

ESET Tech Center

Kennisbank > Endpoint Solutions > Create or edit firewall rules for client workstations in ESET PROTECT (8.x-9.x)

Create or edit firewall rules for client workstations in ESET PROTECT (8.x-9.x)

Lesley | ESET Nederland - 2025-03-06 - Reacties (0) - Endpoint Solutions

Issue

Required user permissions

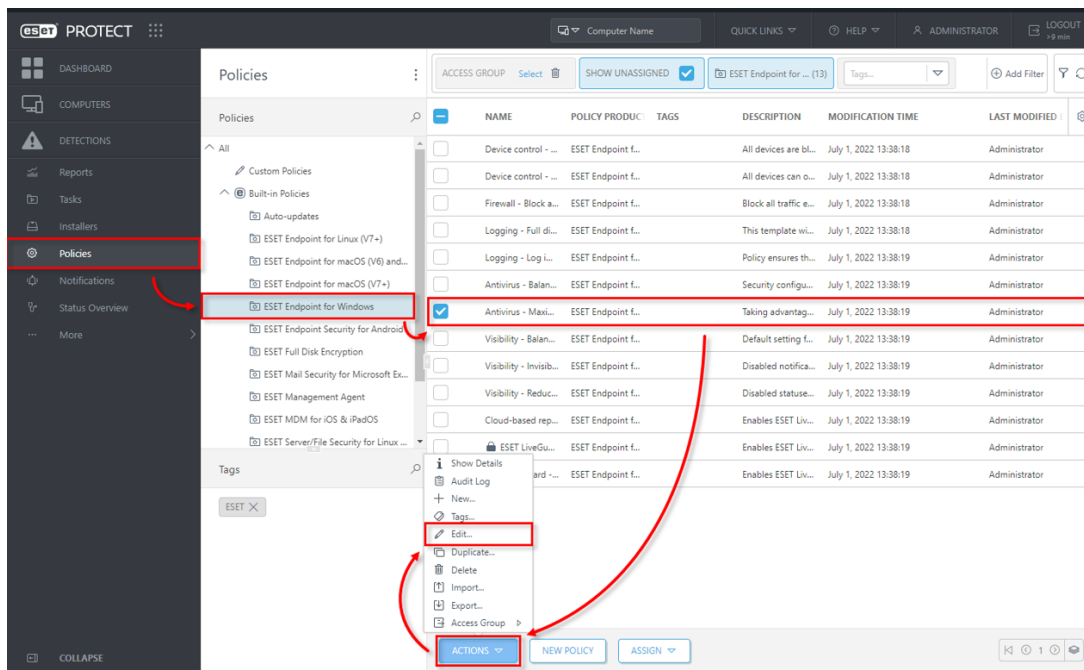
This article assumes that you have the appropriate [access rights and permissions](#) to perform the tasks below.

If you use the default Administrator user or are unable to perform the tasks below (the option is unavailable), create a second administrator user with all access rights.

