Upgrade ESET Security Management Center 7.2 to the latest ESET PROTECT 8 via Web Console

Steef | ESET Nederland - 2021-01-14 - Comments (0) - Legacy

Issue

- Upgrade individual ESET Security Management Center components (Agent, Server) to the latest ESET PROTECT

Solution

Before you start

- **Linux users:** [KB7733] Upgrade ESET Remote Administrator 6.5 (and later) for Linux to the ESET PROTECT 8.

Prerequisites

Before upgrading to ESET PROTECT 8, make sure that you have met all ESET PROTECT 8 installation prerequisites.

Important recommendations before the upgrade

You must have ESET Remote Administrator (ERA) version 6.5 and later to upgrade to ESET PROTECT 8. Check which version of ESMC you have installed.

Upgrading from ESMC 7.0-7.1? ESET PROTECT Server component is not compatible with 32-bit machines (x86 architecture). Upgrading a 32-bit Server machine to ESET PROTECT 8 will fail.

- If you have already run the upgrade and now your system is not working, you need to manually reinstall all ESMC components to the original version.
- If you want to upgrade, you need to migrate your current ESMC to a 64-bit machine, and after successful migration, you can run the upgrade task.

If you have an older unsupported database installed (MySQL 5.5 or MSSQL 2008), upgrade your database to a compatible database version before upgrading the ESMC Server.

Perform a full backup of ESMC 7:

- **Database**: Follow [KB6725] Create a backup of the ESET Security Management Center database (7.x) to back up the ESMC database.
- **Configuration**: Copy the Startupconfiguration.ini file, located at: C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData
- **Certificates**: Export the Certification Authorities and Peer Certificates.
- **Mobile Device Connector**: If this component is used, copy the Startupconfiguration.ini located at: C:\ProgramData\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configuration.

The following steps will upgrade both ESMC components (Server, Console) and the ESET Management Agent(s). When upgrading to the latest version, your policies will be preserved. Update your ESMC Server first. Select a few client machines to use as a test for the update and run the task on them (use at least one client from each system/bit category).

Upgrade ESMC Server using the Components Upgrade task in the Web Console

Components Upgrade task may take some time to complete

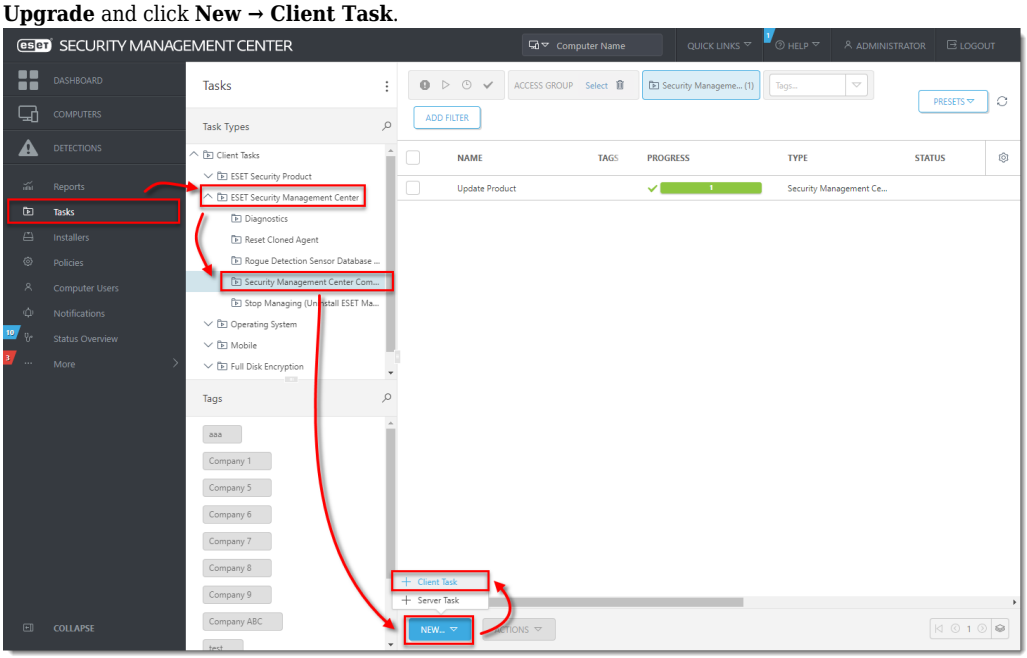
Please be patient during the Components Upgrade task process. It may take some time to complete. Do not restart your ESMC Server until the task has completed.

