Recommended settings for ESET Server Security for Windows Server installed on a terminal or Citrix server (8.x)

Steef | ESET Nederland - 2021-06-25 - Comments (0) - Server Solutions

Issue

- ESET recommends you configure Citrix and other terminal servers using these parameters when running ESET products
- Disable all Citrix API hooks on a per-application basis

Details

ESET server products can run in virtualized environments (such as Citrix) using default settings. Make a few small changes to minimize the impact on performance ESET products have on your virtual machine.

Normally, ESET Server Security GUI starts up every time a remote user logs onto the server and creates a terminal session. This is usually undesirable on terminal servers.

Solution

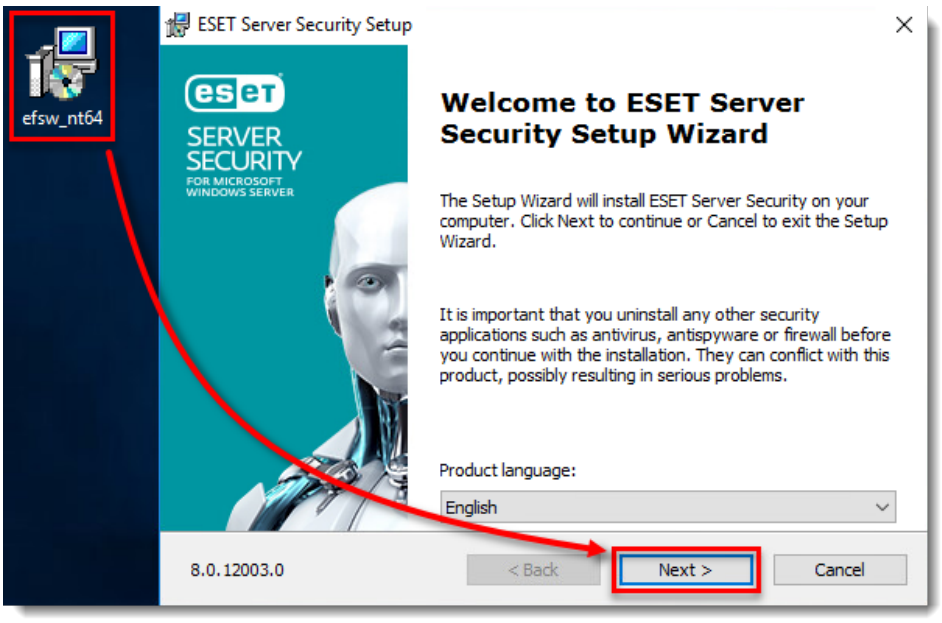
Complete the steps below in sequence to achieve the best performance on a server with ESET Server Security for Microsoft Windows Server installed.

1. Verify that Network protection module is installed
2. Disable the ESET Server Security graphic user interface (GUI) to prevent it from starting up every time a user logs in
3. Scan file execution events and local drives only (Citrix servers only)
4. Add needed exclusions (Citrix servers only)

