ESET Tech Center

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

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

Steef | ESET Nederland - 2021-04-30 - Reacties (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

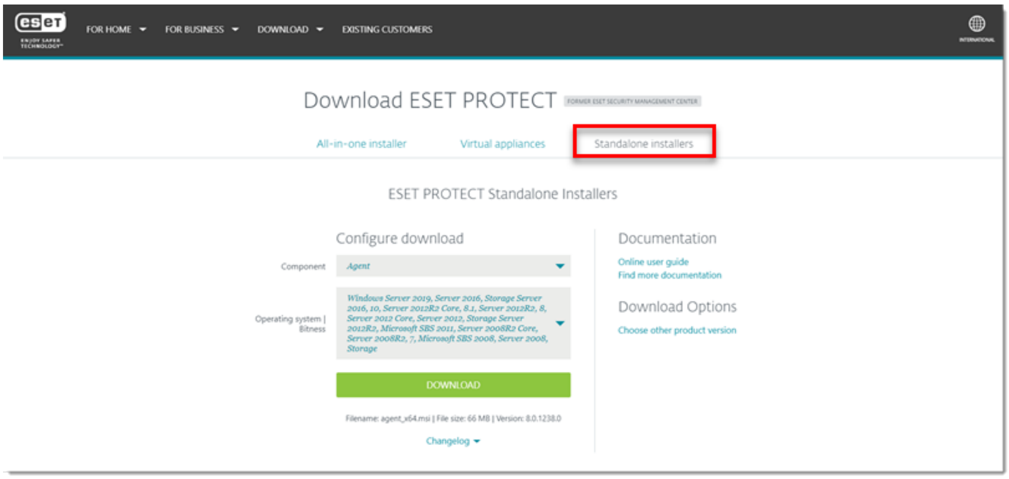
Details

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.**

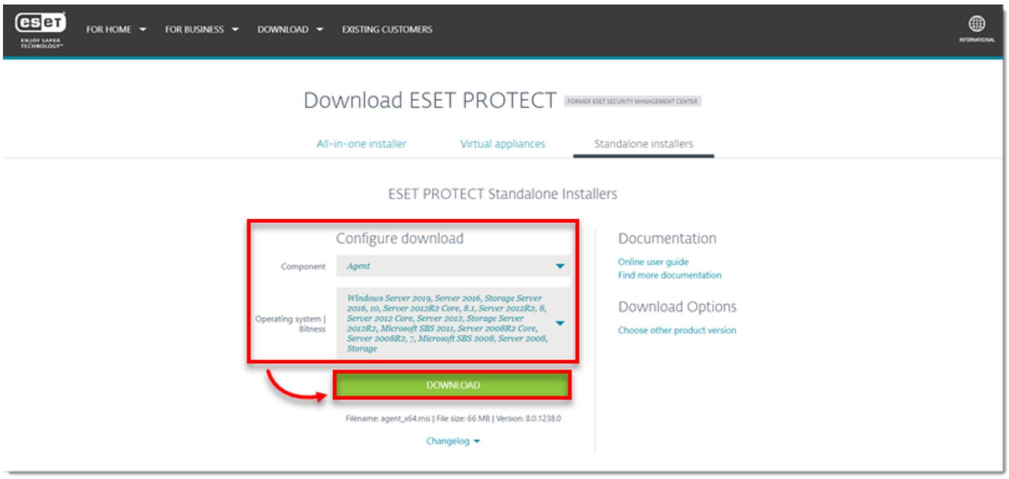


Component: Agent

Operating system | Bitness: Windows Server 2019, Server 2016, Storage Server 2016, 10, Server 2012R2 Core, 8.1, Server 2012R2, 8, Server 2012 Core, Server 2012, Storage Server 2012R2, Microsoft SBS 2011, Server 2008R2 Core, Server 2008R2, 7, Microsoft SBS 2008, Server 2008, Storage

Filename: agent_x64.msi | File size: 66 MB | Version: 8.0.1238.0

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**.



