ESET Tech Center

Deploy the ESET Management Agent using a Group Policy Object (GPO) (8.x–9.x)

Mitch | ESET Nederland - 2022-08-17 - Comments (0) - ESET PROTECT On-prem

Issue

- Deploy the ESET Management Agent using GPO in enterprise environments or environments with a high number of client computers
- Create the installer file in ESET Security Management Center
- Create the installer file in ESET PROTECT
- Deploy the ESET Management Agent using GPO
- Update the ESET Management Agent using GPO

Solution

Windows users only
The procedure described in this article is available for Windows only.

Conventional deployment methods
If you want to use conventional methods for deployment of ESET Management Agent, follow the instructions below:

- ESET PROTECT: Deploy ESET Management Agent 8.x using conventional methods
- ESET Security Management Center: Deploy ESET Management Agent 7.x using conventional methods

Before you proceed
Verify that you have your ESET Security Management Center, ESET PROTECT, or Server configured with network visibility to client machines. Your server machine and client computers need to be joined to a domain.

Depending on the security product you are using, perform these steps on the Domain Controller:

Create the installer file in ESET Security Management Center

1. Create the `install_config.ini` configuration script. It contains the parameters for the Agent to communicate with your ESET Security Management Center Server.

a. Open the ESET Security Management Center in your web browser and log in.

b. Click **Installers → Create Installer → GPO or SCCM script**.

c. Follow the script creation wizard and save the `install_config.ini`.

2. Download an earlier version of the ESET Management Agent installer .msi file from the ESET download page.

3. Save the Agent installer `.msi` file and the `install_config.ini` file to a shared folder on the domain controller so that all of your client computers can access it with read and execute permissions.

Continue with the section Deploy the ESET Management Agent using GPO below.

Create the installer file in ESET PROTECT

1. Create the `install_config.ini` configuration script. It contains the parameters for the Agent to communicate with your ESET PROTECT Server.

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

b. Click **Installers → Create Installer**.

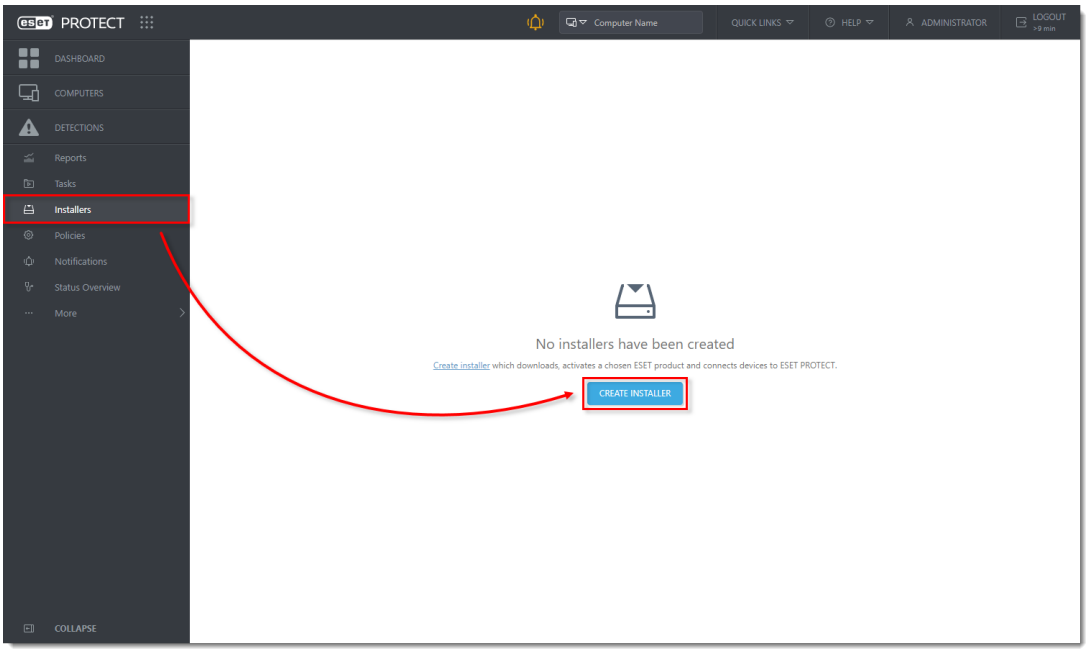

Figure 1-1

c. Select **Windows** and select the **Use GPO or SCCM for deployment** option. 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** number (2222 by default), **Peer Certificate**, or **Certificate passphrase** if needed. Optionally, click **Customize more settings** to view other options.

Click **Finish**.

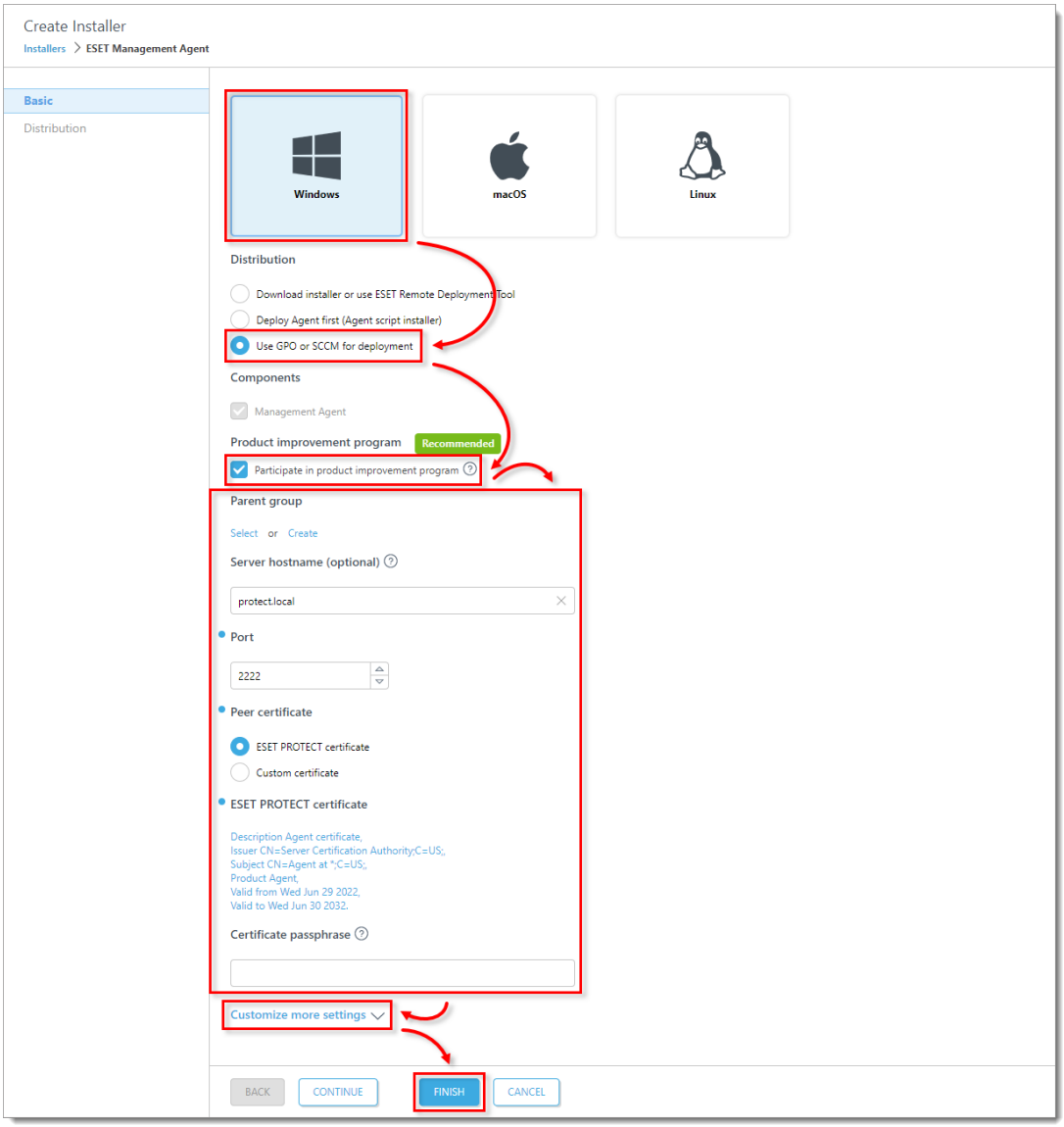

Figure 1-2

d. Click the **Configuration GPO/SCCM script** icon and click your preferred **Agent** to download `install_config.ini` file and Agent installer `.msi` file respectively. When the download is completed, click **Finish**.