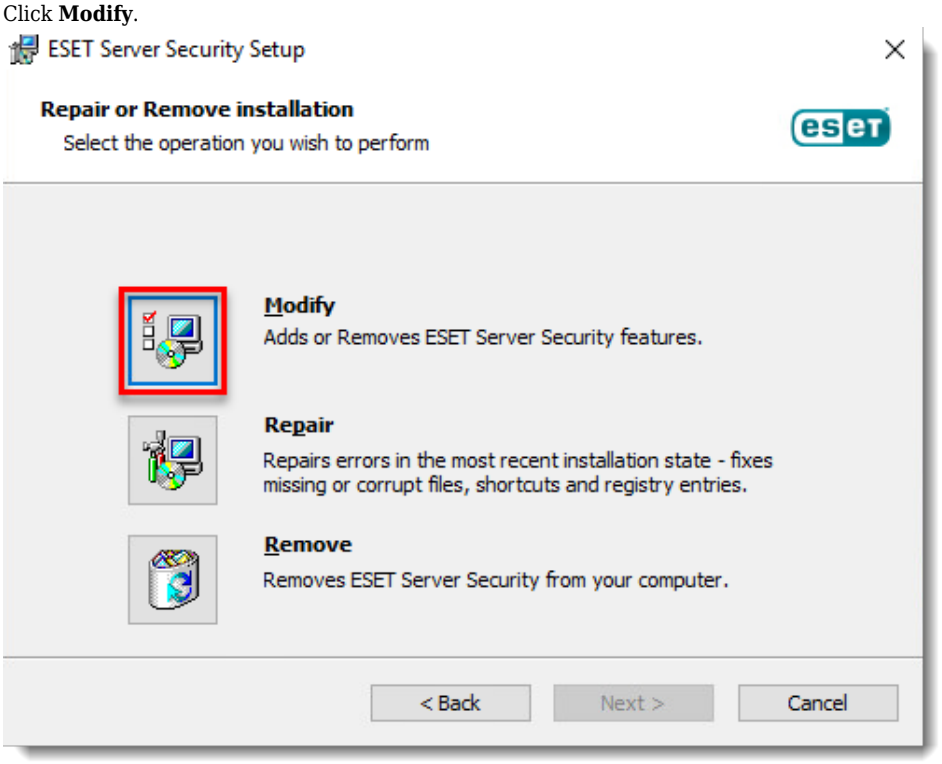
I. Verify that Network protection module is installed

Server 2008/2008R2 users: There are 2 ways to verify that the **Network protection** module in ESET Server Security for Microsoft Windows Server is installed.

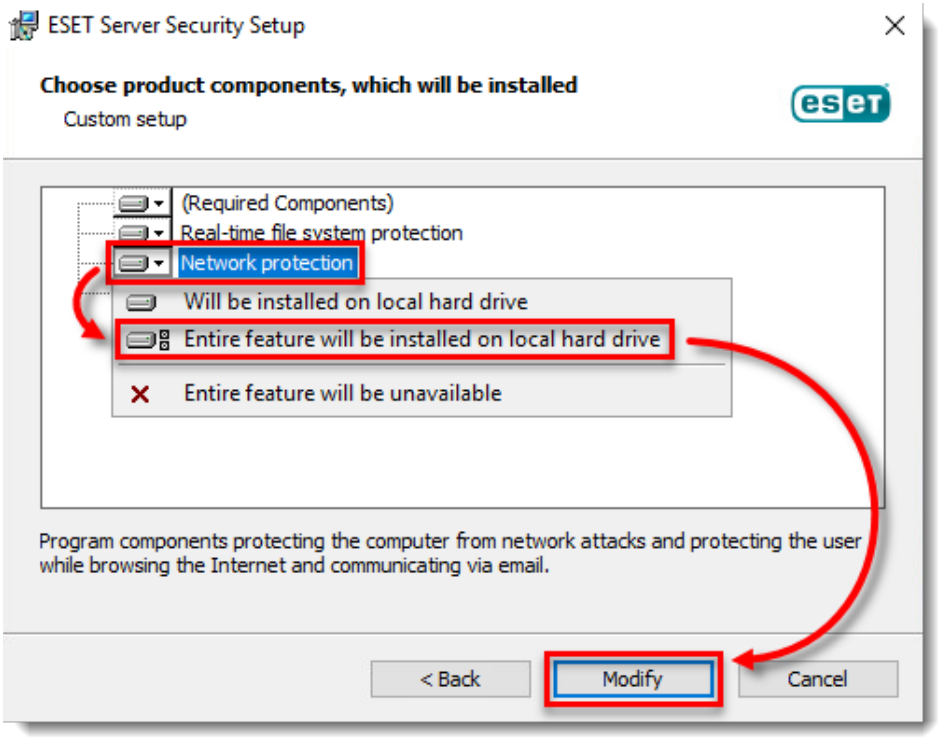
- If you have already installed ESET Server Security, enable the **Network protection** module:
    - Double-click the installer you used to install ESET Server Security (for example, efsw_nt64_ENU.msi) and then click **Next**.



- Click **Modify**.



- From the product component drop-down menu next to **Network Protection**, select **Entire feature will be installed on local hard drive** and then click **Modify**.

