ESET Tech Center

How do I create or edit permission sets in ESET Remote Administrator Web Console? (6.x)

https://support.eset.com/kb3624

Issue

Create permissions for users to view, use and edit objects, tasks and licenses in ESET Remote Administrator. Permissions are an important part of Access Rights in ESET Remote Administrator.

In this example, we will create a permission set for a small office scenario where all users can access all tasks and objects except for server settings. You can make changes to this example to create more specific permission sets according to your needs.

Details

Solution

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in. [Open ERA Web Console](#).

2. Click **Admin** ☒ → **Access Rights** → **Permission Sets** → **New**.

    Figure 1-1

    Click the image to view larger in new window

3. Type a name for your new permission set, the **Description** field is optional.

4. Expand **Static Groups** and click **Add Static Group**.

Figure 1-2

Click the image to view larger in new window

5. Select the check box next to each static group this permission set will apply to.

   We have selected the **All** Static Group in this example, to apply these permissions for all users. Click **OK** when you are finished.

Figure 1-3

Click the image to view larger in new window

6. Expand **Functionality** to view a table of objects and tasks. Use the check boxes next to each object and task to define permissions:

   Read: Users can view, but cannot carry out the task or assign tasks to an object. Users cannot edit the task or object.

   Use: Users can carry out a task or assign tasks to the object, but cannot edit the task or object.

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

Figure 1-4

Click the image to view larger in new window

7. In this example, click **Grant All Functionality Full Access**. Deselect the check boxes next to tasks and objects for which you do not want to allow permissions. In this example, **Server Settings** 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 tructure to your company environment.

Figure 1-5

8. The **User Groups** and **Users** sections can be used to apply permissions to specific user groups or individual users. Skip these sections if you are not creating permissions sets customized by user.

9. Click **Finish** to save your changes.

Figure 1-6

Tags
ERA 6.x