Component: Agent

Operating system | Bitness: Windows Server 2019, Server 2016, Storage Server 2016, 10, Server 2012R2 Core, 8.1, Server 2012R2, 8, Server 2012 Core, Server 2012, Storage Server 2012R2, Microsoft SBS 2011, Server 2008R2 Core, Server 2008R2, 7, Microsoft SBS 2008, Server 2008, Storage

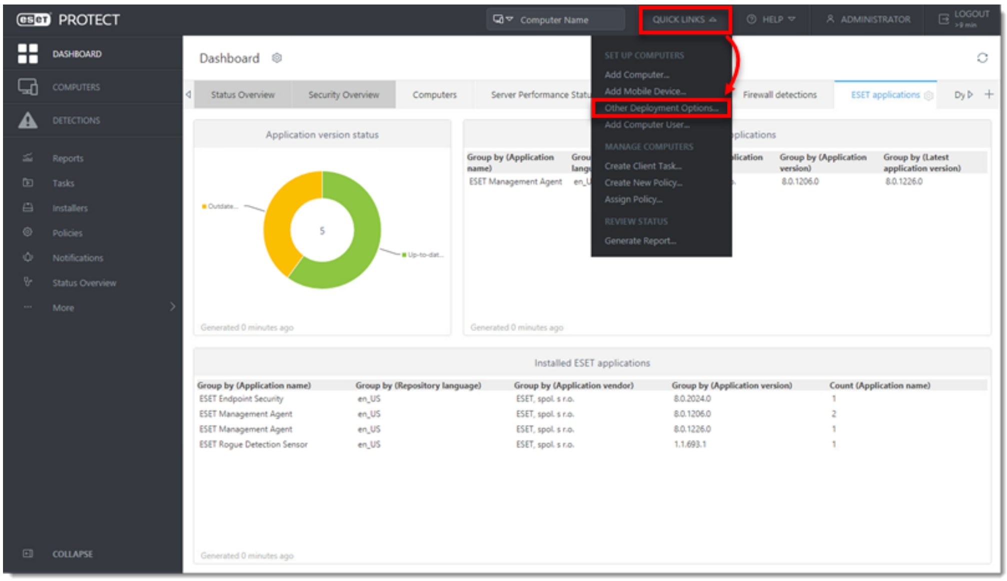
Filename: agent_x64.msi | File size: 66 MB | Version: 8.0.1238.0

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

Use GPO or SCCM for deployment

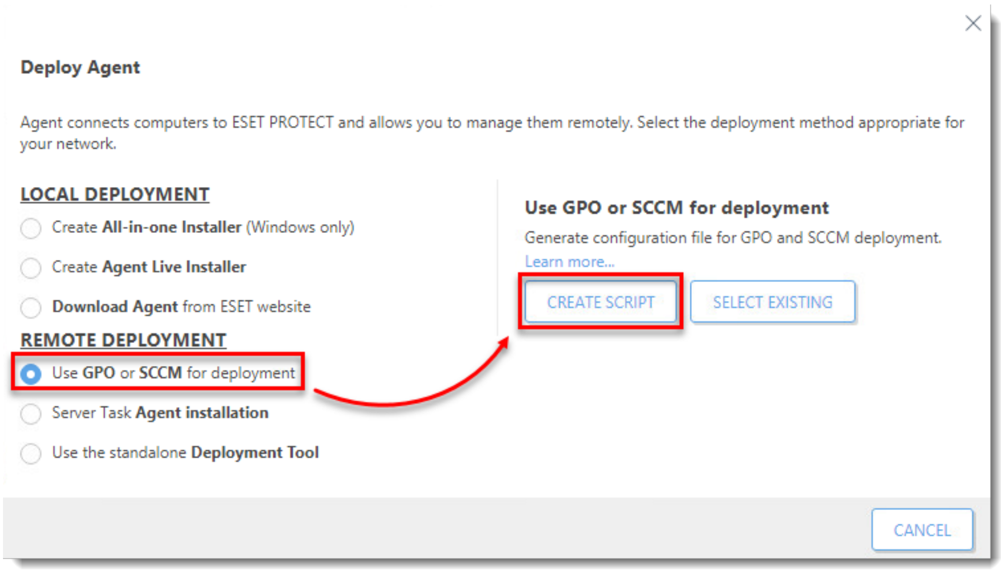
1. Open ESET PROTECT Web Console in your web browser and log in.

2. Click **Quick Links → Other Deployment Options**.



Group by (Application name)	Group by (Repository language)	Group by (Application vendor)	Group by (Application version)	Count (Application name)
ESET Endpoint Security	en_US	ESET, spol. s r.o.	8.0.2024.0	1
ESET Management Agent	en_US	ESET, spol. s r.o.	8.0.1206.0	2
ESET Management Agent	en_US	ESET, spol. s r.o.	8.0.1226.0	1
ESET Rogue Detection Sensor	en_US	ESET, spol. s r.o.	1.1.693.1	1

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



Deploy Agent

Agent connects computers to ESET PROTECT and allows you to manage them remotely. Select the deployment method appropriate for your network.

