Recommended settings for ESET File Security installed on a terminal or Citrix server (6.x)

Ondersteuning | ESET Nederland - 2020-02-26 - Reacties (0) - ESS for Windows Server

Recommended settings for ESET File Security installed on a terminal or Citrix server (6.x)

Issue

- Citrix and other terminal servers should be configured using these parameters when running ESET products
- Disable the ESET File Security GUI to prevent it from starting up every time a user logs in

Details

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

Normally, ESET File 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

A new version is available

ESET File Security for Microsoft Windows Server version 7.x is available. We highly recommend that you upgrade to the latest version.

Complete the procedures below in sequence to achieve the best performance on a server with ESET File Security for Microsoft Windows Server (EFSW) installed.

I. Prerequisites

Server 2008/2008R2 users: Verify that the **Web and email** module in ESET File Security for Microsoft Windows Server (EFSW) is installed.

A. Existing ESET File Security installations

If you have already installed EFSW, follow the instructions below to enable the **Web and email** module.

1. Double-click the installer you used to install EFSW (for example, efsw_nt64_ENU.msi), click **Run** and then click **Next**.

2. Click **Modify** from the **ESET File Security Setup** screen.

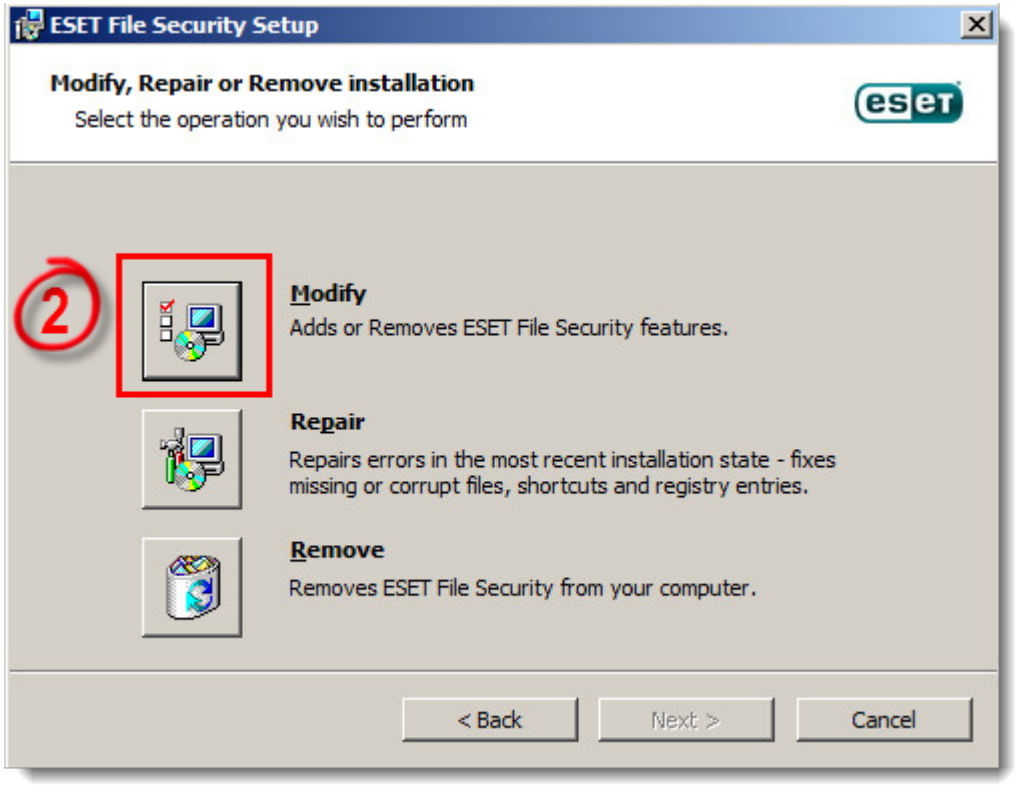

Figure 1-1

1. Click the product component drop-down menu option next to **Web and email**, click **Entire feature will be installed on local hard drive** and then click **Modify**.

