Active Directory Configuration

Build 2.2

2020-04-07

Table of Contents

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:

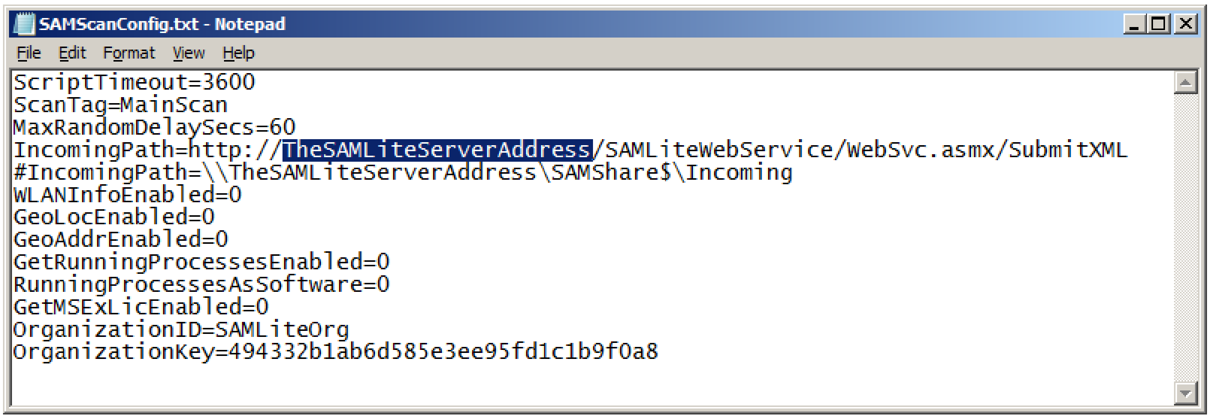
```
C:\Windows\SYSVOL\sysvol\domain\scripts\SAMLite
```

Next, logon to your SAMLite server.

Go to:

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

Edit the *SAMScanConfig.txt* file



```
ScriptTimeout=3600
ScanTag=MainScan
MaxRandomDelaySecs=60
IncomingPath=http://TheSAMLiteServerAddress/SAMLiteWebService/WebSvc.asmx/SubmitXML
#IncomingPath=\\TheSAMLiteServerAddress\SAMShare$\Incoming
WLANInfoEnabled=0
GeoLocEnabled=0
GeoAddrEnabled=0
GetRunningProcessesEnabled=0
RunningProcessesAsSoftware=0
GetMSExLicEnabled=0
OrganizationID=SAMLiteOrg
OrganizationKey=494332b1ab6d585e3ee95fd1c1b9f0a8
```

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`

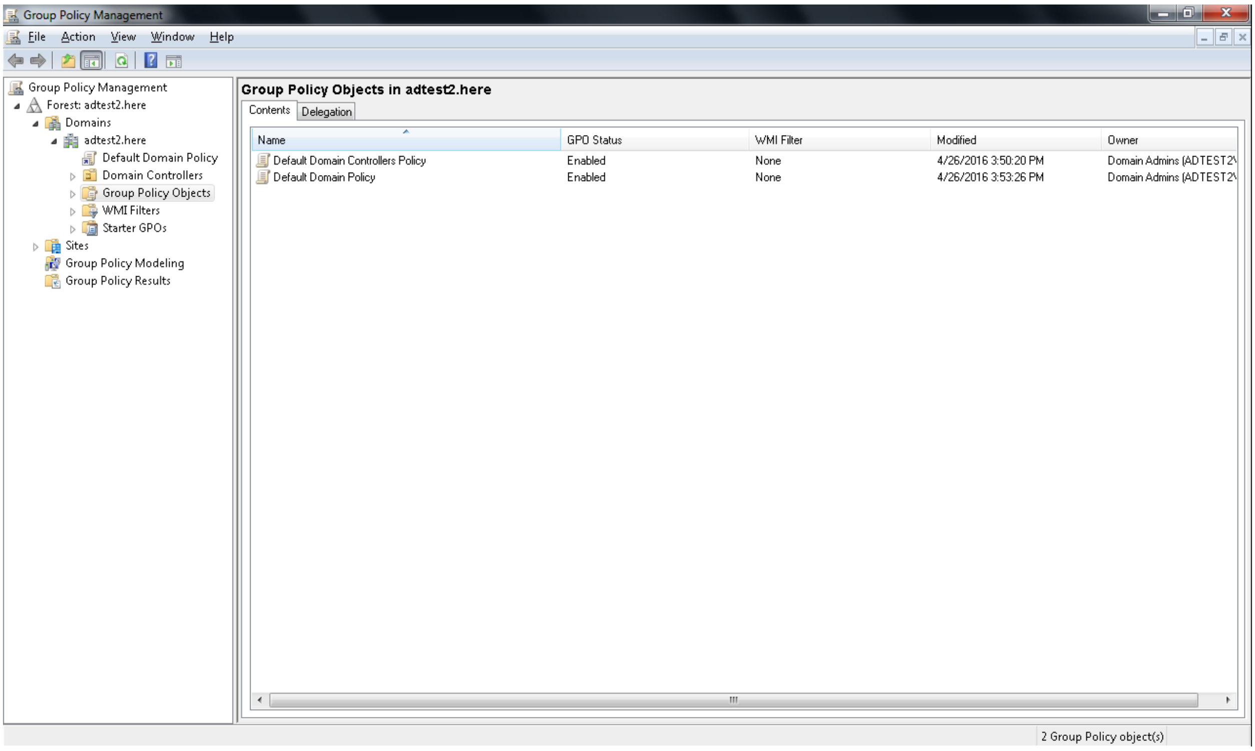
SAM.bat
localscan.vbs
SAMScanConfig.txt
wifihelper.exe

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.

