Download the ESET Management Agent from the ESET website (8.x – 9.x)

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

Issue

- Install ESET Management Agent on all client computers with ESET PROTECT components or ESET Endpoint products
- Facilitate communication between client computers and other ESET PROTECT components such as the ESET PROTECT Server

Solution

1. On the client workstation, go to the ESET PROTECT Standalone installers download page.

2. In the **Configure download** section, select the information below and then click **Download**.

- **ESET PROTECT component:** Select **Agent**
- **Operating system and Bitness:** Select the operating system of the client

> Supported operating systems for ESET Management Agent
> Some older operating systems may not be supported with the latest version of the ESET Management Agent. See our related article for information on how to download an earlier version of the ESET Management Agent.

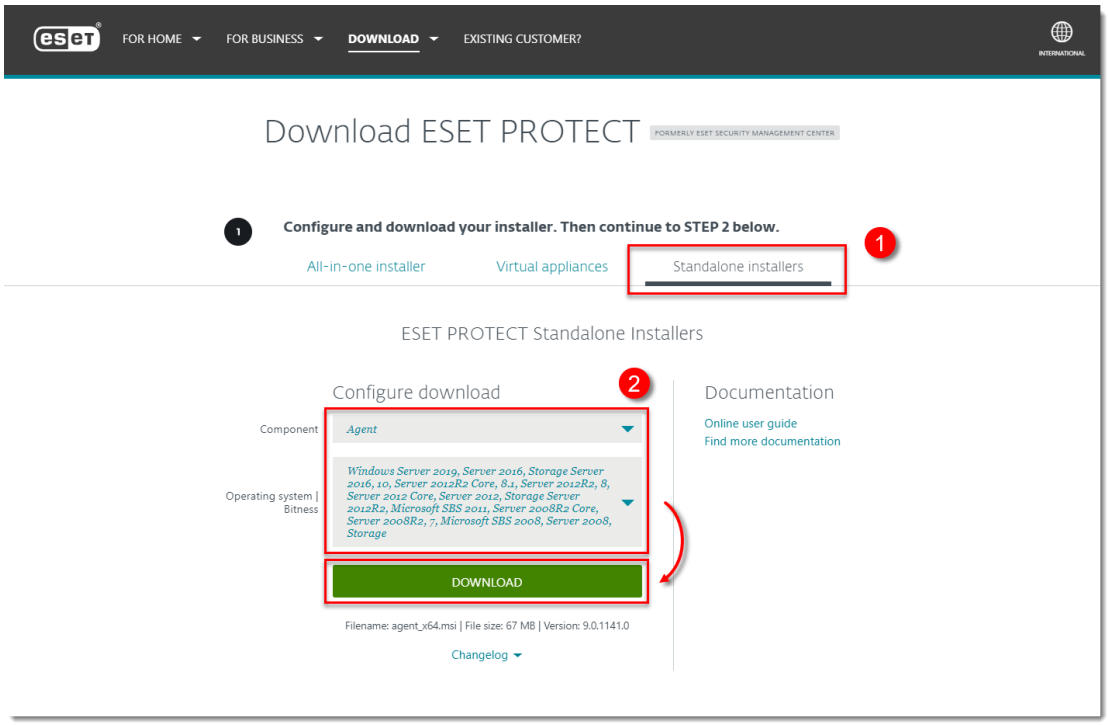

Figure 1-1

3. Double-click the downloaded .msi file and click **Next** to continue to the Setup Wizard.

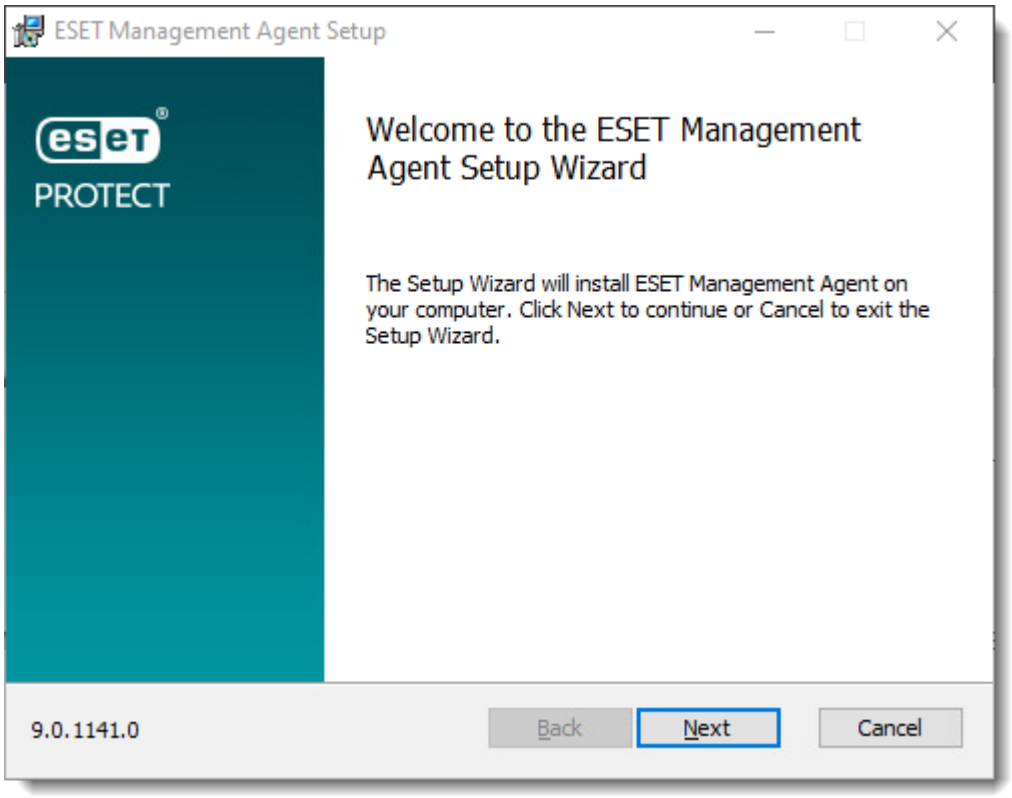

Figure 1-2

4. Select **I accept the terms of the License Agreement** and click **Next**.

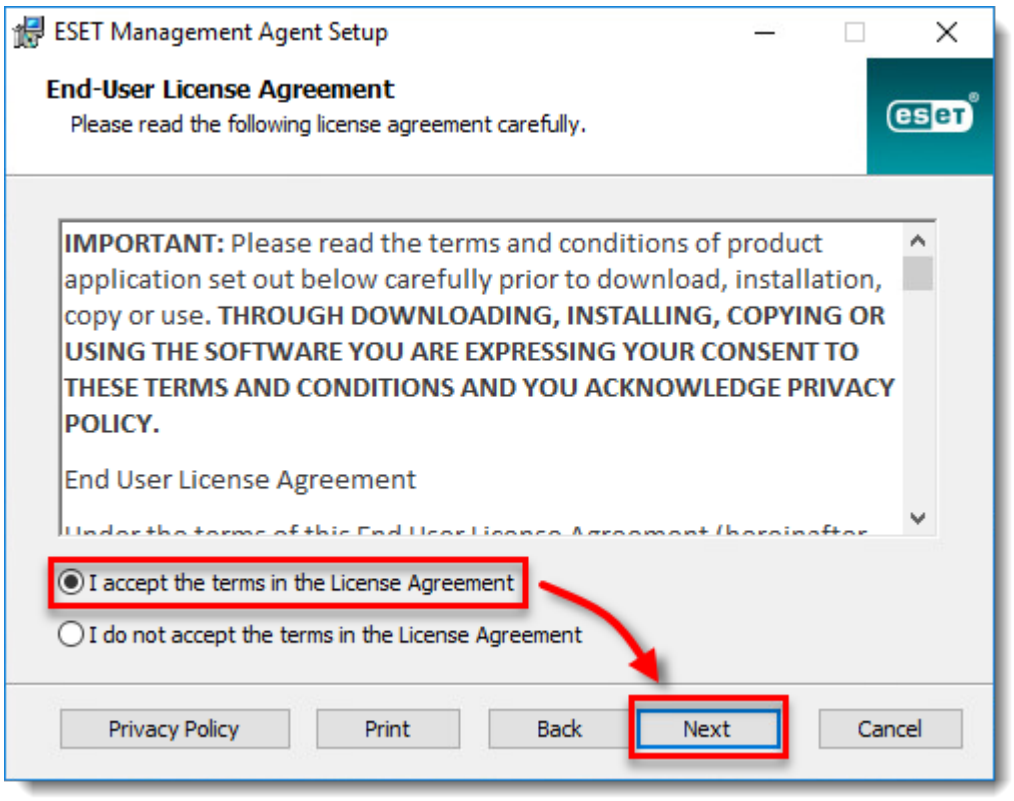

Figure 1-3

5. Click **Next** to agree to send crash reports and telemetry data to ESET. If you do not agree, deselect the check box next to **Participate in product improvement program**.

