ESET Tech Center

Enable advanced logging in ESET Endpoint Security (6.x)

Anish | ESET Nederland - 2018-03-07 - Reacties (0) - Legacy

Issue

Create a log of all connections blocked by the ESET firewall
Enable advanced logging of the firewall

Solution

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

Perform these steps on individual client workstations.

I. Activate logging of blocked connection in ESET Remote Administrator

ERA 6.5 User Permissions

This article assumes that your ERA 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 Remote Administrator 6.5

View permissions needed for least privilege user access

1. Open ESET Remote Administrator Web Co

ns ole (ERA Web Console) in your web browser and log in.

2. Click **Admin** → **Policies** → **New Policy**

.
To edit an existing policy, select the endpoint policy that you want to modify and click the gear icon

→ **Edi**

t.

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

3. Type a name for the new policy in the

Name field.

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

4. Expand the **Settings** section and select

Endpoint for Windows.

5. Click **Tools → Diagnostics**.
6. Click the slider bar next to **Enable Firewall advanced logging**.

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

7. Expand the **Assign** section, click **Add Computers**,

select the client for the policy and then click **OK**.

Figure 1-4 Click the image to view larger in new window

8. Click **Finish**. The policy will be applied on the client computer. With logging enabled, repeat the action that is blocked by the firewall

and then continue to Part II.

II. Download and run the ESET Log Collector tool

The ESET Log

Collector will create the firewall log along with other logs to help ESET technical support resolve your

issue quickly.

9. Download and run the ESET Log Collector tool.

10. Include the log file that the tool produces in your email respon

se to ESET technical support. If you have not already opened a case with ESET technical support, complete a technical support request

st and submit the file you just saved to ESET technical support for analysis.

11. To stop recording logs of all blocked connections, rep

eat the steps in the Activate logging of the firewall section and click the slider bar next to **Enable firewall advanced logging** to

disable it in step 6. Click **Finish**. If advanced logging is not disabled, it will generate a large log file.

Figure 1-5 Click the ima

ge to view larger in new window
Using Override mode in ESET Remote Admi

nis
tra
tor

ESE
T
end
poi
nt
ver
sion
6.5
pro
duc
ts
incl
ude
s an
Ove
rrid
e
mo
de
opti
on.
Wh
en
Ove
rrid
e
mo
de
is

enabled from ERA Web Console, a user on a client machine can change the settings in the installed ESET

endpoint product, even if the settings were locked by another policy. After the changes have been configu

red on the client machine, the configuration can be requested and saved as a new policy that can be then applied

on other computers.

Click for more information about Override mode.

Activate logging

of blocked connections in ESET Endpoint Security

1. Open the main program window

of your Windows ESET product.

2. Press the **F5** key to access Advanced setup.
3. Click **Tools → Diagnostics**.
4. Click the

slider bar next to **Enable Firewall advanced logging** and then click **OK**.

Figure 2-1

5. With logging enabled, repeat

the action that is blocked by the firewall and then continue to Part II.

II. Download and run the ESET

Log Collector tool

The ESET Log Collector will create the firewall log along with other logs to help

ESET technical support resolve your issue quickly.

6. Download and run the ESET Log Collector tool.

7. Include the log

file that the tool produces in your email response to ESET technical support. If you have not already opened a case with ESET tec

hnical support, complete a technical support request and submit the file you just saved to ESET technical support for analysis.

8. To

stop recording logs of all blocked connections, repeat the steps in the Activate logging of the firewall section and click the slider bar

next to **Enable firewall advanced logging** to disable it in step 6. Click **Finish**.

Disable advanced logging when you have finished collecting logs

Make sure you disable advanced logging after you collect the logs you need. It will generate a large log file if you forget to disable it.