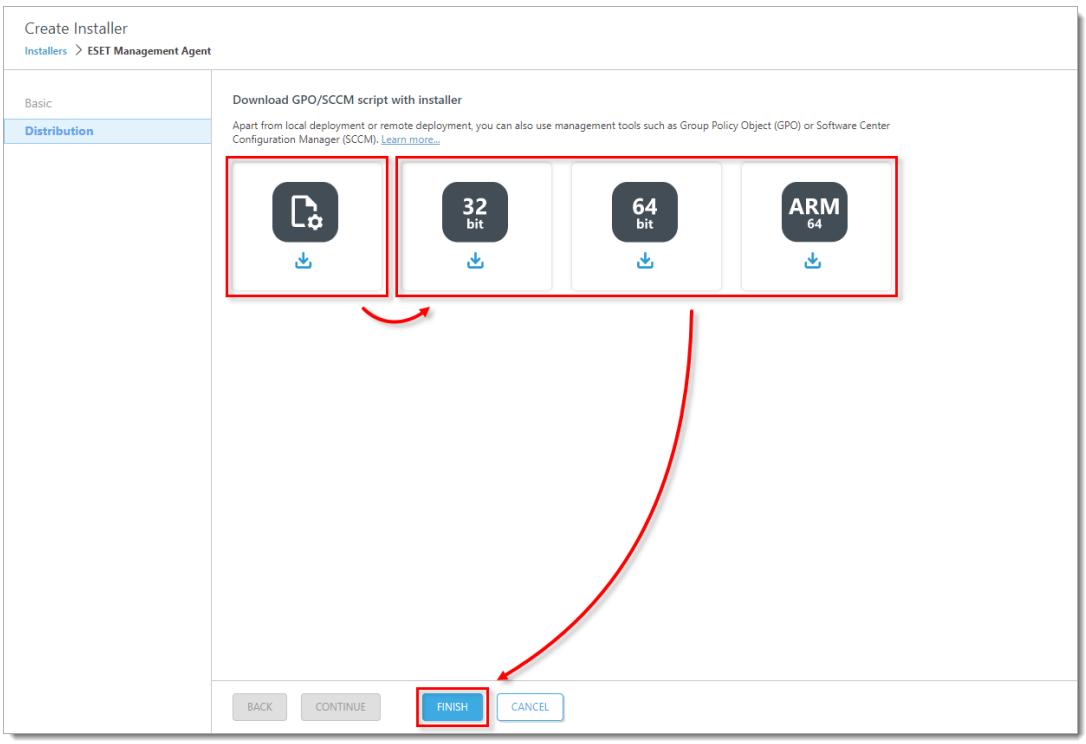

Figure 1-3

2. Alternatively, you can download the ESET Management Agent installer .msi file from the ESET download page.

3. Save the Agent installer `.msi` file and the `install_config.ini` file to a shared folder on the domain controller so that all of your client computers can access it with read and execute permissions.

Deploy the ESET Management Agent using GPO

1. Install Microsoft Group Policy Management Console (GPMC) on your Domain Controller server.

2. Open **Server Manager**, click **Manage** → **Add Roles and Features**.

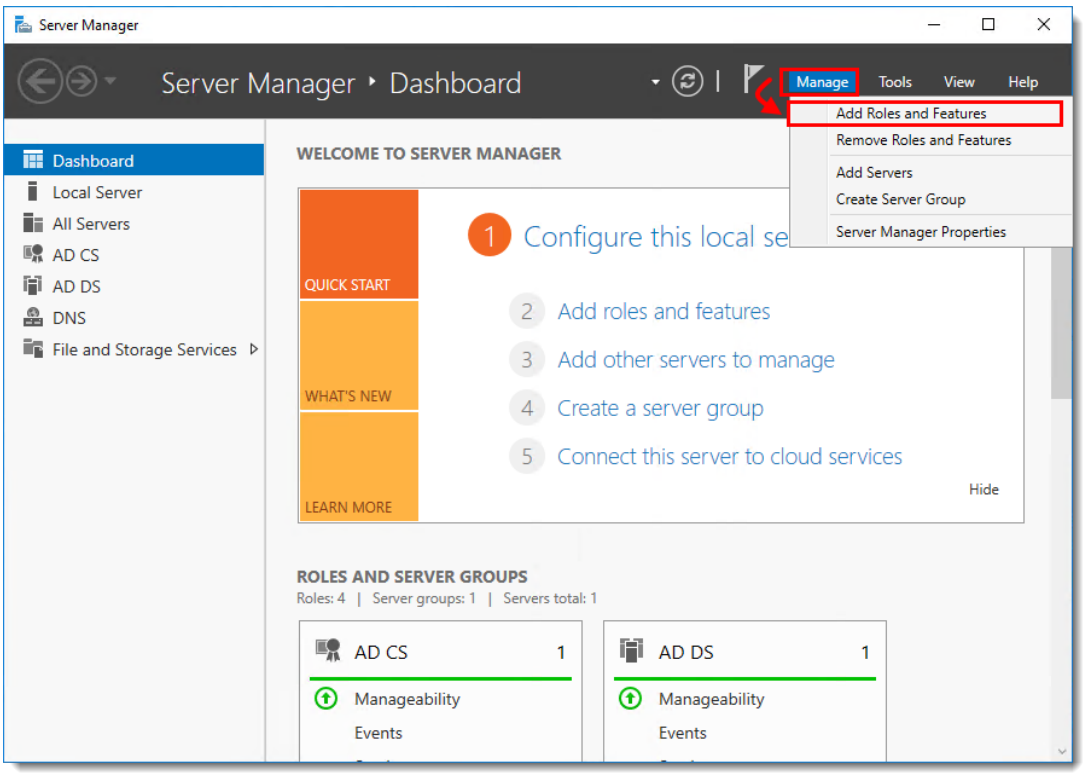

Figure 1-4

3. Follow the wizard and in **Add Roles and Features** select the check box next to **Group Policy Management**. Click **Next** and **Install**.