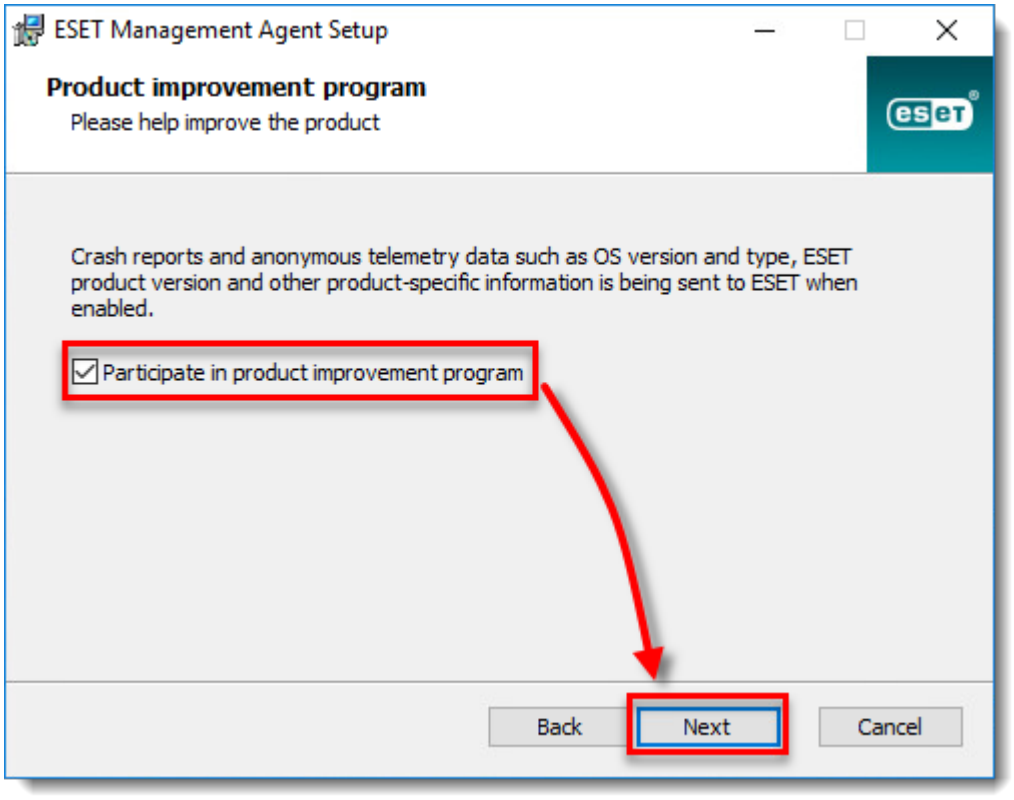

Figure 1-4

6. Specify the **Server host** (name or IP address) and **Server port** of your ESET PROTECT Server (the default Server port is 2222). If you are using a different port, replace the default port with your custom port number. If you use a proxy for Agent - Server connection, you can configure this connection after selecting the check box **Use Proxy**.

