ESET Tech Center

Knowledgebase > ESET PROTECT On-prem > Deploy the ESET Management Agent using a Group Policy Object (GPO) (8.x-9.x)

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

Mitch | ESET Nederland - 2025-03-06 - 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
- <u>Create the installer file in ESET Security Management Center</u>
- 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: <u>Deploy ESET Management Agent 8.x using conventional methods</u>
- 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. <u>Open the ESET Security Management Center</u> in your web browser and log in.

- b. Click Installers \rightarrow Create Installer \rightarrow 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 <u>Deploy the ESET Management Agent using GPO</u> 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.
- COLUMSE

 Image: Computer Name
 OUCK LINCK IN INTERPORT

 Image: Computer Name
 OUCK LINCK IN INTERPORT

 Image: Computer Name
 OUCK LINCK IN INTERPORT

 Image: Computer Name
 Image: Computer Name

 Image: Computer Name</
- 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**.

Create Installer	
Installers / ESET management Agent	
Basic	Download GPO/SCCM script with installer
Distribution	Apart from local deployment or remote deployment, you can also use management tools such as Group Policy Object (GPO) or Software Center Configuration Manager (SCCM). <u>Learn more</u>
	Lo 22 bit 64 bit 64 to 464 to
	BACK CONTINUE FINISH CANCEL



2. Alternatively, you can <u>download the ESET Management Agent installer .msi file</u> 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 \rightarrow Add Roles and Features.

ᡖ Server Manager	– 🗆 X
Server M	lanager 🕻 Dashboard 🛛 🗸 🕑 l 🍢 Manage Tools View Help
	Add Roles and Features
🔛 Dashboard	WELCOME TO SERVER MANAGER
Local Server	Create Server Group
All Servers	1 Configure this local se
🖳 AD CS	
AD DS	QUICK START
🛱 DNS	2 Add roles and features
■ File and Storage Services ▶	3 Add other servers to manage
	WHAT'S NEW 4. Create a server group
	4 Cleate a server group
	5 Connect this server to cloud services
	Hide
	ROLES AND SERVER GROUPS Roles: 4 Server groups: 1 Servers total: 1
	R AD CS 1 I AD DS 1
	Manageability Manageability
	Events Events

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**.

📓 Group Policy Management						-	ПX
🛋 File Action View Window Help							_ 8 ×
Group Policy Management	Group Policy Objects in Contents Delegation Name Default Domain Controller Default Domain Policy	mydomain GPO Status Enabled Enabled	WMI Filter None None	Modified 11/12/2018 1:3 11/12/2018 2:3	Owner Domain Admi Domain Admi		
 ☑ Default Domain C ☑ Default Domain P > ☑ Will Filters > ☑ Starter GPOs > ☑ Sites ☑ Group Policy Modeling ☑ Group Policy Results 	New Back Up All Manage Backups Open Migration Table Editor View New Window from Here	>	New GPO Name: Agent deployment Source Starter GPO: (roope)			×	
	Help			ОК	Cance	ł	
< >							
Create an unlinked GPO	_,						
						_	

Figure 1-6

📓 Group Policy Management		-	ΟX
🔣 File Action View Window Help			_ & ×
🔶 🔿 📶 🖸 🖬			
 Torest mydomain.net Torest Domain Controllers Torest Group Policy Modeling Group Policy Results 	e Corterts Delegation Cort		
<;		·Ohiotí	

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

7. In the **Computer Configuration** section, expand **Policies** \rightarrow **Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer** \rightarrow **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.

