Create IDS rules for client workstations in ESET PROTECT (8.x)

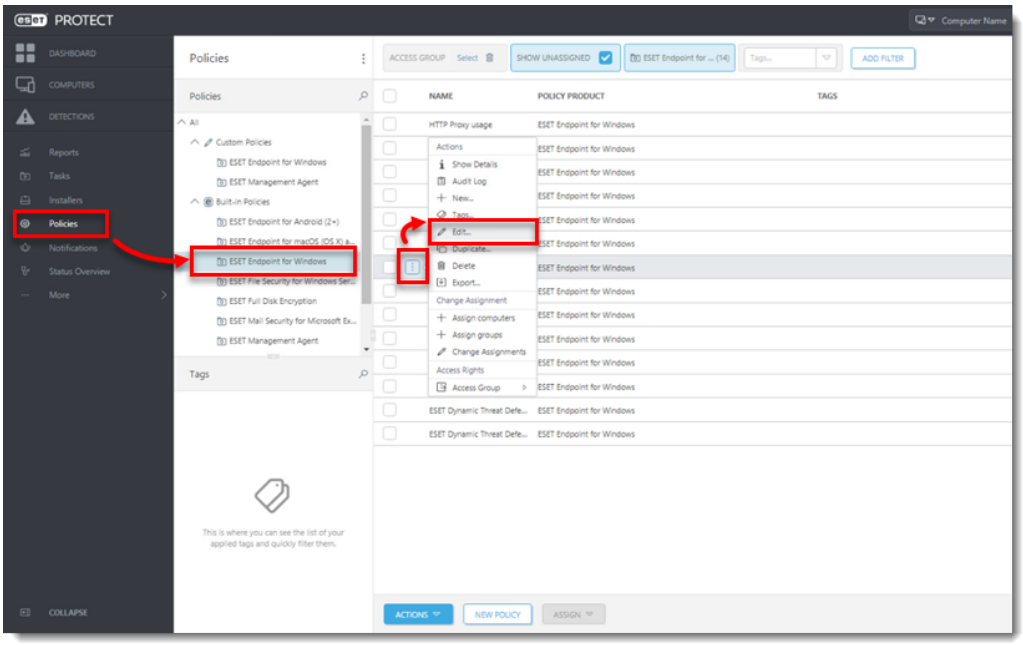
Steef | ESET Nederland - 2020-12-10 - Reacties (0) - Legacy