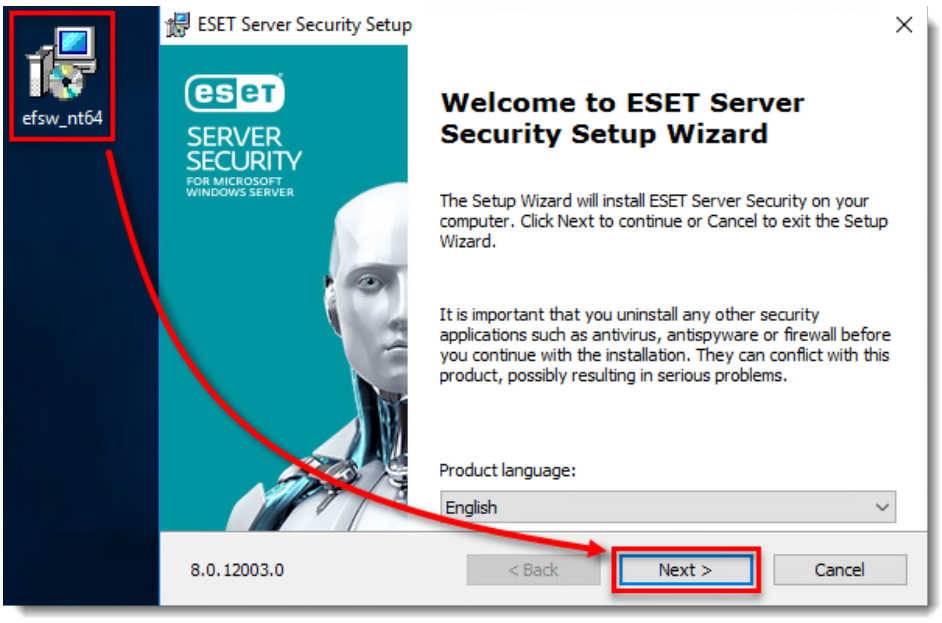


- Wait for the installation to finish. In the **Setup → Web and email** section of ESET Server Security, you will now see the **Web access protection** and **Email client protection** modules.

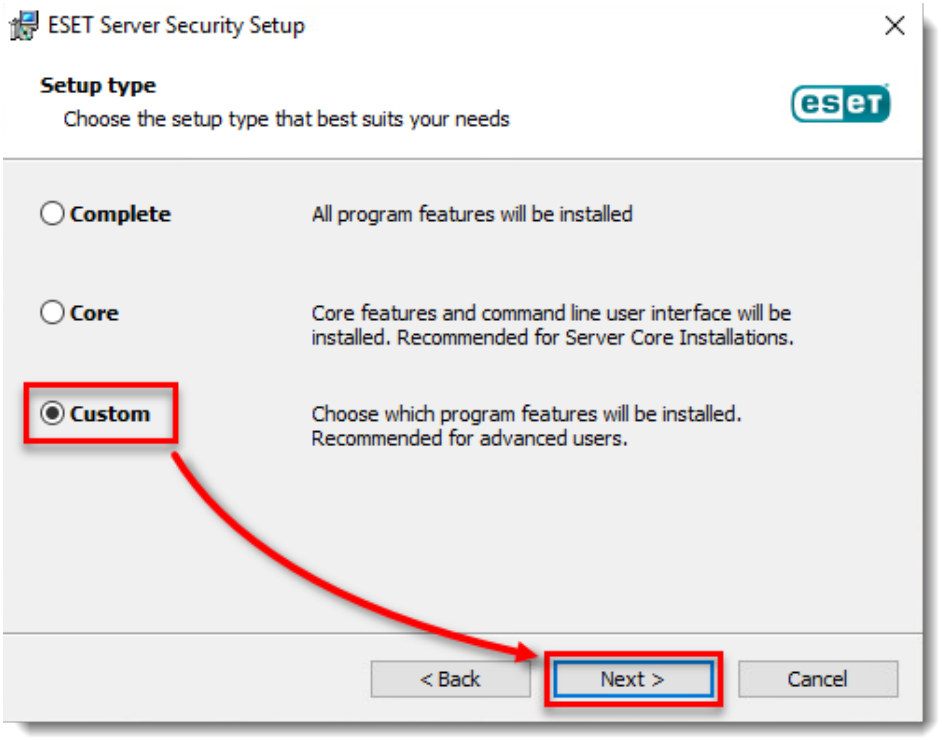
- If you are installing ESET Server Security for the first time, follow the instructions below to enable the **Network Protection** module. You can modify installed components anytime by running the installer. This can be done without a server restart. The GUI will restart and you will see only the components you chose to install.