2.1 Creating the SAMLiteScan Group Policy Object

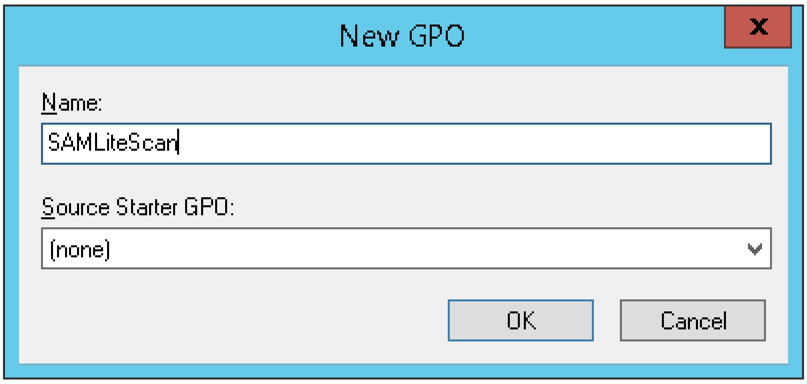


Group Policy Objects in adtest2.here

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	4/26/2016 3:50:20 PM	Domain Admins (ADTEST2\
Default Domain Policy	Enabled	None	4/26/2016 3:53:26 PM	Domain Admins (ADTEST2\

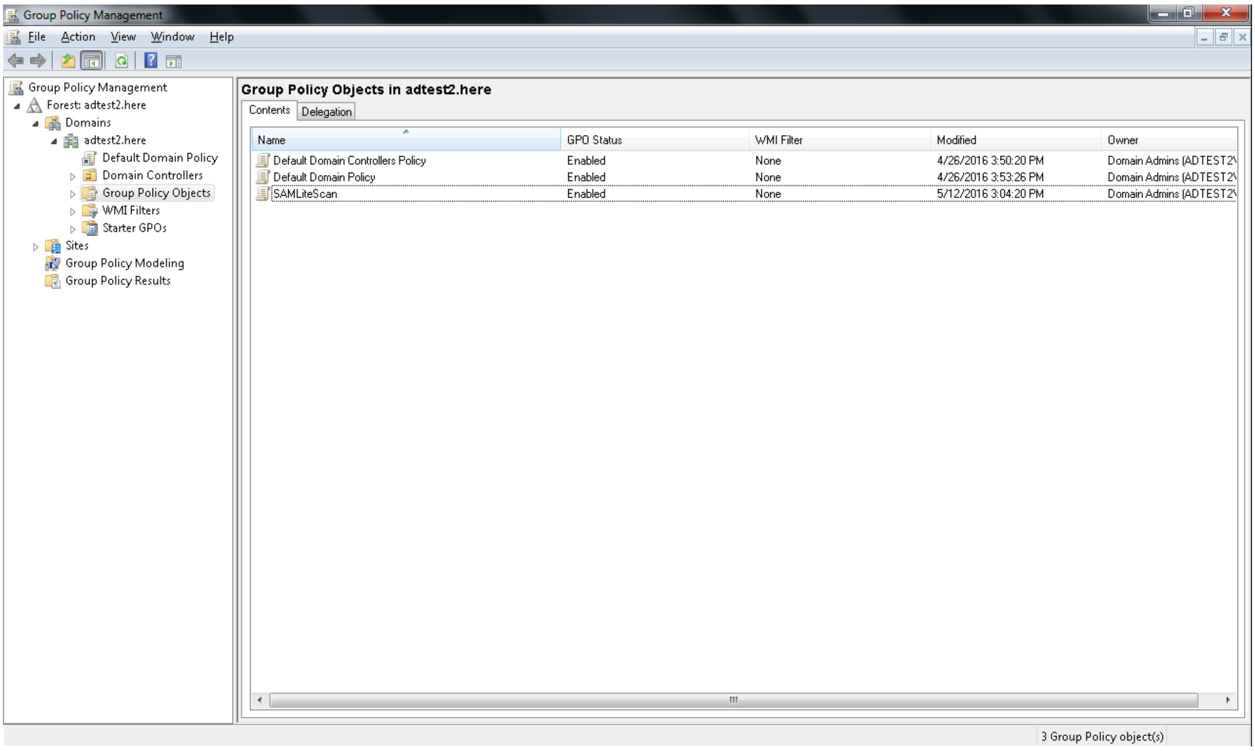
Launch Group Policy Management and select Group Policy Objects

Right-click blank space and select New



Name: SAMLiteScan

Source Starter GPO: (none)



Group Policy Objects in adtest2.here

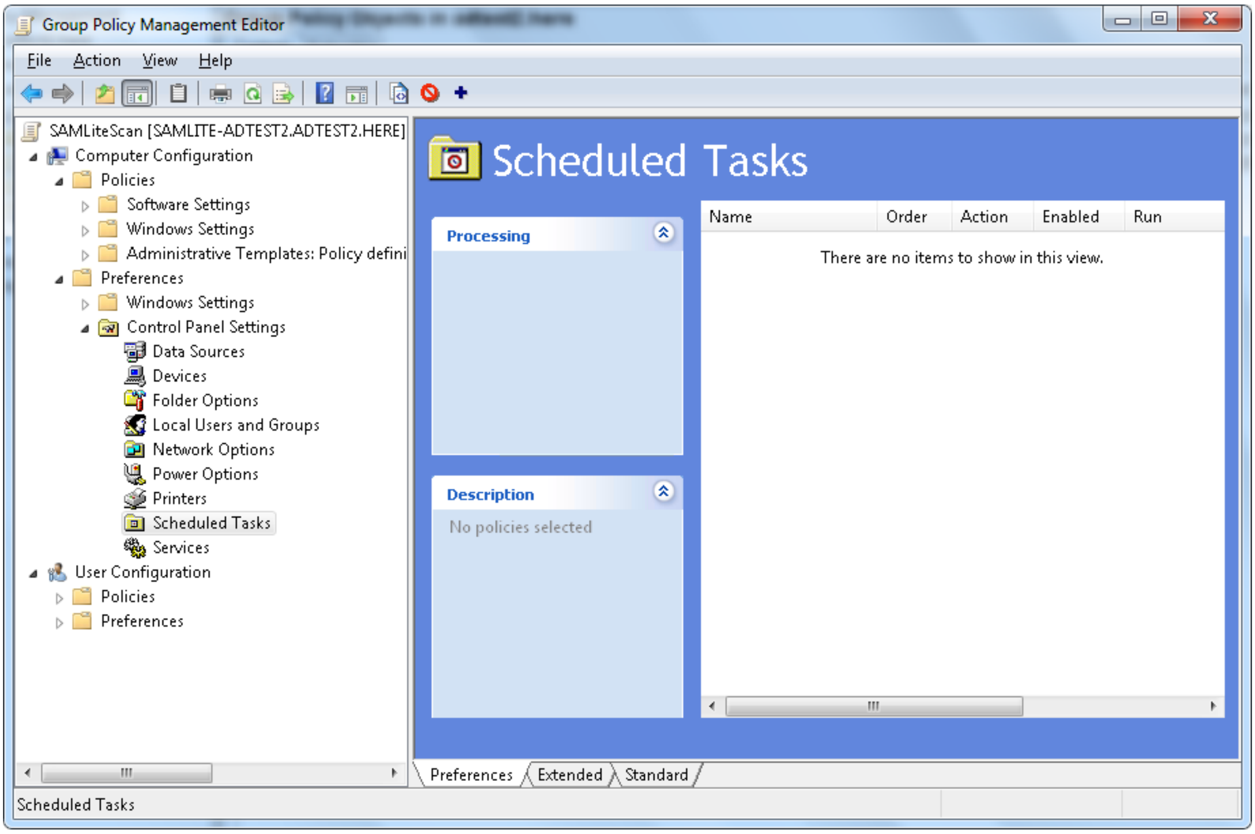
Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	4/26/2016 3:50:20 PM	Domain Admins (ADTEST2\
Default Domain Policy	Enabled	None	4/26/2016 3:53:26 PM	Domain Admins (ADTEST2\
SAMLiteScan	Enabled	None	5/12/2016 3:04:20 PM	Domain Admins (ADTEST2\

