ESET Tech Center

Create a permission set in ESET PROTECT (8.0)

Steef | ESET Nederland - 2023-09-14 - Reacties (0) - Legacy

Issue

- You want to create permissions to allow users to view, use and edit objects, tasks and licenses in ESET PROTECT
- In the example below, we create a permission set for a small office scenario to allow all users to access all tasks and objects except for server settings. You can customize this example to create more specific permission sets according to your needs

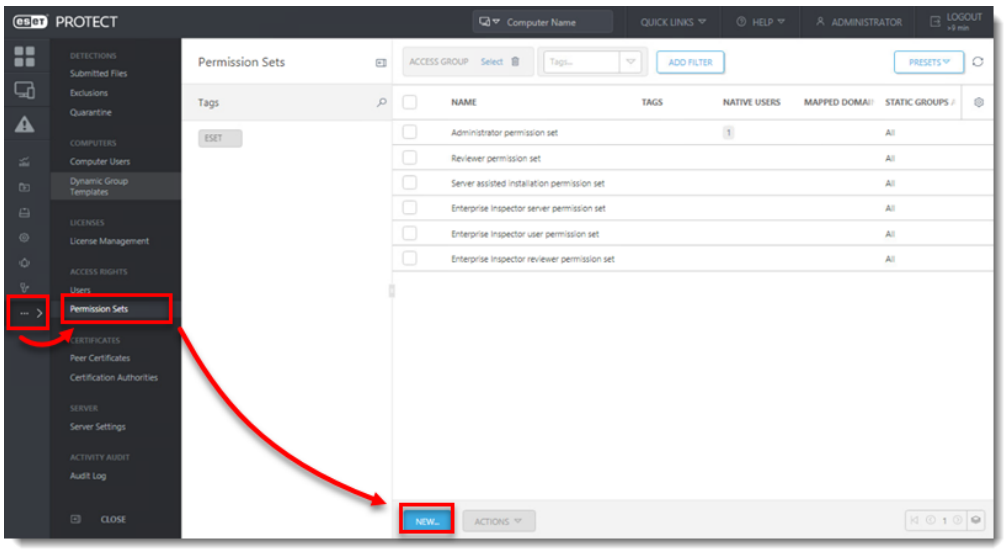
Details

Permissions are an important part of Access Rights in ESET PROTECT. A permission set defines the objects and tasks a user can access in ESET PROTECT Web Console. Native users have their own permissions while domain users inherit permissions from their mapped security group.

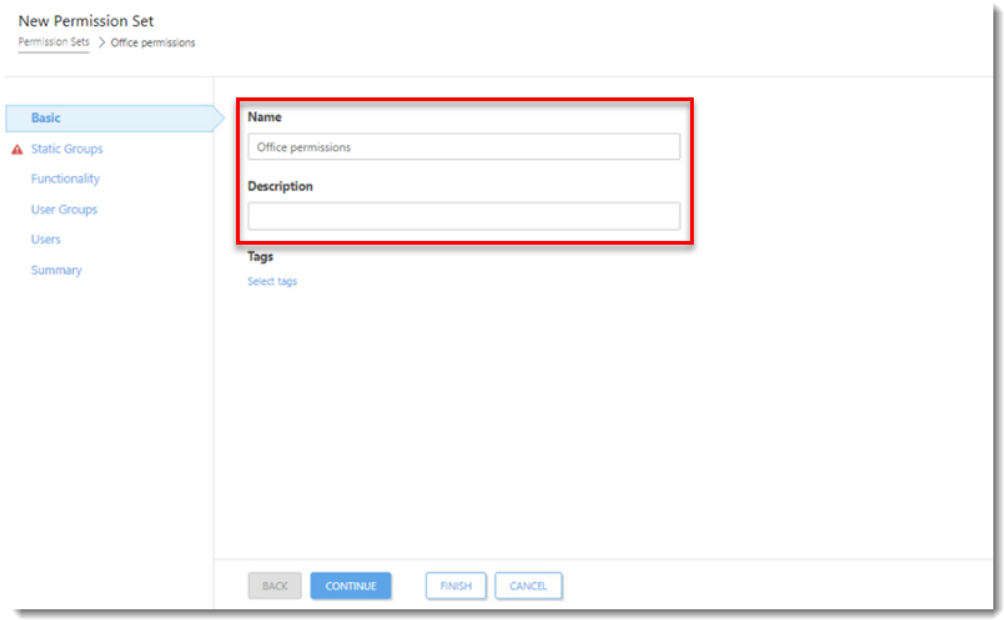
When you create a permission set, it is associated with a home group. The home group is a static group that includes the objects, tasks and users that the permissions set will apply to. When you create a new permission set, the permissions you select in the **Functionality** section will apply to all objects in each Static Group that you select for that permission set. Users that have access to a Static Group also have access to all subgroups of that Static Group.

