# Create or edit firewall rules for client workstations in ESET Security Management Center (7.x)

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

## Issue

- Create, edit, or delete a firewall rules for client workstations running ESET Endpoint Security

## Solution

**Endpoint users:** Perform these steps on individual client workstations

### ESET Security Management Center (ESMC) 7 User Permissions

This article assumes that your ESMC user has the correct access rights and permissions to perform the tasks below.

If you are still using the default Administrator user, or you are unable to perform the tasks below (the option is grayed out), see the following article to create a second administrator user with all access rights (you only need to do this once):

- Create a second administrator user in ESET Security Management Center 7.x

View permissions needed for least privilege user access

1. Open ESET Security Management Center Web Console (ESMC Web Console) in your web browser and log in.
2. Click **Policies**, select the policy that you want to edit and then click **Policies → Edit**.

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

1. To apply a rule, click **Settings → Network Protection → Firewall → Advanced** and click **Edit** next to **Rules**.

**Figure 1-2**
**Click the image to view larger in new window**

1. Click **Add** and set the parameters for your rule in the **General**, **Local**, and **Remote** tabs.

### Editing and removing rules

**To edit a rule**: Select the rule you want to modify and click **Edit**.
**To remove a rule**: Select the rule you want to remove and click **Remove**.

**Figure 1-3**

1. Set any combination of the following parameters in the **General** tab to define your new rule:
    - 
    - Type a name for your rule into the **Name** field.
    - Select **Both**, **In** or **Out** from the **Direction** drop-down menu.
    - Select **Allow**, **Deny** or **Ask** from the **Action** drop-down menu.
    - The **Protocol** and **Profile** settings are not mandatory, but can be used to more precisely target a rule.
    - Select the **Logging severity** and check box next to **Notify user** to have ESET Security Management Center automatically perform these actions when the rule is triggered.

**Figure 1-4**

1. Set any combination of the following parameters in the **Local** tab:
    - 
    - **Port**: specify a port or range of ports this rule will target. Multiple entries must be delimited by a comma, or you can specify a range of ports, for example 1000-2000.
    - **IP**: specify an IP address or range this rule will target.
    - **Zones**: click **Add** to specify zones where this rule will apply.
    - **Application**: to target a specific application, type the .exe file for the application into this field.
    - **Service**: to target a specific service, type the name of the service into this field.

**Figure 1-5**

1. Set any combination of the following parameters in the **Remote** tab:
    - 
    - **Port**: specify a port or range of ports this rule will target. Multiple entries must be delimited by a comma, or you can specify a range of ports, for example 1000-2000.
    - **IP**: specify an IP address or range this rule will target.
    - **Zones**: click **Add** to specify zones where this rule will apply.

**Figure 1-6**

1. When you are finished making changes to rule parameters, click **OK**. Your new rule will appear in the **Firewall rules** window. Click **OK** again to close the **Firewall rules** window.

**Figure 1-7**

1. Click **Finish**. Client workstations will receive your new rule the next time that they check in to ESET Security Management Center.

---

KB Solution ID: KB6802 |Document ID: 25662|Last Revised: August 21, 2018