

Active Directory Configuration

Build 2.2

2020-04-07

Table of Contents

1	Cr	reating a folder in NETLOGON for SAMLite scan scripts	3
2	Se	etting up Scheduled Tasks scanning	4
	2.1	Creating the SAMLiteScan Group Policy Object	4
	2.2	Setting up Scheduled Scans for Windows Vista/2008	6
	2.3	Setting up Scheduled Scans for Windows 7 and later	10
3	Se	etting up Logon Script Scanning	20
	3.1	Creating the SAMLiteLogonScan Group Policy Object	20
	3.	1.1 Copy Logon script files to the Group Policy Object	22
4	Cr	reating a WMI Filter for Windows XP and 2003	26
	4.1	Applying the WMI Filter to the SAMLiteLogonScan GPO	28
5	Ex	xcluding Computers from the SAMLiteScan policy	30

1 Creating a folder in NETLOGON for SAMLite scan scripts

Logon to your AD Server and go to the NETLOGON folder. The NETLOGON folder normally is:

C:\Windows\SYSVOL\sysvol\domain\scripts

Create a folder in scripts called SAMLite. Example:

C:\Windows\SYSVOL\sysvol\domain\scripts\SAMLite

Next, logon to your SAMLite server.

Go to:

C:\Program Files (x86)\SAMLite\V5\WebDash\LoginScripts

Edit the SAMScanConfig.txt file



Replace TheSAMLiteServerAddress in the IncomingPath with the correct IP address or the working fully qualified domain name for the SAMLite server. Replace http with https if you wish to use https and have set up https and have a valid https certificate installed.

Copy the following files to C:\Windows\SYSVOL\sysvol\domain\scripts\SAMLite

SAM.bat localscan.vbs SAMScanConfig.txt wifihelper.exe

The wifihelper.exe file is only useful if you are going to use the geolocation features. It rescans the WiFi information so that the machine's geographical location can be more accurate.

2 Setting up Scheduled Tasks scanning

The Scheduled tasks scan only works for Windows Vista/2008 and later machines by default. For scanning Windows XP/2003 machines please refer to the "Setting up Logon Script Scanning" section.

😹 Group Policy Management					- 0 - X-
<u> F</u> ile <u>A</u> ction <u>V</u> iew <u>W</u> indow <u>H</u> elp	3				_ 8 ×
📓 Group Policy Management	Group Policy Objects in adtest2.here				
A Forest: adtest2.here	Contents Delegation				
⊿ 📑 Domains		000.01		1.4 197 1	
A patest2.here	Name	GPU Status	WMI Hilter	Modified	Uwner
Deradic Domain Policy Demain Controllers	Default Domain Controllers Policy Default Domain Relicy	Enabled	None	4/26/2016 3:50:20 PM	Domain Admins (ADTEST2)
Group Policy Objects		Lindbied	None	4/20/2010 3:33:201 M	Domain Admins (ADTEST2
WMI Filters					
D Image Starter GPOs					
Sites					
Group Policy Modeling					
Croup Policy Results					
	•				Þ
	JL				

2.1 Creating the SAMLiteScan Group Policy Object

Launch Group Policy Management and select Group Policy Objects

Right-click blank space and select New

	New GPO	x
<u>N</u> ame: SAMLiteScan		
Source Starter GPO: (none)		~
	OK	Cancel

SAMLite: Active Directory Configuration

🛒 Group Policy Management					- 0 - X-
<u> F</u> ile <u>A</u> ction <u>V</u> iew <u>W</u> indow <u>H</u> el	p				_ 8 ×
🗇 🔿 🙍 💼 🙆 📷					
📓 Group Policy Management	Group Policy Objects in adtest2.here				
A A Forest: adtest2.here	Contents Delegation				
a 📑 Domains					
adtest2.here	Name	GPD Status	WMI Filter	Modified	Owner
🛒 Default Domain Policy	🧾 🖉 Default Domain Controllers Policy	Enabled	None	4/26/2016 3:50:20 PM	Domain Admins (ADTEST2\
Domain Controllers	Default Domain Policy	Enabled	None	4/26/2016 3:53:26 PM	Domain Admins (ADTEST2)
Group Policy Objects	SAMLiteScan	Enabled	None	5/12/2016 3:04:20 PM	Domain Admins (ADTEST2)
Wivii Filters					
Starter GPOS					
R Group Policy Modeling					
Group Policy Results					
	•				F.
				3 Grou	n Policy object(s)