Solution

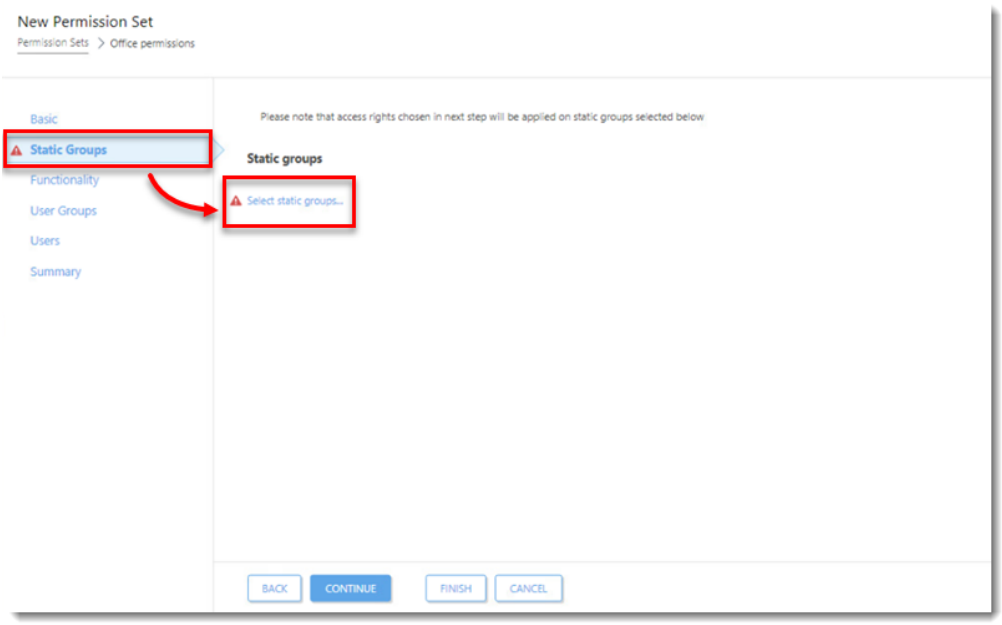
1. Open ESET PROTECT Web Console in your web browser and log in.
2. Click **More** → **Permission Sets** → **New**.



