ESET Tech Center

Deploy the ESET Management Agent via SCCM or GPO (8.x – 9.x)

Mitch | ESET Nederland - 2025-03-06 - Comments (0) - ESET PROTECT On-prem

Issue

- Configure the ESET Management Agent installer file for deployment via Group Policy Object (GPO) or System Center Configuration Manager (SCCM)
- Configure an alternative method to deploy the ESET Management Agent for enterprise environments or environments with a high number of client computers
- Use GPO or SCCM for deployment

Details

Create a modified version of the ESET Management Agent installer file for deployment in large to enterprise-level environments. The .msi file for the ESET Management Agent is separated from the .bat file available from ESET PROTECT. The .msi file is 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.

Solution

Getting Started with ESET PROTECT: Step 4 of 6

← Add Client Computers | Deploy ESET endpoint solutions →

Use GPO or SCCM for deployment

1. Open the **ESET PROTECT Web Console** in your web browser and log in.
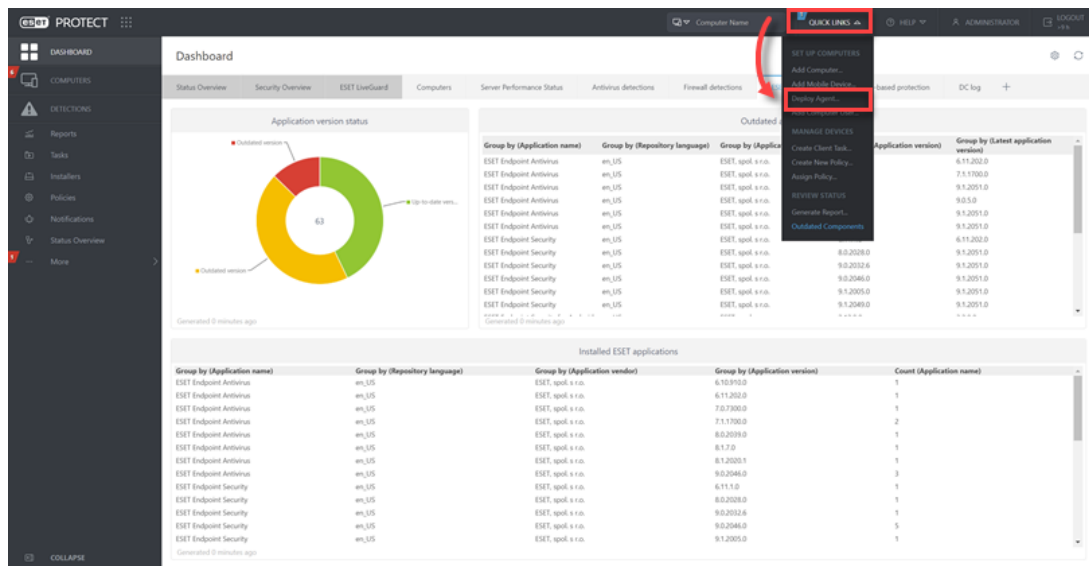
2. Click **Quick Links → Deploy Agent**.

Figure 1-1

3. Confirm the Windows operating system is selected, select **Use GPO or SCCM for deployment** next to **Distribution** and scroll down.
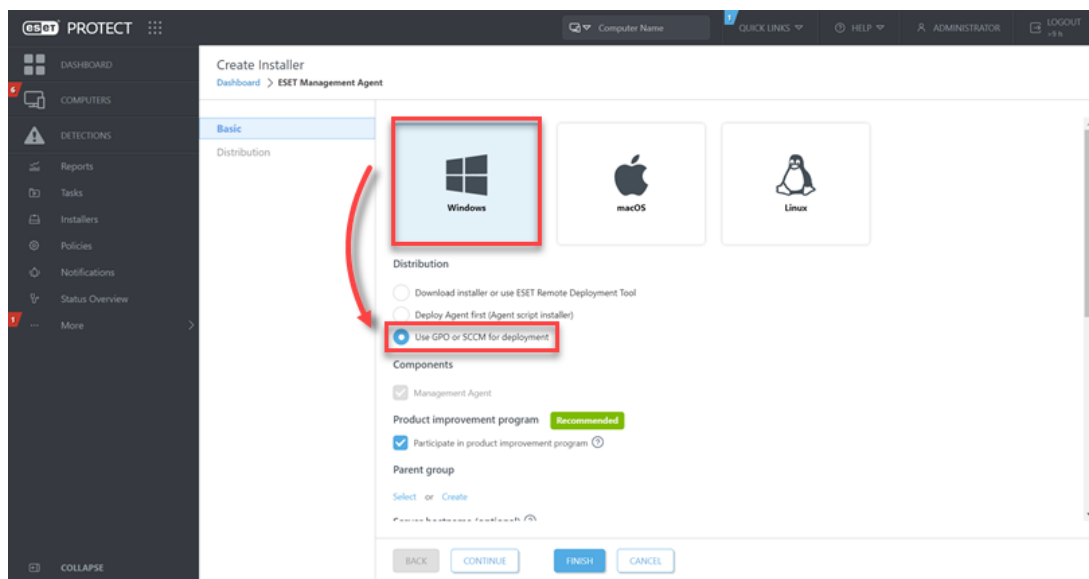

