Deploy the ESET Management Agent via SCCM or GPO (8.x)

Steef | ESET Nederland - 2021-04-30 - Comments (0) - Legacy

Issue

- Prepare the ESET Management Agent installer file for distribution via Group Policy Object (GPO) or System Center Configuration Manager (SCCM)
- Alternative method to distribute ESET Management Agent for enterprise environments or environments with a high number of client computers
- Download installer
- Use GPO or SCCM for deployment

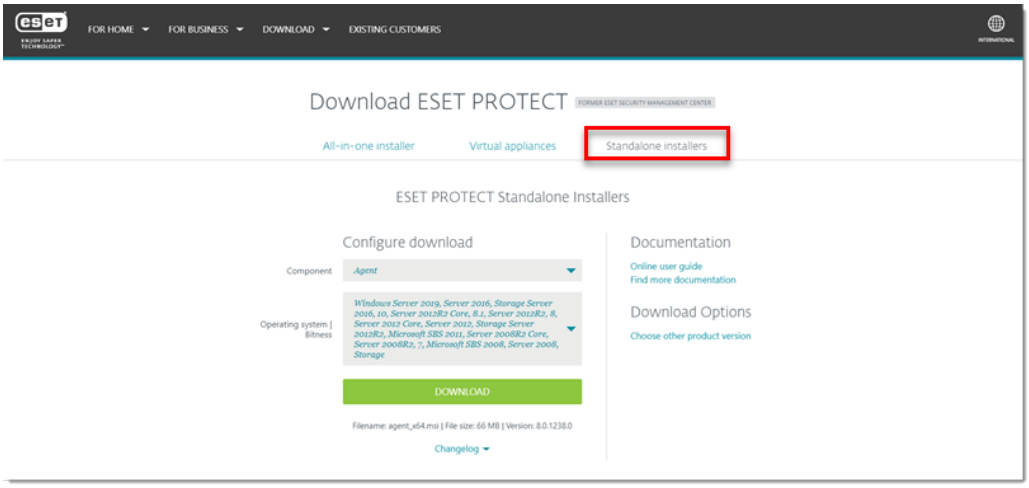
Details

Create a modified version of the ESET Management Agent Installer file for distribution in large to enterprise-level environments. The .msi file for the ESET Management Agent is separated from the .bat file available from ESET PROTECT and then modified so that it will be able to recognize the proper certificate and port for communication with your ESET PROTECT Server after distribution to client computers.

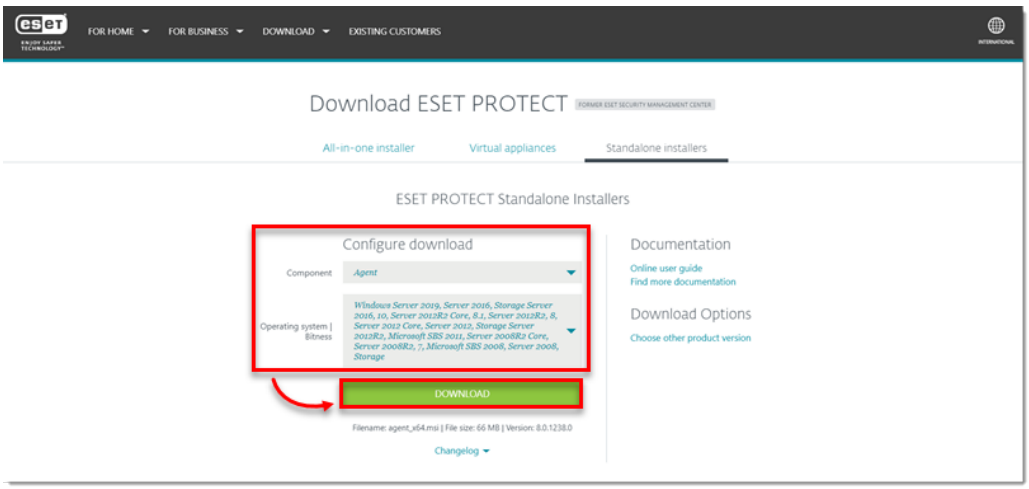
Download Installer

Peer certificates and Certification Authority created during the installation are by default contained in the static group All.