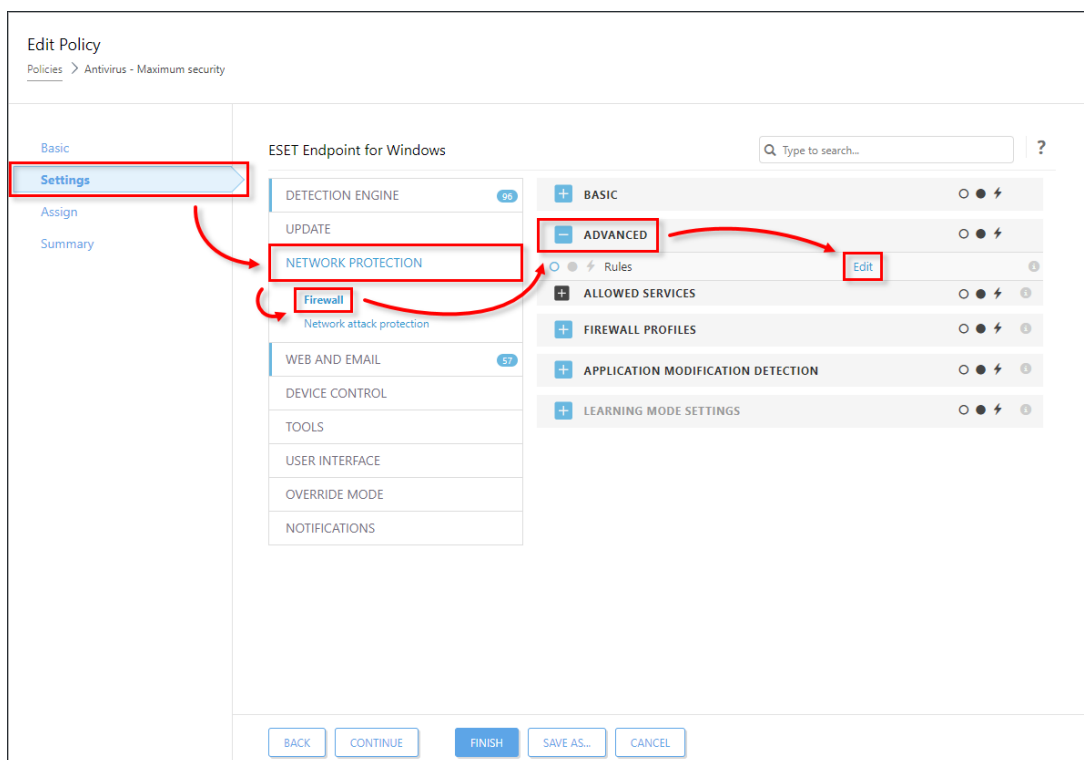
- **ESET PROTECT users:** [Create a second administrator user in ESET PROTECT](#)
- **ESET Security Management Center (ESMC) users:** [Create a second administrator user in ESET Security Management Center 7.x](#)
- Create, edit, or delete firewall rules for client workstations running ESET Endpoint Security via ESET PROTECT

Solution

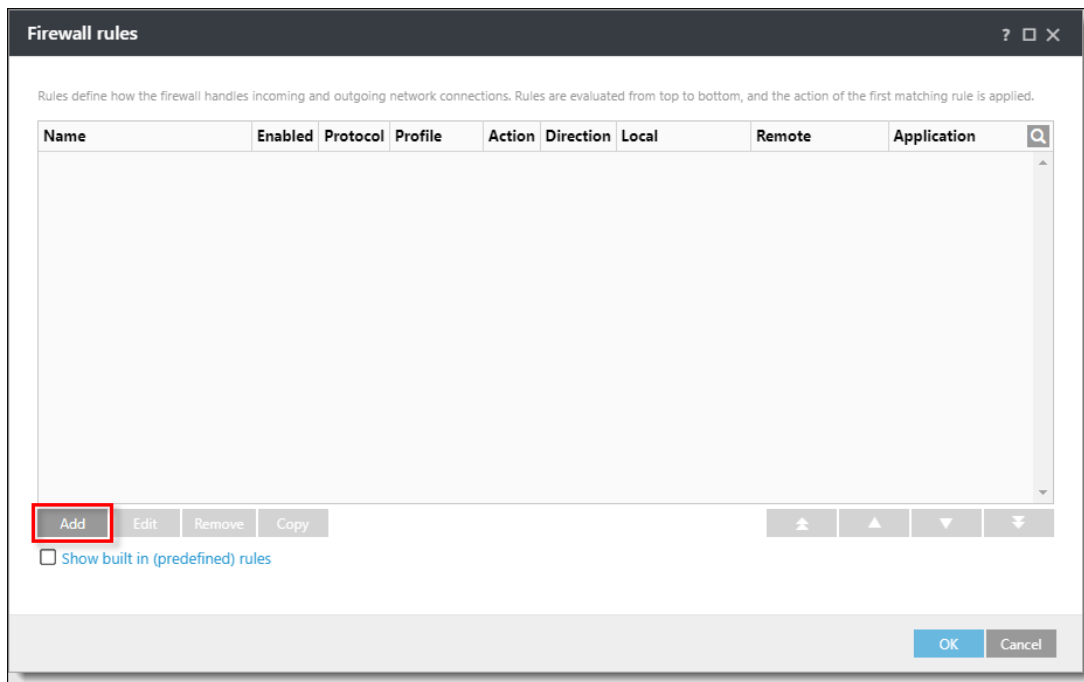
1. [Open the ESET PROTECT Web Console](#) in your web browser and log in.
2. Click **Policies**, select the desired **Built-in policy**, select the check box next to the policy that you want to edit and click **Policies** → **Edit**.



3. **Settings** → **Network Protection** → **Firewall** and expand **Advanced**. Click **Edit** next to **Rules**.