3 Group 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.

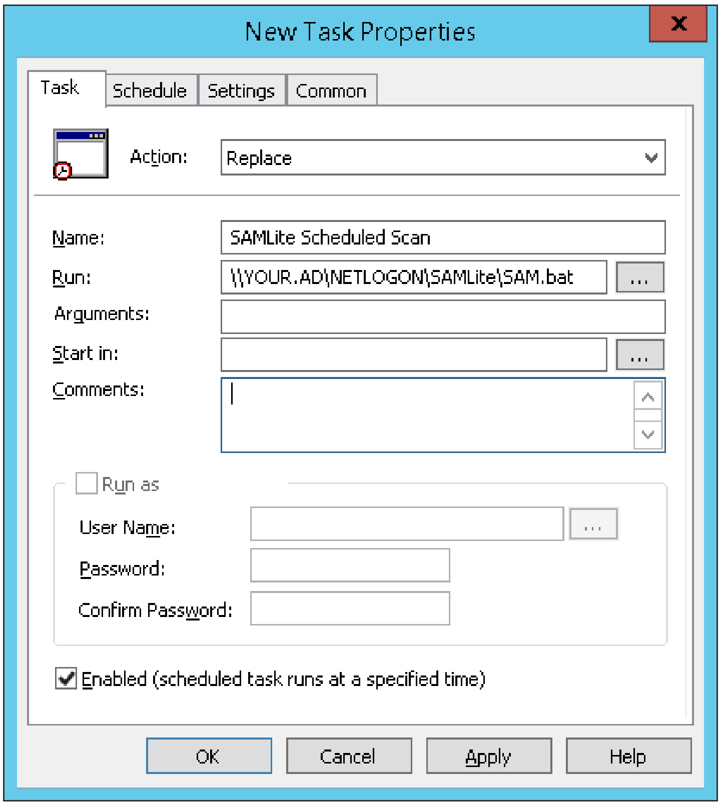


No policies selected

There are no items to show in this view.

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

Right click blank spot and select New -> Scheduled Task



Action: Replace

Name: SAMLite Scheduled Scan

Run: \\YOUR.AD\NETLOGON\SAMLite\SAM.bat

Arguments:

Start in:

Comments:

□ Run as

User Name:

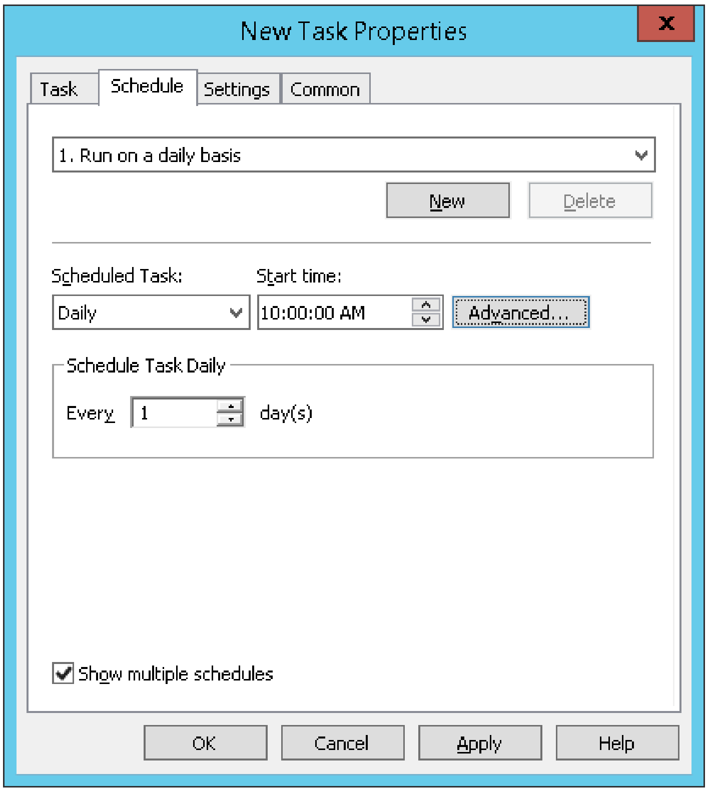
Password:

Confirm Password:

☑ Enabled (scheduled task runs at a specified time)

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.



