

Active Directory Deployment Guide



Version 2.0

Date 11.11.2022

Table of Contents

Document Changelog	1
1. Introduction	2
2. Create the WMI filters	3
3. Create the deployment GPO	8
4. Link the WMI to GPO	10
5. Link the GPO to OU	11
6. Disclaimer	12

Document Changelog

Version	Date	Notes
1.0	2019	The document was created
2.0	11.11.2022	Updated document with the current template

1. Introduction

Endpoint Protector Client software is delivered as a Microsoft Installer file 'msi', to be easily deployed using Active Directory, but also using third-party software.

Endpoint Protector comes in two versions: 32-bit and 64-bit targeted installers, as the driver contained within the application can only be built and installed separately for each of the two operating system types.

Because of the two versions of the Endpoint Protector Client installer, two different Group Policy objects will be created in the Active Directory, each having set parameters to install each of the two clients.

The two Group Policy objects will then be filtered using Windows Management Instrumentation filters to be applied only on the computers for which they are created. The Group Policy objects will be later linked to each Organization Unit on which you want to perform the deployment.

This document presents a basic and functional overview of the deployment strategy of Endpoint Protector Client software. You can modify and adjust these techniques to his environment.

2. Create the WMI filters

To create the Windows Management Instrumentation (WMI) filters, follow these steps:

1. Open the **Group Policy Management** console, expand **Domains** and then the domain tree;

🛃 Group Policy Management				-	o x
🔜 File Action View Window Help					- 8 ×
🗢 🔿 🔁 📅 📋 🧟 🔢 🎫					
 Torup Policy Management Torup Policy Management TestEPPQA.com TestEPPQA.com TestEPPQA.com Default Domain Policy Domain Controllers Torup Policy Objects Torup Policy Objects Starter GPOs Sites Group Policy Modeling Group Policy Results 	WMI Filters in Contents Delegati	TESTEPPQA.com	Linked GPO	Author	Created

📕 Group Policy Management		_	
📓 File Action View Window Hel			_ & ×
🗢 🔿 🖄 📰 📋 🙆 🔽 📷			
Group Policy Management A Forest: TESTEPPQA.com Comparis	WMI Filters in TESTEPPQA.com Contents Delegation		
 TESTEPPQA.com Default Domain Policy Domain Controllers Group Policy Objects WMI Filters Starter GPOs Group Policy Modeling Group Policy Results 	New WMI Filter × Name: New WMI Filter Description: Queries: Namespace Query Add Remove Edit	Author	Created
	Save Cancel		>

2. Right-click **WMI Filters** and select **New** – this will open the **New WMI Filter** window;

3. On the **New WMI Filter** window, add entries for **32-bit** and **64-bit** WMI filters by providing the **name**, **description**, and **queries**;

👪 Group Policy Management		- 🗆 🗙
📓 File Action View Window Help		_ 8 ×
🗢 🔿 🙍 🗊 🗎 🙆 🛐		· · · · · · · · · · · · · · · · · · ·
Group Policy Management	WMI Filters in TESTEPPQA.com	
A Forest: TESTEPPQA.com Domains	Contents Delegation	
✓ in Domains ✓ in TESTEPPQA.com	w WMI Filter X	Author Created
Default Domain Policy		
> 📴 Domain Controllers	ame: 2 bit Mindowe	
WMI Filters		
> 🛅 Starter GPOs	escription: 2 hit Windows	
> 📑 Sites		
Croup Policy Results		
	aniespace duery Add pot/CIMv2 Select * from Win32_Processor where	
	AddressWidth = '32' Remove	
	Edit	
	Save Cancel	
L		-
	<	>

🛃 Group Policy Management		- 0	I X
📓 File Action View Window	v Help		_ & ×
🗢 🔿 🙍 📅 📋 🔯 👔	A Contraction of the second se		
Group Policy Management A Forest: TESTEPPQA.com C B Domains	WMI Filters in TESTEPPQA.com Contents Delegation		
V 🚔 TESTEPPQA.com	New WMI Filter ×	Author	Created
 Jefault Domain Jomain Control Group Policy Ob WMI Filters 32 bit Windo Starter GPOs Sites Group Policy Modeling 	Name: 64 bit Windows Description: 64 bit Windows Queries: Namesnace	Administrator@	8/19/2(
🕞 Group Policy Results	root\CIMv2 Select * from Win32_Processor where AddressWidth = "64" Edit		
	Save Cancel		>

4. The new filters will be displayed in the **WMI Filters** folder.



Selecting the 32-bit and 64-bit operating systems:

- **32-bit Operating System:** Select * from Win32_Processor where AddressWidth = '32'
- **64-bit Operating System:** Select * from Win32_Processor where AddressWidth = '64'

You can add the following queries to target certain oeprating systems and/or type of computers:

- Workstation: Select * from WIN32_OperatingSystem where ProductType=1
- **Domain Controller:** Select * from WIN32_OperatingSystem where ProductType=2
- Server: Select * from WIN32_OperatingSystem where ProductType=3

• Windows XP: Select * from WIN32_OperatingSystem where Version='5.1.2600' and ProductType=1

• Windows Vista: Select * from WIN32_OperatingSystem where Version='6.0.6002' and ProductType=1

• Windows 7: Select * from WIN32_OperatingSystem where Version='6.1.7600' and ProductType=1

• Windows 8: SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "6.2%" AND ProductType="1" • Windows 8.1: SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "6.3%" AND ProductType="1"

• Windows 10: SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10%" AND ProductType="1"

• Windows Server 2003: Select * from WIN32_OperatingSystem where Version='5.2.3790' and ProductType>1