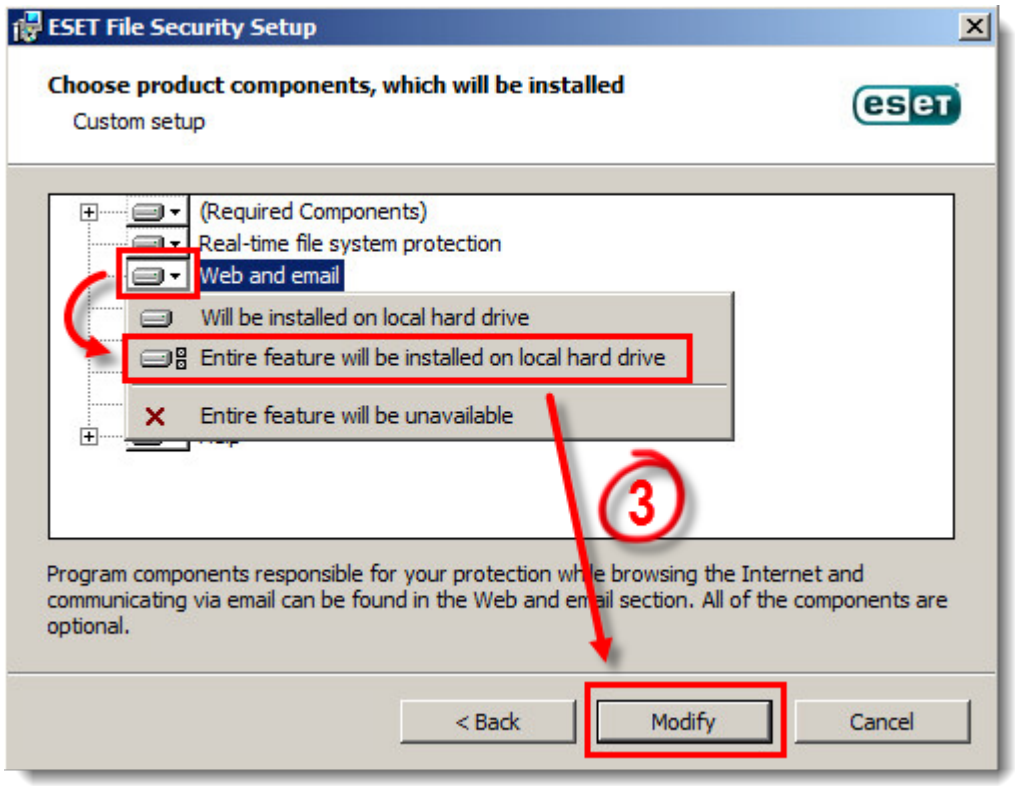

Figure 1-2

You will now see the **Web access protection** and **Email client protection** modules in the **Setup → Computer** section of EFSW.

B. New ESET File Security installations

If you are installing EFSW for the first time, follow the instructions below to enable the **Web and email** 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.

1. Double-click the EFSW installer you downloaded (for example, efsw_nt64_ENU.msi), click **Run** and then click **Next**.

   For illustrated instructions to download and install ESET File Security, see the following ESET Knowledgebase article:

   - How do I install and activate ESET File Security for Microsoft Windows Server? (6.x)

2.