1. Run on a daily basis

Scheduled Task: Daily

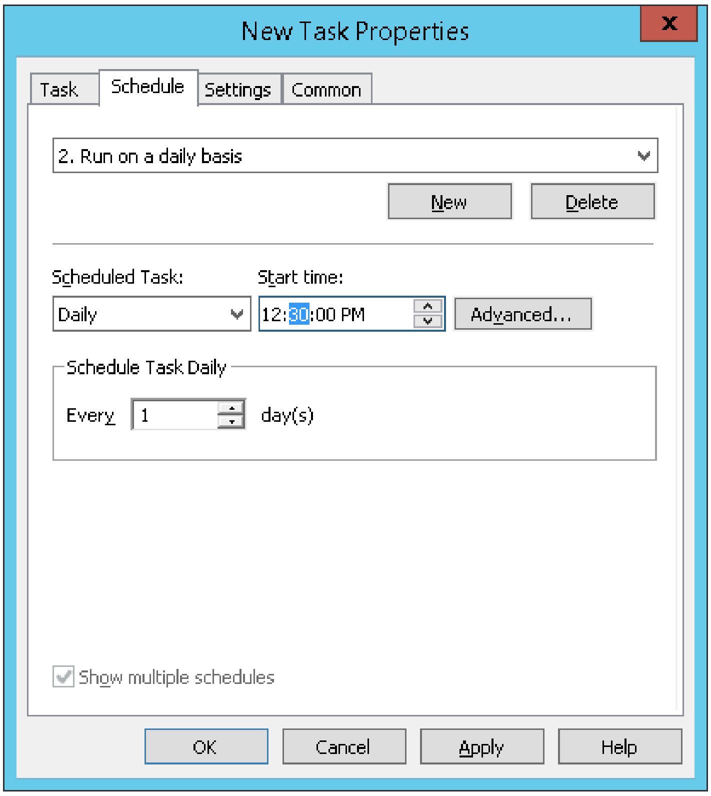
Start time: 10:00:00 AM

Schedule Task Daily

Every 1 day(s)

☑ Show multiple schedules

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



2. Run on a daily basis

Scheduled Task: Daily

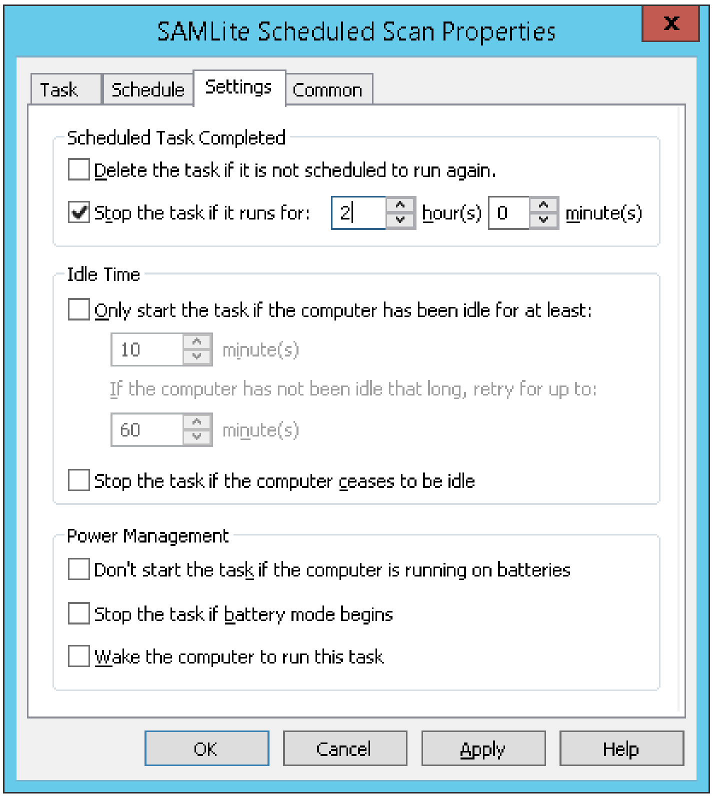
Start time: 12:30:00 PM

Schedule Task Daily

Every 1 day(s)

☑ Show multiple schedules

Click on the Settings tab:



Scheduled Task Completed

□ Delete the task if it is not scheduled to run again.

☑ Stop the task if it runs for: 2 hour(s) 0 minute(s)

Idle Time

□ Only start the task if the computer has been idle for at least:

10 minute(s)

If the computer has not been idle that long, retry for up to:

60 minute(s)

□ Stop the task if the computer ceases to be idle

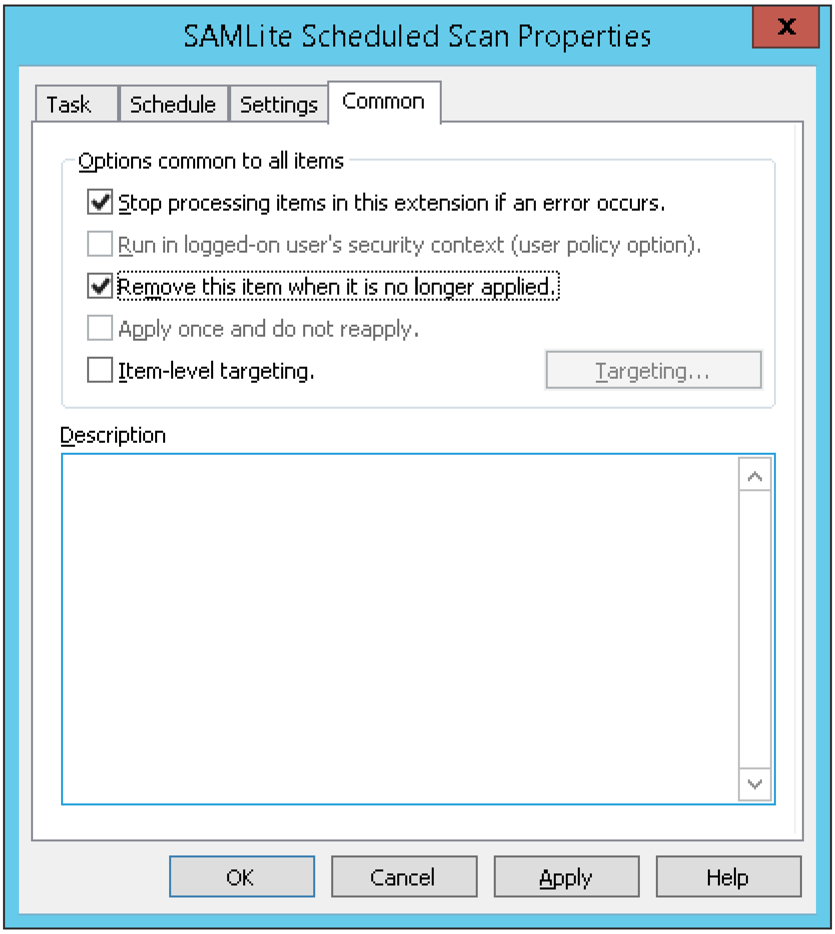
Power Management

□ Don't start the task if the computer is running on batteries

□ Stop the task if battery mode begins

□ Wake the computer to run this task

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



SAMLite Scheduled Scan Properties

Options common to all items

☑ Stop processing items in this extension if an error occurs.