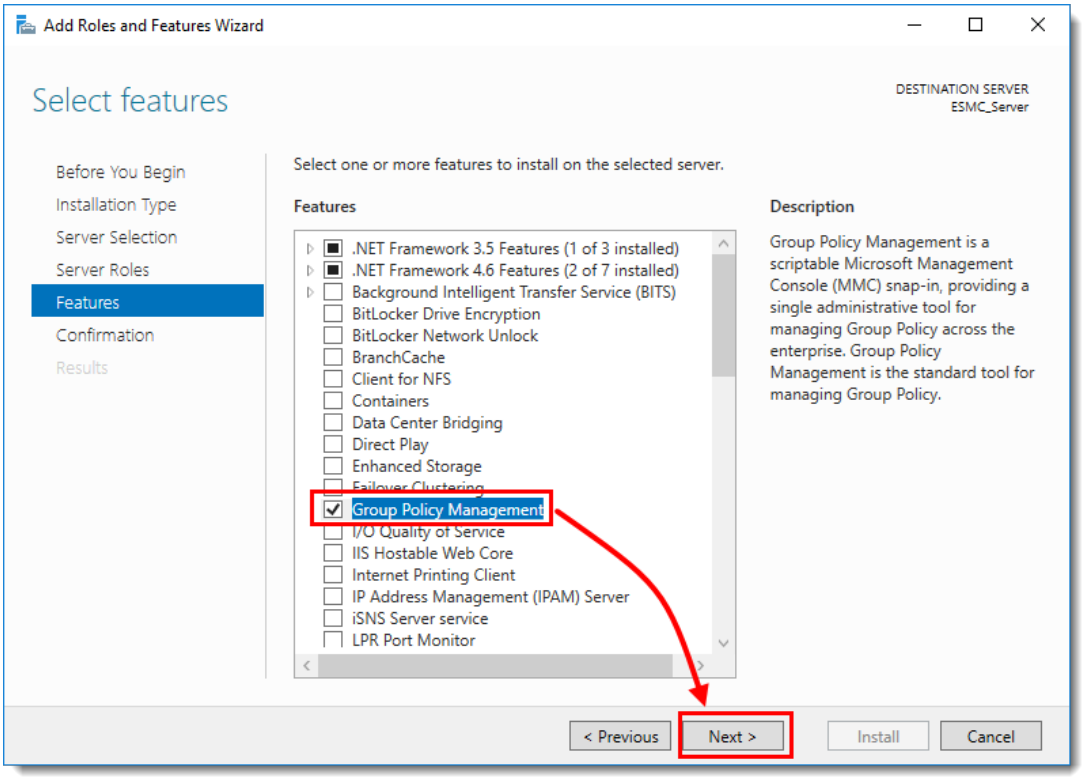

Figure 1-5

4. To open **Group Policy Management**, press the **Windows** key + **R**, type `gpmc.msc` and click **OK**.

5. Create a new Group Policy Object (GPO) to deploy the ESET Management Agents. Right-click **Group Policy Objects** and select **New**. Type a name in the **Name** field, for example, **Agent deployment**, and click **OK**.

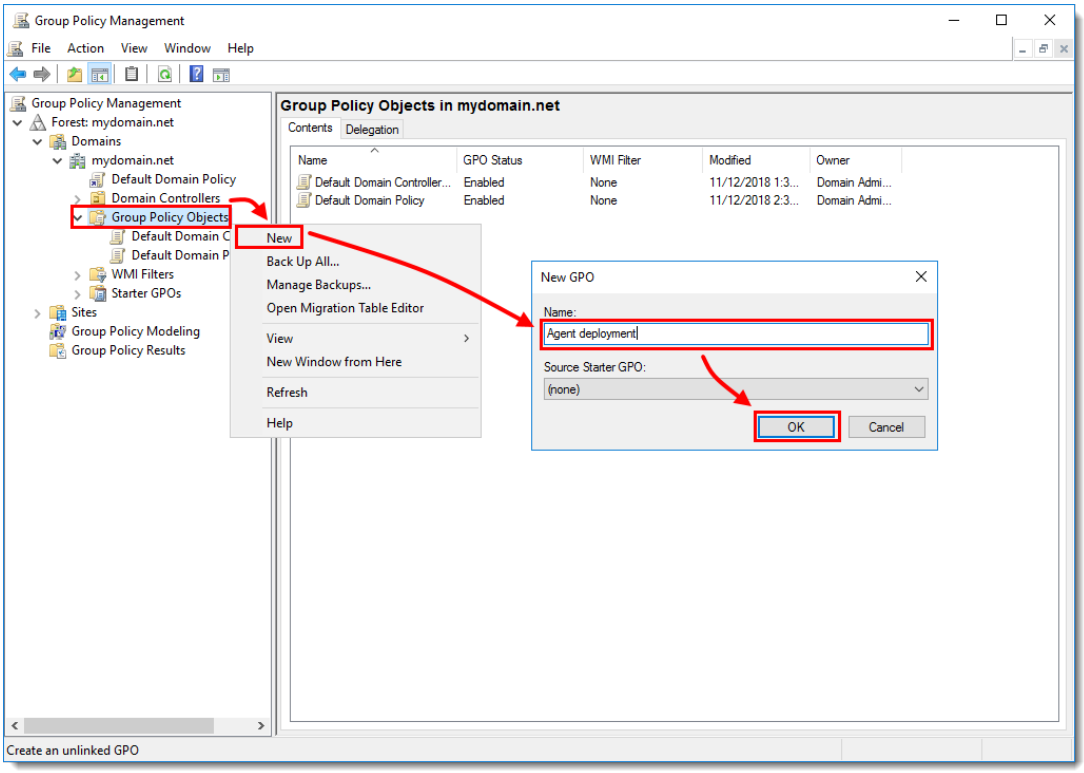

Figure 1-6

6. Right-click **Agent deployment** GPO and click **Edit**.

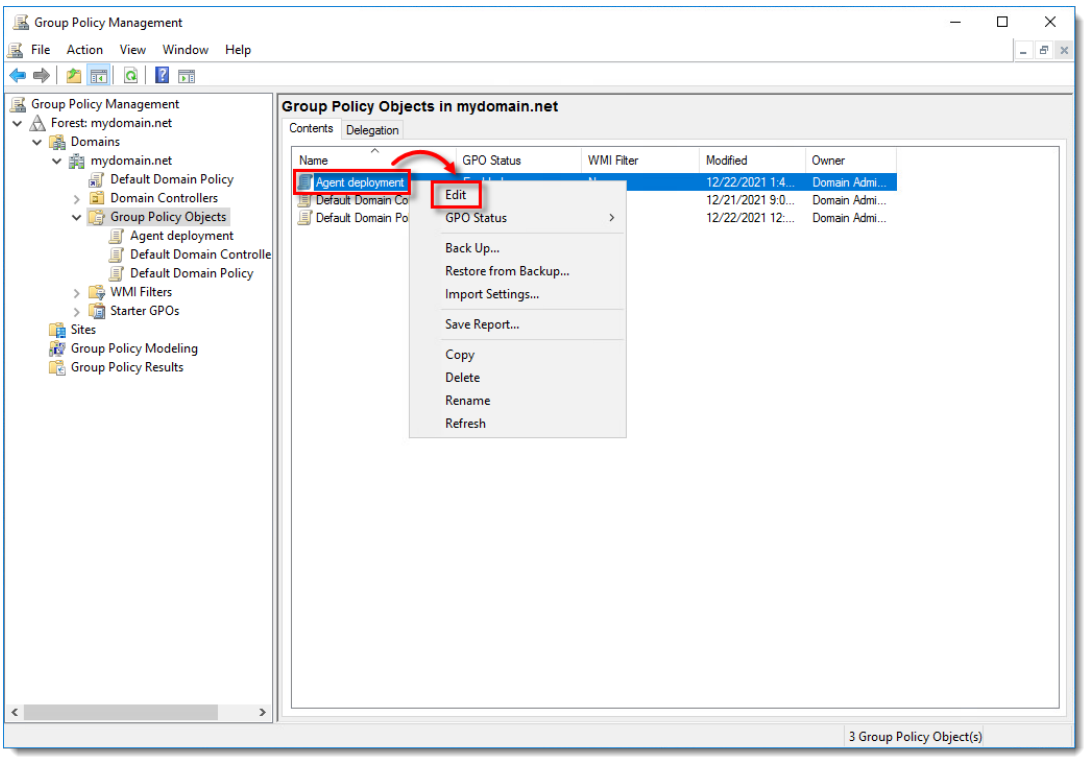

Figure 1-7

7. In the **Computer Configuration** section, expand **Policies → Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer → System** and click **Logon**. On the right side of the window, double-click **Always wait for the network at computer startup and logon**. In the dialog window, select **Enabled** and click **OK**.