3. Choose **Custom** from the **Setup type** installation screen and click **Next**.

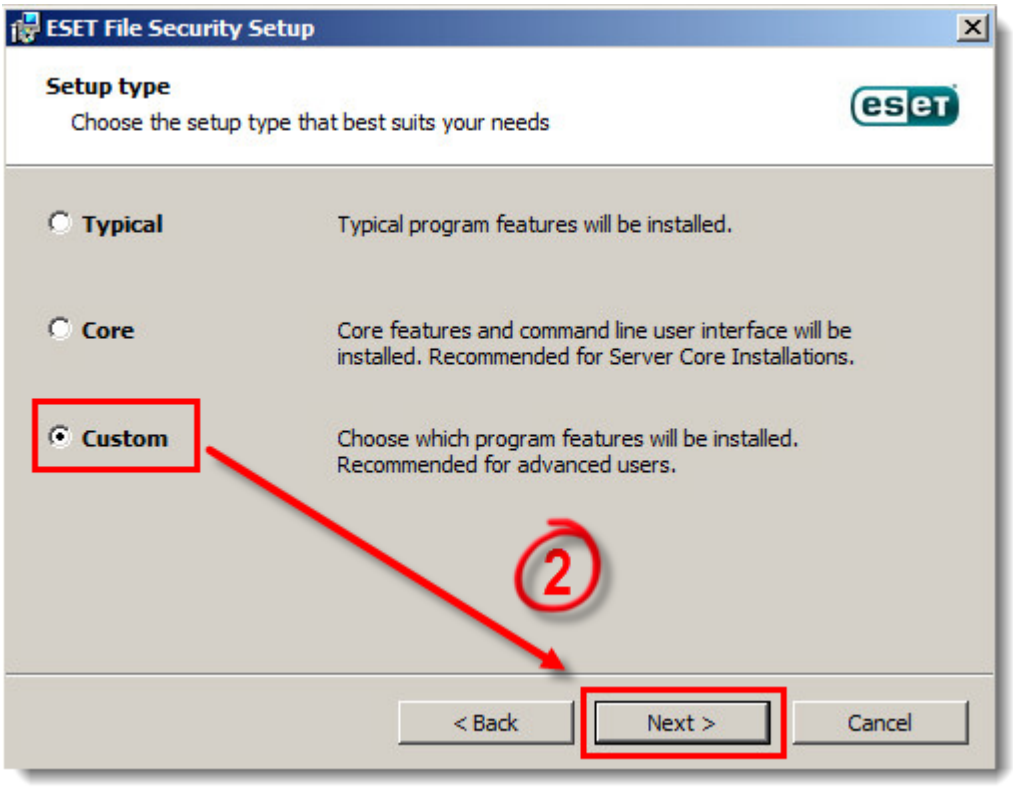

Figure 1-3

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

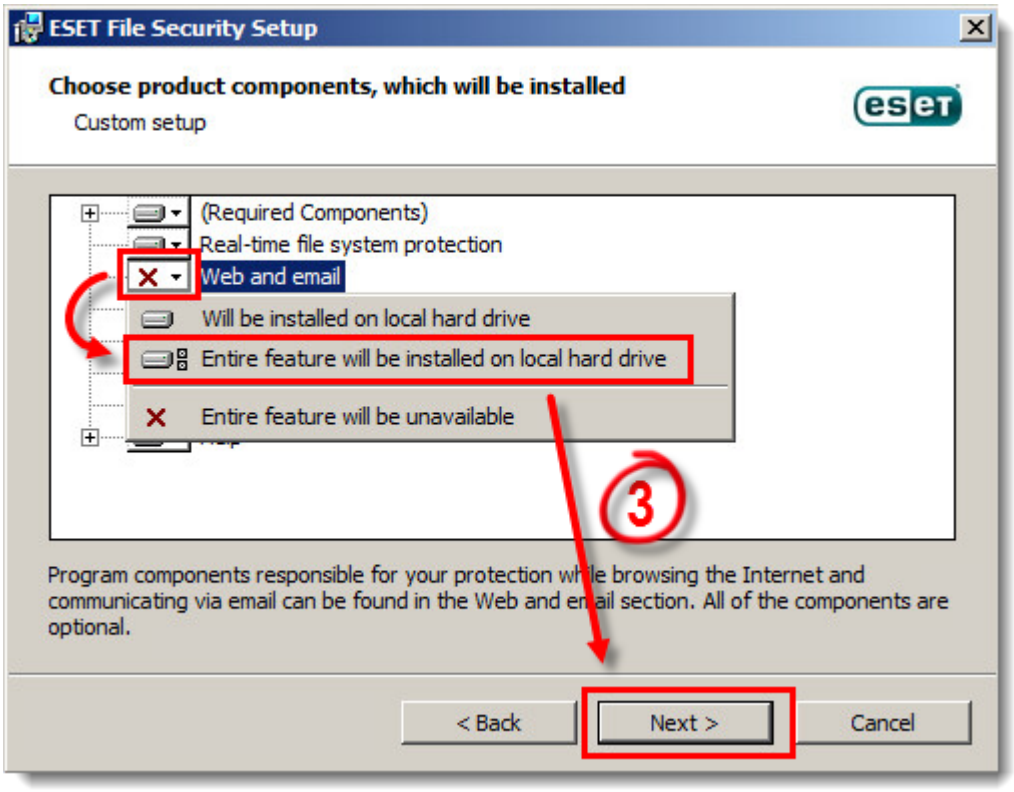

Figure 1-4

1. Click **Install**.

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.

Perform these steps using the ESET Remote Administrator

Applying the ESET Remote Administrator (ERA) policy "File Security for Windows Server – Visibility silent mode" will enable silent mode on any server assigned to that policy. This has the effect of running the command "set ui ui gui-start-mode minimal" locally (* see below for descriptions of each mode).

1. Click **Admin → Groups → Group**, or click the cogwheel icon next to the group name, and select **Manage Policies**.
2. In the **Policy application order** window, click **Add Policy**. Select the check box next to the policy select the policy "File Security for Windows Server – Visibility silent mode" and click **OK**.
3. Click **Save**.

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

To see what policies are assigned to a particular 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

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 you are using:

set ui ui gui-start-mode full

set ui ui gui-start-mode none

1. Open ESET Shell by clicking **Start → All Programs → ESET → ESET File Security** (for Windows Server 2012, type **ESET Shell** into the **Search** field).

2. Right-click **ESET Shell** and select **Run as administrator** from the context menu. If prompted, type in the username and password for the administrative account.