Special characters may cause upgrade to fail

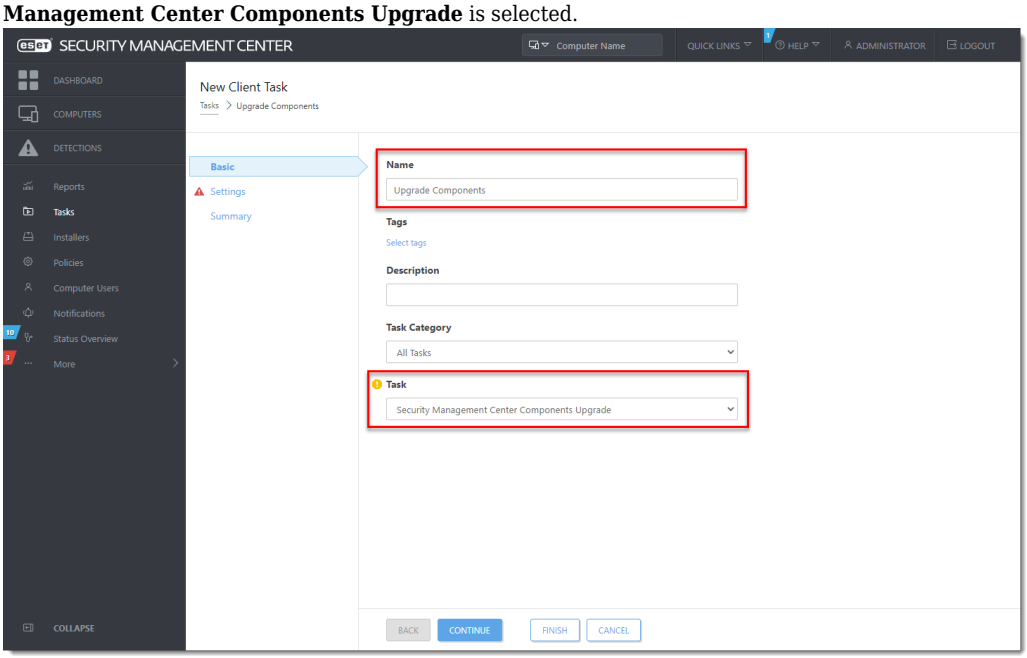
If you have met the requirements for upgrading and your upgrade to the latest version of ESET PROTECT fails, it could be due to the use of special characters in your ESMC password. To resolve this issue, change your ESMC Web Console password and attempt the upgrade again.

1. Open the ESET Security Management Center Web Console (7.x) (ESMC Web Console) in your web browser and log in.

2. Click **Tasks → ESET Security Management Center → Security Management Center Components Upgrade** and click **New → Client Task**.