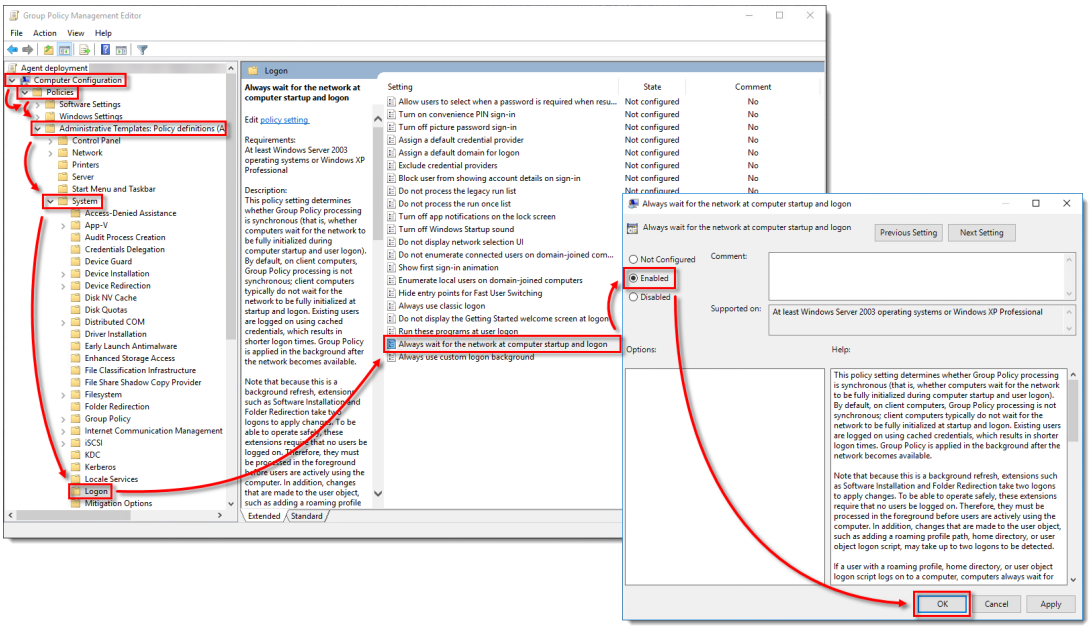

Figure 1-8

8. Click **Group Policy** and on the right side of the window, double-click **Specify startup policy processing wait time**. In the dialog window, select **Enabled** and ensure that the **Amount of time to wait (in seconds)** is set to **120**. You can set a different time to wait, but we recommend setting at least 30 seconds. Click **OK**.

