ESET Tech Center

Create a permission set in ESET Security Management Center (7.x)

Anish | ESET Nederland - 2018-09-14 - Comments (0) - ESET Security Management Center

Issue

- Create permissions to allow users to view, use and edit objects, tasks and licenses in ESET Security Management Center. Permissions are an important part of Access Rights in ESET Security Management Center.

- In this example, we will 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

Solution

1. Open ESET Security Management Web Console (ESMC Web Console) in your web browser and log in.
2. Click **More** → **Access Rights** → **Permission Sets** → **New**.

Figure 1-1

Click the image to view larger in new window

1. Type a name for your new permission set; the **Description** field is optional.
2. Click **Static Groups** → **Add Static Groups**.

Figure 1-2

Click the image to view larger in new window

1. 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.

Figure 1-3

Click the image to view larger in new window

1. Click **Functionality** to view a table of objects and tasks. Select the check boxes next to each object and task to define the 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

1. 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

1. 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.

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

Figure 1-6
Click the image to view larger in new window

KB Solution ID: KB6770 |Document ID: 25577|Last Revised: August 16, 2018