1. On your ESET PROTECT Server, go to the ESET PROTECT 8 Download page and click **Standalone installers.**



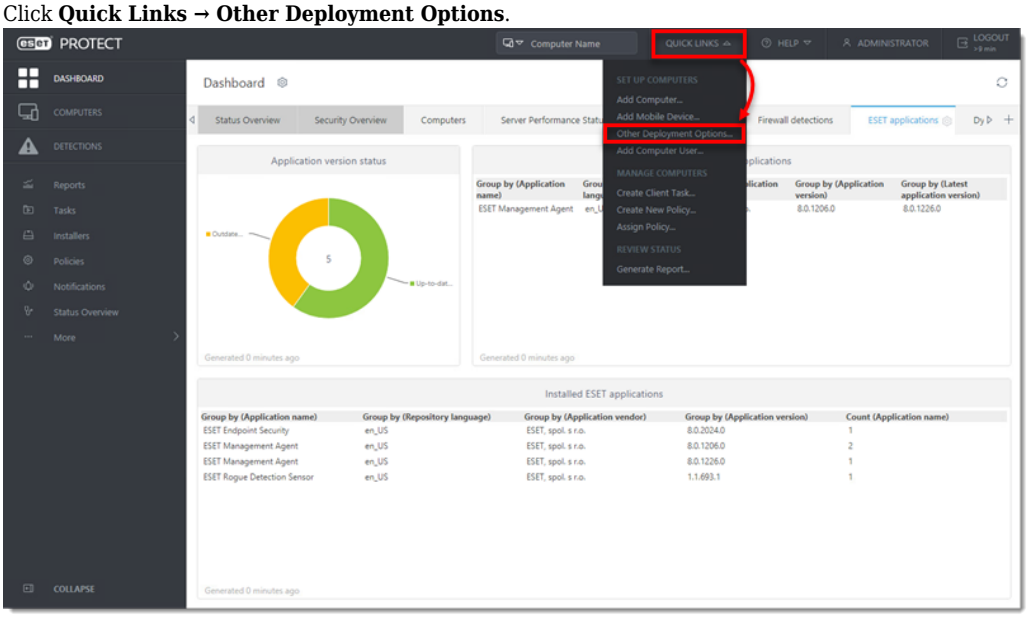
2. In the **Configure download** section, beside **Component:** select **Agent**, and beside **Operating system | Bitness:** select a 32-bit or 64-bit Windows operating system. Click **Download**.



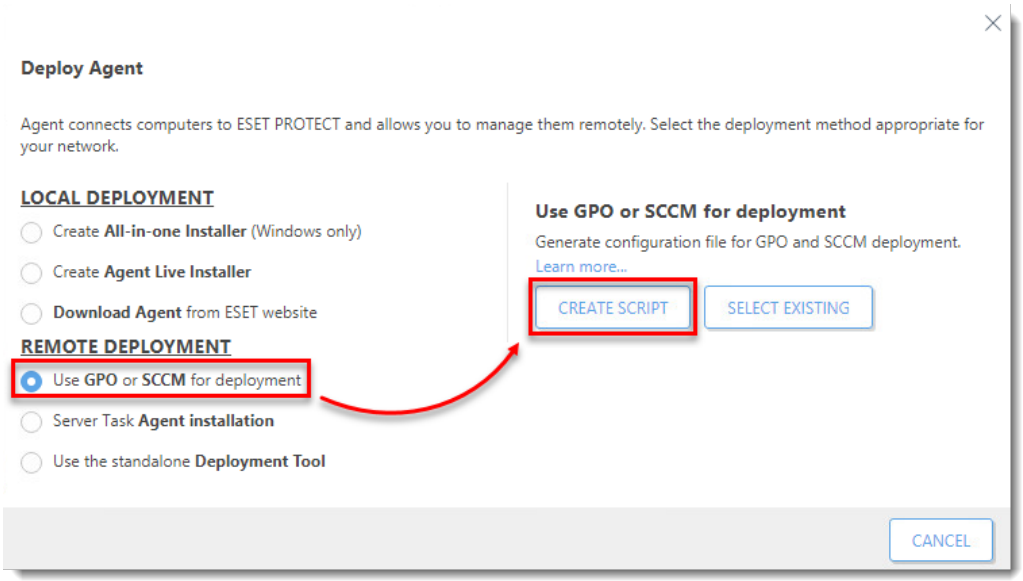
3. Save the ESET Management Agent installer **`.msi`file to a shared folder your client computers can access.**