K Group Policy Management			-	□ ×		
📓 File Action View Window Help						
🗢 🔿 🙍 🛅 📋 🔚 🖬						
Group Policy Management mydo	omain.net					
Forest: mydomain.net Status	us Linked Group Policy Objects Group	Policy Inheritance Delegation				
mydomain.net		any and SYSVQL (DESR) replication for this domain as it relates to Group Policy				
Default Dc Create a GPO in this	s domain, and Link it here					
Softain G Link an Existing GPO	0					
J Agent Block Inheritance						
Defaul Group Policy Modeli Defaul	ling Wizard	seline domain controller for this domain.		Change		
> 🙀 WMI Filter	nizational Unit					
> iii Starter GP Search		ation in progress				
Group Policy Mod Remove	ontroller	ation in sync				
Group Policy Resi	ers and Computers					
View						
New Window from H	Here					
Refresh						
Properties						
Help						
< >>		Infrastructure status was last gathered: 5/3/2019 2:08 PM	[Detect Now		
Toggle block inheritance						

Figure 1-10

10. Select the GPO that you created and click $\boldsymbol{OK}.$

Select GPO	×
Look in this domain:	
mydomain.net	~
Group Policy objects:	
Name	
Agent deployment	
Default Domain Controllers Policy Default Domain Policy	
★	
ОК	Cancel



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

📓 Group Policy Management							– 🗆 ×
📓 File Action View Windo	ow Help						_ 8 ×
🔶 🍬 🞽 📰 🗙 🙆 📓							
Group Policy Management Group Policy Management Group Policy Management Group Policy Management Group Policy Group Pol Group P	ent Edit Enforced Link Enabled Save Report View New Window	Agent deployme Scope Details Se Links Display links in this lo	ent tings Delegation cation: myda mains, and OUs are lin	main net sked to this GPO: Enforced No	Link Enabled Yes	Path mydomain.net	~
 Sites Group Policy Mod Group Policy Rest 	Delete Rename Refresh		² O can only apply to th	e following groups, use	ars, and computers:		
	nep	Name Authenticated L Add WMI Filtering This GPO is linked to <pre>crone></pre>	Remove	Properties	Open		
<	>						

Figure 1-12

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

Group Policy Management Editor						-	×
File Action View Help							
🗢 🔿 🙍 📆 🗐 🙆 🛃							
 Agent deployment [W16DC.MYDON Computer Configuration Policies Software Settings Software installation 	Name		Version The	Deployment st re are no items to s	Source		
> 📔 Windows Settings	<u>N</u> ew	>	<u>P</u> ackag	e			
 Administrative Templa Preferences User Configuration Policies Preferences 	View Paste Refresh Export List Properties Help	>					
Creates a new item in this container.							

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.

J Open					×
$\leftrightarrow \rightarrow \cdot \uparrow$	W	\Users\Administrator\Desktop\share	✓ [™] Sea	arch share	Q
Organize 🔻 🛛 N	lew folde	er			
🕹 Quick access	^	Name	Date modified	Туре	Size
Desktop	*	😼 Agent_x64	4/30/2019 11:5	9 AM Windows In	staller 92
Downloads	*		1		
Documents	*				
Pictures	*				
share					
System32					
This PC					
📄 Network	~	<			>
	File <u>n</u> a	ame: Agent_x64		/indows Installer pack	cages (*.r ∨ Cancel

Figure 1-14



Figure 1-15

14. Select Assigned and click OK.

Deploy Software	×
Select deployment method:	
Published Assigned	
Advanced	_
Select this option to Assign the application without modifications.	
OK Cancel	

Figure 1-16

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

Group Policy Management Editor					—		×
File Action View Help							
🗢 🔿 🙍 📊 🔒 👔 🖬							
Agent deployment [W16DC.MYDON Nam	ne ^	Version	Deployment st	Source			
Computer Configuration Policies	SET Management Ag		Assigned	\\\ Users\Admini	strator\	De	
✓							
Software installation							
Administrative Templates							
> Preferences							
V 😢 User Configuration							
> Policies							

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**.

