

Use the Agent Script Installer to deploy the ESET Management Agent (8.x-9.x)

Mitch | ESET Nederland - 2022-08-17 - [Comments \(0\)](#) - [ESET PROTECT On-prem](#)

Issue



Required user permissions

This article assumes that you have the appropriate [access rights and permissions](#) to perform the tasks below.

If you use the default Administrator user or are unable to perform the tasks below (the option is unavailable), create a second administrator user with all access rights.

- **ESET PROTECT users:** [Create a second administrator user in ESET PROTECT](#)
- **ESET Security Management Center (ESMC) users:** [Create a second administrator user in ESET Security Management Center 7.x](#)

- The ESET Management Agent facilitates communication between client computers and the other ESET PROTECT components such as ESET PROTECT Server
- Install ESET Management Agent on all client computers where other ESET PROTECT components or ESET Endpoint products are installed
- Read more information on how to [create an Agent and ESET security product installer](#)

Solution

Are you a macOS or Linux user?



Windows users only

The deployment of the ESET Management Agent and the ESET endpoint product together from ESET PROTECT is available on Windows only.



"Failed to get installers" or "Failed to synchronize package repository"

If you receive a "Failed to get installers" or "Failed to synchronize package repository" error while performing the steps below, it is possible your third-party firewall is blocking certain communications based on the country of origin. If this is the case, we recommend [allowing communications for ESET PROTECT repository](#).



Error 1603 when installing the ESET Management Agent

Occasionally during ESET Management Agent installation, the notification "Error code 1603- Installation ended prematurely" will be displayed. Use the following troubleshooting steps to resolve this error:

- If you are running the ESET script installer (formerly ESET live installer) from a shared location, copy the script installer file to the local disk and attempt the installation again.
- When you run the Agent script installer, right-click it and select **Run as Administrator** from the context menu.
- If the issue persists, [collect and submit an ESET Sysinspector log](#) to ESET Technical Support.



Peer certificates and Certification Authority in the Static Group All

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

1. [Open the ESET PROTECT Web Console](#) in your web browser and log in.