> ESET Server Security installation guide
> For illustrated instructions to download and install ESET Server Security, see Download, install, and activate ESET Server Security for Microsoft Windows Server.

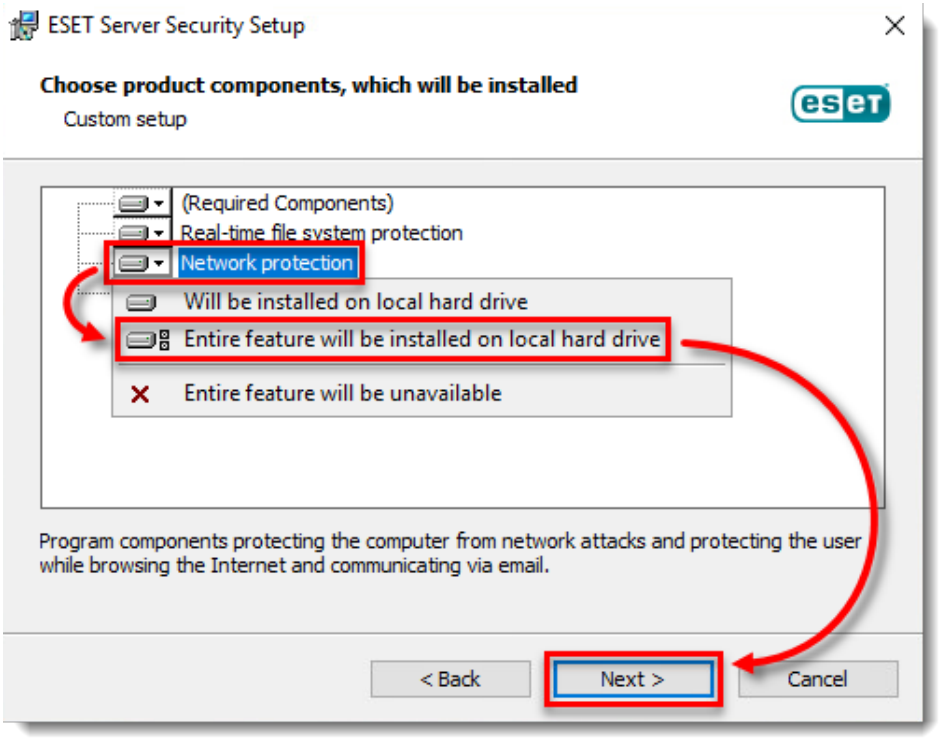
  - Double-click the ESET Server Security installer you downloaded (for example, efsw_nt64_ENU.msi) and then click **Next**.