📓 Group Policy Management				- 🗆 ×
📓 File Action View Window Help				_ 8 ×
🗢 🔿 🙍 🗔 🚺				
Group Policy Management	Agent deployment			
V A Forest: mydomain.net	Scope Dataile Settingen Delegation Statum			
🗸 📑 Domains	Linke			
✓ jii mydomain.net	Display links in this location:			
Agent deployment	The first and the second secon	t opp		~
> Domain Controllers	The following sites, domains, and OUs are linked to the	his GPU:		
Group Policy Objects	Location	Enforced Link Enabled	Path	
📑 Agent deployment	🚔 mydomain.net	No Yes	mydomain.net	
🗾 Default Domain Controlle				
Default Domain Policy				
> a Starter GPOs				
> 🙀 Sites				
🔯 Group Policy Modeling	Group Policy Ma	nagement	×	
Group Policy Results				
	The activities in this GPO error and	u want to remove this deleg	ation privilege?	
		a want to remove and deleg	adon principel	
	Name			
	Authenticated Users	OK	Cancel	
		ŬK.	Cancer	
	Add Remove	Properties		
	WMI Filtering			
	This GPU is linked to the following WMI filter:			
<	<none></none>	V Open		
	r.			

Figure 1-18

- 17. Assign GPO to client computers:
 - Assign GPO to all Domain computers: Click $\mathbf{Add} \rightarrow \mathbf{type}\ \mathbf{domain}\ \mathbf{computers}$ and click $\mathbf{OK}.$

📓 Group Policy Management					- 🗆 ×
😹 File Action View Window Help					_ 8 ×
🗢 🔿 📶 🖸 🔢 🗊					
Group Policy Management A Forest: mydomain.net	Agent deployment Scope Details Settings Delegation Status Links Display links in this location: mydomain.net The following sites, domains, and OUs are linked to this GPO: SPO:				×
🗸 📑 Group Policy Objects	Location	Enforced	Link Enabled	Path	
Agent deployment	🚔 mydomain.net	No	Yes	mydomain.net	
Select User, Computer, or Group Select this object type: User, Group, or Built-in security principal From this location: mydomain.net Enter the object name to select (examples): domain computeral Advanced	Check Names	e following groups, use	rs, and computers:		
	Add Kemove	Properties			
< >>	WMI Filtering This GPO is linked to the following WMI filte <none></none>	r: ~	Open		

Figure 1-19

• Alternatively, you can assign GPO to the selected computers only: Click $Add \rightarrow Object Types \rightarrow$ 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.

📓 Group Policy Management	- D >	<
📓 File Action View Window Help	- 5	×
🗢 🔿 📶 🖸 🚺		
Group Policy Management A Forest: mydomain.net	Agent deployment Scope Details Settings Delegation Status Links Display links in this location: mydomain.net Note that the following sites, domains, and OUs are linked to this GPO:	
Group Policy Objects	Location Enforced Link Enabled Path	
Agent deployment Default Domain Controll	Diject Types X	
Select User, Computer, or Group	X Select the types of objects you want to find.	
Select this object type:	Object types:	
User, Group, or Built-In security principal	Object Types	
From this location: mydomain.net	Locations	Ë,
Enter the object name to select (<u>examples</u>):	Check Names	
	nun nenove Properces	_
	WMI Ritering	
	Inis Group Inis and the following WMI filter:	
< >		

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.

📓 Group Policy Management					-	o x
🕵 File Action View Window Help						_ 8 ×
 Group Policy Management ▲ Forest: mydomain.net ▲ Domains ▲ Agent deployment ④ Default Domain Policy > ◎ Domain Controllers > ◎ Group Policy Objects > ◎ Stater GPOs > ◎ Group Policy Results 	Agent deployment Scope Details Settings Delegat Links Display links in this location: The following sites, domains, and OL Location	ion mydomain.net s are linked to this GPO: Enforced No	Link Enabled Yes	Path mydomain.net		×
	Security Filtering The settings in this GPO can only ap Name Add Rem	ply to the following groups, use ^ N\Domain Computers) ove Properties	rs, and computers:			
	WMI Filtering This GPO is linked to the following V <none></none>	VMI filter:	Open			

Figure 1-21

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

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. <u>Download the latest version of ESET Management Agent</u>. 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.

I Group Policy Management Editor	×
File Action View Help	
Image: Deploy ESET Management Agent Name Version Deployment st Source Image: Computer Configuration Image: Computer Configuration Assigned Assigned Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings Image: Computer Settings	
Sector Sector <td></td>	
< >>	