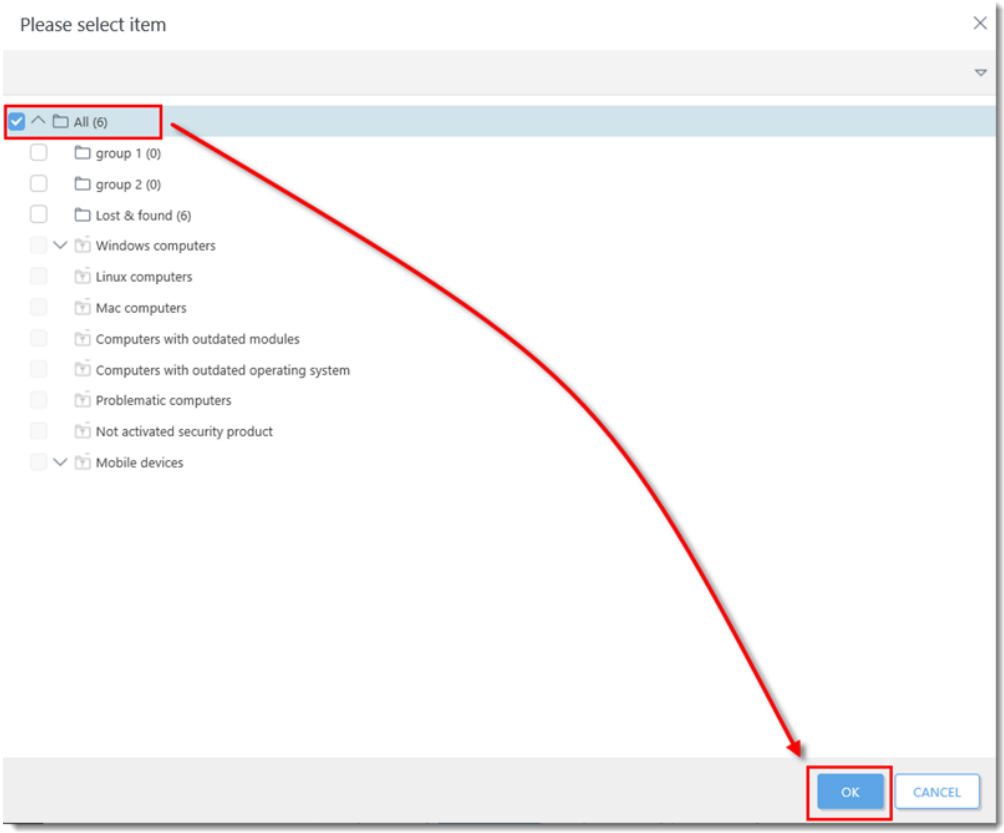
3. Next to **Name**, type a name for your new permission set; the **Description** field is optional.



4. Click **Static Groups → Select static group(s)**.

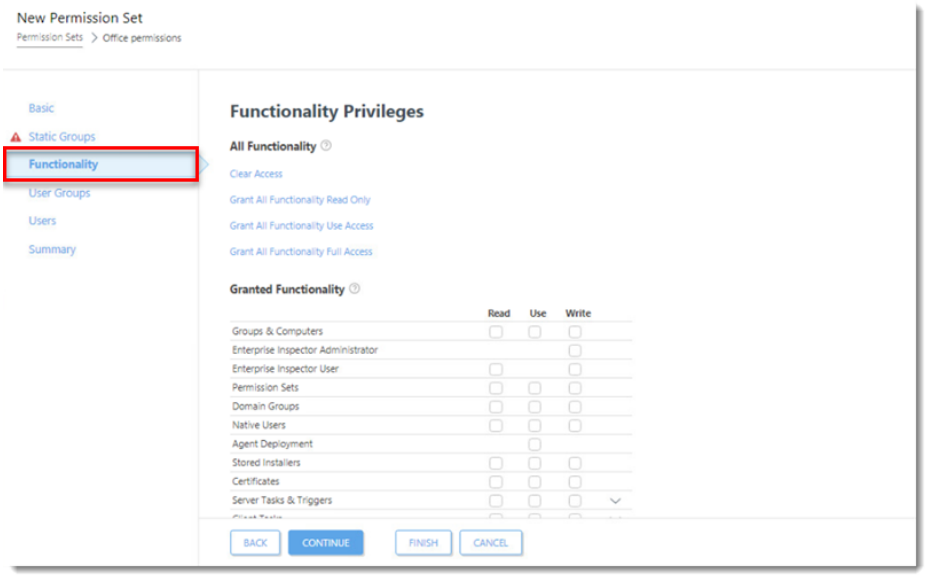


5. Select the check box next to each static group this permission set will apply to. In this example, we have selected the Static Group **All** to apply this permission set to all users. Click **OK** when you are finished.