Right click on SAMLiteScan and select Edit, to set up the Scheduled tasks.

2.2 Setting up Scheduled Scans for Windows Vista/2008

Note: this older type of Scheduled Task may be incompatible with Windows 10 or Windows Server 2016 and newer operating systems. Please refer to the next section for configuring the newer type of Schedule Task.



Go to Computer Configuration, Preferences, Control Panel Settings, Scheduled Tasks

	New Task Properties			
Task Schedule	Settings Common			
Action:	Replace 🗸			
<u>N</u> ame:	SAMLite Scheduled Scan			
<u>R</u> un:	\\YOUR.AD\NETLOGON\SAMLite\SAM.bat			
Arguments:				
<u>S</u> tart in:				
<u>C</u> omments:				
R <u>u</u> n as				
User Na <u>m</u> e:				
Password:				
Confirm Password:				
✓ Enabled (scheduled task runs at a specified time)				
OK Cancel <u>A</u> pply Help				

Right click blank spot and select New -> Scheduled Task

Replace Your.AD with your AD domain e.g. yourdomain.com

Then click on the Schedule tab, check Show Multiple Schedules and select a desired start time for the scan. Notice the 1. This means you are editing the first schedule.

New Task Properties
Task Schedule Settings Common
1. Run on a daily basis
Scheduled Task: Start time: Daily V 10:00:00 AM Advanced Schedule Task Daily Every 1 day(s)
✓ Show multiple schedules
OK Cancel <u>A</u> pply Help

Click New to add more start times if you want. Notice the "2." This means you are editing the second schedule.

New Task Properties			
Task Schedule Settings Common			
2. Run on a daily basis V			
Scheduled Task: Start time: Daily V 12:00 PM Advanced Schedule Task Daily Every 1 day(s)			
✓ Show multiple schedules			
OK Cancel <u>A</u> pply Help			

Click on the Settings tab:

SAMLite Scheduled Scan Properties				
Task Schedule Settings Common				
Scheduled Task Completed				
Delete the task if it is not scheduled to run again.				
✓ Stop the task if it runs for: 2				
Idle Time				
Only start the task if the computer has been idle for at least:				
10 ninute(s)				
If the computer has not been idle that long, retry for up to:				
60 ininute(s)				
\Box Stop the task if the computer <u>c</u> eases to be idle				
Power Management				
Don't start the task if the computer is running on batteries				
Stop the task if battery mode begins				
<u>W</u> ake the computer to run this task				
OK Cancel Apply Help				

Stop task if it runs for 2 hours. Start task even if on batteries. Don't stop if battery mode begins.

	SAMLite Scheduled Scan Pr	operties ×
Task	Schedule Settings Common	
<u>O</u> pt	ons common to all items	
	Stop processing items in this extension if an	error occurs.
	<u>R</u> un in logged-on user's security context (us	er policy option).
 ✓ 	Remove this item when it is no longer applied	<u>.</u>
	Apply once and do not reapply.	
	Item-level targeting.	Targeting
Descri	ption	
		<u>^</u>
		~
	OK Cancel g	Apply Help

Common tab should look like the above. Ensure that "Remove this item when it is no longer applied" is selected so that the task is removed when the policy no longer applies.

2.3 Setting up Scheduled Scans for Windows 7 and later

This section is if you don't have any computers with older Windows OSes and want to setup a Scheduled Task for Windows 7 and later operating systems.