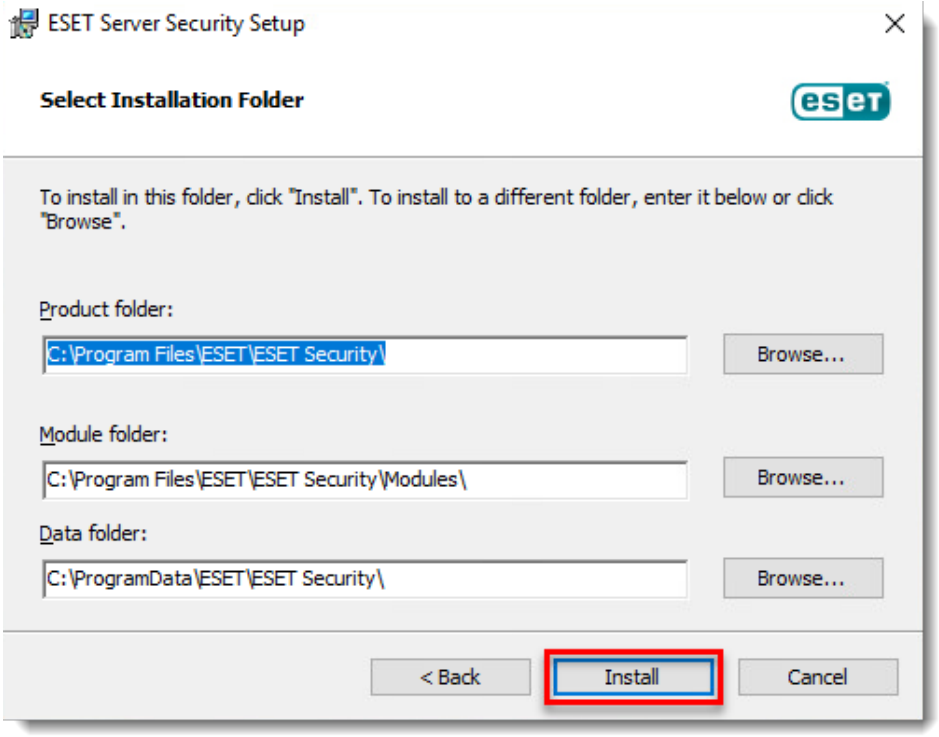
- Select **Custom** and click **Next**.



- Click the product component drop-down menu option next to **Network protection**, click **Entire feature will be installed on local hard drive** and then click **Next**.



- Click **Install** and wait for the installation to finish.



II. Disable the graphic user interface (GUI)

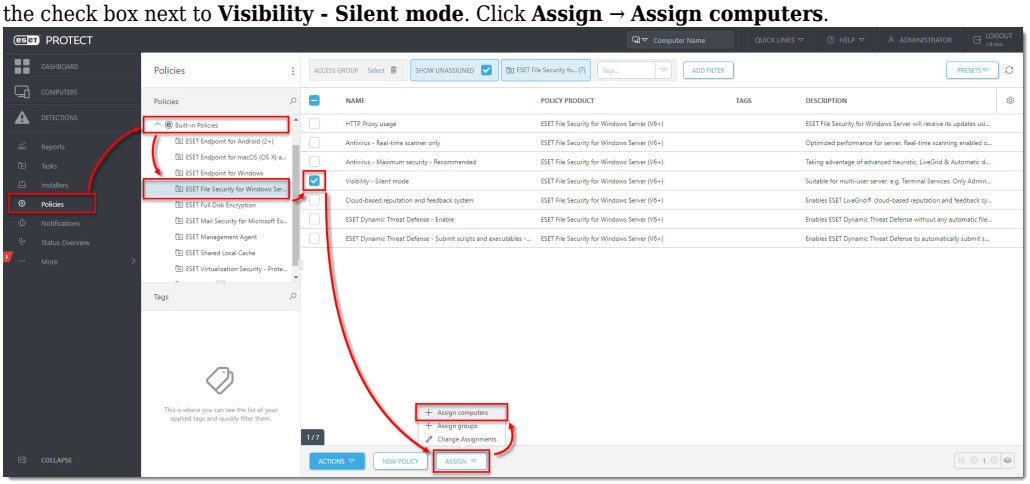
The steps in this section will disable the GUI from launching automatically at startup. However, you can still access the GUI at any time from the Start Menu.

