ESET Tech Center

Knowledgebase > Legacy > Create a permission set in ESET PROTECT (8.0)

Create a permission set in ESET PROTECT (8.0)

Steef | ESET Nederland - 2023-09-14 - Comments (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. <u>Native</u> <u>users</u> have their own permissions while domain users inherit permissions from their <u>mapped</u> <u>security group</u>.

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 <u>Static Group</u> 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 \rightarrow Permission Sets \rightarrow New.

eser	PROTECT				Gr⊽ Comp	uter Name	QUICK LINKS 🗢	③ HELP ▼	A ADMINIST	ATOR 🗄 🔐	IGOUT min
		Permission Sets	•	ACCESS	GROUP Select 🗊	Tags	ADD FILTE	R		PRESETS **	0
G	Exclusions Quarantine	Tags	,p		NAME		TAGS	NATIVE USERS	MAPPED DOMAIN	STATIC GROUPS /	٥
A		ESET			Administrator permiss	ion set		1		All	
					Reviewer permission s	et				All	
De	Dynamic Group Templates				Server assisted installa	tion permission set				All	
a					Enterprise Inspector se	erver permission set				All	
0					Enterprise Inspector u	ser permission set				AI	
Ĩ.	Ucerse Management				Enterprise Inspector re	viewer permission se	e			Al	
Č.											
Ŷ	Users										
>	Permission Sets										
	CERTIFICATES										
	Server Settings										
				NEW.	ACTIONS 🔝					K @ 1 @	9

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

lew Permission Set		
Basic	Name	
Static Groups	Office permissions	
Functionality	Description	
Jser Groups		
Users		
Summary	lags Select taos	

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

New Permission Set	s
Basic Static Groups	Please note that access rights chosen in next step will be applied on static groups selected below Static groups
Functionality User Groups	Select static groups
Users Summary	
	BACK CONTINUE FINISH CANCEL

 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.

Basic	Functionality Privileg	es			
Static Groups	All Functionality ③				
unctionality	Case Acres				
Jser Groups	Cond All Exactions The Read Only				
leare	Grant All Punctionality Read Only				
73615	Grant All Functionality Use Access				
Summary	Grant All Functionality Full Access				
	Granted Eurotionality				
	Granted Functionality ③	Read	Use	Write	
	Granted Functionality ③ Groups & Computers Enterprise Inspector Administrator	Read	Use	Write	
	Granted Functionality Groups & Computers Enterprise Inspector Administrator Enterprise Inspector User	Read	Use	Write	
	Granted Functionality ③ Groups & Computers Enterprise Inspector Administrator Enterprise Inspector User Permission Sets	Read	Use	Write	
	Granted Functionality ③ Groups & Computers Enterprise Inspector Administrator Enterprise Inspector User Permission Sets Domain Groups	Read		Write	
	Granted Functionality ③ Groups & Computers Enterprise Inspector Administrator Enterprise Inspector User Permission Sets Domain Groups Native Users	Read		Write	
	Granted Functionality ③ Groups & Computers Enterprise Inspector Administrator Enterprise Inspector User Permission Sets Domain Groups Nature Users Agent Deployment	Read		Write	
	Granted Functionality ③ Groups & Computers Enterprise Inspector Administrator Enterprise Inspector User Permission Sets Domain Groups Native Users Agent Deployment Stored Installers	Read		Write	
	Granted Functionality ③ Groups & Computers Enterprise Inspector Administrator Enterprise Inspector User Permission Sets Domain Groups Native Users Agent Depiopment Stored Installers Certificates			Write	

 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.

Functionality Privileges

All Functionality 🕐

Clear Access

Grant All Functionality Read Only

Grant All Functionality Use Access

Grant All Functionality Full Access

oranica ranctionanty 🕖	_			
	Read	Use	Write	
Groups & Computers				
Enterprise Inspector Administrator			\checkmark	
Enterprise Inspector User				
Permission Sets		\checkmark		
Domain Groups		\checkmark		
Native Users		\checkmark		
Agent Deployment		\checkmark		
Stored Installers	\checkmark	\checkmark	\checkmark	
Certificates	\checkmark	\checkmark		
Server Tasks & Triggers	Sector 10	 Image: A set of the set of the		\sim
Client Tasks	\checkmark		\checkmark	\sim
Dynamic Groups Templates	\checkmark	\checkmark	\checkmark	
Reports and Dashboard	Sector 10	 Image: A set of the set of the		
Policies	Sector 10	\checkmark		
Send Email		 Image: A set of the set of the		
Send SNMP Trap		\checkmark		
Export report to file		 Image: A set of the set of the		
Licenses		\checkmark		
Notifications				
Server Settings	\square		\square	

- 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

	Granted Functionality ③				
Basic		Read	Use	Write	
A Static Groups	Groups & Computers	~			
- same croops	Enterprise Inspector Administrator				
Functionality	Enterprise Inspector User				
User Groups	Permission Sets		~		
0.000	Domain Groups				
Users	Native Users		~		
Summary	Agent Deployment		 Image: A set of the set of the		
Samuely	Stored Installers		 Image: A set of the set of the		
	Certificates		 	 Image: A set of the set of the	
	Server Tasks & Triggers		~	~	\sim
	Client Tasks		~		\sim
	Dynamic Groups Templates		~		
	Encryption recovery		 Image: A set of the set of the		
	Reports and Dashboard		 Image: A set of the set of the		
	Policies				
	Send Email		~		
	Send SNMP Trap		~		
	Export report to file		 		
	Licenses		~		
	Notifications				
	Server Settings				
	BACK CONTINUE FINIS	CANCEL			