Go to Computer Configuration, Preferences, Control Panel Settings, Scheduled Tasks

Right click blank spot and select New -> Scheduled Task (At Least Windows 7)

	New Task (At least Windows 7) Properties	x
General Triggers	Actions Conditions Settings Common	
	Action:	
Na <u>m</u> e:	SAMLite Scheduled Scan 2	
Author:	ISAT\admlylyeoh	
Description:	SAMLite Scan for Windows 7 and later	
- Security options		
When running th	ne task, use the following user account:	
	Change User or Group	
Run only whe	en user is logged on	
O Run <u>w</u> hether	r user is logged on or not	
🗌 Do not st	ore <u>p</u> assword. The task will only have access to local resources.	
🗌 Run with hig	hest privileges	
🗌 Hidd <u>e</u> n	Configure for: Windows Vistaïć1⁄2 or Windows Serverïč1⁄2 2008 ✔	
	OK Cancel Apply Help	

Click on Change User or Group.

Select User or Group	x
Select this object type:	
User or Built-in security principal	Object Types
Erom this location:	
isat.com	Locations
Enter the object name to select (<u>examples</u>):	
system	<u>C</u> heck Names
,	
Advanced UK	U Uancel

Type system and click Check Names

Multiple Names Found						
More than one object matches the following object name: "system". Select an object from this list or, to reenter the name, click Cancel. Matching names:						
Name	Logon Name (pre-Win	E-Mail Address	In Folder			
SYSTEM						
System Managed A SystemMailbox(1f0 SystemMailbox(2CE SystemMailbox(8cc SystemMailbox(92C SystemMailbox(92C SystemMailbox(1E SystemMailbox(00 SystemMailbox(00	System Managed Acc SM_fa4f4f0bf00f44e68 SM_32e4644a21bd47 SM_b6d1683b46c248 92CCA9E2-4E6F-47C SM_e7d62720001e4c C1E63E92-861E-44E SM_be49625200af41 SM_b47eeda5465b45	SystemMailbox(1f05a SystemMailbox(2CE34 SystemMailbox(8cc37 SystemMailbox(92CC SystemMailbox(b558 SystemMailbox(C1E63 SystemMailbox(D0E4 SystemMailbox(e0dc1	isat.com/Builtin isat.com/Users isat.com/Users isat.com/Users isat.com/Microsoft Ex isat.com/Users isat.com/Microsoft Ex isat.com/Users isat.com/Users			
L		[OK Cancel			

Select SYSTEM and click OK.

Select User or Group	x
<u>S</u> elect this object type: User or Built-in security principal	Dbject Types
Erom this location: isat.com	Locations
Enter the object name to select (<u>examples</u>): <u>SYSTEM</u>	<u>C</u> heck Names
Advanced OK	Cancel

Click OK.

		New Task (At least Windows 7) Properties	x
General Triggers	Actions Conditions	Settings Common	
	Ac <u>t</u> ion: Re	place v	
Na <u>m</u> e:	SAMLite Scheduled	Scan 2	
Author:	ISAT\admlylyeoh		
Description:	SAMLite Scan for V	/indows 7 or later	
Security options	ne task, use the follow	ing user account:	
NT AUTHORITY	/\System	Change User or Group	
O <u>R</u> un only wh	en user is logged on		
● Run <u>w</u> hether	user is logged on or r ore password. The ta	not sk will only have access to local resources.	
Run with hig	hest privileges		
- Hidd <u>e</u> n	<u>C</u> onfigure for:	Windows Vistaič 1/2 or Windows Serverič 1/2 2008	
		OK Cancel Apply Help	

Select Run whether user is logged on or not. And Run with highest privileges.

Then click on the Triggers tab.

	New Task (At le	ast Windows 7) Proper	rties	X
General Triggers Actions	Conditions Settings Common			_
When you create a task, "	you can specify the conditions that (vill trigger the task.		
Trigger	Details		Status	
<u>N</u> ew <u>E</u> di	t <u>D</u> elete			
-		OK Cancel	<u>A</u> pply Help	

Click New to create a new trigger.