LOCAL DEPLOYMENT

○ Create **All-in-one Installer** (Windows only)

○ Create **Agent Live Installer**

○ **Download Agent** from ESET website

REMOTE DEPLOYMENT

● Use **GPO** or **SCCM** for deployment

○ Server Task **Agent installation**

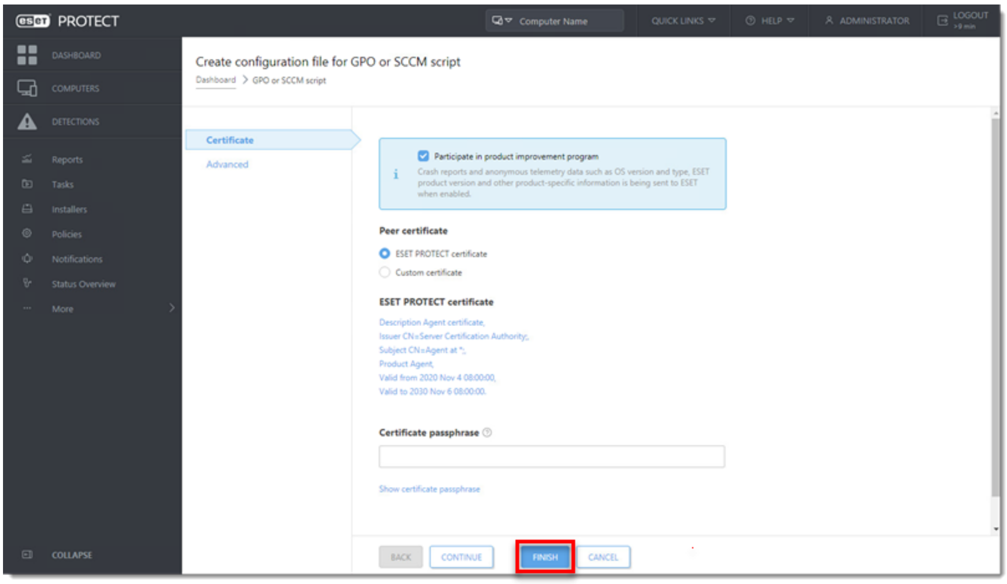
○ Use the standalone **Deployment Tool**

Use GPO or SCCM for deployment

Generate configuration file for GPO and SCCM deployment.

Learn more...

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.



Create configuration file for GPO or SCCM script

☑ Participate in product improvement program

Crash reports and anonymous telemetry data such as OS version and type, ESET product version and other product-specific information is being sent to ESET when enabled.

Peer certificate

● ESET PROTECT certificate

○ Custom certificate

ESET PROTECT certificate

Description Agent certificate,
Issuer CN=Server Certification Authority;,
Subject CN=Agent at *;,
Product Agent,
Valid from 2020 Nov 4 08:00:00,
Valid to 2030 Nov 6 08:00:00.

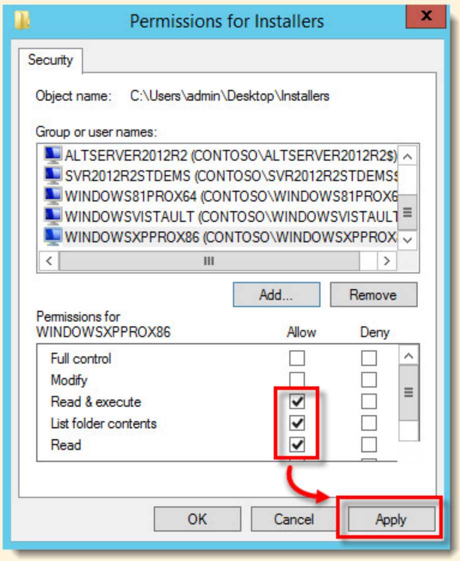
Certificate passphrase

Show certificate passphrase

> **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**.



Object name: C:\Users\admin\Desktop\Installers

Group or user names:

- ALTSERVER2012R2 (CONTOSO\ALTSERVER2012R2$)
- SVR2012R2STDEMS (CONTOSO\SVR2012R2STDEMS
- WINDOWS81PROX64 (CONTOSO\WINDOWS81PROX6
- WINDOWSVISTAULT (CONTOSO\WINDOWSVISTAULT
- WINDOWSXPPROX86 (CONTOSO\WINDOWSXPPROX

Permissions for WINDOWSXPPROX86	Allow	Deny
Full control	☐	☐
Modify	☐	☐
Read & execute	☑	☐
List folder contents	☑	☐
Read	☑	☐

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.