a. Enable silent mode on the server

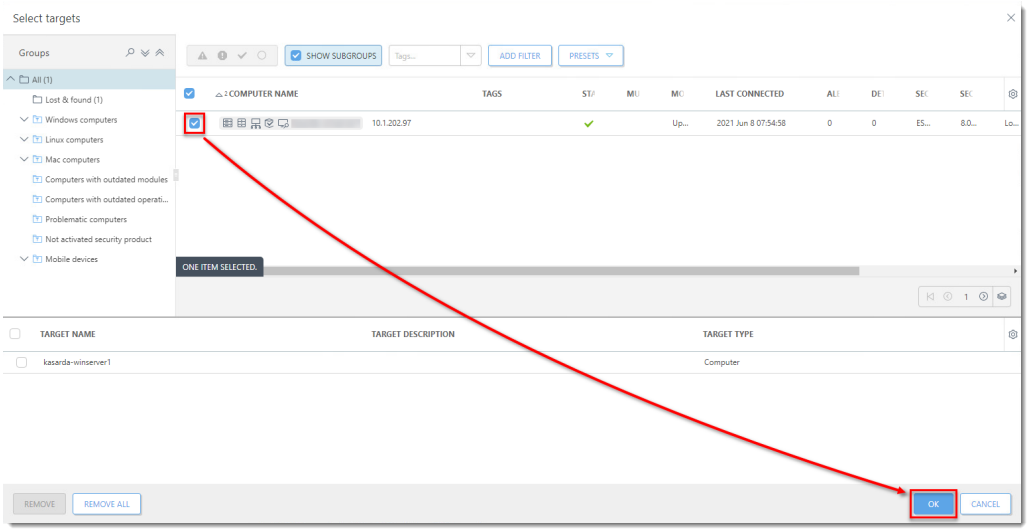
Assign the **Visibility - Silent mode** policy on ESET Server Security in ESET PROTECT to enable silent mode on a server.

1. Open the ESET PROTECT Web Console in your web browser and log in.

2. Click **Policies**, expand **Built-in Policies**, select **ESET File Security for Windows Server** and select the check box next to **Visibility - Silent mode**. Click **Assign → Assign computers**.



3. Select the check box next to the computer that you want to assign the policy to and click **OK**.



Continue to part III below if you are using a Citrix server.

b. Manually update individual client workstations using ESET Shell.

Check or Change your GUI Mode

If you want to find out what mode is currently used, run the following command in ESET Shell:

```
get ui ui gui-start-mode
```

The following commands will change the GUI mode that you are using:

```
set ui ui gui-start-mode full
```

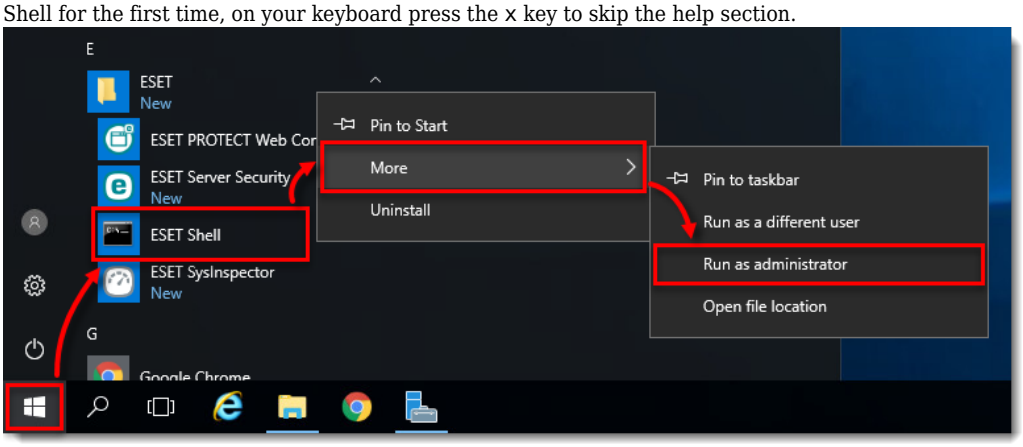
```
set ui ui gui-start-mode none
```

To see what policies are assigned to a specific group, select that group and click the **Policies** tab to view a list of policies assigned to the group. For more information about policies, see the Policies chapter in Online Help.