	New Trigger
Begin the task: Settings One time Daily Weekly Monthly	On a schedule V Start: 3/24/2020 V 12:30:10 PM Synchronize across time zones Regur every: 1 days
Advanced Setting Delay task for Repeat task e Stop all run	ps up to (random delay): 1 minute wery: 1 hour for a duration of: 1 day nning tasks at end of repetition duration runs leases these
Expire:	3/24/2020 V Caped

Click OK.

				New 1	as <mark>k</mark> (At	least Wi	indow	rs 7) Pro	perti	es		
General	Triggers	Actions	Conditions 9	5ettings	Common							
Whe	n you crea	te a task,	you can specil	fy the co	nditions tha	t will trigge	er the ta	ask.				
Tri	gger		Details	;						Status		
Da	ily		At 12:	30:10 PM	l every day					Enabled		
	<u>N</u> ew	Ē	dit	<u>D</u> elete					1		1	
						ОК		Cancel		Apply		Help

Create more triggers as desired. Example:

	Indicons Seconds Common	
Vhen you create a task, yo	u can specify the conditions that will trigger the task.	
Trigger	Details	Status
Daily	At 1:05:05 PM every day	Enable
At startup	At system startup	Enable
Daily	At 10:05:02 AM every day	Enable
Daily	At 4:20:08 PM every day	Enable
At log on	At log on of any user	Enable
	On manhakaking malaglu af ann man	Feeble

Some possible options:

- At startup = on machine startup
- At log on = at local logon or remote desktop logon (but not reconnect)
- On connection to user session (remote) if remote desktop reconnect
- On connection to user session (local) if reconnect to existing session locally.
- On workstation unlock only if unlocking screen locally
- On an event when an Event occurs (e.g. System, Microsoft-Windows-Power-Troubleshooter, Event ID:1 for wakeup/resume)

More than one trigger can be active. E.g. you can add "At log on" and "On workstation unlock".

Suggested are a daily scan and a log on or start up and wake up event scan with delays of 1 minute or 30 minutes.

Next, click on the Action tab.

				New 1	Task (At least Windows 7) Properties
General	Triggers	Actions	Conditions	Settings	Common
Whe	en you crea	ite a task,	you must sp	ecify the a	action that will occur when your task starts.
Ac	tion			Deta	ails
	<u>N</u> ew		lit	Delete	
L					OK Cancel Apply Help

Click on New...

	l	New Actio	on		x
You must spe	cify what action th	is task will pe	rform.		
Action:	Start a program				~
Settings	. L.				
Program/se	:ript: \\NETLOGON\SAMLi	ite\SAM.bat		Browse	1
<u>A</u> dd argum	ents(optional):				
S <u>t</u> art in(op	tional):				
			ОК	Cancel	

Replace Your.AD with your AD domain e.g. yourdomain.com

Click on the Conditions tab.

New Task	(At least Windows 7) Properties
General Triggers Actions Conditions Settings Com	nmon
Specify the conditions that, along with the trigger, de run if any condition specified here is not true.	etermine whether the task should run. The task will not
Idle	
\Box Start the task only if the computer is idle for:	5 minutes V
W <u>a</u> it for idle for:	1 hour v
Stop if the comput <u>e</u> r ceases to be idle	
Restart if the idle state res <u>u</u> mes	
Power	
Start the task only if the computer is on AC power	
Stop if the computer switches to battery power	
$\hfill \underline{W}$ ake the computer to run this task	
81-burredi	
Network	
Vetwork	allable
Network ✓ Start only if the following network connection is av-	ailable:
Network Start only if the following network connection is avected as a second start on the following network connection is a second start of the following	ailable:]

Start only if the computer might have network connectivity.

Click on the Settings tab.