Use GPO or SCCM for deployment

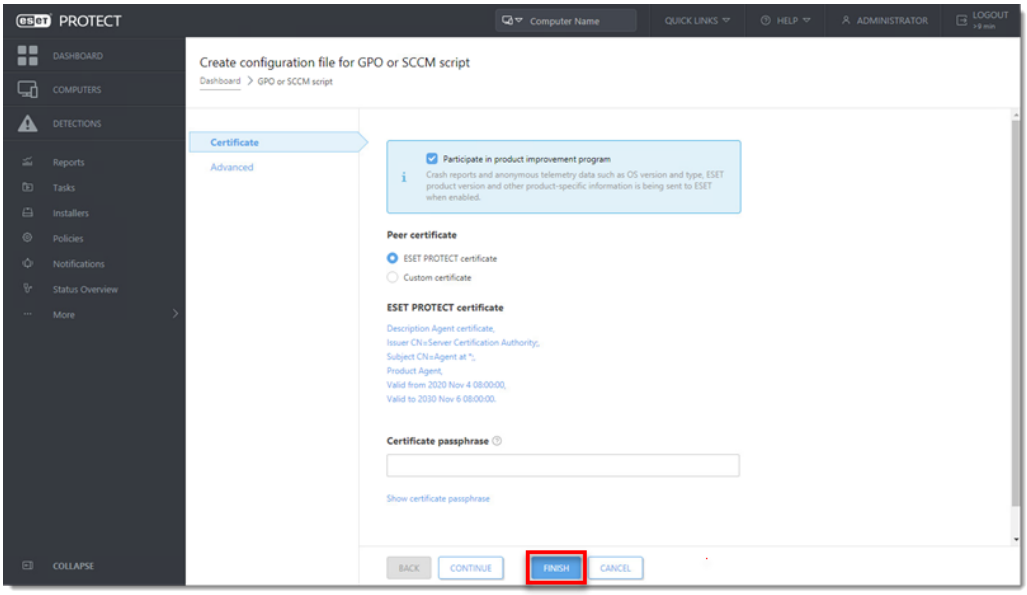
1. Open ESET PROTECT Web Console in your web browser and log in.
2. Click **Quick Links → Other Deployment Options**.



3. Click **Use GPO or SCCM for deployment** and click **Create Script**.



4. Click **Finish**. Save the `install_config.ini` file to the same shared folder from Step 2. For customers using custom certificates, refer to the Custom certificates with ESET PROTECT Online Help topic for more details.



Install_config.ini filename dependency

Do not change the name of the install_config.ini file. The .msi will look for this filename specifically when trying to configure the agent during the install. If it's not there because the name was changed, the agent will complete its install without configurations & certificates!

Client computers need read/execute access

Verify all appropriate client computers have read/execute access to the folder containing the `.msi` and `.ini` files. Right-click the folder from Step 2 and click **Properties**. Click the **Security** tab. Review each machine and confirm the check box next to **Read & execute** is selected under the **Allow** column. If not, click **Edit**, adjust the settings and click **Apply**.

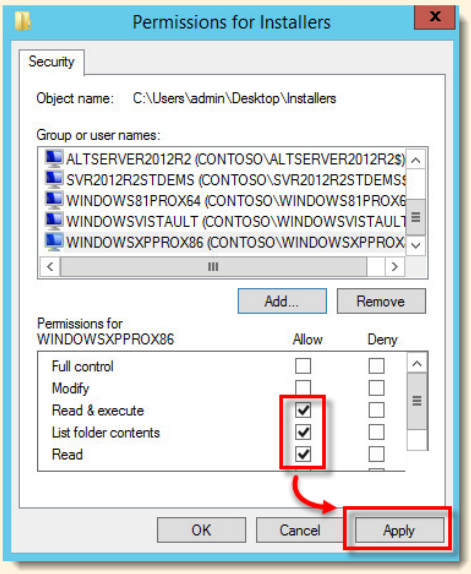


Figure 2-4

5. Refer to one of the processes below to deploy the package:
   - Deploy the ESET Management Agent using a Group Policy Object (GPO)
   - Deploy the ESET Management Agent using System Center Configuration Manager (SCCM)
6. Once you have completed the instructions from the appropriate article, proceed to Step 5, deploy ESET endpoint products to your client computers if you are performing a new installation of ESET PROTECT.