□ Run in logged-on user's security context (user policy option).

☑ Remove this item when it is no longer applied.

□ Apply once and do not reapply.

□ Item-level targeting.

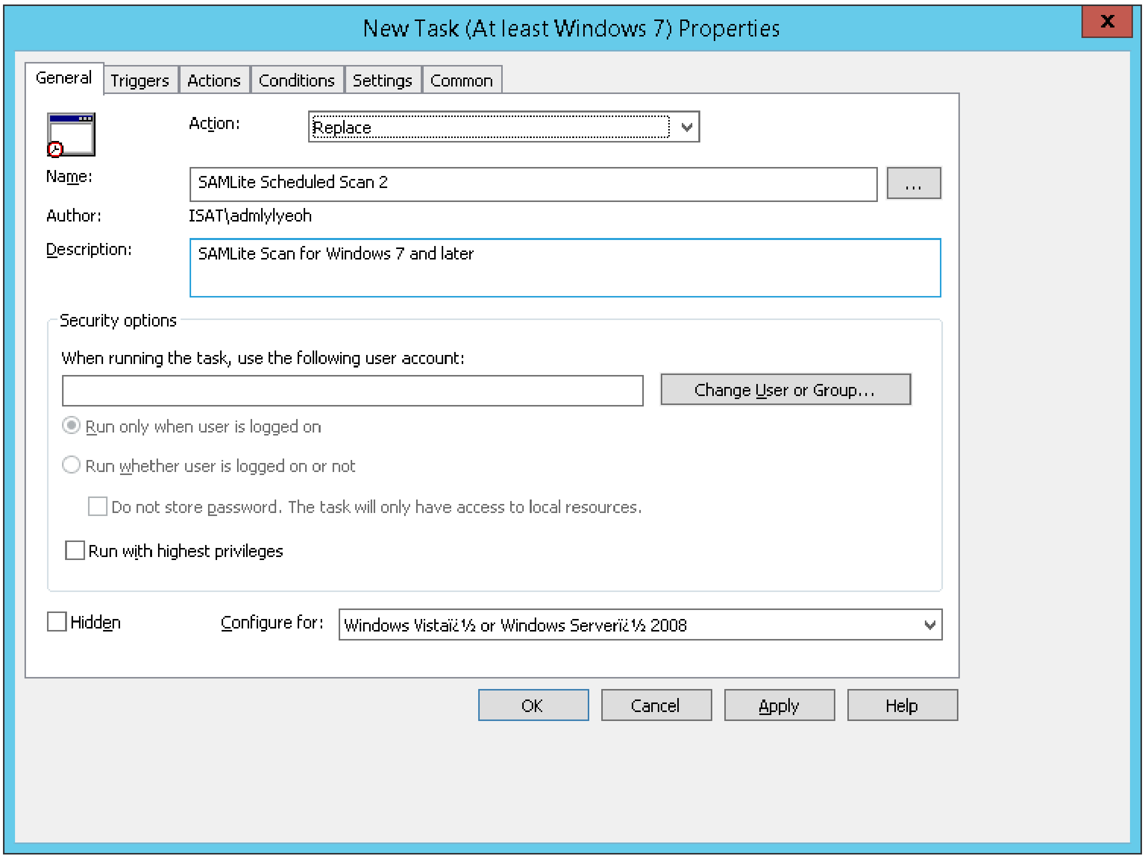
Common tab should look like the above. Ensure that “Remove this item when it is no longer applied” is selected so that the task is removed when the policy no longer applies.

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)



Action: Replace

Name: SAMLite Scheduled Scan 2

Author: ISAT\admlylyeoh

Description: SAMLite Scan for Windows 7 and later

Security options

When running the task, use the following user account:

● Run only when user is logged on

○ Run whether user is logged on or not

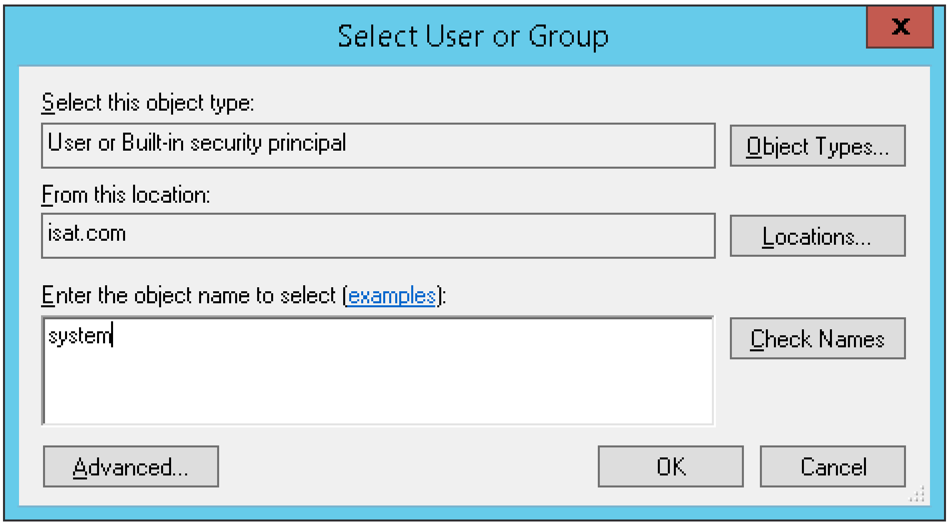
□ Do not store password. The task will only have access to local resources.