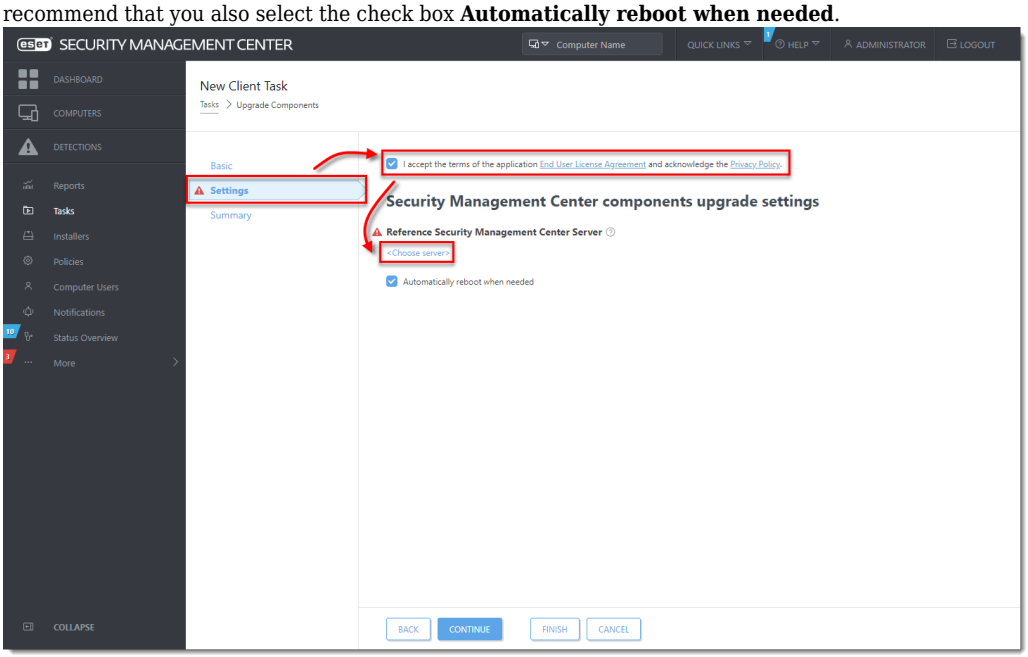


3. In the **Name** field, type a name for your task. In the **Task** drop-down menu, verify that **Security Management Center Components Upgrade** is selected.