6. Click **Functionality** to view a table of objects and tasks. Select the check box next to each object and task to define the permissions:
    1. **Read**: Users can view, but cannot carry out the task or assign tasks to an object. Users cannot edit the task or object.
    2. **Use**: Users can carry out a task or assign tasks to the object, but cannot edit the task or object.

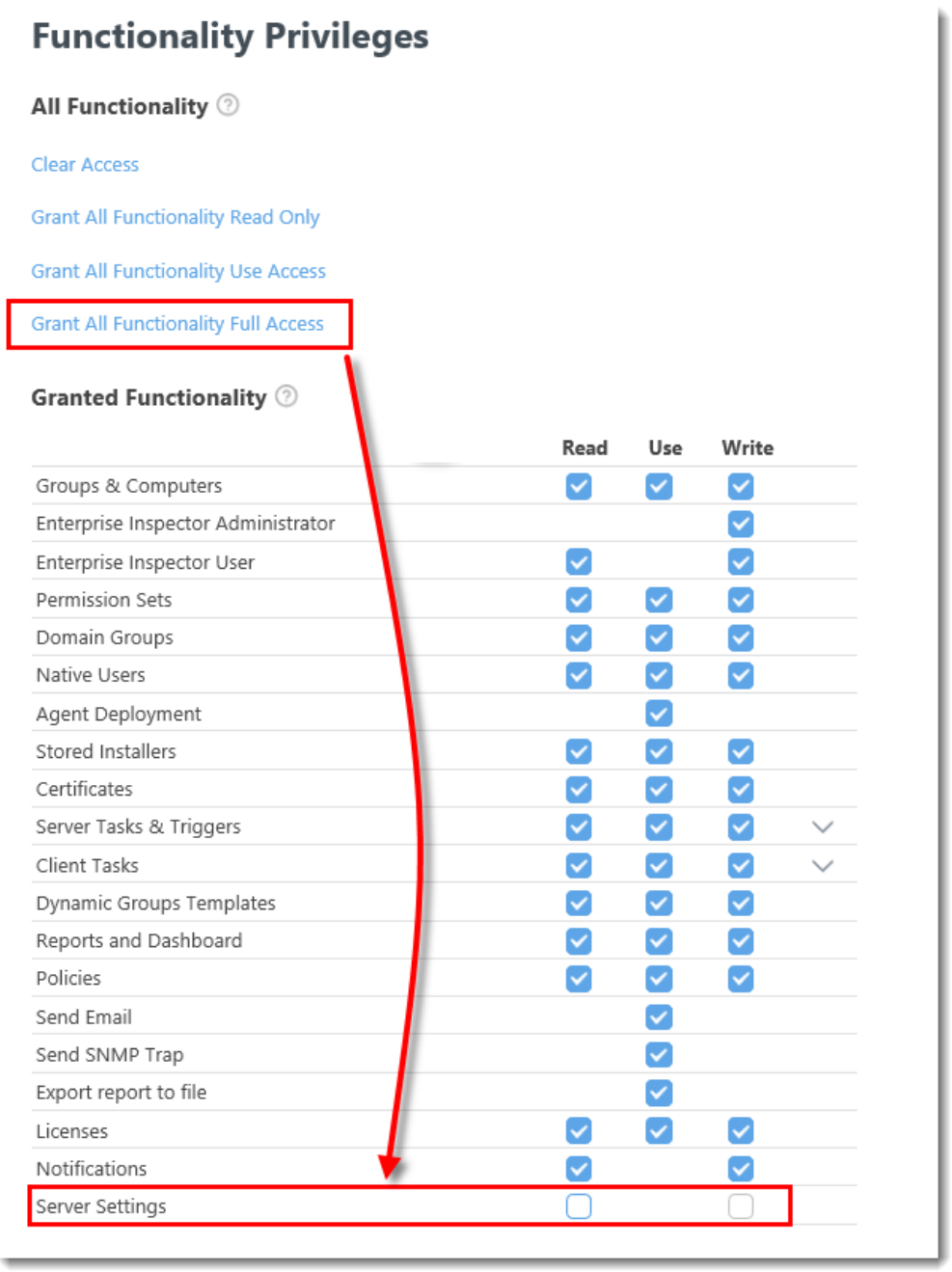
3. **Write**: Users can read, use and make changes to the task or object.



