How do I create a rule to allow or deny a connection to/from a remote IP address in ESET Endpoint Security? (5.x)

Ondersteuning | ESET Nederland - 2025-03-07 - Comments (0) - 5.x

https://support.eset.com/kb3567

Issue

You are unable to connect to (or from) another computer or device, such as a printer on your network, because it is outside the trusted range of IP addresses defined on the computer you are trying to connect from
You want to add IP addresses or IP ranges of certain computers/devices to the trusted list in your ESET product
You want to deny access to a suspicious IP address

Details

Solution

A new version has been released

Version 6 of ESET Remote Administrator (ERA) and ESET business products were released in North America December 11th, 2014, and globally February 25th, 2015. This article applies to version 5.x and earlier ESET business products. For information about what's new in the latest version and how to upgrade, see the following article:

What's new in ESET version 6 business products?

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

Perform these steps on individual client workstations.

In ESET Remote Administrator

1. Open the ESET Remote Administrator Console (ERAC) by clicking **Start → All Programs → ESET → ESET Remote Administrator Console → ESET Remote Administrator Console**, or by double-clicking the ERAC icon on your desktop.
2. Click **Tools → Policy Manager**.
3. Select the policy for clients on which you want to create your IP exception and click **Edit Policy**.



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

4. Expand **Windows desktop v5 → Personal firewall → Settings** and click **Filtering mode**.
5. Select **Automatic mode with exceptions** from the **Value** drop-down menu**.**



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

6. Click **Rule setup → Edit**.



Figure 1-3
Click the image to view larger in new window

7. Click the **Zones** tab, select the trusted zone on which you want to create the new exception and then click **Edit**.



Figure 1-4

8. Click **Add IPv4 address**. Select **Single address**, **Address range** or **Subnet** depeding on your needs, type the IP address, range, or subnet for which you want to create an exclusion into the **Address** field and then click **OK**.



Figure 1-5
Click the image to view larger in new window

9. Click **OK** → **OK** to exit the **Zone setup** and **Zone and rule setup** windows.
10. Click **Console** → **Yes** to save your changes. Client workstations will receive the new rule the next time that they check into ESET Remote Administrator.

On an individual client workstation

1. Open ESET Endpoint Security. How do I open my ESET product?
2. Click **Setup** → **Network**.



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

3. Click **Switch to automatic filtering mode with exceptions**.



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

4. Click **Configure rules and zones**.



Figure 2-3
Click the image to view larger in new window

5. Click **New**.



Figure 2-4

6. Type a name for the rule into the **Name** field, select **Both** from the **Direction** drop-down menu and then select **Allow** or **Deny** from the **Action** drop-down menu, depending on whether or not you want to block or allow this specific IP address.



Figure 2-5

7. Click the **Remote** tab and click **Add IPv4 address**. In the **Remote IP address** window, enter the IP address, range or subnet that you would like to allow or deny.



Figure 2-6

8. Click **OK → OK → OK** to save your changes.

- Tags
- ERA 5.x