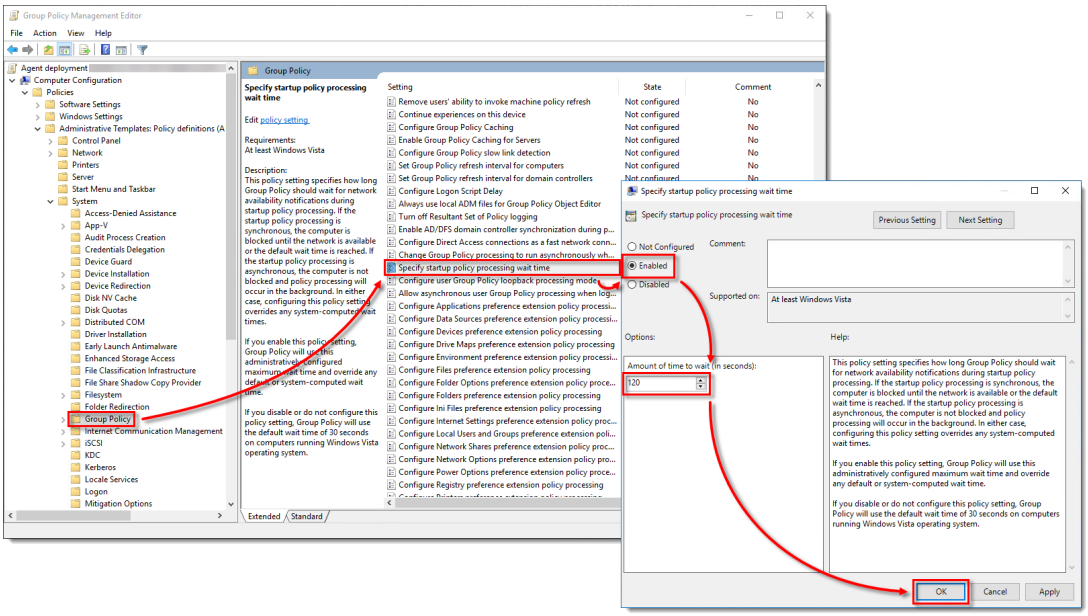

Figure 1-9

9. Right-click the domain and select **Link an Existing GPO**.

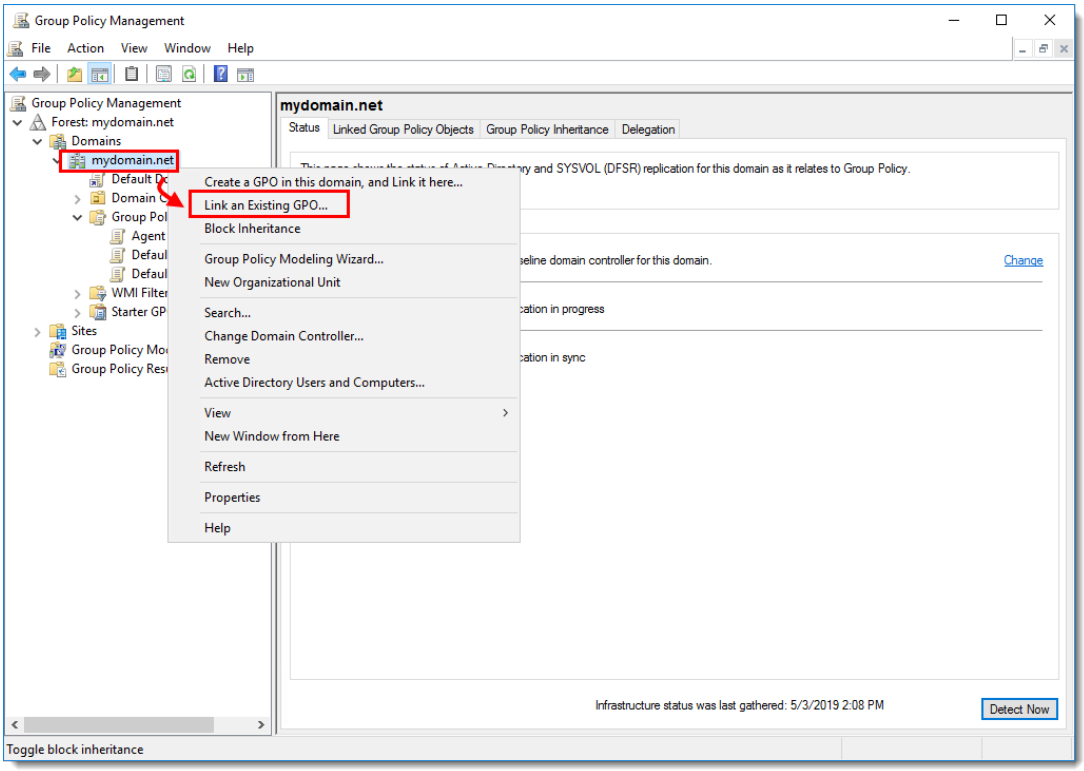

Figure 1-10

10. Select the GPO that you created and click **OK**.

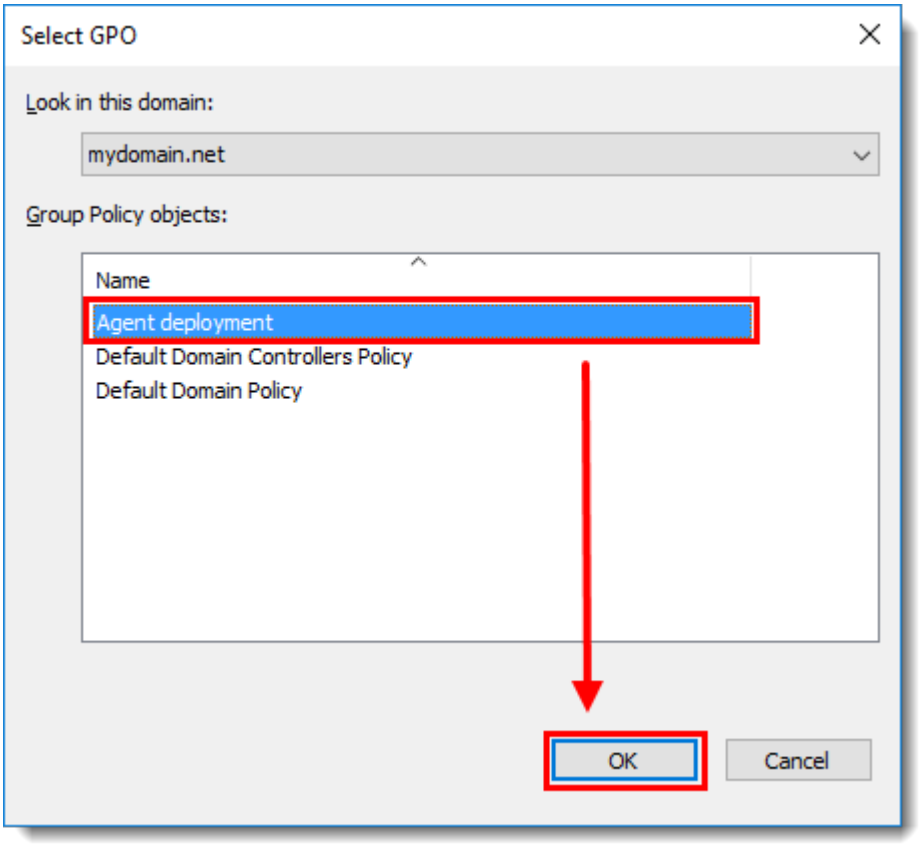

Figure 1-11

11. Right-click the linked GPO and click **Edit** to edit the GPO in **Group Policy Management Editor**.

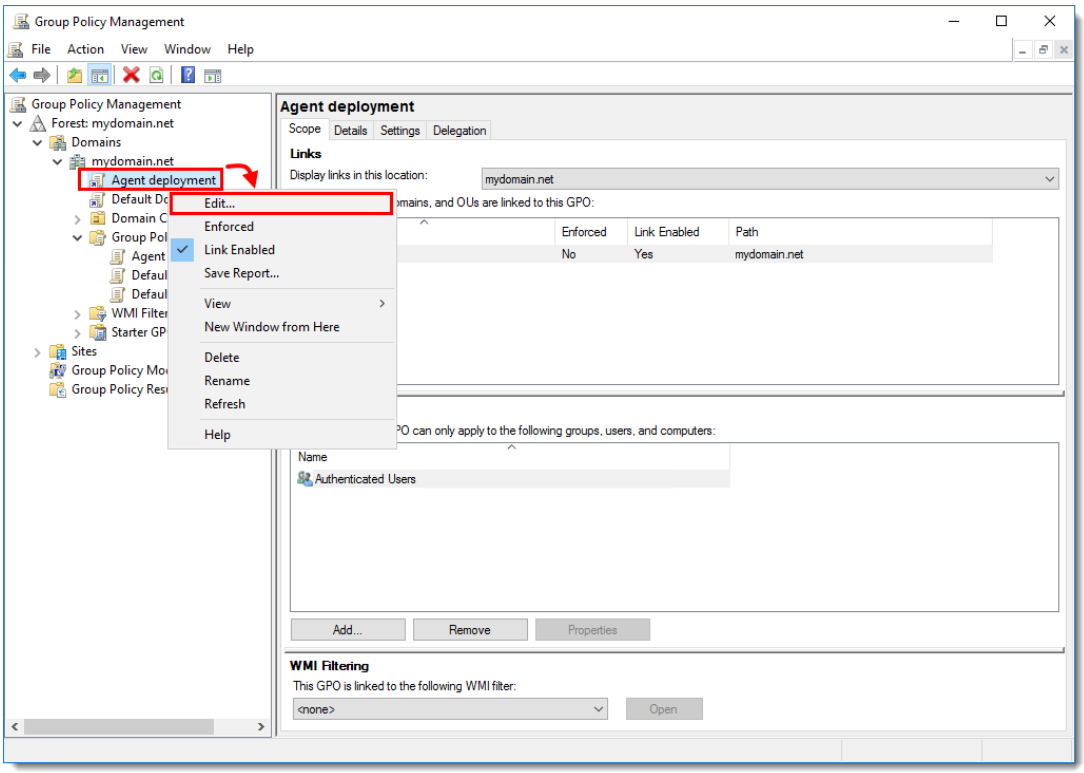

Figure 1-12

12. Expand **Computer Configuration** → **Policies** → **Software settings**. Right-click **Software installation**, select **New** → **Package**.

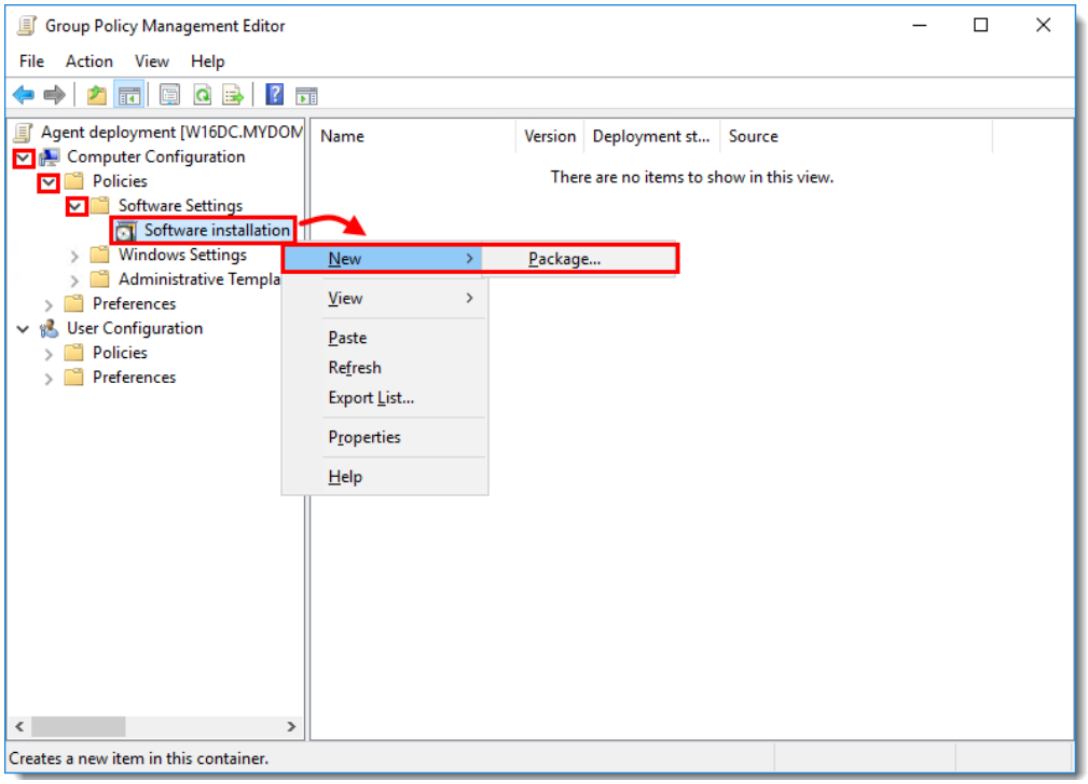

Figure 1-13

13. Navigate to the location where the ESET Management Agent installer `.msi` is saved. Type the full Universal Naming Convention (UNC) path of the shared installer package (for example, `\\fileserver\share\filename.msi`) and click **Open**.

If you are deploying to 64-bit and 32-bit clients, repeat this step for both installer packages (Agent_x64.msi and Agent_x32.msi) and then follow the steps in **Deploy ESET Management Agents to both 32-bit and 64 bit systems** below.

