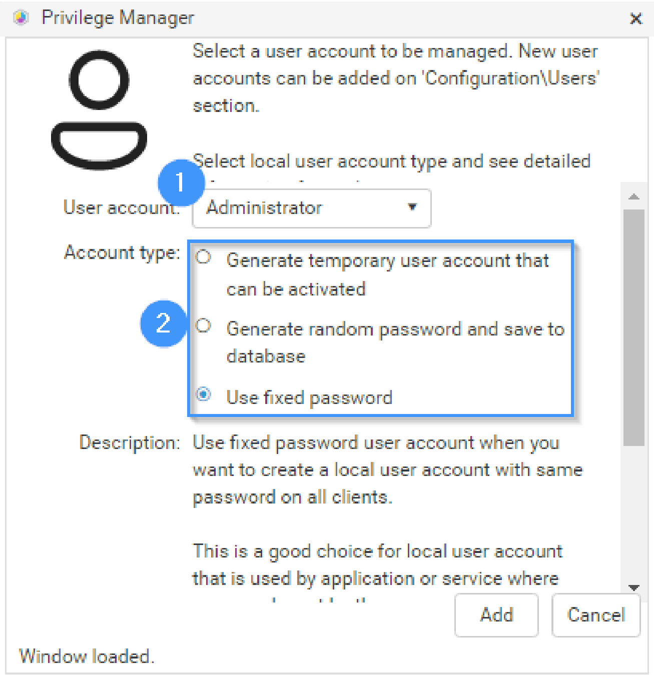
Create or Modify a Managed User Rule

Creating a new managed group rule allows you to add a specified member to a selected local group on a selected target.



Privilege Manager

Select a user account to be managed. New user accounts can be added on 'Configuration\Users' section.

Select local user account type and see detailed

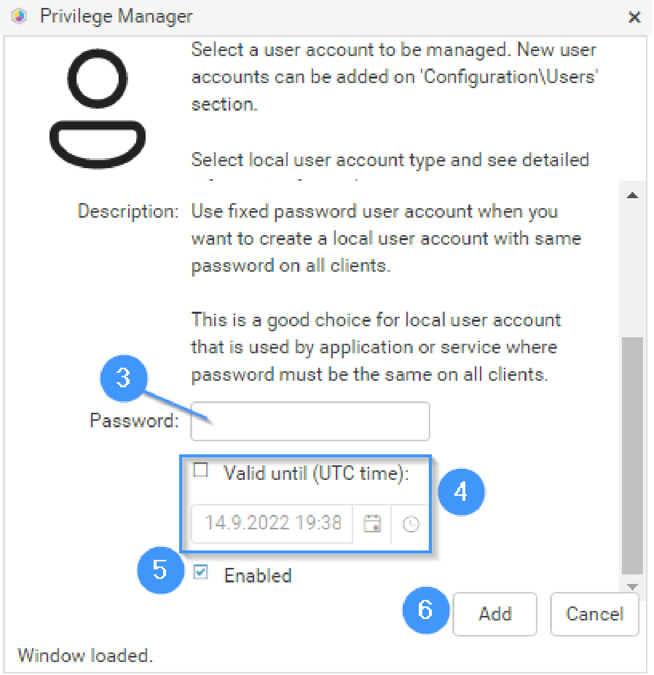
User account: Administrator

Account type:
○ Generate temporary user account that can be activated
○ Generate random password and save to database
● Use fixed password

Description: Use fixed password user account when you want to create a local user account with same password on all clients.

This is a good choice for local user account that is used by application or service where

Window loaded.



Privilege Manager

Select a user account to be managed. New user accounts can be added on 'Configuration\Users' section.

Select local user account type and see detailed

Description: Use fixed password user account when you want to create a local user account with same password on all clients.

This is a good choice for local user account that is used by application or service where password must be the same on all clients.

Password:

□ Valid until (UTC time): 14.9.2022 19:38

☑ Enabled

Window loaded.

1. Select the local **User account** to manage. Local user accounts must be first created before management rules can be defined for the local user. For more information, see Create a Local User.
2. Select an **Account type** for this rule.
   - **Generate temporary user account that can be activated** will create local user account as a Recast Privilege Manager temporary user account.
   - **Generate random password and save to database** will create unique random password to the local user account and save the password information to the Recast Privilege Manager database where the specified

user can retrieve the passwords.

    - **Use fixed password** will reset local user account password to one specified on rule.

3. If **Use fixed password** is selected, enter a **Password** for the local user account on target computer(s). The password will be shown on screen!
4. Add an option to manage a user rule for a specified time and set the expiry time. The maximum validity time is specified by the Recast Privilege Manager Administrator.

   This field is available only if enabled by the Recast Privilege Manager administrator. See more information in the **Recast Privilege Manager Administration Guide**.
5. Enable or disable the managed user group rule. When the rule is enabled, it will be applied to target computer(s).
6. Click **Add**.