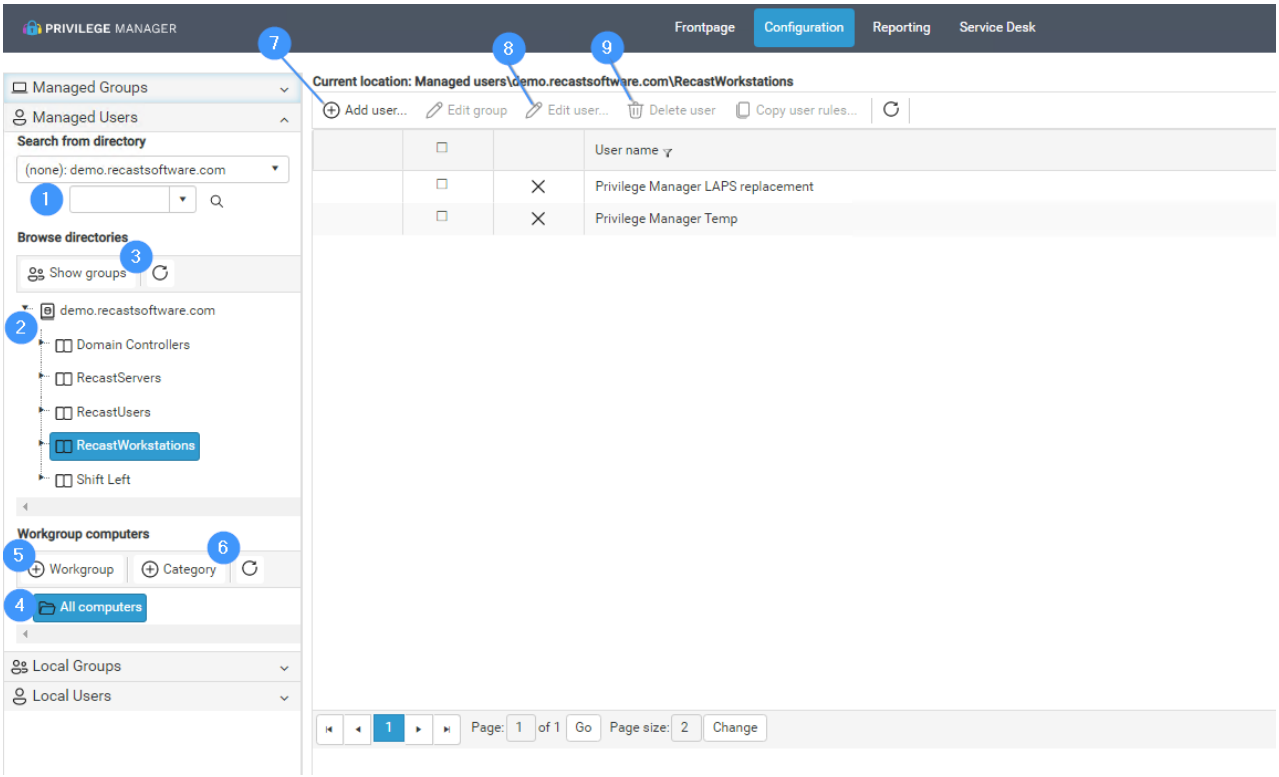
1. Active Directory or workgroup computer account (highest priority)
2. Active Directory groups
3. Active Directory organizational units
4. Active Directory domain (lowest priority)

Rules can be created for multiple levels and Recast Privilege Manager creates a collection of rules for the Privilege Manager Client when several rules are available for the Privilege Manager Client. Example of the 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 a Recast Privilege Manager temporary account. This rule will be applied to all Privilege Manager Clients that are in the organizational unit 'Workstations' or in any of its sub organizational units.

  In this example Privilege Manager Clients that belong to the 'Workstations' organizational unit will have two user management rules, one that specifies local Administrator account passwords and another that sets the Recast Privilege Manager temporary user account. Privilege Manager Clients that do not belong to the 'Workstations' organizational unit will have only one rule (from domain management level) and therefore only local Administrator account passwords are set but Recast Privilege Manager temporary user accounts are not available.

Rule collections works quite like GPOs in Active Directory. The main difference is that you can also use Active Directory groups and single computers as the 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 have 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. For more information, see Active Directory Search.

2. Browse Active Directory

   Browse Active Directory organizational units to manage rules linked to the Active Directory domain or organizational units. If **Show groups and computers** is selected then rules for Active Directory groups and computers can also

   be managed.

3. Show groups and computers

   Select if Active Directory groups and computer objects should be shown on the browse Active Directory tree view. By default, group and computer objects are not shown. If group and computer objects should be shown, page load times might slow down because larger amounts of nodes will appear in the tree view.

4. Workgroup computers

   Select workgroup computers to manage rules linked to workgroup computers.

5. Add Workgroup computer

   Create a new workgroup computer. See Create workgroup computer' chapter.

6. Add Category

   Create a new category to organize local groups, local users and workgroup computers. See Create a Category.

7. Add managed user rule

   Create a new managed user rule. See Create or Modify a Managed User Rule .

8. Modify selected user rule

   Modify selected managed user rule. This is available only if the managed user rule is selected. See Create or Modify

a Managed User Rule

9. Delete selected user rules

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