3. Type the letter "x" (without quotes) to skip the help section.

4. Type the following command:

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

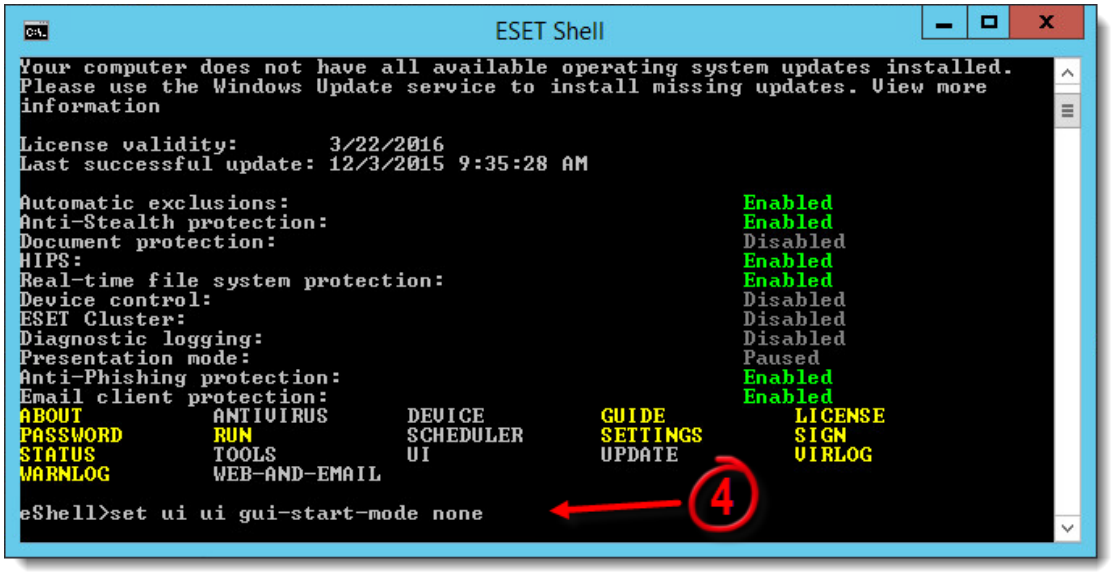

Figure 2-1

1. Press **Enter** and wait for the command to complete.

2. Close the window. Continue to part II below if you are using a Citrix server.

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

1. Open ESET File Security by clicking **Start → All Programs → ESET → ESET File Security → ESET File Security**.

2. Press **F5** to access Advanced setup.

3. Click **Real-time file system protection** from the main menu on the left and expand **Basic**.
4. Turn off the following four features by clicking the slider bars next to **Network drives**, **File open**, **File creation** and **Removable media access** and then click **OK**.

   Continue to part III below to add exclusions for a Citrix server.

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

III. (only Citrix servers) Add needed exclusions

1. Open ESET File Security by clicking **Start → All Programs → ESET → ESET File Security → ESET File Security**.

2. Press **F5** to access Advanced setup.

3. Click **Antivirus** from the main menu on the left, expand **Basic** and then click **Edit** in the **Exclusions** section.

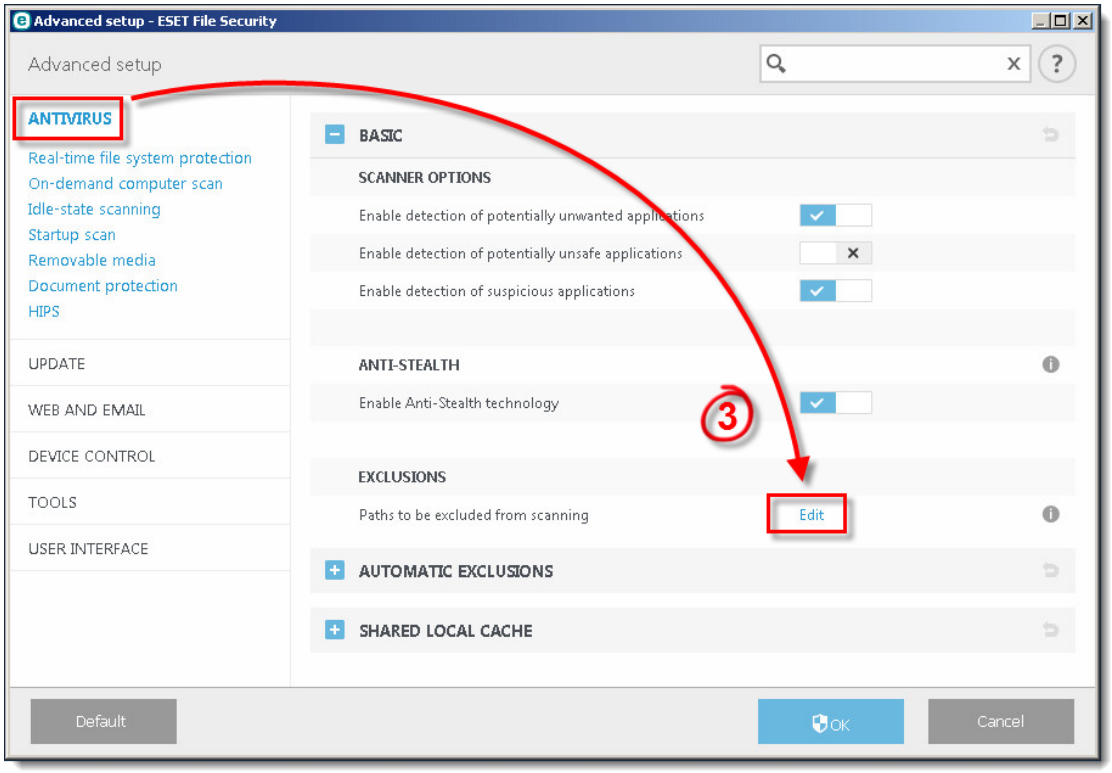

Figure 3-2

Click **Add** and exclude the following directory:
C:\Program Files\Citrix

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]

1. Click **OK** three times to save your changes.

- Tags
- File Security