• Windows Server 2008: Select * from WIN32_OperatingSystem where Version='6.0.6002' and ProductType>1

• Windows 2008 R2: Select * from WIN32_OperatingSystem where Version='6.1.7600' and ProductType>1

• Window Server 2012: SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "6.2%" AND ProductType="2"

• Windows Server 2012R2: SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "6.3%" AND ProductType="2"

• Windows Server 2016: SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0%" AND ProductType="2"

• Windows Server 2019: SELECT * FROM Win32_OperatingSystem WHERE BuildNumber >= 17763 AND (ProductType="3" OR ProductType="2")

3. Create the deployment GPO

To create the deployment Group Policy Objects (GPO), follow these steps:

 Open the Group Policy Management console, right-click Group Policy Objects and click New;

- 2. Add Endpoint Protector 32 bit as the GPO name;
- 3. Right-click the new GPO and click Edit;

Group Policy Management Edito	r			-	×
File Action View Help					
🗇 🏟 🔲 📰 📓 📓 🖬					
 Endpoint Protector 32 bit [W201 Computer Configuration Policies Preferences User Configuration Policies Preferences Preferences 	Endpoint Protector 32 bit [W2019 Select an item to view its description.	SERV.TESTEPPQA.COMJ Polic Name Computer Configuration User Configuration	y		

4. Expand **Computer Configuration / Software Settings** and right-click **Software Installation**, and then select **New/Package**;

Note: When browsing the 'msi' file, ensure it is located in a folder shared over your network and accessible by the computers on your AD.

Group Policy Management Editor					-	×
File Action View Help						
🗢 🧼 🗖 📰 🖾 🗟 🛛 👔						
 Endpoint Protector 32 bit [W201 Computer Configuration Policies Software Installat Windows Settings Administrative Temp Preferences User Configuration Policies Preferences Preferences 	Name	Version 4.9	Deployment st Assigned	Source C:\Shared\EPPClientSetup_x86_3	32	
< >>						

5. Close the **Group Policy Object Editor** console and repeat this step for the **Endpoint Protector 64 bit64-bit** GPO.

4. Link the WMI to GPO

To link the WMI filters to each GPO, follow these steps:

1. Open the **Group Policy Management** console, select the **Endpoint Protector 32-bit** policy, and on the **WMI Filtering** section, select **32-bit Windows** filter;

2. Repeat this step for **Endpoint Protector 64-bit GPO**.

🔜 Group Policy Management	- 🗆 X
🔜 File Action View Window Help	_ <i>8</i> ×
🗢 🔿 📶 🖸 🔢 🖬	
Group Policy Management Group Policy Management Group Policy Management Group Policy Objects Group Policy Objects Group Policy Objects Default Domain Controller Default Domain Controller Default Domain Policy Endpoint Protector 32 bit Group Policy Objects Group Policy Object	Endpoint Protector 32 bit Scope Details Settings Delegation Status Links Display links in this location: TESTEPPQA.com The following sites, domains, and OUs are linked to this GPO: Location Enforced Link Enabled Path Security Filtering The settings in this GPO can only apply to the following groups, users, and computers:
> 📑 Sites	Name Authenticated Users
	Add Remove Properties
< >>	WMI Filtering This GPO is linked to the following WMI filter: <none> <none> 32 bit Windows 64 bit Windows</none></none>

5. Link the GPO to OU

Once you have created the GPOs, link them to any of your Organization Units (OU).

To do so, follow these steps:

- 1. Right-click the **OU** and then select **Link an Existing GPO**;
- 2. From the **Group Policy objects**, select **Endpoint Protector 32 bit** and then click **OK**;
- 3. Repeat these steps and select the **Endpoint Protector 64-bit**.

Note: The new policies will be applied only when the target computers are rebooted.

📕 Group Policy Management		- 🗆 X
📓 File Action View Window	Help	_ & ×
🗢 🔿 🙋 📅 📋 🗶 📑	ù 🛛 🖬	
📓 Group Policy Management	EPP Deployment	
✓ A Forest: TESTEPPQA.com	Select GPO X	
 Bomains TESTEPPQA.com Default Domain Puiss Domain Controlle EPP Deployment Group Policy Obje WMI Filters Starter GPOs Sites Group Policy Modeling Group Policy Results 	Look in this domain: TESTEPPQA.com Group Policy objects: Name Default Domain Controllers Policy Default Domain Policy Endpoint Protector 32 bit Endpoint Protector 64 bit OK Cancel	GPO Status WMI
		>

6. Disclaimer

The information in this document is provided on an "AS IS" basis. To the maximum extent permitted by law, CoSoSys disclaims all liability, as well as any and all representations and warranties, whether express or implied, including but not limited to fitness for a particular purpose, title, non-infringement, merchantability, interoperability, and performance, in relation to this document. Nothing herein shall be deemed to constitute any warranty, representation, or commitment in addition to those expressly provided in the terms and conditions that apply to the customer's use of Endpoint Protector.

Each Endpoint Protector Server has the default SSH Protocol (22) open for Support Interventions, and there is one (1) System Account enabled (epproot) protected with a password. The SSH Service can be disabled at customers' request.

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.

© 2004 – 2022 CoSoSys Ltd.; Endpoint Protector, My Endpoint Protector, Endpoint Protector Basic and EasyLock are trademarks of CoSoSys Ltd. All rights reserved. Windows is a registered trademark of Microsoft Corporation. Macintosh, Mac OS X, and macOS are trademarks of Apple Corporation. All other names and trademarks are property of their respective owners.

Confidential. © CoSoSys 2022. Not to be shared without the express written permission of CoSoSys

EndpointProtector.com