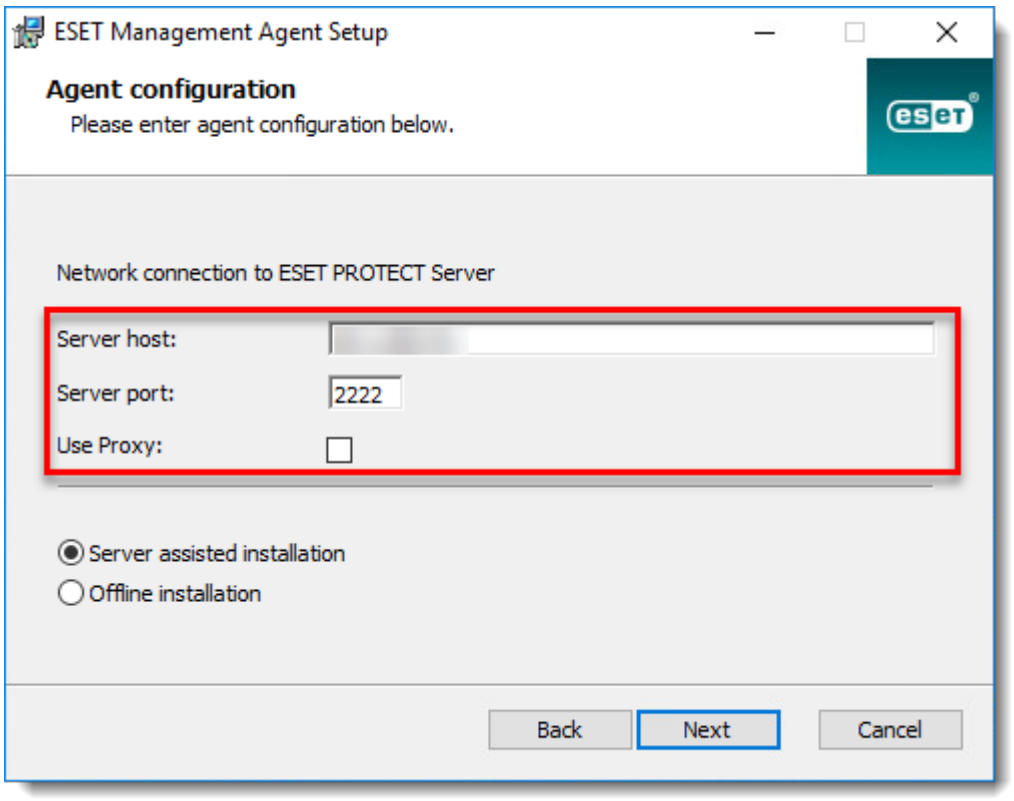

Figure 1-5

7. Select the type of installation you want to perform:

Server-assisted installation

Do not use a user with two-factor authentication

You cannot use a user with two-factor authentication for server-assisted installations.

To install ESET Management agent on a computer with a user with two-factor authentication, allow Server-assisted installation by another user and make sure the user has following permissions:

- **Use** permission for the **Certification Authority** that signed the server peer certificate and **Use** permission for at least one peer certificate. If no such certificate exists, the user will need **Write** permission to create a new one.
- **Write** permission for the static group where the user wants to add the computer.

For more information, see the Online Help topic.

Your client computer must be able to communicate with ESET PROTECT Server over the network.

a. Select **Server assisted installation** and click **Next**.

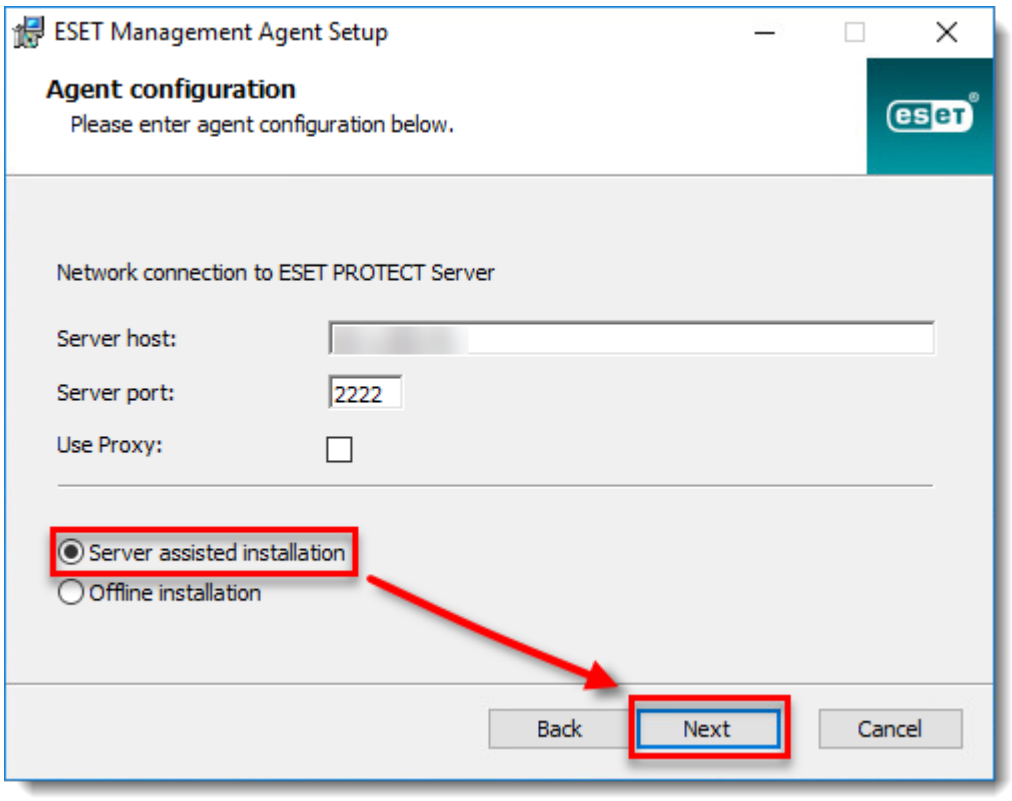

Figure 1-6

b. Enter the **Username** and **Password** used to access your ESET PROTECT Web Console to allow the Agent to download updates and new certificates. To log in as a domain user, select the check box next to **Log Into Domain**. Click **Next** and then click **Yes** to accept the server certificate.