□ Run with highest privileges

□ Hidden

Configure for: Windows Vistaï¿½ or Windows Serverï¿½ 2008

Click on Change User or Group.

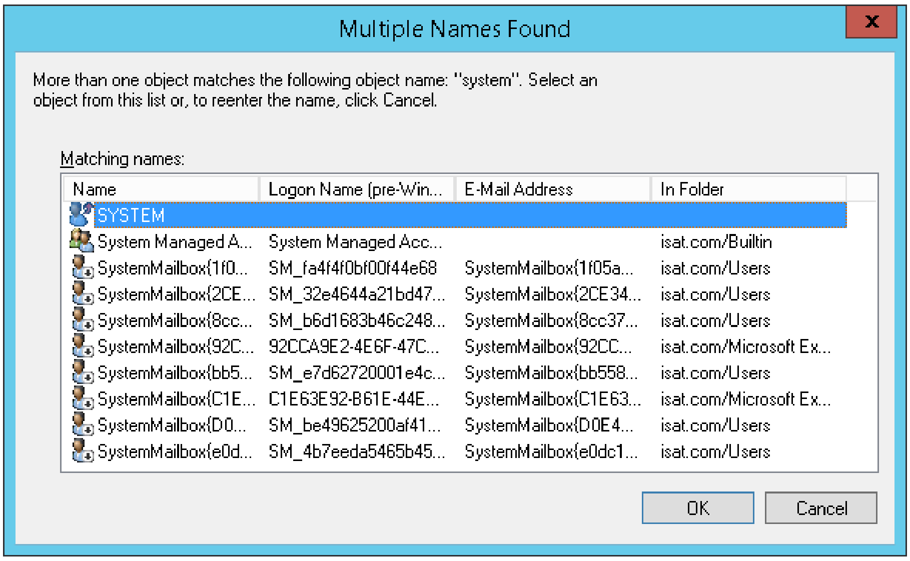


Select this object type: User or Built-in security principal

From this location: isat.com

Enter the object name to select (examples): system

Type system and click Check Names

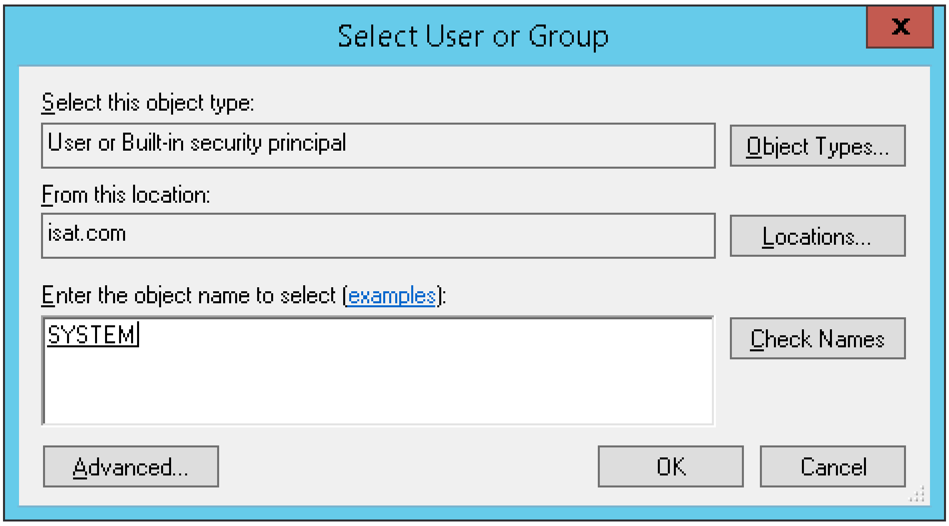


More than one object matches the following object name: "system". Select an object from this list or, to reenter the name, click Cancel.

Matching names:

Name	Logon Name (pre-Win...	E-Mail Address	In Folder
SYSTEM			
System Managed A...	System Managed Acc...		isat.com/Builtin
SystemMailbox{1f0...	SM_fa4f4f0bf00f44e68	SystemMailbox{1f05a...	isat.com/Users
SystemMailbox{2CE...	SM_32e4644a21bd47...	SystemMailbox{2CE34...	isat.com/Users
SystemMailbox{8cc...	SM_b6d1683b46c248...	SystemMailbox{8cc37...	isat.com/Users
SystemMailbox{92C...	92CCA9E2-4E6F-47C...	SystemMailbox{92CC...	isat.com/Microsoft Ex...
SystemMailbox{bb5...	SM_e7d62720001e4c...	SystemMailbox{bb558...	isat.com/Users
SystemMailbox{C1E...	C1E63E92-B61E-44E...	SystemMailbox{C1E63...	isat.com/Microsoft Ex...
SystemMailbox{D0...	SM_be49625200af41...	SystemMailbox{D0E4...	isat.com/Users
SystemMailbox{e0d...	SM_4b7eeda5465b45...	SystemMailbox{e0dc1...	isat.com/Users

Select SYSTEM and click OK.