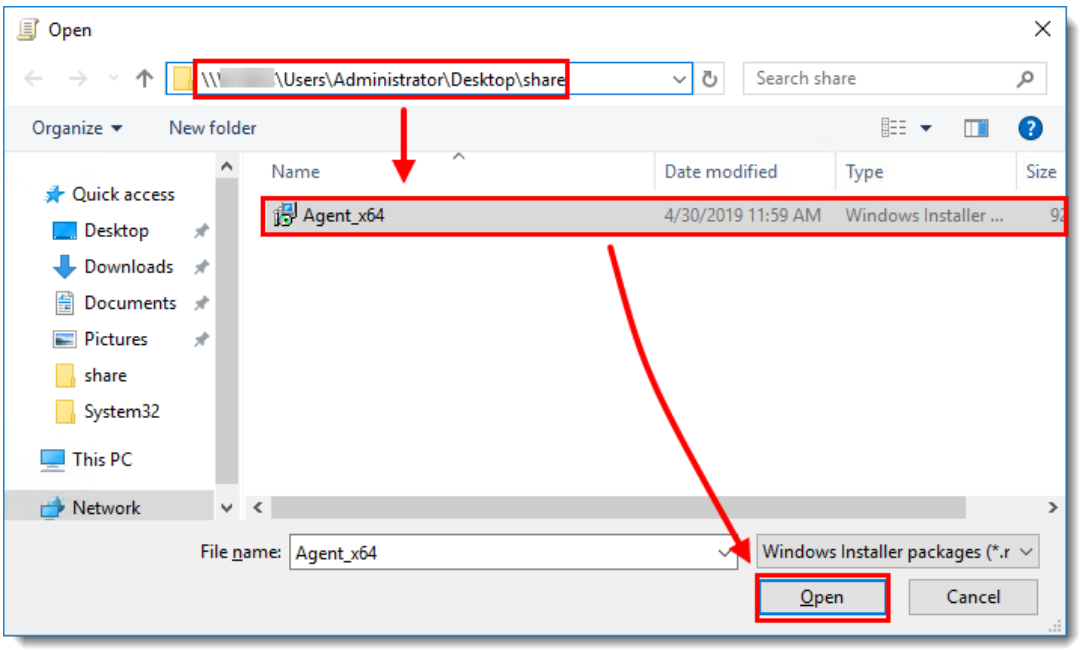

Figure 1-14

Deploy ESET Management Agents to both 32-bit and 64-bit systems

To deploy ESET Management Agents to both 32-bit and 64-bit systems, add the 64-bit and 32-bit `.msi` files to the shared folder.

In **Advanced settings** for the `32-bit.msi` file, deselect the check box next to **Make this 32-bit X86 application available to Win64 machines**.

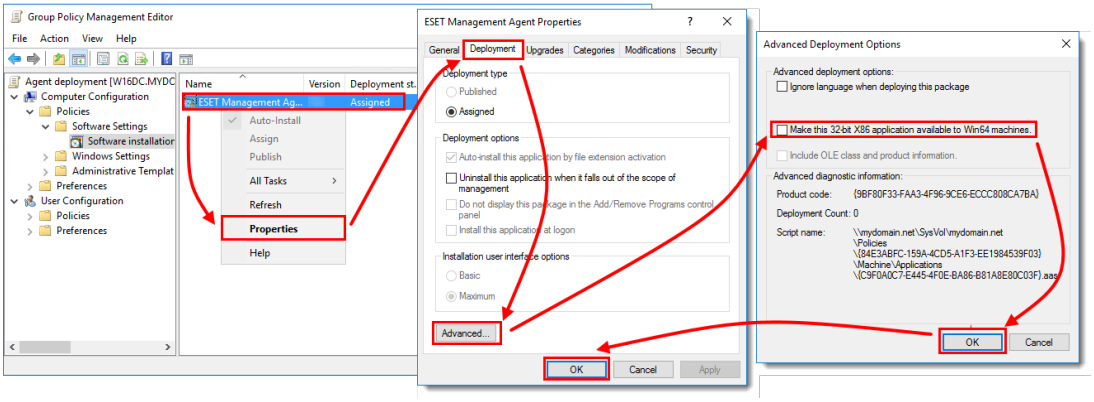

Figure 1-15

14. Select **Assigned** and click **OK**.

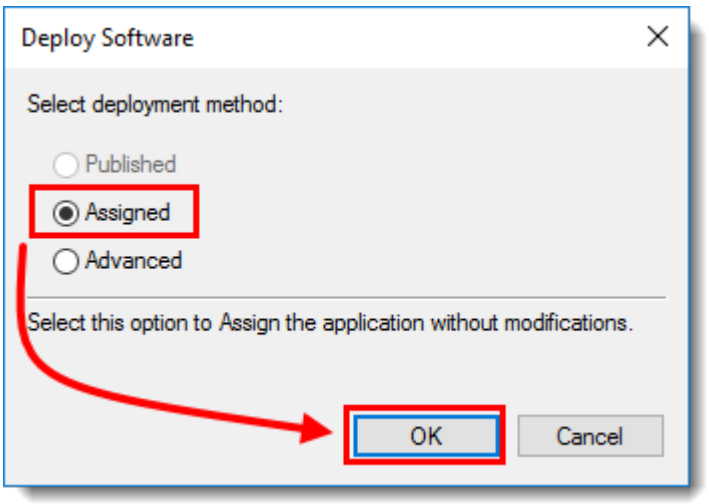

Figure 1-16

15. The package is displayed in the **Group Policy Management Editor**.

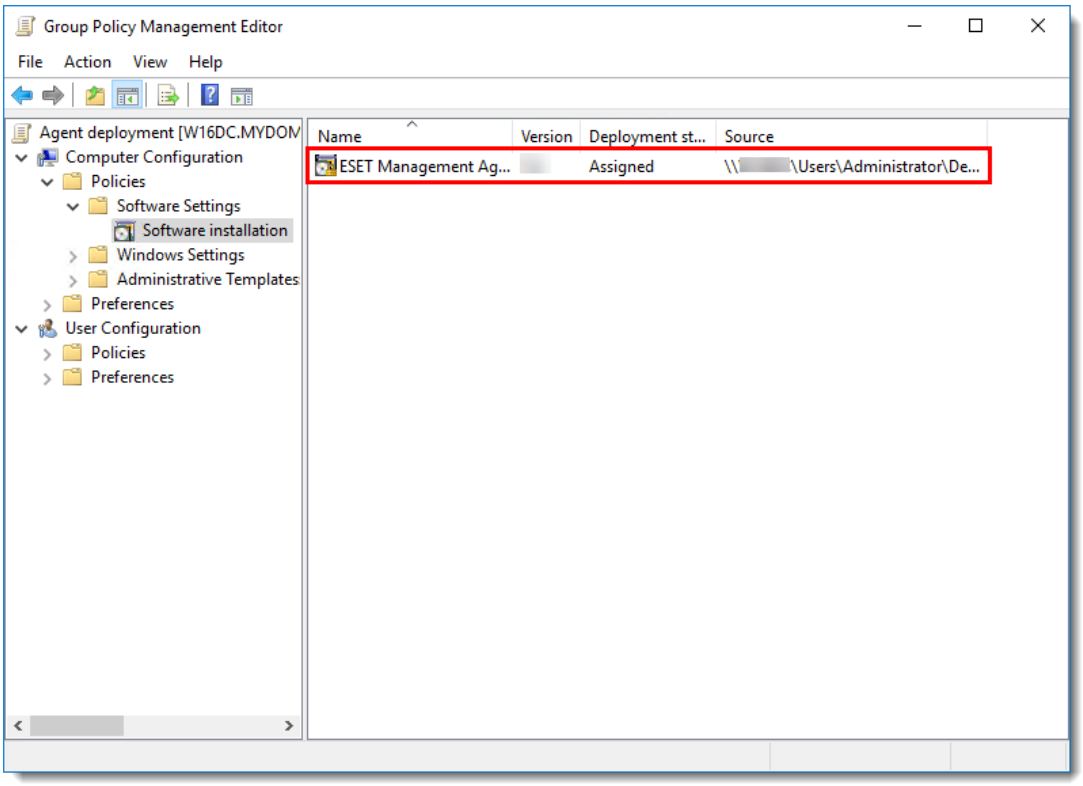

Figure 1-17

16. Close the **Group Policy Management Editor** window. In the left tree of **Group Policy Management** window, select the GPO you created. In the **Security Filtering** section, select **Authenticated Users**, click **Remove** and **OK**.