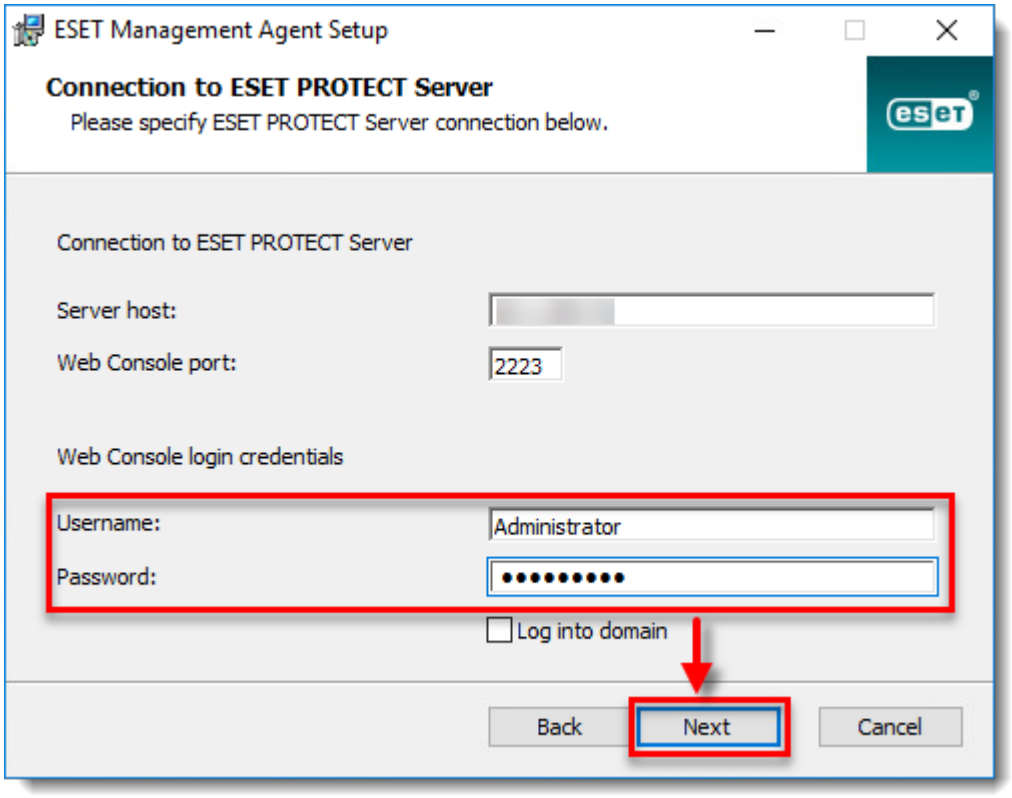

Figure 1-7

c. Select **Do not create computer (computer will be created automatically during the first connection)**

or **Choose custom static group**. If you click **Choose custom static group** you will be able to select from a list of existing Static groups in ESET PROTECT. The computer will be added to the group you have selected. Click **Choose custom static group** and use the drop-down menu to select the appropriate static group for the client computer.