New Task (A	At least Windows 7) Properties							
General Triggers Actions Conditions Settings Commo	n							
Special additional settings that affect the behavior of the	e task.							
Allow task to be run on demand								
Run task as soon as possible after a scheduled start is	s missed							
If the task fails, restart every:	1 minute V							
Attempt to restart up to:	3 times							
Stop the task if it runs longer than:	2 hours ¥							
\blacksquare If the running task does not end when requested, for	ce it to stop							
\Box If the task is not scheduled to run again, delete it after	ar: 30 days 🗸							
If the task is already running, then the following rule applies:								
Stop the existing instance								
	OK Cancel <u>A</u> pply Help							

Recommended settings are as above. Click on the Common tab.

				New 7	Tas <mark>k</mark> (At l	east V	vindo	ws 7) Pi	ropert	ies	
General	Triggers	Actions	Conditions	Settings	Common						
Optio	ns common	i to all iten	ns								
√ S	top proces:	sing items	in this exten	sion if an e	error occurs.						
R	un in logge	d-on user	's security co	ntext (use	r policy opti	on).					
∠ R	emove this	item whe	n it is no long	er applied							
	pply once a	and do no	t reapply.								
	em-level ta	argeting.		[Targeti	ng					
Descrip	tion					_	< >				
						OK		Cancel		Apply	Help

Recommended settings as above. Click OK.

You now have created the SAMLiteScan group policy object.

Next link it to the domain or OUs you wish it to be applied to.

Right click on the target domain.

ilie Action View Window Help iii Action View Window Help iii Goup Picity Managenet: iii Goup Picity Managenet: iii Goup Picity Danian Controllers iii Default Domain Controllers iii Goup Picity Millikes iii Goup Picity Results iii Goup Picity Results iii Goup Picity Results	up Policy Management										x
A Const dest Likere Commans Computer Stackbard Formskan Computer Stackbard	Action View Window Help									-	Б×
Image: Step Policy Management Image: Step Policy Results) 🖄 📰 📋 💿 🔍 🔽 📰										
▲ Sorvets attest2.here	oup Policy Management	adtest2.here									
Converse Sector 2015 Converse Sector	Forest: adtest2.here	Linked Group Policy Objects	Group Policy Inheritance	Delegation							
I Default Domain Controllers I Offault Domain Controllers I Offault Domain Controllers I Offault Domain Controllers I Offault Domain Controllers I WMITHERS I MMITHERS I MMITHERS I MMITHERS I MULTINES I Stee I Group Policy Modeling I Group Policy Results	a 🚔 adtest2.here	Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain		
Computeristiculated romain Controllers Computeristiculated romain Controllers Computeristiculated romain Controllers Softer BODs Stef Group Policy Medeling Computeristiculated romain Controllers Computeristiculated romain Contromain Controllers Computeristiculated romain Controllers C	🛒 Default Domain Policy	会 1	🗊 Default Domain Policy	No	Yes	Enabled	None	4/26/201	adtest2		
ComputerSclubedFromScale ComputerScale Computer	Domain Controllers Default Domain Controllers										
 Group Policy Objects MML Filters Stater OPO: Stes Group Policy Results 	ComputersExcludedFromScan	~									
Image: State GPO: Image	Group Policy Objects	~									
Image: Stass Image: Group Policy Results	WMI Filters Starter GPOs										
	👔 Sites										
	👸 Group Policy Modeling										
	ered of the provide y nesters										
	······································]									
				_							

> 2 24	Create a GPO in this domain, and Link it here
> 🔤 SC	Link an Existing GPO
S Sh	Block Inheritance
> 🖬 Te	Group Policy Undate
> 🗊 Te	
> 🗊 Te	Group Policy Modeling Wizard
🛯 📑 Gr	New Organizational Unit

Select Link an Existing GPO.

Select GP	×
Look in t	this domain:
a	dtest2.here
<u>G</u> roup P	olicy objects:
r	Name
[[Default Domain Controllers Policy Default Domain Policy
	SAMLiteScan
	OK Cancel

Select SAMLiteScan, click OK.

