Create IDS exclusions for client workstations in ESET Security Management Center (7.x)

Anish | ESET Nederland - 2019-02-04 - Reacties (0) - ESET Security Management Center

Create IDS exclusions for client workstations in ESET Security Management Center (7.x)

Applies to: ESET Security Management Center | Product version: 7.x

Solution

Endpoint users: Perform these steps on individual client workstations

Create IDS exclusions in ESET Security Management Center

ESET Security Management Center (ESMC) 7 User Permissions

This article assumes that your ESMC user has the correct access rights and permissions to perform the tasks below.

If you are still using the default Administrator user, or you are unable to perform the tasks below (the option is grayed out), see the following article to create a second administrator user with all access rights (you only need to do this once):

- Create a second administrator user in ESET Security Management Center 7.x

View permissions needed for least privilege user access

1. Open ESET Security Management Web Console (ESMC Web Console) in your web browser and log in.
2. Click **Policies**, select the policy in the **ESET Endpoint for Windows** section that you want to edit and then click **Policies → Edit**.

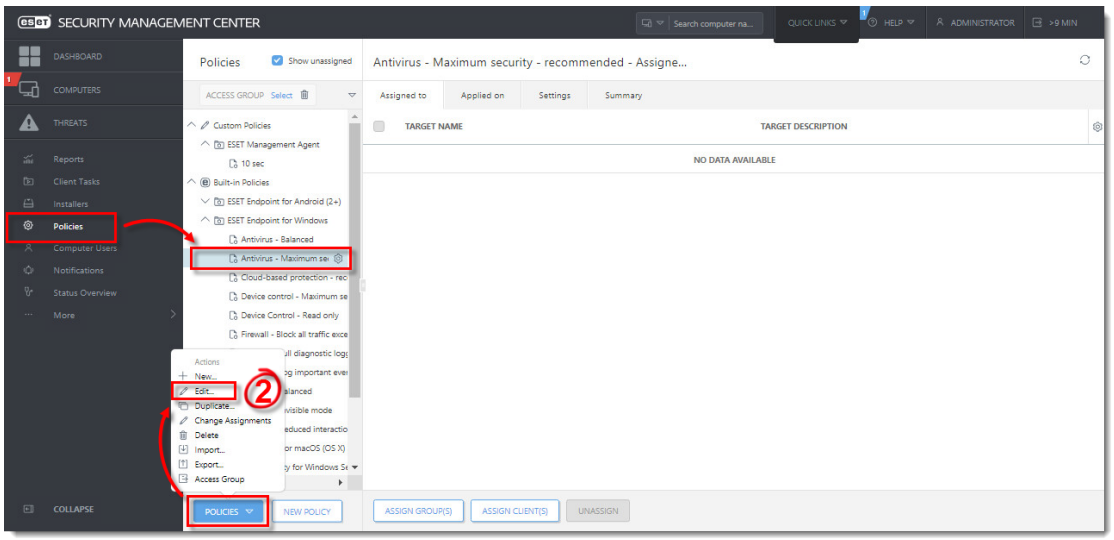

Figure 1-1
Click the image to view larger in new window

1. Expand **Settings → Network Protection → Network attack protection** and click **Edit** next to **IDS exceptions**.

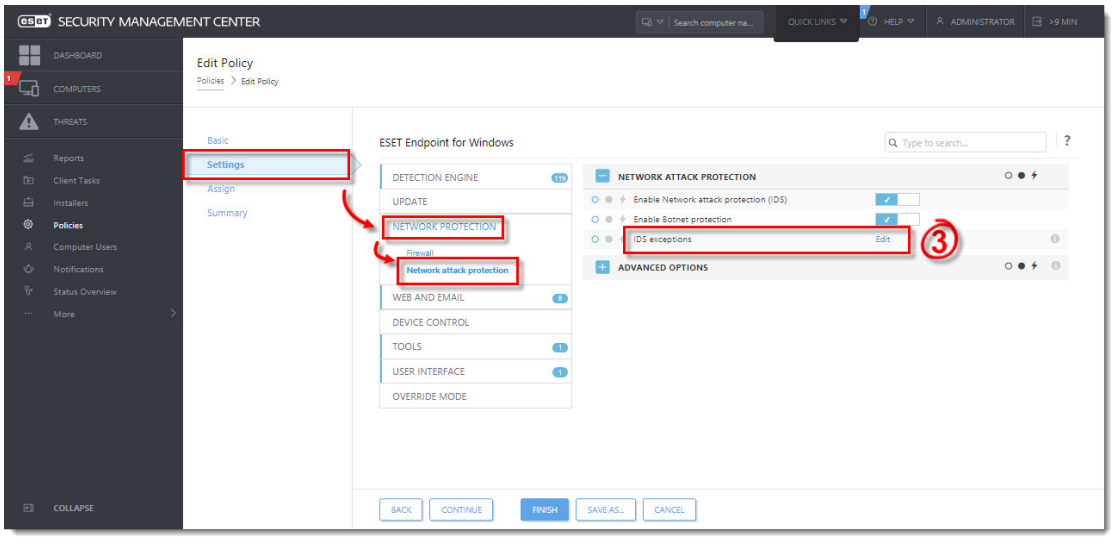

Figure 1-2
Click the image to view larger in new window

1. Click **Add**.

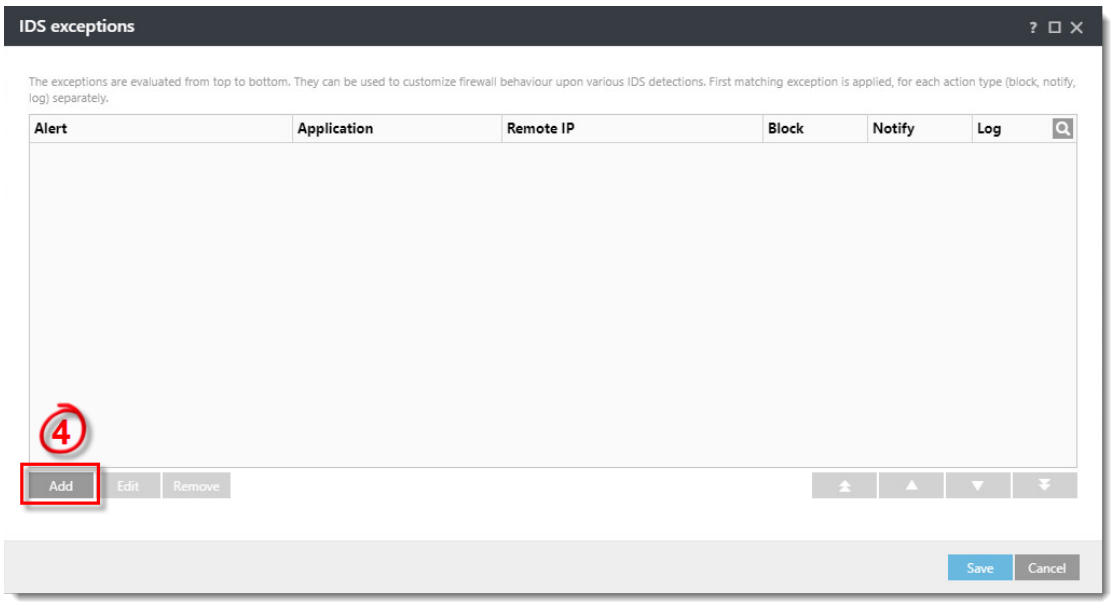

Figure 1-3

1. 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).

2. 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.

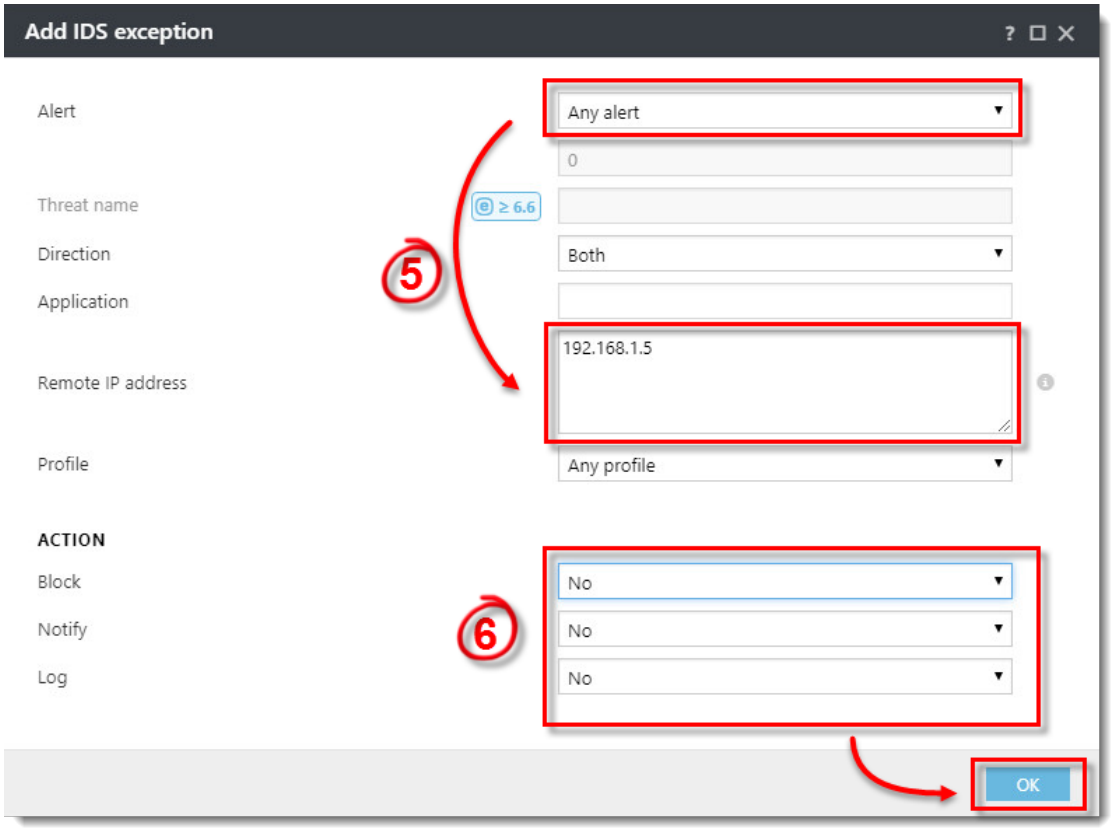

Figure 1-4

KB Solution ID: KB7054 |Document ID: 26426|Last Revised: January 22, 2019