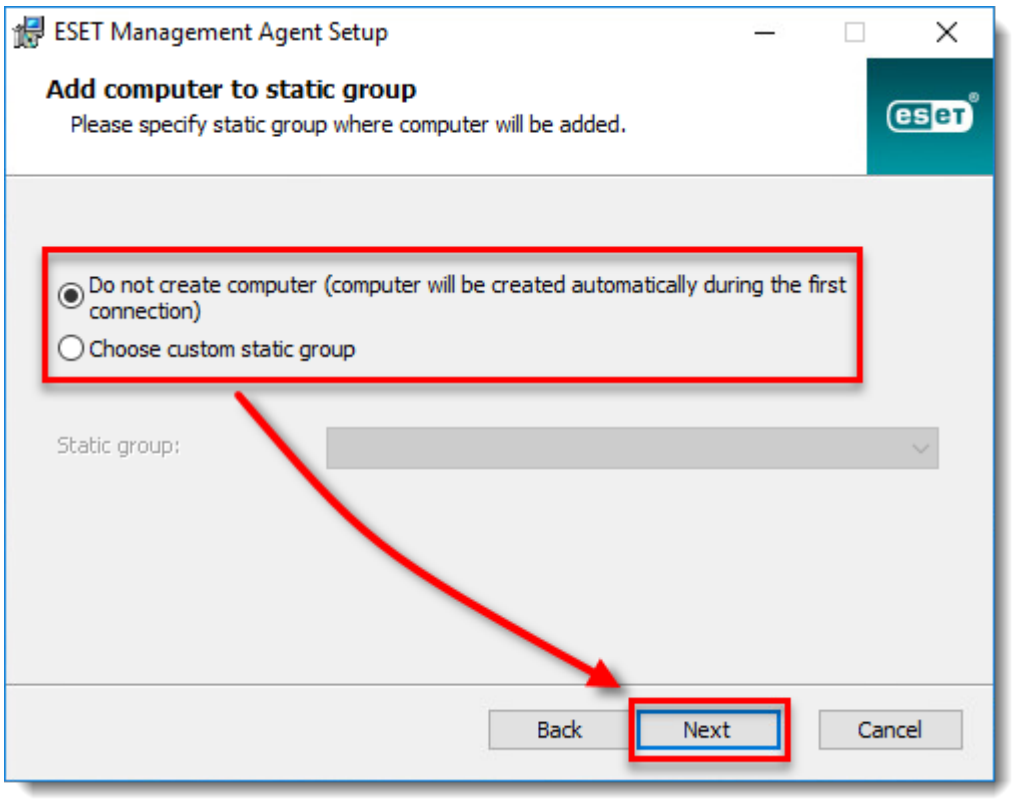

Figure 1-8

Offline installation

Your client computer is unable to communicate with the ESET PROTECT Server. Before performing an offline installation, verify you have the Agent certificate available on the targeted client computer.

Default certificates
Peer certificates and Certification Authority that are created during installation are, by default, contained in the Static Group All.

a. Select **Offline installation** and click **Next**.

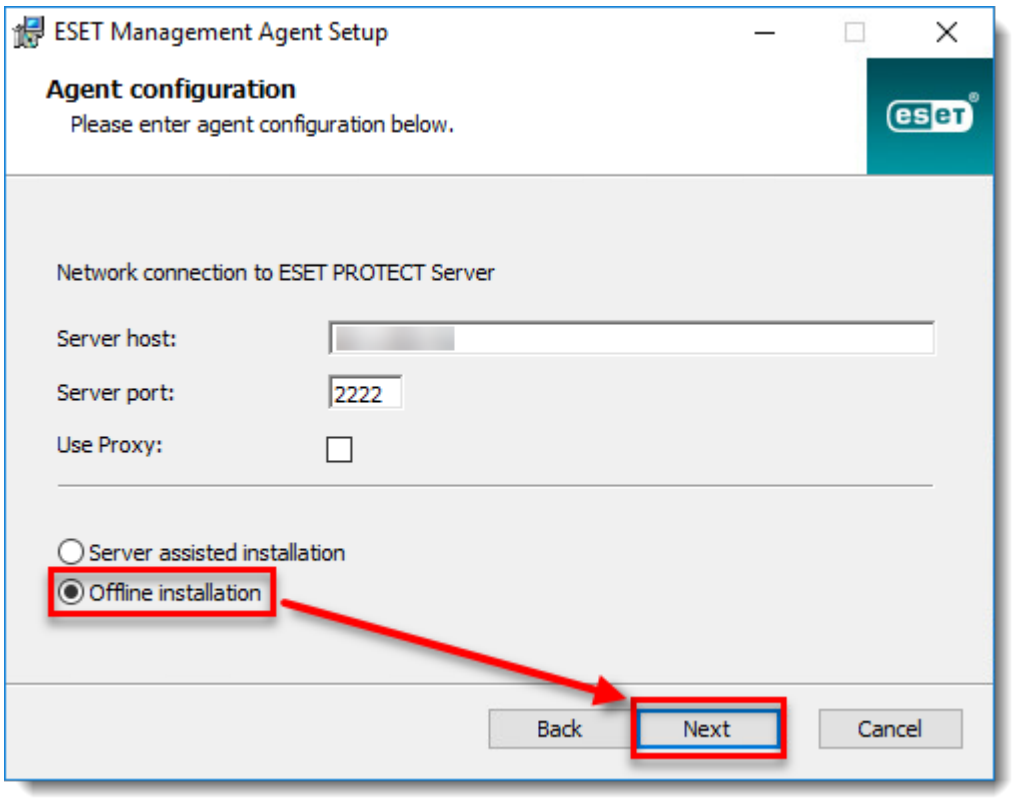

Figure 1-9

b. Open the ESET PROTECT Web Console in your web browser and log in. Click **More** → **Peer Certificates**. Select the certificate you want to use for this installation and click **Export**. Transfer the exported certificate to the client computer using removable media or another method of your choice.