3 Setting up Logon Script Scanning

This method works on Windows XP/2003 machines. For more recent Windows versions it is recommended to use the Scheduled Task method which does not require users to logon regularly.

😹 Group Policy Management					
📓 Eile Action View Window Help					
📓 Group Policy Management	Group Policy Objects in adtest2.here				
A A Forest: adtest2.here	Contents Delegation				
a 📑 Domains					
adtest2.here	Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Policy	I Default Domain Controllers Policy	Enabled	None	4/26/2016 3:50:20 PM	Domain Admins (ADTEST2)
Domain Controllers	🧾 🧾 Default Domain Policy	Enabled	None	4/26/2016 3:53:26 PM	Domain Admins (ADTEST2\
> Group Policy Objects					
Starter GBOr					
Sites					
R Group Policy Modeling					
Group Policy Results					
					>
	11			2 Grou	n Policy object(c)

3.1 Creating the SAMLiteLogonScan Group Policy Object

Launch Group Policy Management and select Group Policy Objects

Right-click blank space and select New

New GPO	X
<u>N</u> ame:	
SAMLiteLogonScan	
Source Starter GPO:	
(none)	•
	OK Cancel

Click OK

🗐 Group Policy Management Edite	or		
<u>File Action View H</u> elp			
🗢 🔿 🖄 🖬 🖬 🔒 👔 🛙	28		
SAMLiteLogonScan [ARCHITECT.IS	😸 Scripts (Logon/Logoff)		
Policies Preferences	Logon	Name	
 M User Configuration Policies 	Display <u>Properties</u>	;;;; Logoff	
	Description: Contains user logon scripts.		
I F	Extended Standard		

Edit the SAMLiteLogonScan policy and go to User Configuration, Policies, Windows Settings, Scripts (Logon/Logoff).

Right click Logon, click Properties.

gon Properties		?
Scripts PowerShell Scrip	ts	
Logon Scrip	ts for SAMLiteScan	
Name	Parameters	
		Цр
		Do <u>w</u> n
		bbA
		Edit
		Bemove
1		Temore
To view the script files st the button below. <u>S</u> how Files	ored in this Group Policy Obje	ect, press
	OK Car	cel Apply

3.1.1 Copy Logon script files to the Group Policy Object

Click Show Files

📙 Logon							- 🗆 ×
() () () () () () () () () () () () () (ere\SysVol\adtest2.here\Policies\{6B4818FC-58CA-4834-	-8619-A93E3C5D5A03}\U	ser\Scripts\Logon	🗸 🚰 Search	n Logon		2
<u>File E</u> dit <u>V</u> iew <u>T</u> ools <u>F</u>	<u>t</u> elp						
Organize 🔻 New folder						•	
★ Favorites	Name ^	Date modified	Туре	Size			
Desktop Downloads Mecent Places		This fold	er is empty.				
🧊 Libraries 📑 Documents 💌							
0 items Of Offline	fline status: Online availability: Not available						

Copy the scan script files into this folder from:

C:\Windows\SYSVOL\sysvol\domain\scripts\SAMLite

🕌 Logon					
i\adtest2.he	re\SysVol\adtest2.here\Policies\{6B4818FC-58CA-4834	+-8619-A93E3C5D5A03}\L	ser\Scripts\Logon	🕶 🛃 🛛 Search Lo	ogon 🙋
<u>File E</u> dit <u>V</u> iew <u>T</u> ools <u>H</u>	elp				
Organize 🔻 New folder					🖽 👻 🛄 🔞
★ Favorites	Name ^	Date modified	Туре	Size	
🧮 Desktop	😹 localscan.vbs	6/28/2016 6:03 PM	VBScript Script File	112 KB	
Downloads	🚳 sam.bat	5/13/2016 3:45 PM	Windows Batch File	1 KB	
🕍 Recent Places	SAMScanConfig.txt	6/29/2016 11:37 AM	Text Document	1 KB	
🔚 Libraries					
Documents					
3 items Off Offline	line status: Online availability: Not available				

Close the window.

ogon Properties			? ×
Scripts PowerShell Scripts			
Logon Scripts f	or SAMLiteScan		
Name	Parameters		
	- 1 didino(ors		Up
			Down
			<u>E</u> dit
			<u>R</u> emove
To view the script files store the button below. <u>S</u> how Files	ed in this Group P	olicy Object, pr	ess
	OK	Cancel	Apply

Go back to Logon Properties and click Add...