2. Click **Quick links** → **Deploy Agent**.

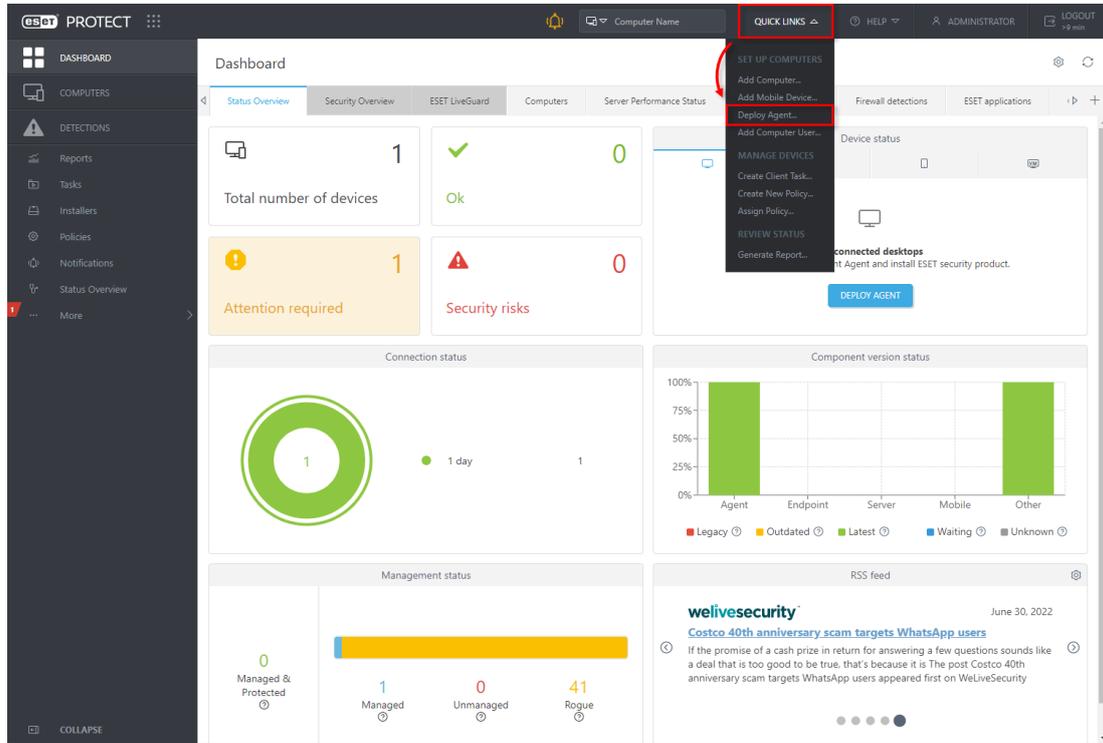


Figure 1-1

Click the image to view larger in new window

3. Select **Windows** and choose **Deploy Agent first (Agent script installer)**. You can deselect the check box next to **Participate in product improvement program** if you do not want to help ESET to improve the product. Configure other settings such as **Parent group**, **Server hostname**, **Port** name (default is 2222), **Peer Certificate** and **Certificate passphrase** if needed. Optionally, click **Customize more settings**. Click **Save & Download**.