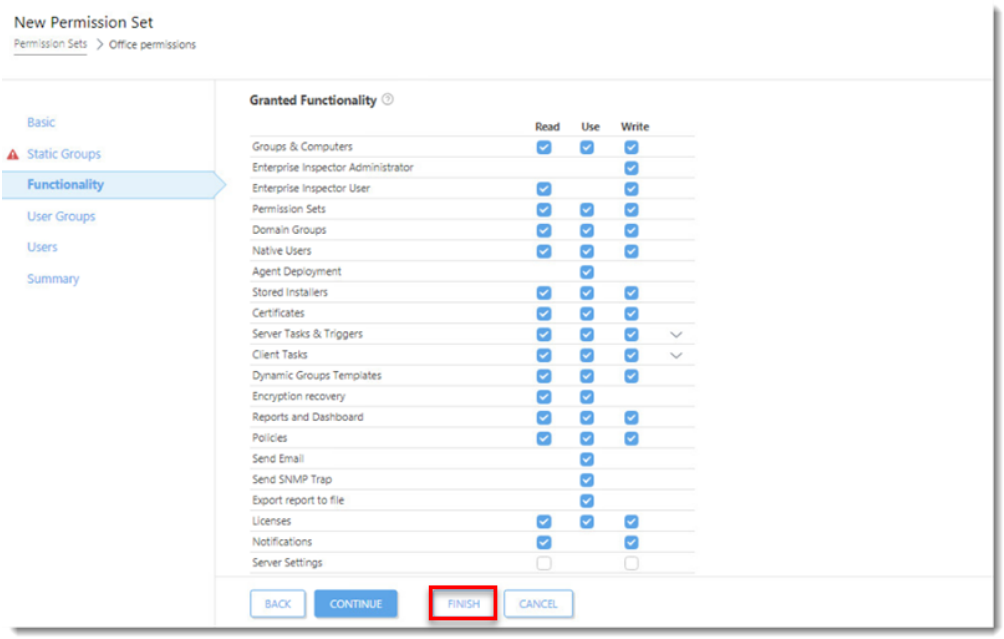
7. In this example, click **Grant All Functionality Full Access**. Deselect the check box next to tasks and objects you do not want to allow permissions for. In this example, **Server Settings** permissions are not allowed.

   Allowing full permissions for all tasks and objects except for server settings will allow all users to perform all necessary actions without the risk of accidental changes to core system settings.

   You can create more restrictive permissions sets and apply them to specific groups to customize the permissions structure to your company environment.



8. The **User Groups** and **Users** sections can apply permissions to specific user groups or individual users. Skip these sections if you are not creating permissions sets customized by the user.
9. Click **Finish** to save your changes.


New Permission Set
Permission Sets > Office permissions
Basic
Static Groups
Functionality
User Groups
Users
Summary
Granted Functionality
Read
Use
Write
Groups & Computers
Enterprise Inspector Administrator
Enterprise Inspector User
Permission Sets
Domain Groups
Native Users
Agent Deployment
Stored Installers
Certificates
Server Tasks & Triggers
Client Tasks
Dynamic Groups Templates
Encryption recovery
Reports and Dashboard
Policies
Send Email
Send SNMP Trap
Export report to file
Licenses
Notifications
Server Settings
BACK
CONTINUE
FINISH
CANCEL