ESET Tech Center

How do I disable the graphical user interface (egui.exe) on client workstations? (5.x)

Ondersteuning | ESET Nederland - 2024-08-28 - Comments (0) - 5.x

https://support.eset.com/kb3083

Issue

Disabling the graphical user interface of your ESET product on a client workstation
Configure ESET Remote Administrator to control terminal computers running instances of `ekrn.exe`

Solution

A new version has been released

Version 6 of ESET Remote Administrator (ERA) and ESET business products were released in North America December 11th, 2014, and globally February 25th, 2015. This article applies to version 5.x and earlier ESET business products. For information about what's new in the latest version and how to upgrade, see the following article:

What's new in ESET version 6 business products?

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

Perform these steps on individual client workstations.

I. Disable the graphical user interface using ESET Remote Administrator

Warning:

Terminal Server networks: It is essential that you first configure ESET Remote Administrator to control terminal computers running instances of `ekrn.exe` because after disabling, there will be no graphical interface on the terminal computer.

1. Open the ESET Remote Administrator Console by clicking **Start → All Programs → ESET → ESET Remote Administrator Console → ESET Remote Administrator Console**.
2. Click **Tools → Policy Manager**.
3. Select the policy you want to modify and click **Edit Policy**.

Figure 1-1

Click the image to view larger in new window

4. Expand **Windows desktop v5 → Settings → Default user interface values**.
5. Select **Graphical user interface: Yes** and deselect the check box next to **Value**.

Figure 1-2

Click the image to view larger in new window

6. Select **Suppress user settings: Yes** and select the check box next to **Value**

Figure 1-3

Click the image to view larger in new window

7. Click **Console → Yes** to save your changes. These settings will be applied to the client workstations assigned to this policy the next time they check into ESET Remote Administrator.

II. Recommended settings for workstations where the graphical user interface has been disabled

Disabling the graphical user interface may cause other issues. Below is a list of potential configurations that can be used to address these issues.

Antivirus and antispyware:

Cleaning

We recommend that you set the cleaning level in the ThreatSense engine parameter setup window to Strict cleaning in all modules.

SSL Protocol filtering

If administration of the SSL protocol is needed, we recommend turning on **Block communication that uses the certificate**. From the main program window, press **F5** on your keyboard. From the Advanced setup window, expand **Web and email → Protocol filtering → SSL → Certificates**. Under **End certificate validity**select **Block communication that uses the certificate**.

Update

We recommend that you select **Never restart computer** and **Never update program components**. From the main program window, press the **F5** key to open the Advanced setup window. From the Advanced setup tree, click **Update → General** and then click **Setup** under **Advanced**

update setup. These options are located in the **Update mode** tab under **Restart after program component upgrade** and **Program component update**, respectively.

Email clients

The lack of a graphical user interface results in a few changes to the way your ESET security product works with email clients:

a. Since you will not receive security notifications, you must configure your ESET security product not to ask for user action when a threat is detected. From the Advanced setup window, click **Web and email →Email client protection**. Click **Setup...** under **ThreatSense engine parameter setup** and select **Cleaning**from the tree on the left. Under **Cleaning level** move the slider to **Strict cleaning**.
b. You must add addresses into antispam lists (trusted addresses, spam, list of inclusions) remotely, since those options will not be available on the client terminal.
c. Some items on the ESET Antispam Toolbar drop-down menu in your email client will be inactive, such as **Antispam setup**, **Address books** and **Help**.

Scheduler

Schedules triggered by the **User logon** event trigger will not work without the graphical user interface because your ESET security product monitors the launch of egui.exe at user logon. If any of your scheduled tasks require user logon to start, reconfigure them to trigger on a different event. From the main program window, toggle your ESET security product to Advanced mode and then select **Tools → Scheduler**. In the **Scheduler/Planner** area, click on existing rules that launch at user logon and click **Edit...**. From the Edit task window, select an event trigger other than **User logon**, such as **Every time computer starts** or **The first time the computer starts each day**.

Personal firewall

ESET strongly discourages installations of ESET Endpoint Security on servers (and ESET technical support North America does not support such installations) for a number of reasons. A primary concern is that the ESET Personal firewall can block connections to the server, even those by an administrator seeking to modify the server after the installation. We strongly recommend that you use the suggestions below to configure Personal firewall on a computer running ESET Endpoint Security with egui.exe disabled.

Filtering mode

We recommend that you use one of the following filtering modes: **Automatic mode**, **Automatic mode with exceptions (user-defined rules)** or **Policy-based mode**.

Rules and zones

ESET recommends that you set your desired Personal firewall behavior when changing the network adapter settings. From the main program window, press the **F5** key. From the Advanced setup window, expand **Personal firewall → Rules and zones → Trusted zone → Setup… → Advanced settings...** and select **Do not show the dialog with protection mode settings of the computer in the network**.

Application modification detection

You will need to add trusted applications that update occasionally to the **List of applications excluded from checking**, since the user will not be able to see alert notifications asking if such updates are permitted. To exclude an application, open the Advanced setup window and click **Personal firewall → Application modification detection**. Then, click **Add...** to add the list of applications that

are allowed to update without being checked.

You can disable Application modification detection entirely by deselecting the check box next to **Enable detection of application modifications** in the **Detect modification of network-aware applications** area, but this will decrease the security of your computer.

III. Troubleshooting

Microsoft Outlook displays the following message:

- "The Add-in **ESET Outlook Plug-in** (C:\PROGRA~1\ESETESETNO~1\EPLGOU~1.DLL) cannot be loaded and has been disabled by Outlook. If no update is available, please uninstall the Add-in."

    a. If this occurs, delete the **extend.dat** file of the user account with the error. By default, this file can be found in **C:\Documents and Settings\Username\Local Settings\Application Data\Microsoft\Outlook**. Outlook will automatically recreate the `.dat` file at the next application startup and the issue should not occur again.

    b. Other clients, such as Microsoft Outlook Express, Microsoft Windows Mail and Microsoft Windows Live Mail can also have very rare integration issues, often caused by the presence of another security program in addition to your ESET security product.

Disable the graphical user interface on individual client workstations

1. Open ESET Endpoint Security or ESET Endpoint Antivirus. How do I open my ESET product?

1. Press **F5** to access Advanced setup. Expand **Computer** and click **HIPS** in the Advanced setup tree .
2. Deselect the check box next to **Enable Self-defense**, and then restart your computer for this change to take effect.

Figure 2-1

Click the image to view larger in a new window

4. Click **Start → Run** (Windows Vista / Windows 7 users: press **Windows key** + **R**).
5. Enter "msconfig" into the command-line field and click **OK**.
6. In the **System Configuration** window, select the **Startup** tab:

    a. **Windows 7/Vista users**: Deselect the check box next to **ESET Endpoint Security**, **ESET Endpoint Antivirus**, **ESET Smart Security** or **ESET NOD32 Antivirus** and click **OK**.

Figure 2-2

    b. **Windows XP users**: Deselect the check box next to **egui** and click **OK**.

Figure 2-3

Once these changes are made, the graphical user interface will no longer appear on startup.

Tags

ERA 5.x

Policy