Perform these steps on individual client workstations:

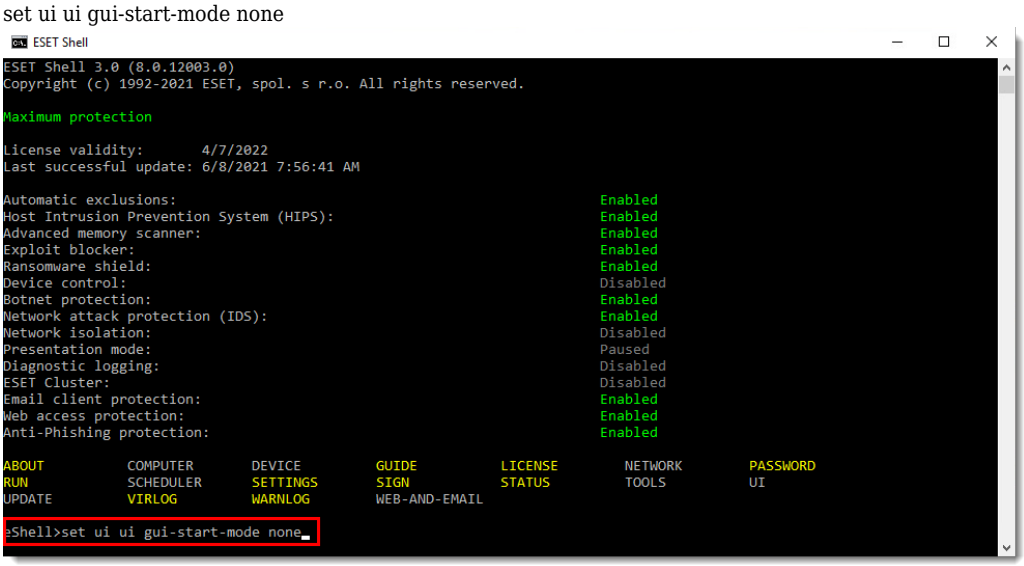
1. To open ESET Shell click **Start** button then navigate to **ESET**. Right-click **ESET Shell** and select **More → Run as administrator** from the context menu. For Windows Server 2012, you can type `ESET Shell` into the Search field.

   If prompted, type in the username and password for the administrative account. If you are opening ESET Shell for the first time, on your keyboard press the `x` key to skip the help section.



2. Type the following command:

   set ui ui gui-start-mode none



3. On your keyboard, press **Enter** and wait for the command to complete. Then close the window.

III. Scan file execution events and local drives only (Citrix servers only)

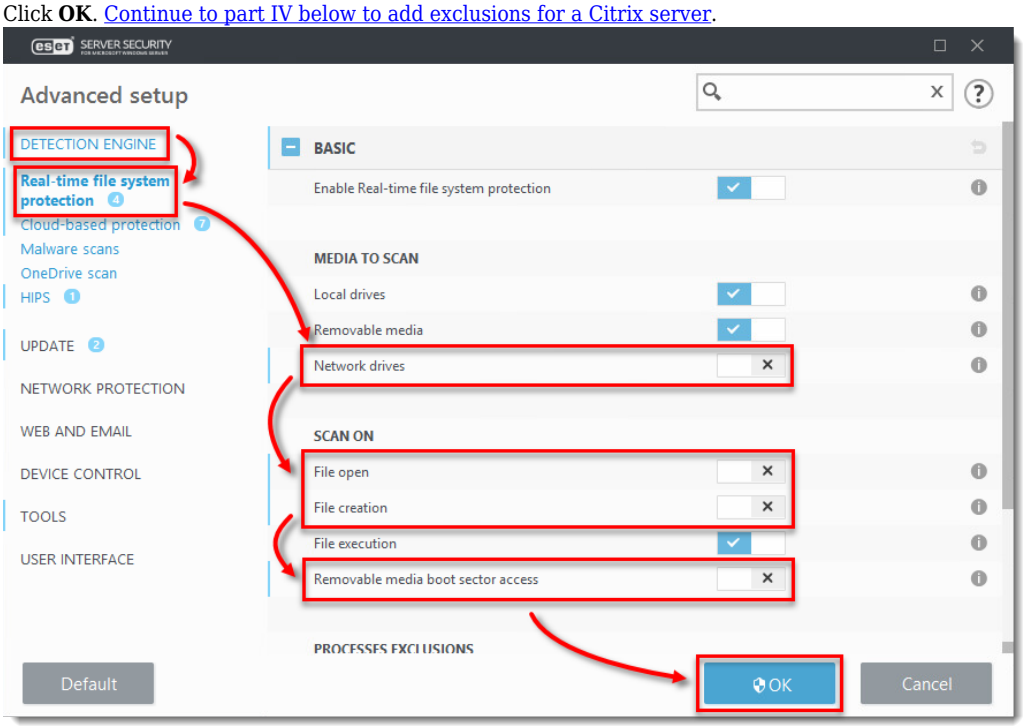
1. Open ESET File Security by clicking **Start** button then navigate to **ESET** and click **ESET File Security**.