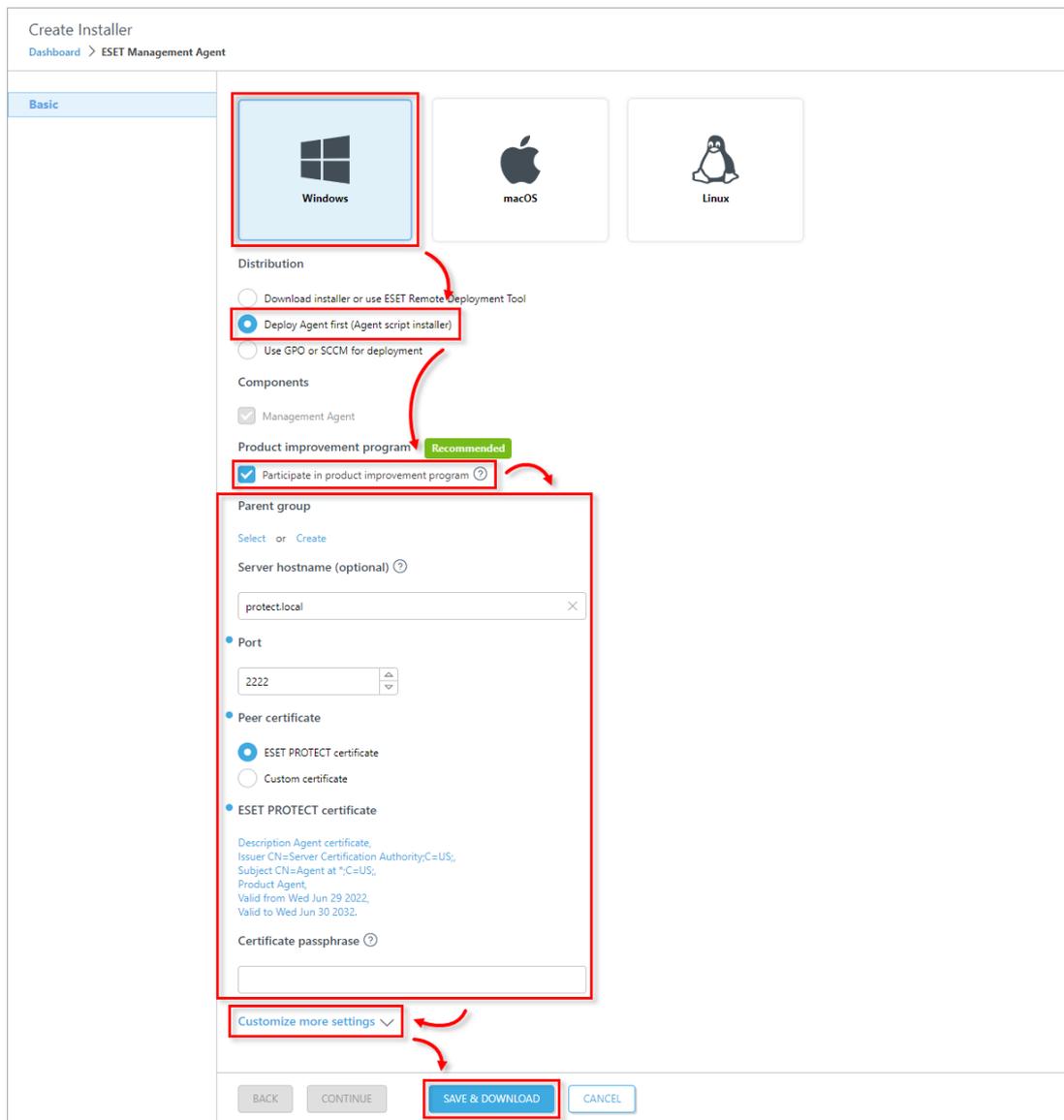


Figure 1-2
Click the image to view larger in new window

Click **Customize more settings** as mentioned in [step 3](#). Optionally, change the **Installer name** or add a **Description**. Optionally, select the **Tags**, select or create **Agent configuration**, or select the check box next to **Enable HTTP proxy settings** (if you enable HTTP proxy settings, type the required details: **Server**, **Port**, **Login**, **Password**). When you are finished customizing settings, click **Save & Download**.

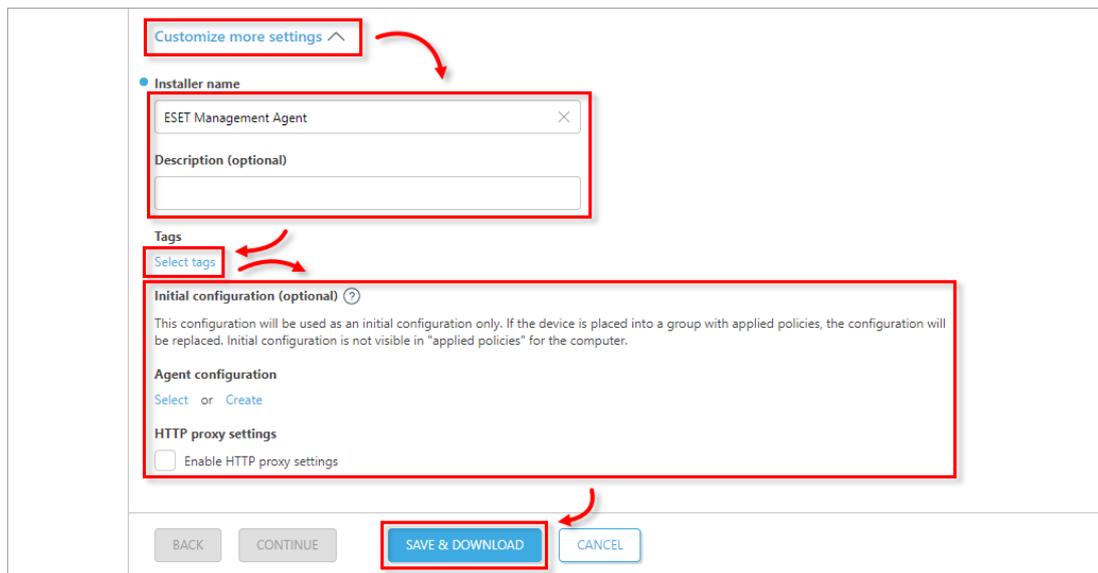


Figure 1-3
Click the image to view larger in new window

 macOS users
Continue with step 8 in the following article to [deploy the ESET Management Agent to a macOS client using Agent Script Installer](#).

4. Extract and run the installation package file on a client computer. It will install the ESET Management Agent and the ESET security product on the device and connect it to ESET PROTECT.

5. If you are performing a new installation of ESET PROTECT, continue to step 5 to [deploy or upgrade ESET endpoint products using ESET PROTECT](#).