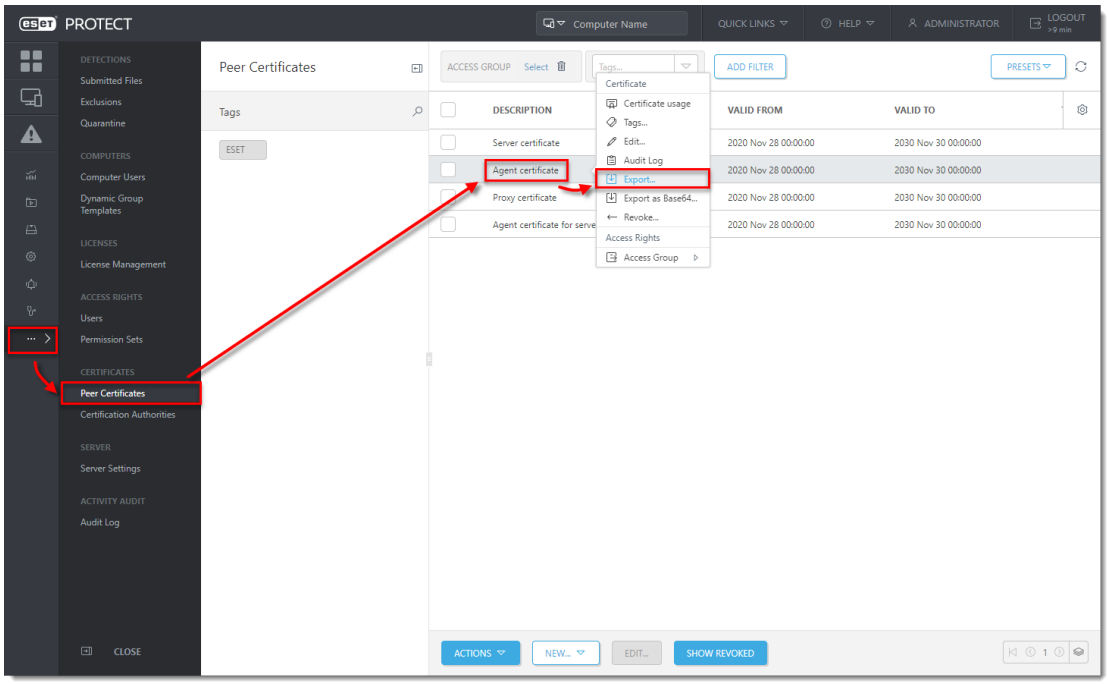

Figure 1-10

c. Click **More** → **Certification Authorities**. Select the **Certification Authority** and click **Export Public Key**. Transfer the exported CA to the client computer.