4. Click **Add**. 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**.



5. 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 target a rule more precisely.
- Select the **Logging severity** if needed.
- Click the slider bar next to **Notify user** to have ESET PROTECT automatically perform these actions when the rule is triggered.

Add rule

General Local Remote

Name: Stop PUA

Enabled: ☒

Direction: In

Action: Deny

Protocol: TCP & UDP

ICMP Type/Code: 0

Profile: Any profile

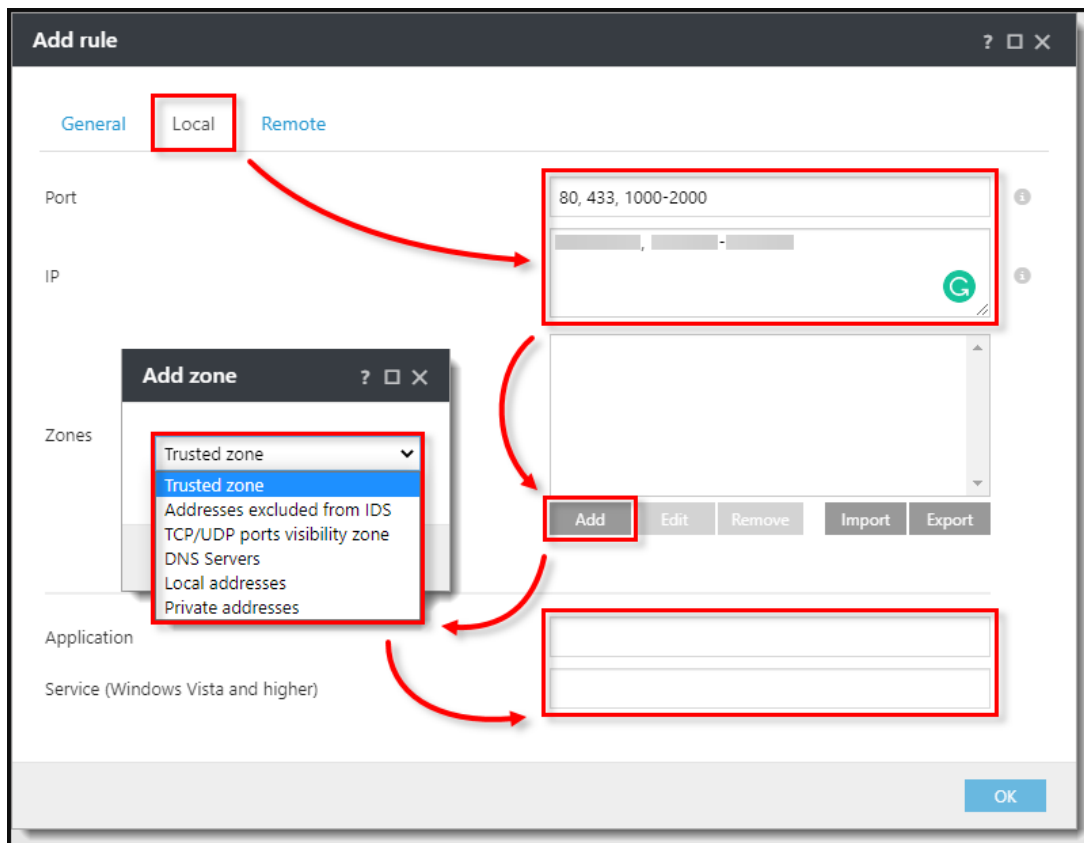
Logging severity: None

Notify user: ☐

OK

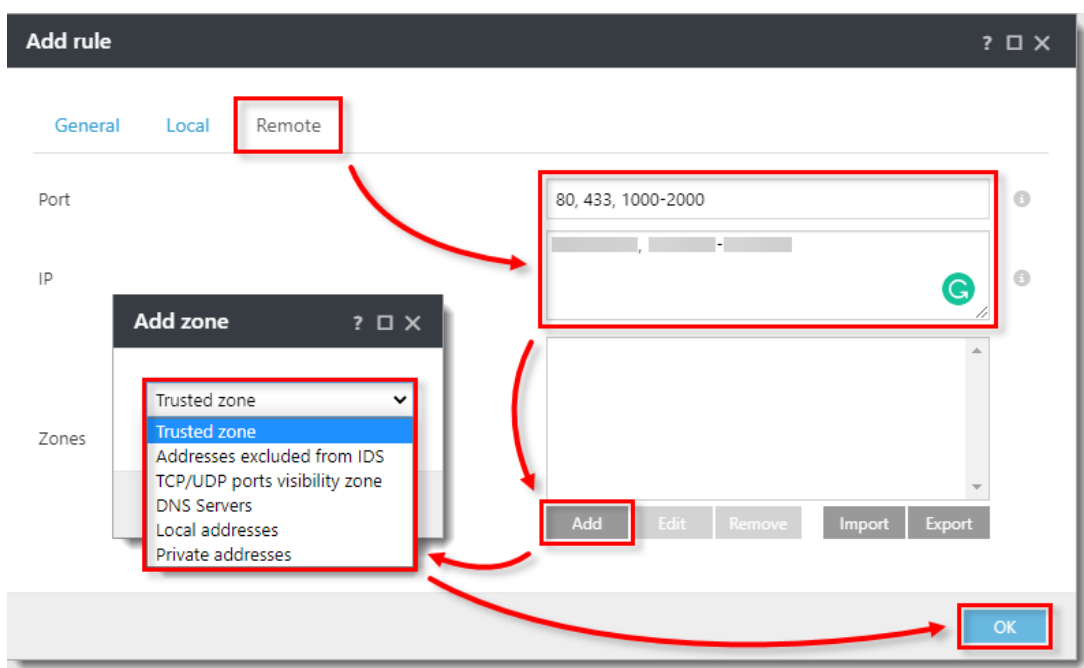
6. Click **Local**. Set any combination of the following parameters in the **Local** tab:

- **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** and select a zone from a drp-down menu to [specify the 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.

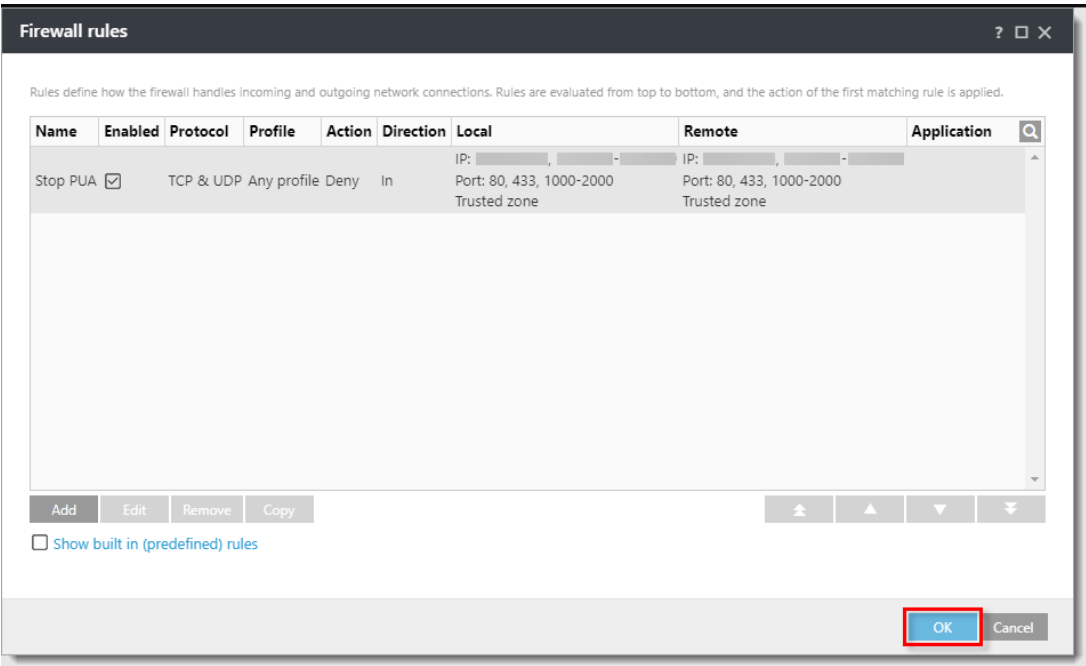


7. Click **Remote**. Set any combination of the following parameters in the **Remote** tab. When you are finished making changes to rule parameters, click **OK**.

- **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** and select a zone from a drop-down menu to [specify the zones where this rule will apply](#).



8. Your new rule will appear in the **Firewall rules** window. Click **OK** to close the **Firewall rules** window



9. Click **Finish**. Client workstations will receive your new rule the next time that they check in to ESET PROTECT.