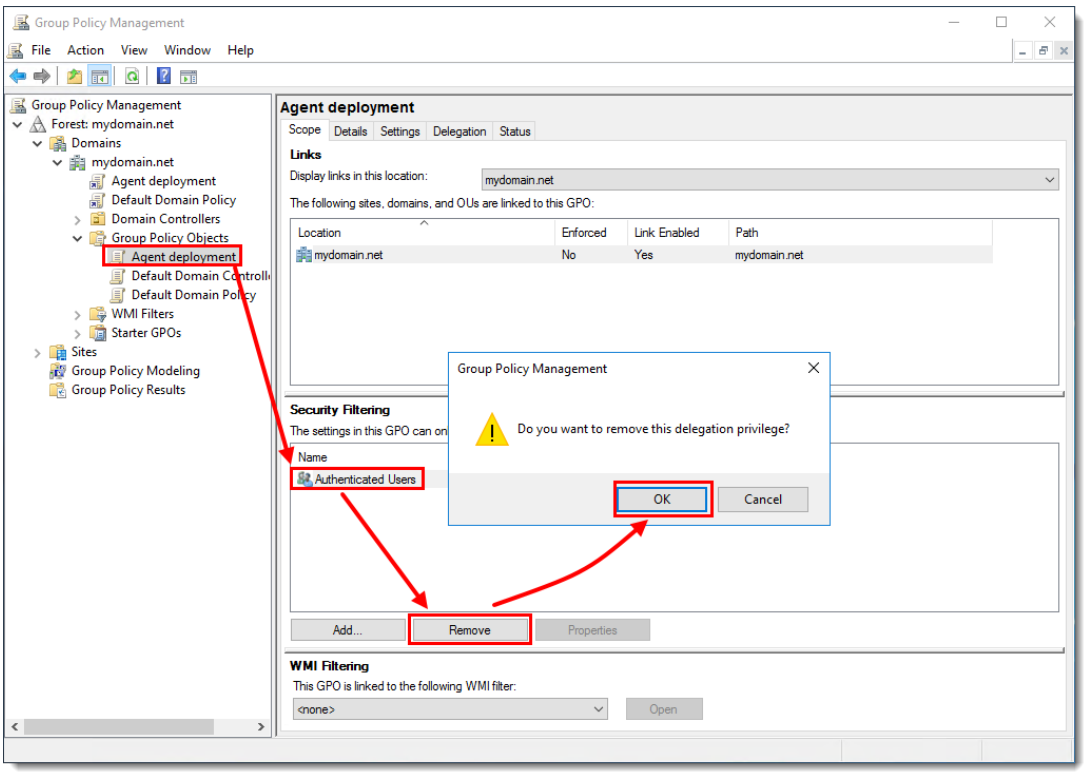

Figure 1-18

17. Assign GPO to client computers:

    - Assign GPO to all Domain computers: Click **Add** → type **domain computers** and click **OK**.

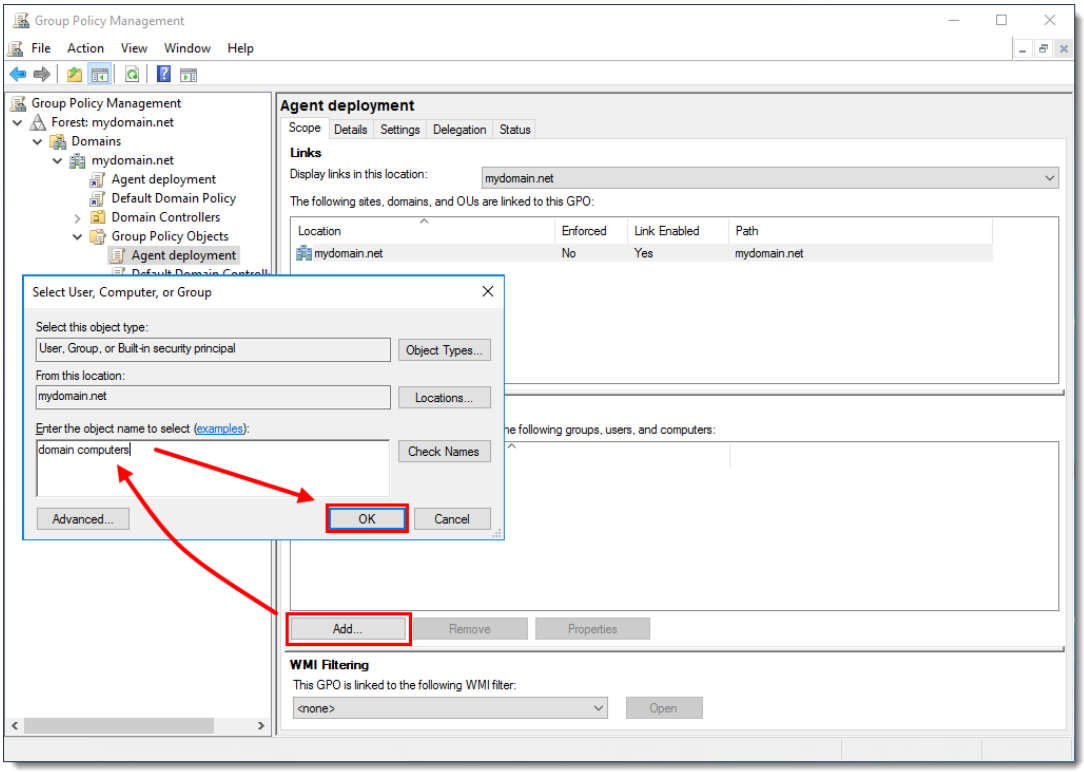

Figure 1-19

- Alternatively, you can assign GPO to the selected computers only: Click **Add** → **Object Types** → select the check box next to **Computers** and click **OK**. Type the name of the computer and click **OK**. You can add more computers by repeating this step.

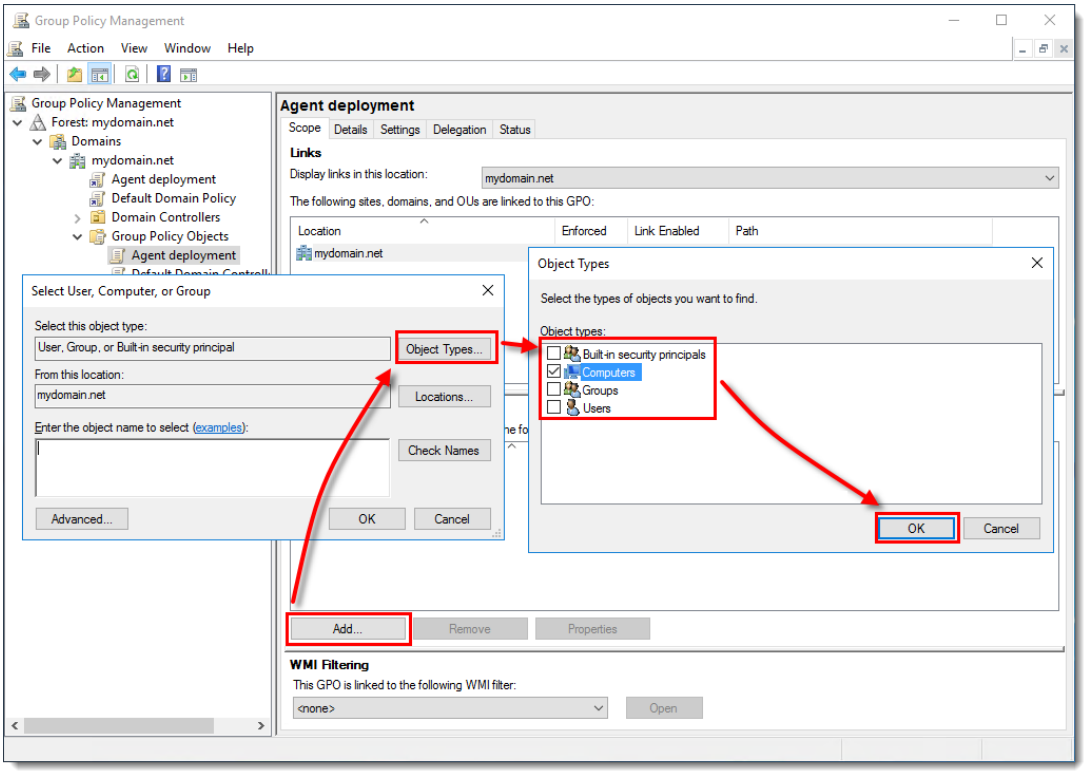

Figure 1-20

18. GPO is now assigned to the selected computers. When the GPO updates, the computers will receive it and ESET Management Agent will be installed.