Add a Script		×
Script <u>N</u> ame:		
		Browse
Script <u>P</u> arameters:		
	01/	
	UK.	Lancel

Click Browse.



Select sam.bat and Open.

Add a Script		×
Script <u>N</u> ame:		
sam.bat		Browse
Script <u>P</u> arameters:		
	OK	Cancel

Click OK.

Logon Properties	? ×
Scripts PowerShell Scripts	
Logon Scripts for SAMLiteScan	
Name Parameters	
sam.bat	Цр
	Do <u>w</u> n
	A <u>d</u> d
	<u>E</u> dit
	<u>R</u> emove
To view the script files stored in this Group Policy Object, p the button below. <u>S</u> how Files	ress
OK Cancel	

Click OK. And you are now done with Configuring Logon Script scanning.

4 Creating a WMI Filter for Windows XP and 2003

Next create a WMI Filter for Windows XP and 2003 only. This is if you wish to limit the SAMLiteLogonScan policy to only XP and 2003 machines (the scheduled task policy will work for newer Windows OS).

E Group Policy Management		
Eile Action View Window Help		_ _ _ _ ×
🗢 🧼 🖄 📰 📋 🙆 🔽 🖬		
	WMI Filters in isat.com Contents Delegation	
 	Name Time Transformer State S	Description
E I Testing Group Policy Objects Group Policy Objects	₩indows Clients	Windows clients only
Group Policy Modeling Group Policy Results	<u>_</u>	

Right click in the blank space and select New...

New WM1 Filter	×
Name:	
Windows XP/2003 only	
Description:	
Only XP and 2003 machines	
Queries:	
Namespace Query Add	
Bemova	
<u>E</u> dit	
Save Cancel	

Click Add

WMI Query	×
Namespace:	
root\CIMv2	owse
<u>Q</u> uery:	
select *from Win32_OperatingSystem where Version like "5.1%" o Version like "5.2%"	r 🔺
	V
ок	ancel

Set the query accordingly. Click OK

New WMI Filter		×
<u>N</u> ame:		
Windows XP/200	3 only	
Description:		
Only XP and 2003	machines	
<u>Q</u> ueries:		
Namespace	Query	Add
root\CIMv2	select * from Win32_OperatingSystem where Version like "5.1%" or Version like "5.2%"	Remove
		Edit
1		J
	<u>S</u> ave	Cancel

Click Save.

4.1 Applying the WMI Filter to the SAMLiteLogonScan GPO

SAMLiteLogonScan
Scope Details Settings Delegation
Links
Display links in this location:
The following sites, domains, and OUs are linked to this GPO:
Location A Enforced Link Enabled Path
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name A
Authenticated Users
Add Remove Properties
WMI Filtering
This GPO is linked to the following WMI filter:
<none></none>

Select the SAMLiteLogonScan GPO.

Click on the drop-down in WMI Filtering and select "Windows XP/2003 only"



Click Yes.

SAMLiteLogonScan
Scope Details Settings Delegation
Links
Display links in this location:
The following sites, domains, and OUs are linked to this GPO:
Location A Enforced Link Enabled Path
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
3 S-1-5-11
Remove Properties
·
WMI Filtering
This GPO is linked to the following WMI filter:
Windows XP/2003 only Open

You now have created the SAMLiteLogonScan group policy object and ensured that it can only apply to the Windows XP/2003 machines.

