ESET Tech Center

Disable HIPS in endpoint products using ESET Security Management Center (7.x)

Anish | ESET Nederland - 2018-09-14 - Reacties (0) - ESET Security Management Center

Details

The ESET 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 pre-defined set of 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

Endpoint users: Perform these steps on individual client workstations

Advanced users only!

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

1. Open ESET Security Management Web Console (ESMC Web Console) in your web browser and log in.
2. Click **Policies** and select the policy you want to modify. Click the gear icon, and select **Edit** from the context menu.

   Figure 1-1
   Click the image to view larger in new window
3. Click **Settings**, click **Detection Engine** → **HIPS**, and then click the slider bar next to **Enable HIPS** to disable it.
4. Click **Finish**. Client computers assigned to the policy you modified will receive this new HIPS rule the next time they check in to the ESET Security Management Center Server (ESMC Server).

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

Re-enable HIPS

We recommend re-enabling HIPS again as soon as possible so that your machine(s) will again be fully protected.

KB Solution ID: KB6796 |Document ID: 25646|Last Revised: August 21, 2018