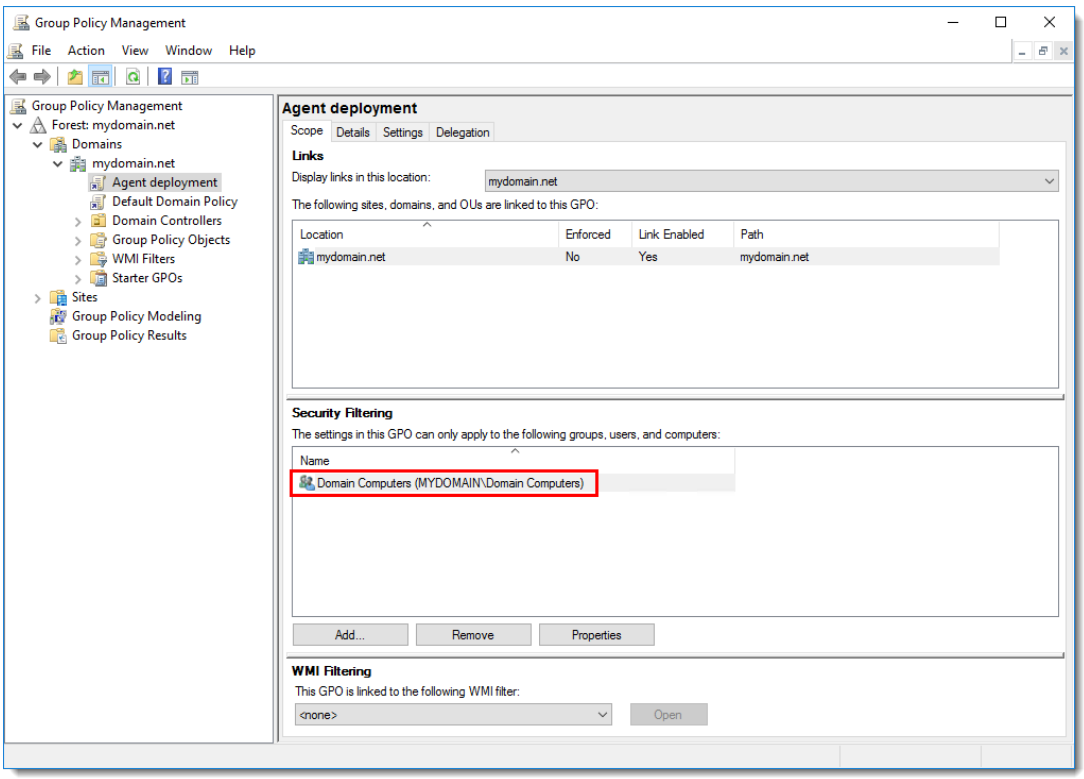

Figure 1-21

See the Microsoft Knowledgebase instructions on how to use Group Policy to remotely install software in Windows Server 2008 (and later).

Update the ESET Management Agent using GPO

> Keep the original installation files
>
> Do not replace or delete the original files used for ESET Management Agent Deployment, including the installer .msi file and the `install_config.ini` file.
>
> ESET recommends keeping all files and packages in the GPO. Deleting or replacing the files or packages may cause issues with the update.

1. Download the latest version of ESET Management Agent. Rename the file to `agent_x64_xxx.msi` (or `agent_x32_xxx.msi`) where xxx is the current version number.

2. Create a folder at a shared location that can be accessed by domain computers and rename the folder to ESET `Agent xxx` where xxx is the current version number. Move the ESET Management Agent installer and the `install_config.ini` file to the folder.

3. Follow steps 12-15 above to create a new installation package. Select the location with the latest version of ESET Management Agent.

4. When you assign the package, GPO automatically detects the version number of the installer. To confirm that the latest package upgrades the earlier version double-click the latest package, click **Upgrade** and verify that the earlier package name is listed.

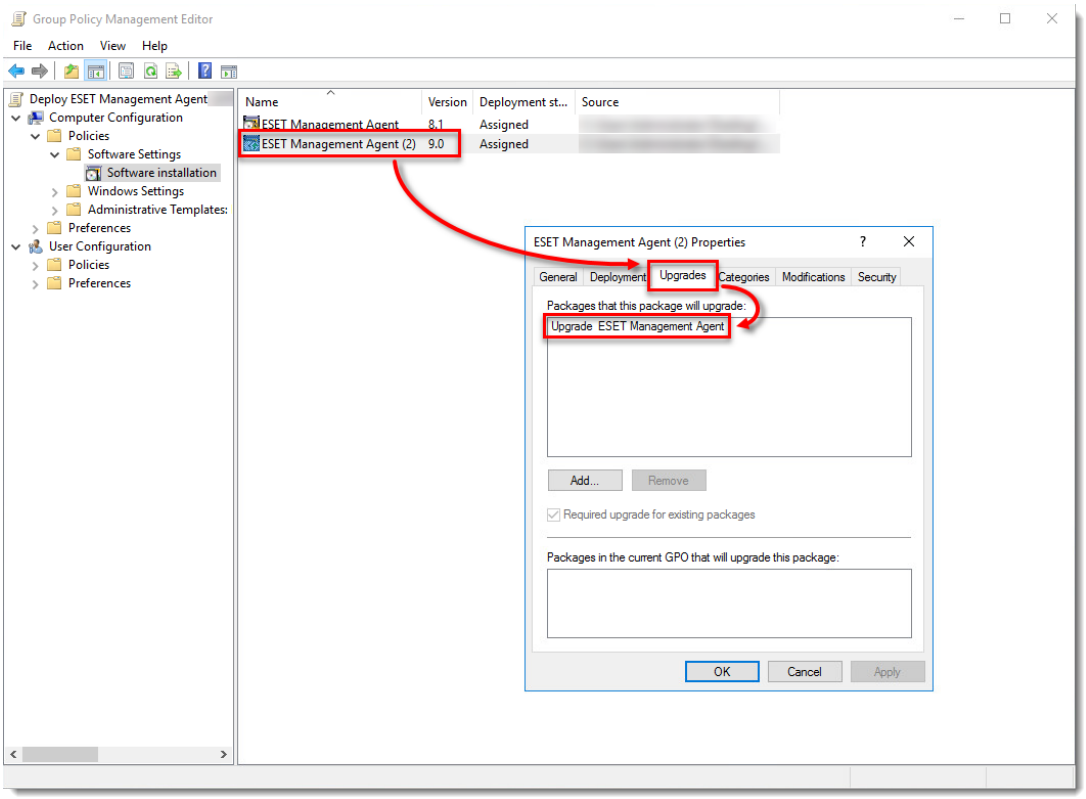
Group Policy Management Editor
File Action View Help
Deploy ESET Management Agent
Computer Configuration
Policies
Software Settings
Software installation
Windows Settings
Administrative Templates:
Preferences
User Configuration
Policies
Preferences
Name
Version
Deployment st...
Source
ESET Management Agent
8.1
Assigned
ESET Management Agent (2)
9.0
Assigned
ESET Management Agent (2) Properties
General
Deployment
Upgrades
Categories
Modifications
Security
Packages that this package will upgrade:
Upgrade ESET Management Agent
Add...
Remove
Required upgrade for existing packages
Packages in the current GPO that will upgrade this package:
OK
Cancel
Apply

Figure 2-1