# ESET Tech Center



## How do I create a HIPS rule and enforce it on a client workstation? (6.x)

Ondersteuning | ESET Nederland - 2017-11-08 - Comments (0) - 6.x

https://support.eset.com/kb5687

## Details

ESET's Host-based Intrusion Prevention System (HIPS) is included in ESET Endpoint Security, ESET Endpoint Antivirus, ESET Mail Security for Microsoft Exchange, and ESET File Security for Microsoft Windows Server. HIPS monitors system activity and uses a set of pre-defined rules to recognize suspicious system behavior. When this type of activity is identified, the HIPS self-defense mechanism stops the offending program or process from carrying out potentially harmful activity. Changes to the Enable HIPS and Enable Self-defense settings take effect after the Windows operating system is restarted.

## Solution

### Advanced users only!

By default, the Host-based Intrusion Prevention System (HIPS) is pre-configured to ensure maximum protection of your system. While the creation of a HIPS rule may be needed to resolve an issue in certain infrequent cases, the manipulation of HIPS rules requires advanced knowledge of applications and operating systems and is **not recommended**.

## Create a HIPS rule from the ESET Remote Administrator Web Console

> If you do not use ESET Remote Administrator to manage your network
>
> Perform these steps on individual client workstations.

1. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in. Open ERA Web Console
2. Click **Admin** → **Policies**, click the gear icon next to the policy you want to modify, and then select **Edit** from the context menu.

**Figure 1-1**

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

3. Expand **Settings**, click **Antivirus** → **HIPS**, and then click **Edit** next to **Rules**.

**Figure 1-2**

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

4. Click **Add**.

**Figure 1-3**

5. Configure your rule. In the example, operations affecting registry entries are blocked, and the end user will be notified when this action is performed by the HIPS module. When you are finished, click **Next**.

**Figure 1-4**

6. In the **Source applications** window, select your desired option from the drop-down menu. In this example, the HIPS rule will block any application that attempts to modify registry values. Click **Next**.

**Figure 1-5**

7. In the **Registry operations** window, specify which operations will trigger this rule. In this example, **Delete from registry** is selected. Click **Next**.

**Figure 1-6**

8. In the **Registry entries** window, select your desired option from the drop-down menu. In this example, we are blocking the deletion of any registry entries. Click **Finish**.

**Figure 1-7**

9. Click **OK** to save the rule.

**Figure 1-8**

10. Click **Finish**. Computers assigned to the policy you modified will receive this new HIPS rule the next time they check into ESET Remote Administrator Server (ERA Server).

> ### Previously defined HIPS rules
>
> Any previously defined HIPS rules on the assigned computers will be replaced with the HIPS rules defined by this policy.

**Figure 1-9**

---

## Create a HIPS rule on individual client workstations

1. Open the main program window of your Windows ESET product.
2. Press the **F5** key to access Advanced setup.

3. Click **Antivirus** → **HIPS** and then click **Edit** next to **Rules**.

**Figure 2-1**

4. Click **Add**.

**Figure 2-2**

5. Configure your rule. In the following example, we will block certain operations affecting applications, and the user will be notified of the action. Click **Next**.

**Figure 2-3**

6. In the **Source applications** window, select your desired option from the drop-down menu. In this example, the HIPS rule will block any application that attempts to modify registry values. Click **Next**.

**Figure 2-4**

7. In the **Application operation** window, click the slider bar next to the operation(s) you want to block. In this example, the HIPS rule will block any application that attempts to debug another application. Click **Next**.

**Figure 2-5**

8. In the **Applications** window, select your desired option from the drop-down menu. In this example, the rule will apply to all applications. Click **Finish**.

**Figure 2-6**

9. Click **OK** to save the new HIPS rule and then click **OK** again to exit advanced setup. Changes will take effect after the Windows operating system is restarted.

### If assigned an ERA policy

If this computer is assigned an ERA policy that defines a set of HIPS rules, that policy will overwrite any rules you define on the individual computer.

**Figure 2-7**

Tags

EEA 6.x

EES 6.x

EFSW

EMSX

ERA 6.x