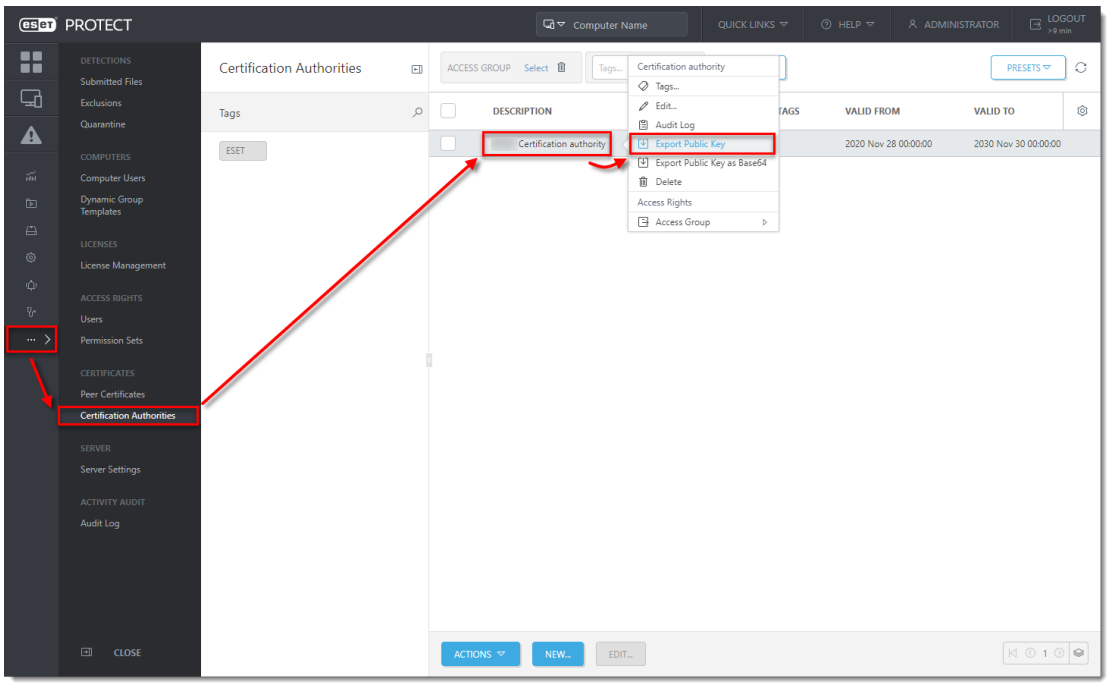

Figure 1-11

d. In the Agent Setup Wizard, click **Browse** next to **Peer certificate**. Navigate to the certificate you want to use for this installation and click **Open**. In the same way, add the **Certification Authority**. Click **Next**.

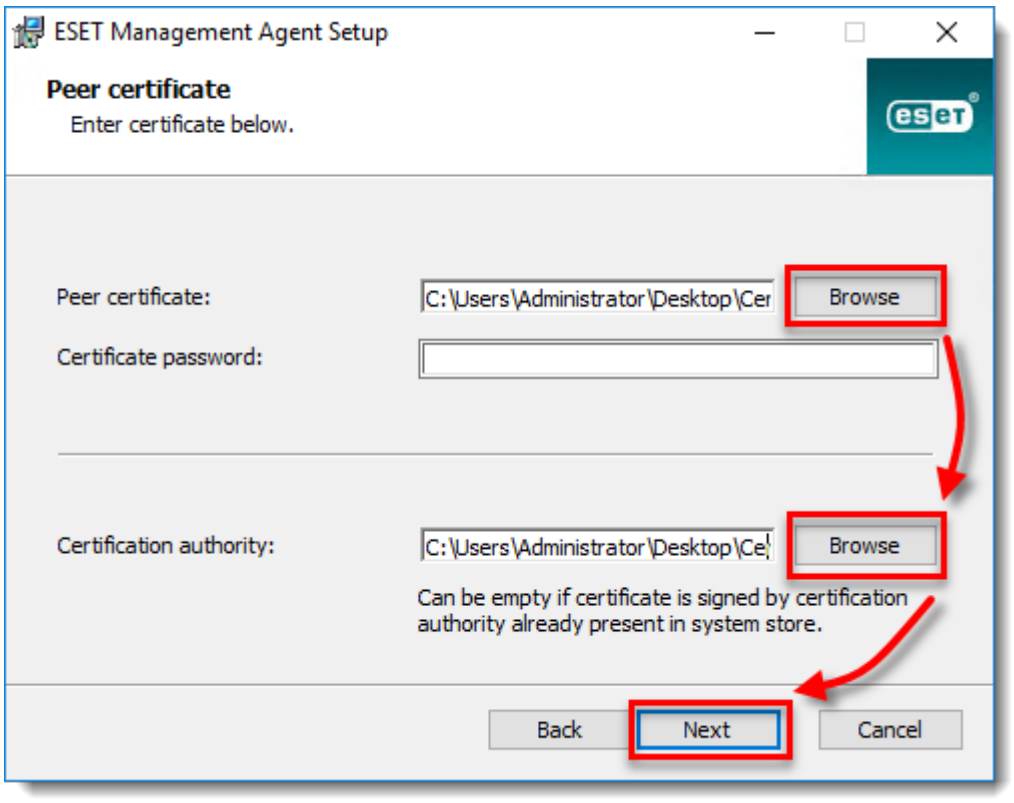

Figure 1-12

8. Follow the on-screen steps to complete the installation. To verify the Agent is working properly, check the status log located at:
C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html.

Error 1603 when installing the ESET Management Agent

During some installations of the ESET Management Agent, the notification **Error code 1603 - Installation ended prematurely** will display. Use the following troubleshooting steps to resolve this error:

- If you are running the installer from a shared location, copy the live installer file to the local disk and attempt the installation again.
- When you run the installer, right-click it and select **Run as Administrator** from the context menu.

If you are performing a new installation of ESET PROTECT, proceed to deploy ESET endpoint products to your client computers.

