

# Use ESET Remote Administrator to configure an ESET Endpoint Security deployment to prevent loss of network connectivity (6.x)

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

<https://support.eset.com/kb5847>

## Issue


---

Prevent loss of internet connectivity on client computers due to firewall settings when deploying ESET Endpoint Security

## Solution

---

### I. Edit Firewall rules in ESET Remote Administrator

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in. [How do I open ERA Web Console?](#)
2. Click **Admin**  → **Policies** → **New Policy**.
3. In the **Basic** section, type in a **Name** and an optional **Description**.



**Figure 1-1**

4. Expand **Settings** and select **ESET Security Product for Windows** from the drop-down menu.
5. Click **Personal Firewall**, expand **Basic** and then click **Edit** next to **Rules**.



**Figure 1-2**

**Click the image to view larger in new window**

6. Click **Show built in (predefined) rules** and deselect the check boxes next to **Block incoming NETBIOS requests** and **Block incoming RPC requests**.



**Figure 1-3**

7. Click **OK** and continue to part II below.

## II. Add the IP range/subnets to the Personal firewall prior to deploying ESET Endpoint Security

1. In the **Personal Firewall** → **Basic** section, click **Edit** next to **Zones**.



**Figure 2-1**

**Click the image to view larger in new window**

2. Select **Trusted zone** and click **Edit**.



**Figure 2-2**

3. In the **Remote computer address** field, add your IPv4 and Remote IP addresses, ranges, masks and subnets (for example, any VPN networks and all subnets inside your network), and then click **OK**.



**Figure 2-3**

4. Click **Save**. Once the system checks in to ERA with the new settings, you can deploy ESET Endpoint Security to your network.

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