2. On your keyboard, press the **F5** key to open Advanced Setup.

3. Click **Detection Engine → Real-time file system protection** from the main menu on the left. Turn off the following four features by clicking the slider bars next to them:

   - **Network drives**
   - **File open**
   - **File creation**
   - **Removable media access**

4. Click **OK**. Continue to part IV below to add exclusions for a Citrix server.

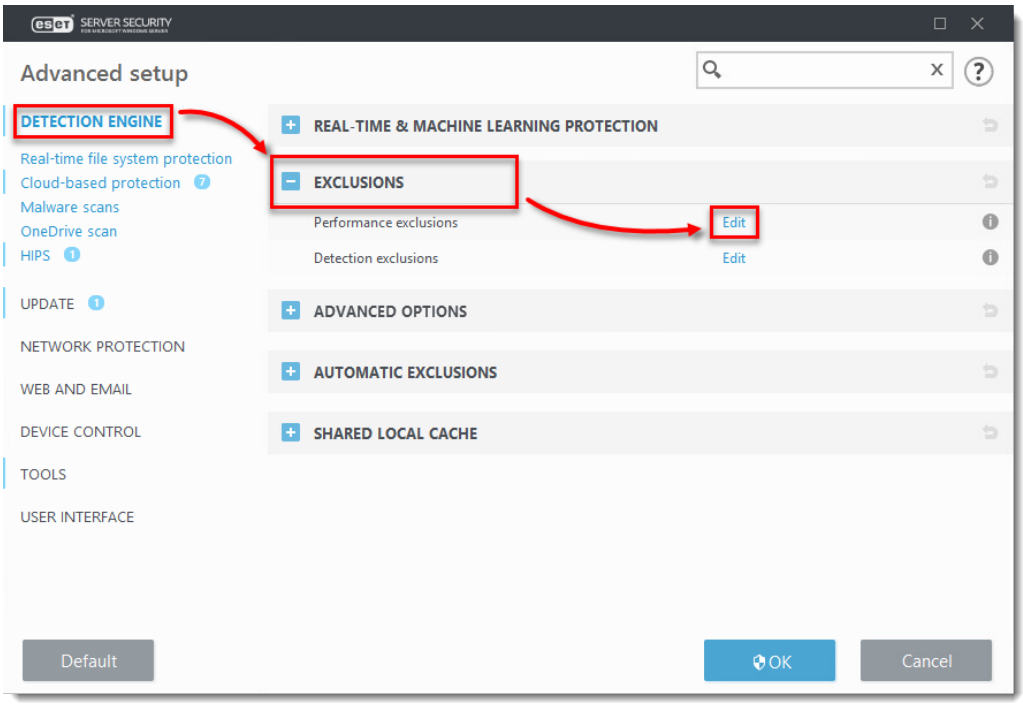


IV. Add needed exclusions (Citrix servers only)

1. To open ESET Server Security click the **Start** button then navigate to **ESET** and click **ESET Server Security**.

2. On your keyboard, press the **F5** key to open Advanced Setup.

3. Click **Detection Engine** from the main menu on the left, then expand **Exclusions**, and then click **Edit** next to **Performance exclusions**.



4. Click **Add**, in the field next to **Path** type C:\Program Files\Citrix\ and click **OK → OK → OK**.

   You can add additional file paths to exclude. Using a \ at the end of the path will cause ESET to treat it as a wildcard, and all children of that path will be excluded.

   [View the Citrix Consolidated list of Antivirus exclusions]