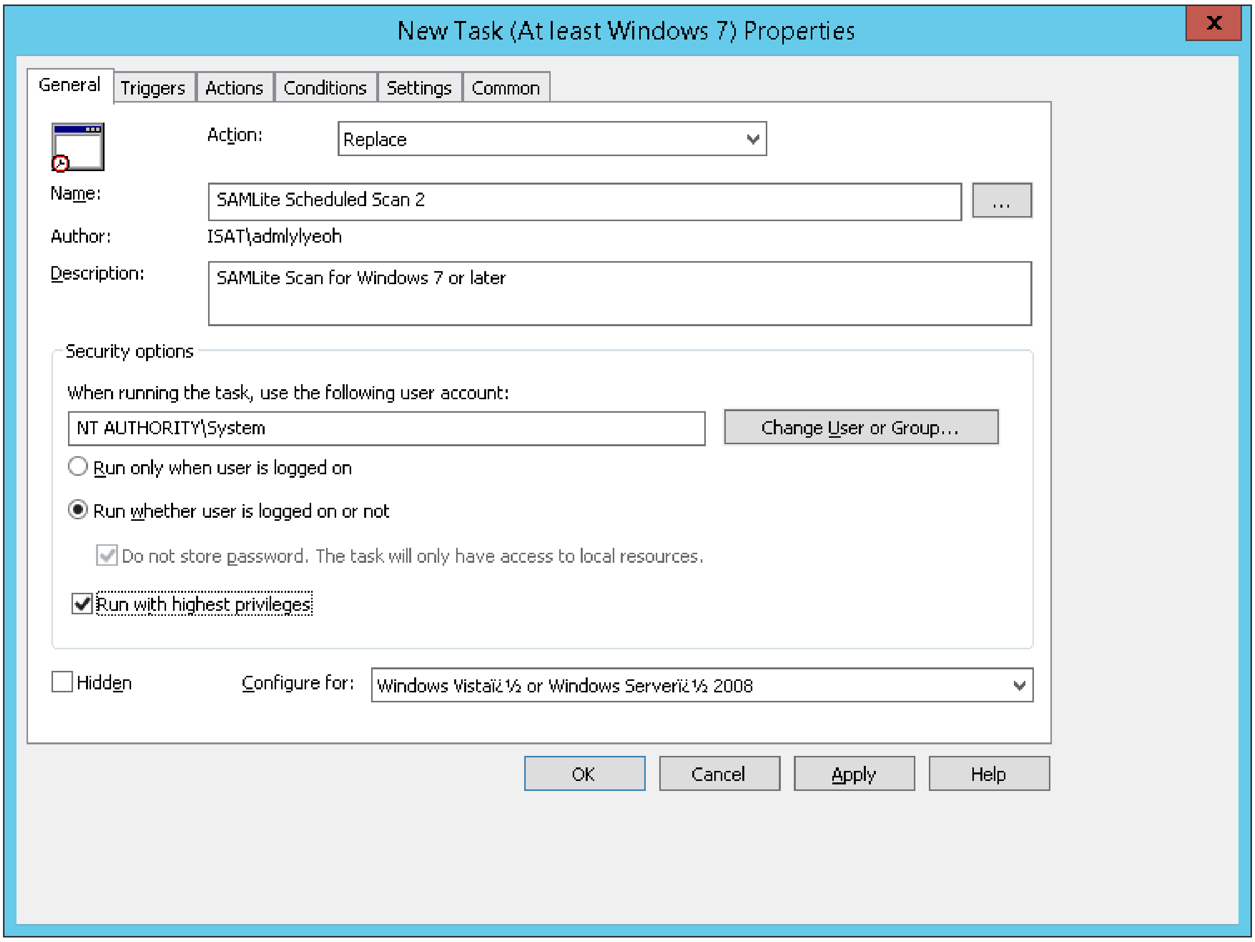


Select this object type:
User or Built-in security principal

From this location:
isat.com

Enter the object name to select (examples):
SYSTEM

Click OK.



New Task (At least Windows 7) Properties

General | Triggers | Actions | Conditions | Settings | Common

Action: Replace

Name: SAMLite Scheduled Scan 2

Author: ISAT\admlylyeoh

Description: SAMLite Scan for Windows 7 or later

Security options

When running the task, use the following user account:

NT AUTHORITY\System

○ Run only when user is logged on

● Run whether user is logged on or not

☑ Do not store password. The task will only have access to local resources.

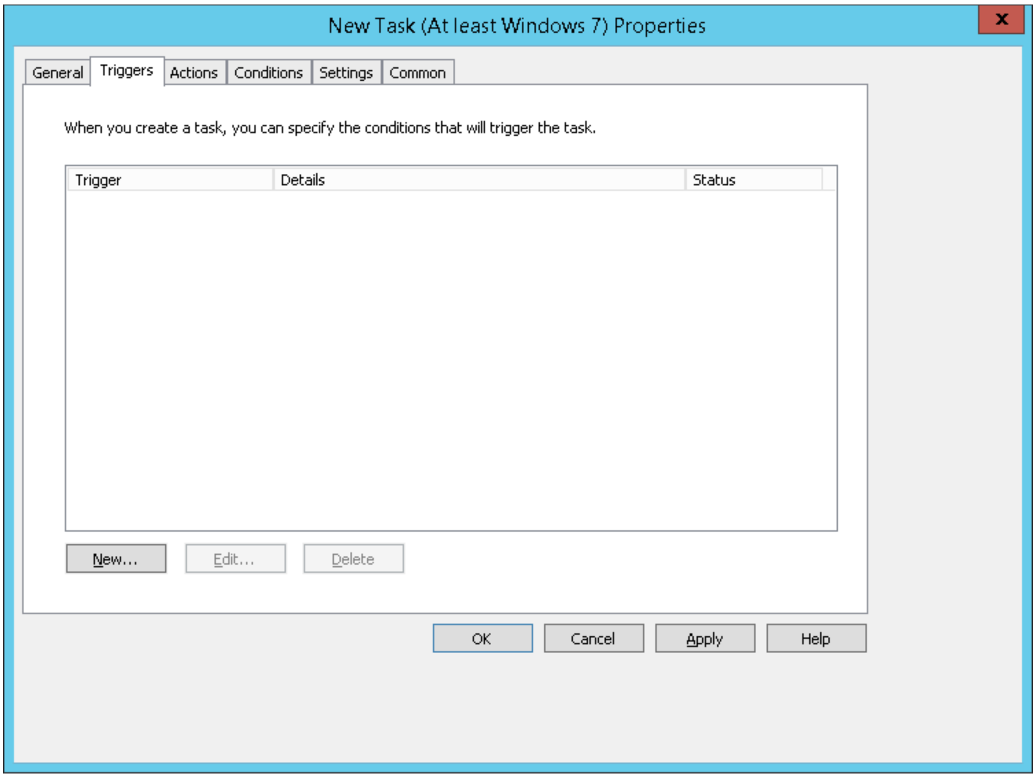
☑ Run with highest privileges

□ Hidden

Configure for: Windows Vistaï¿½ or Windows Serverï¿½ 2008

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

Then click on the Triggers tab.