You may also wish to add the Software Restriction policies to this group policy object. To do that refer to Section 2 "Adding Software Restriction Policies."

Next link it to the domain you wish it to be applied to.

5 Excluding Computers from the SAMLiteScan policy

To apply the SAMLiteScan policy on only certain computers. Select the SAMLite Scan GPO then in the Security Filtering section remove *Authenticated Users* and add the Group containing the computers you want scanned.

To apply the SAMLiteScan policy on all computers except certain computers or groups (

https://support.microsoft.com/en-us/kb/816100)

K Group Policy Management			
📓 Eile Action View Window Help			_ <i>B</i> ×
🧇 🔿 🔽 🖬 🤷 🔢 🖬			
Group Policy Management Group Policy Management Group Policy Management Group Policy Group Policy Group Policy Group Policy Objects Default Domain Controllers Default Domain Controllers Group Policy Results	SAMLiteScan Scope Details Setting: Delegation These groups and users have the specified permission for this GPO Groups and users: Name Anternicated Users Domain Anthrins (ADTEST2NO-main Anthrins) Enterprise Anthrins (ADTEST2NO-main Anthrins) Enterprise Anthrins (ADTEST2NO-main Anthrins) Strategy DomAin CONTROLLERS SYSTEM	Allowed Permissions Read (from Security Filering) Edit settings, delete, modify security Read Edit settings, delete, modify security	Inherited No No No No No
	Add Bemove Properties		Advanced
۰ III ا	Touroso Tidheires		marageou

Click on Add...

Select User, Computer, or Group	? ×
Select this object type:	
User, Group, or Built-in security principal	Object Types
Erom this location:	
adtest2.here	Locations
Enter the object name to select (<u>examples</u>):	
GRPComputersExcludedFromScan	Check Names
Advanced	OK Cancel

Add the object (click on Object Types and select Computers if you want to add Computers individually instead of groups)

Add Group or User	×
Group or user name:	
ADTEST2\GRPComputersExcludedFromScan	Browse
Permissions:	
Read	
ОК	Cancel

Click OK.

Then click on Advanced... (at bottom right of main GPMC console)

SAMLiteScan Security Settings		×	
Security			
Group or user names:			
& CREATOR OWNER		*	
Authenticated Users & SYSTEM		=	
GRPComputersExcludedFromS ADD Domain Admins (ADTEST2\Do	can (ADTEST2\ main Admins)	GRPComp	
· · · · · · · · · · · · · · · · · · ·			
	A <u>d</u> d	<u>R</u> emove	
Permissions for CREATOR	Allow	Deny	
Full control			
Read			
Write			
Create all child objects			
Delete all child objects			
For special permissions or advanced click Advanced.	settings,	Advanced	
Learn about access control and per	nissions		
ОК	Cancel	Apply]

SAMLiteScan Security Settings		×	
Security			
Group or user names:			
& CREATOR OWNER			
Authenticated Users		=	
SYSTEM			
GRPComputersExcludedFromS	ican (ADTEST2) Interiment	GHPCompt	
	main Aumins)	•	
		Denen	
Barmianiana far	A <u>a</u> a	<u>H</u> emove	
GRPComputersExcludedFromSca	Allow	Deny	
Write			
Create all child objects			
Delete all child objects		=	
Apply group policy		V	
Special permissions		-	
For special permissions or advanced click Advanced.	l settings,	Ad <u>v</u> anced	
Learn about access control and per	missions		
OK	Cancel]

Select the object/group and scroll down in the permissions and click on Deny for "Apply group policy"

Windows S	iecurity 📃
	You are setting a deny permissions entry. Deny entries take precedence over allow entries. This means that if a user is a member of two groups, one that is allowed a permission and another that is denied the same permission, the user is denied that permission. Do you want to continue?
	<u>Y</u> es <u>N</u> o

Click Yes



Note: policy changes due to a change in a machine's group membership only take into effect after the machine is rebooted.