Figure 1-2

4. Click **Finish**. The **ESET PROTECT certificate** is selected by default. For **custom certificate** users, refer to the custom certificates with ESET PROTECT Online Help topic for more details. Peer certificates and Certification Authority created during the installation are by default contained in the static group labeled **All**.
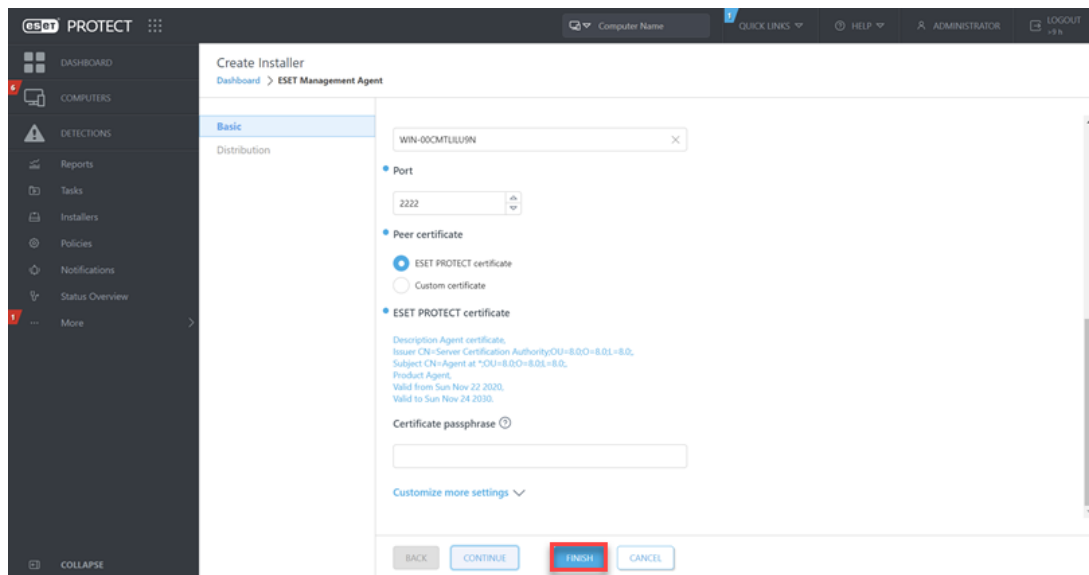
Figure 1-3

5. Click the file icon to download the `install_config.ini` file. Click the desired agent installer icon (**32-bit-64-bit, ARM64**) to download the agent installer `.msi` file and save them to the same shared folder.

> **ESET PROTECT 9.0 and earlier users**
> Download the agent installer `.msi` file in the **Standalone Installers** section from the ESET PROTECT Download page. Select **Agent** from the **Component** drop-down menu, then select a **32-bit** or **64-bit** Windows operating system from the **Operating system | Bitness** drop-down menu and click **Download**.
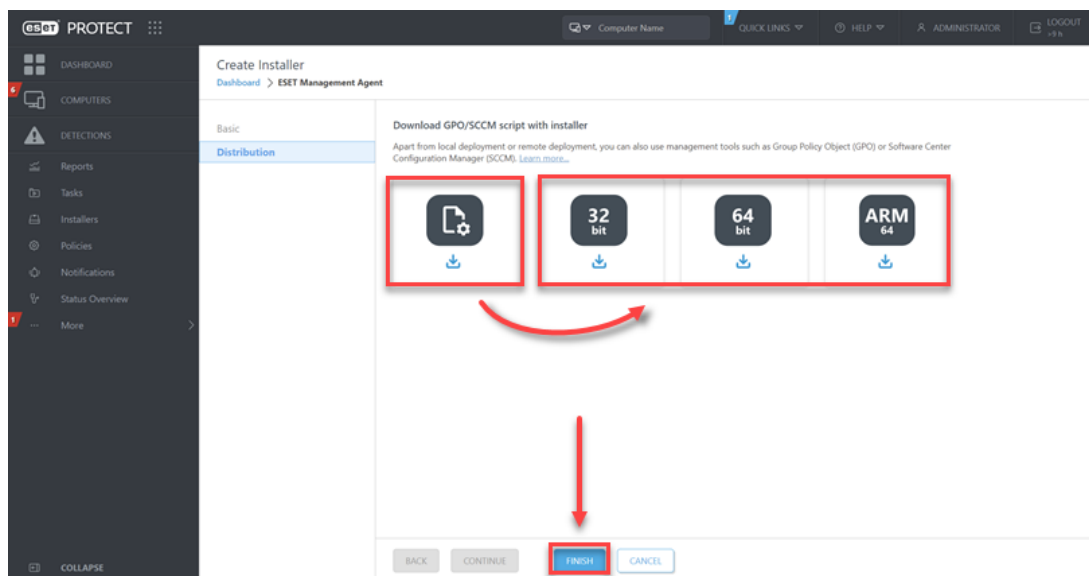

Figure 1-4

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 section 1, 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**.
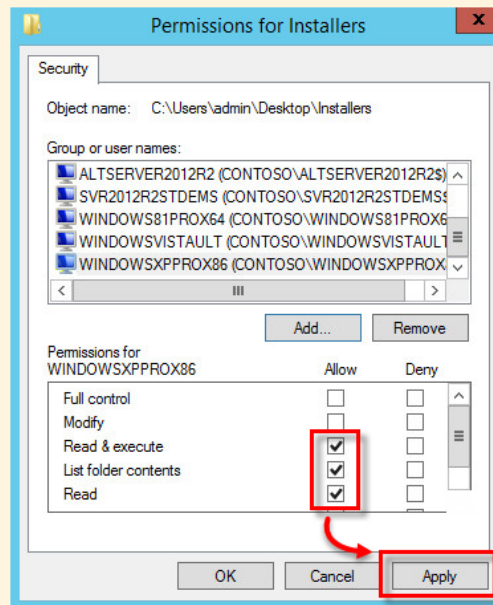
Figure 1-5

6. 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)

7. When 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.