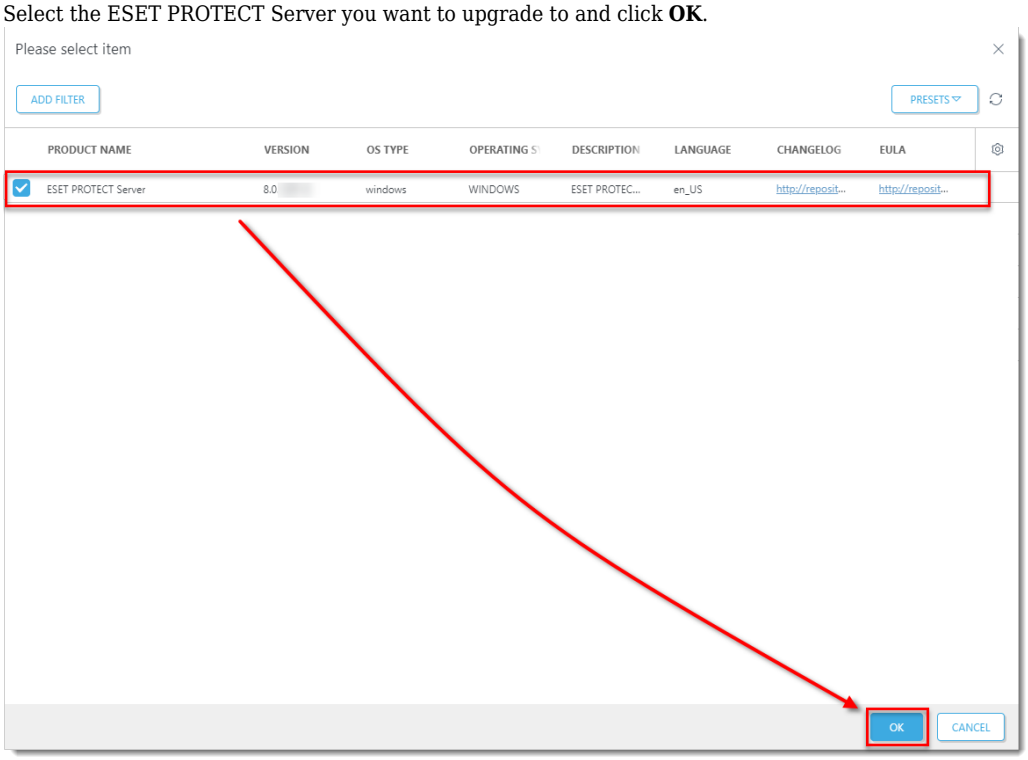


4. Click the **Settings** section, select the check box next to **I accept the terms of the application End User License Agreement and acknowledge the Privacy Policy** and then click **Choose server**. We

recommend that you also select the check box **Automatically reboot when needed**.



5. Select the ESET PROTECT Server you want to upgrade to and click **OK**.

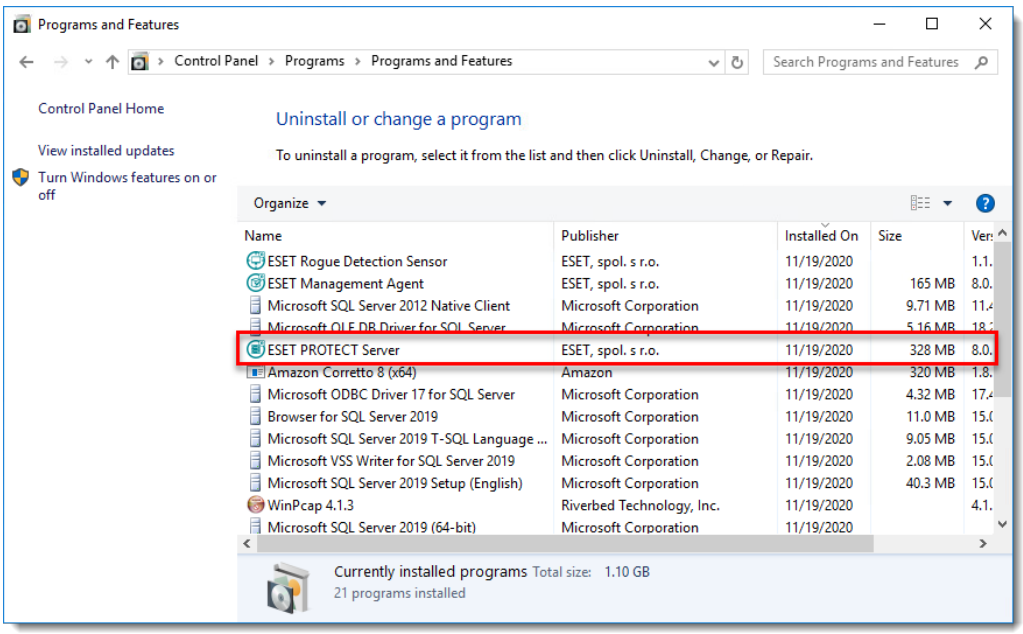


6. Click **Finish**.
7. Create a trigger and add the ESMC Server computer as a target to execute the task.

> **Do not add more target computers**
> Add only the computer where ESMC Server is installed as a target. Do not add more target computers at this point in the upgrade.

8. Wait a few minutes until all ESMC components installed on the server machine are upgraded. Apache Tomcat service can get turned off during the update. If the Web Console is unavailable after the update, open the services management (run `services.msc`) and **Start** the Apache Tomcat service.

9. To verify that your server upgraded to ESET PROTECT, check **Programs and Features** in the **Control Panel**. You will see **ESET PROTECT Server** listed as a program if it has been upgraded.



Upgrade ESET Management Agents on managed computers

When the task is finished on the ESET PROTECT Server machine, verify that the ESET PROTECT Server works properly. Wait an hour to see if any problems occur. Afterwards, you can upgrade Agents on the managed computers using the Components Upgrade task and selecting the static group **All** as its target. See the step-by-step guide.

