

How do I create or edit firewall rules for client workstations in ESET Remote Administrator? (6.x)

Ondersteuning | ESET Nederland - 2025-03-07 - [Comments \(0\)](#) - [6.x](#)

<https://support.eset.com/kb3718>

Issue

Create, edit, or delete a firewall rule for client workstations running ESET Endpoint Security
Create, edit, or delete firewall rules on individual client workstations

Solution

If you do not use ESET Remote Administrator to manage your network

[Perform these steps on individual client workstations.](#)

Create or edit firewall rules in ESET Remote Administrator

Permissions changes in ESET Remote administrator 6.5 and later

Before proceeding, please note important changes to user access rights and permissions in the latest versions of ESET Remote Administrator.

[View Permissions Changes](#)

[View permissions](#)

Once these permissions are in place, follow the steps below.


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

3. To apply a rule Expand **Settings** → **Personal Firewall** → **Advanced** and click **Edit** next to **Rules**.



Figure 1-2

Click the image to view larger in new window

4. 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

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 more precisely target a rule.
 - Select the check box next to **Log** and/or **Notify user** to have ESET Remote Administrator automatically perform these

actions when the rule is triggered.



Figure 1-4

6. 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

7. 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

8. 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

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

Edit firewall rules on individual client workstations

1. Open ESET Endpoint Security. [Open my ESET product](#).
2. Press the **F5** key to access Advanced setup. Click **Firewall** and then click **Edit** next to **Rules**.



Figure 2-1

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



Figure 2-2

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**.

4. 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.
 - Use the **Logging severity** drop-down menu to set your preference for the types of events to log. Select **None** to record no logs when this rule is triggered. **Diagnostic** will log all events. **Information** will log notifications about updates. **Warning** will log warning notifications not related to system errors.
 - Select the check box next to **Notify user** to have ESET Endpoint Security display a notification when the rule is

triggered.



Figure 2-3

5. Set 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](#).
 - To target a specific application with your rule, click browse (...) under **Application**, navigate to the .exe file for the target application and then click **Open**.
 - To target a specific service with your rule, use the **Service** drop-down menu to select the target services from services running on your computer.



Figure 2-4

6. Set the following parameters in the **Remote** tab:
 - **Port:** specify a port 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 2-5

7. 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 2-6

8. Click **OK** to save your changes and exit Advanced setup. Client workstations will receive your new rule the next time they check in to ESET Remote Administrator.

- Tags
- [Endpoint](#)
- [ERA 6.x](#)