Solution

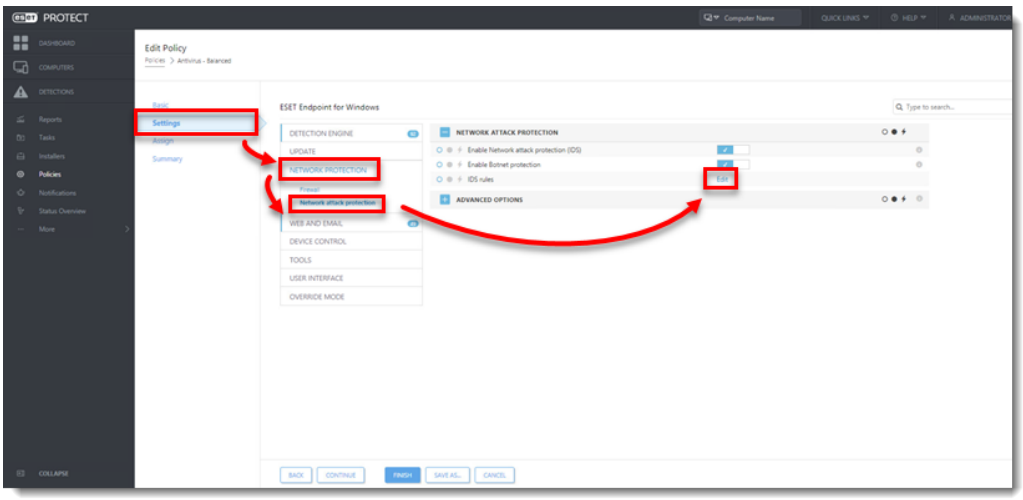
Create IDS exclusions in ESET PROTECT

1. Open ESET PROTECT Web Console in your web browser and log in.

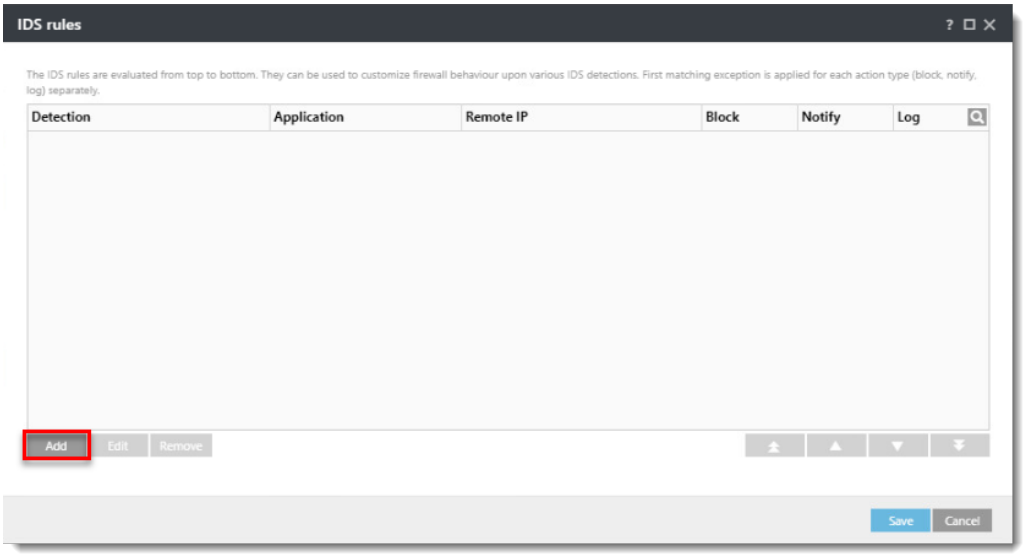
2. Click **Policies → ESET Endpoint for Windows**, then click the ellipses next to the policy you want to edit and click **Edit**.



3. Click **Settings → Network Protection → Network attack protection** and click **Edit** next to **IDS exceptions**.

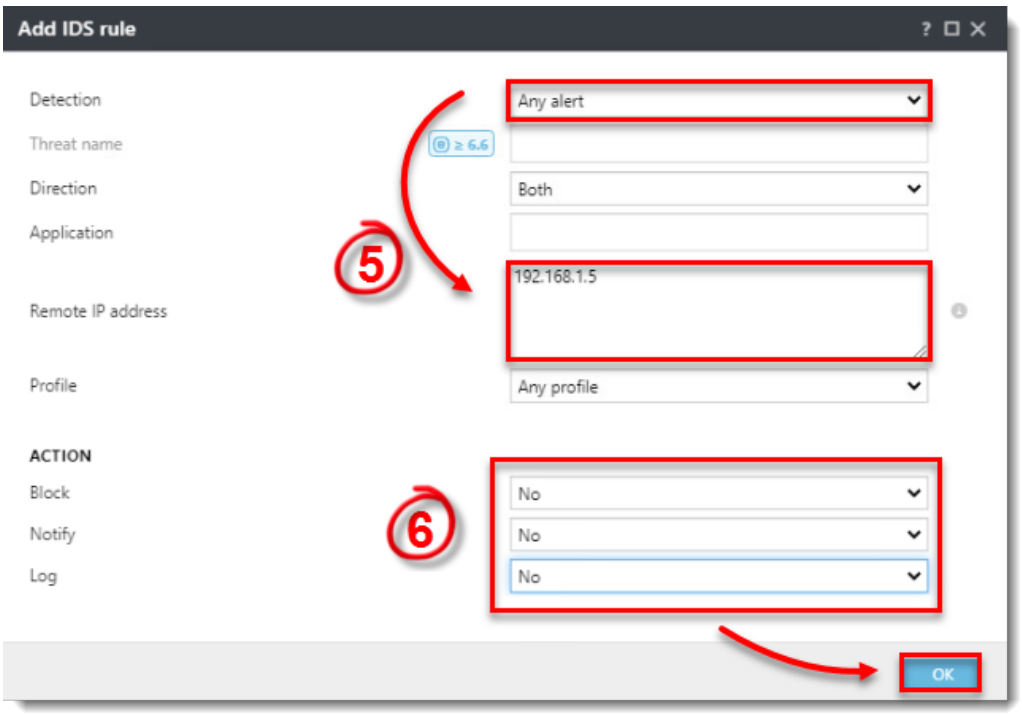


4. Click **Add**.



5. Select the **Alert**, type the **Remote IP address** (IP address of the machine with the software that scans the network).
   Alternatively, to set up an IDS exclusion for a locally installed application, type the full path to the `.exe` file in **Application** (e.g. C:\Windows\system32\cmd.exe).

6. In the **Action** section, select **No** from each drop-down menu. Click **OK** → **Save** → **Finish** to save the policy. If this is a new policy, assign the policy to the correct groups. After the computers check in, they will get the policy change.


Add IDS rule
Detection
Any alert
Threat name
≥ 6.6
Direction
Both
Application
5
Remote IP address
192.168.1.5
Profile
Any profile
ACTION
Block
No
6
Notify
No
Log
No
OK