If you are running a larger network, with hundreds or more client computers:

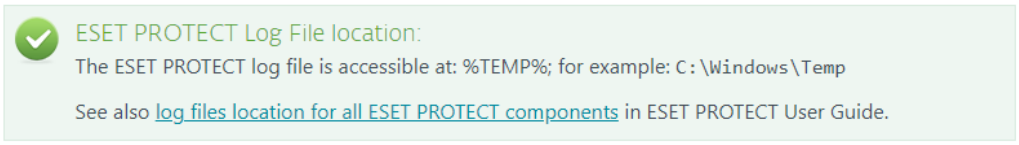
1. Choose a sample of clients for a test update (include at least one client for each operating system/bit category) and run the task.
2. We recommend using Apache HTTP Proxy (or any other transparent web proxy with enabled caching) to limit network load. The test client machines will trigger the download/caching of the installers. When the task is run again, the installers will be distributed to client computers directly from the cache.
3. After a successful test update, proceed with the rest of your clients. Alternatively, target the **All** group. The upgrade is not performed on computers that have already been upgraded.

If the Components Upgrade task is not working properly, try upgrading Agents using **Run Command** task.

Alternative method: Upgrade ESET Management Agent(s) using Run Command client task

This is an alternative method recommended for advanced users or if the **Components Upgrade** task is unsuccessful.

1. Create a new Dynamic Group based on the operating system (32-bit or 64-bit).
    - **For 32-bit systems:**
        - Operation "AND"
        - Add rule OS edition > OS platform = (equal) 32-bit
        - Add rule OS edition > OS type contains Windows
    - **For 64-bit systems:**
        - Operation "AND"
        - Add rule OS edition > OS platform = (equal) 64-bit
        - Add rule OS edition > OS type contains Windows
2. Create a new Client Task for 32-bit systems.



1. In the **Basic** section, select **Run Command** from the **Task** drop-down menu.
2. In the **Settings** section, in the **Command line to run** field, type: `msiexec /qn /i "\\SERVER\readonlyshare\Agent_x86.msi" /l*v! %TEMP%\era-agent-upgrade.txt`

   (replace `server` with your actual server name and `readonlyshare` with your share name).
   - When using the installer package via HTTP:

     ```
     msiexec /qn /i "http://SERVER/share/agent_x86.msi" /l*v!
     %TEMP%\era-agent-upgrade.txt

     msiexec /qn /i
     "http://repository.eset.com/v1/com/eset/apps/business/era/agent/v8/
     8.0.1238.0/agent_x86.msi" /l*v! %TEMP%\era-agent-upgrade.txt
     ```
3. **Create Trigger** for this Client Task and in the **Targets** section, select the dynamic group for 32-bit operating systems created in Step 1.

3. Create a new Client Task for 64-bit systems.
   1. In the **Basic** section, select **Run Command** from the **Task** drop-down menu.
   2. In the **Settings** section, in the **Command line to run** field, type: `msiexec /qn /i "\\SERVER\readonlyshare\Agent_x64.msi" /l*v! %TEMP%\era-agent-upgrade.txt`

      (replace `server` with your actual server name and `readonlyshare` with your share name).
      - When using the installer package via HTTP:

        ```
        msiexec /qn /i "http://SERVER/share/agent_x64.msi" /l*v!
        %TEMP%\era-agent-upgrade.txt

        msiexec /qn /i
        "http://repository.eset.com/v1/com/eset/apps/business/era/agent/v8/
        8.0.1238.0/agent_x64.msi" /l*v! %TEMP%\era-agent-upgrade.txt
        ```
   3. **Create Trigger** for this Client Task and in the **Targets** section, select the dynamic group for 64-bit operating systems created in Step 1.
4. To view client task details, click **Computers**, select the applicable client computer, click **Show Details** and then click **Installed Applications**.

   There will be a brief period where two versions of Agent are running on a single client machine. This is only temporary. Create an Outdated applications report to monitor the status of client computers hourly.