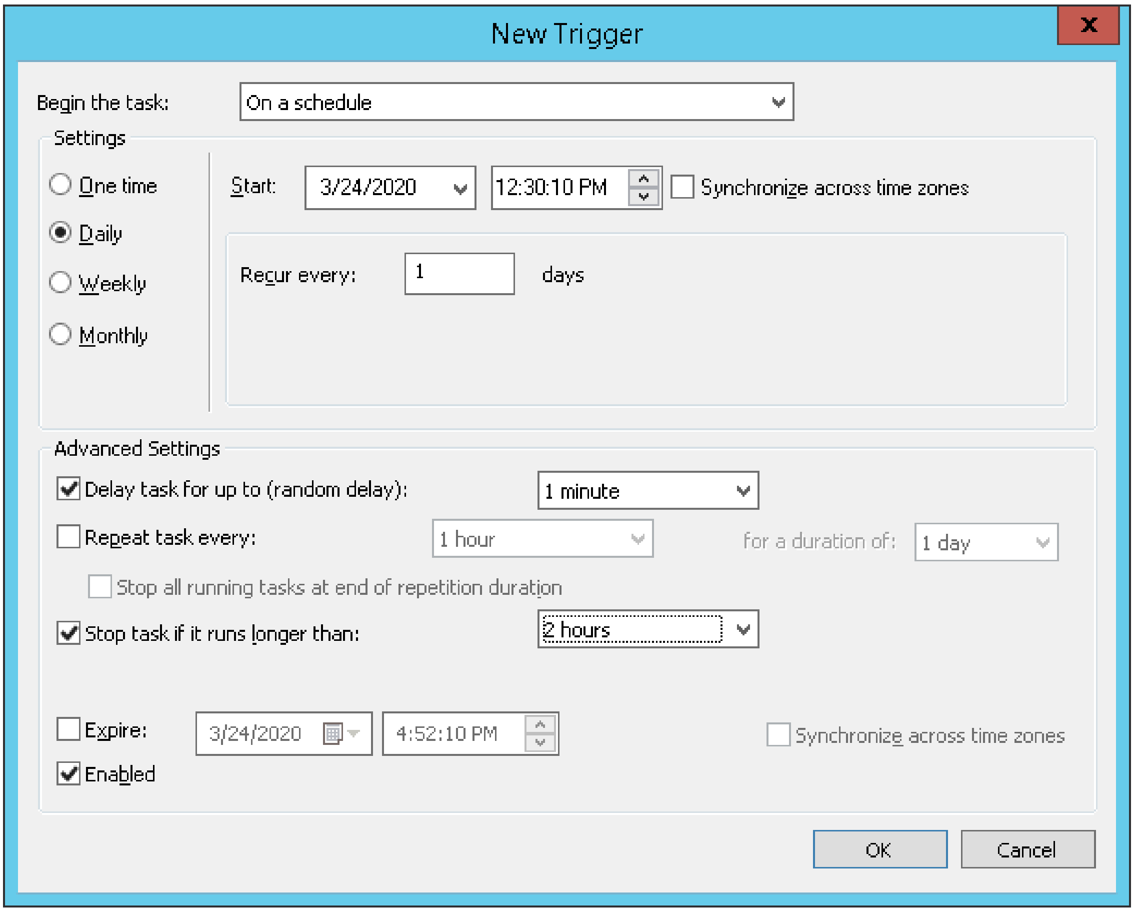
New Task (At least Windows 7) Properties

General | Triggers | Actions | Conditions | Settings | Common

When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status

Click New to create a new trigger.



New Trigger

Begin the task: On a schedule

Settings

○ One time
● Daily
○ Weekly
○ Monthly

Start: 3/24/2020 12:30:10 PM □ Synchronize across time zones

Recur every: 1 days

Advanced Settings

☑ Delay task for up to (random delay): 1 minute

□ Repeat task every: 1 hour for a duration of: 1 day

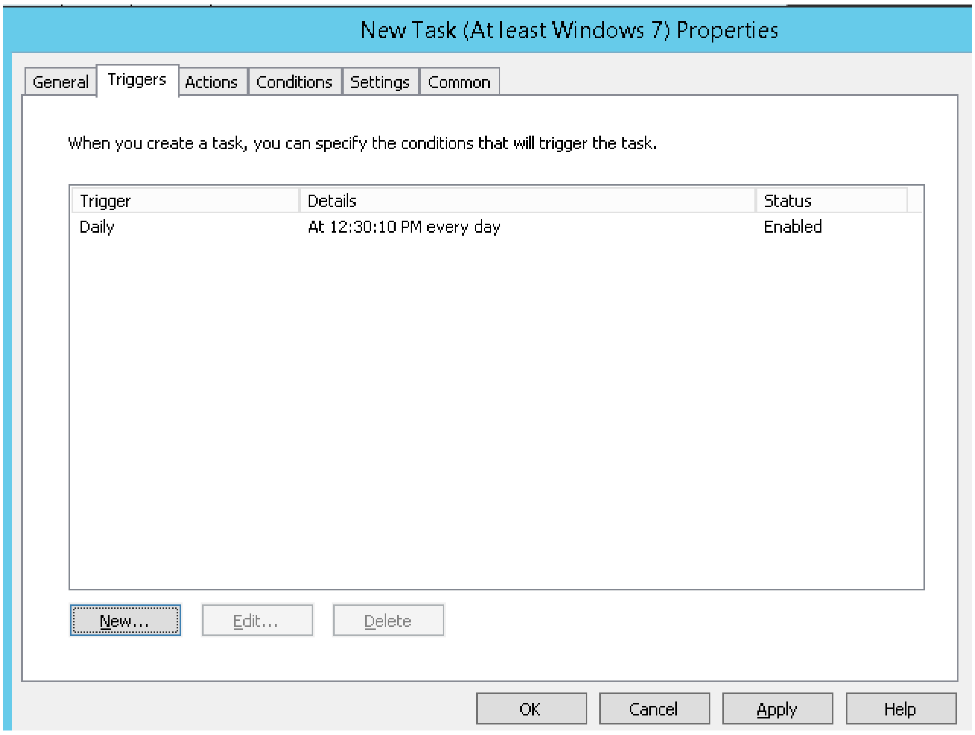
□ Stop all running tasks at end of repetition duration

☑ Stop task if it runs longer than: 2 hours

□ Expire: 3/24/2020 4:52:10 PM □ Synchronize across time zones

☑ Enabled

Click OK.

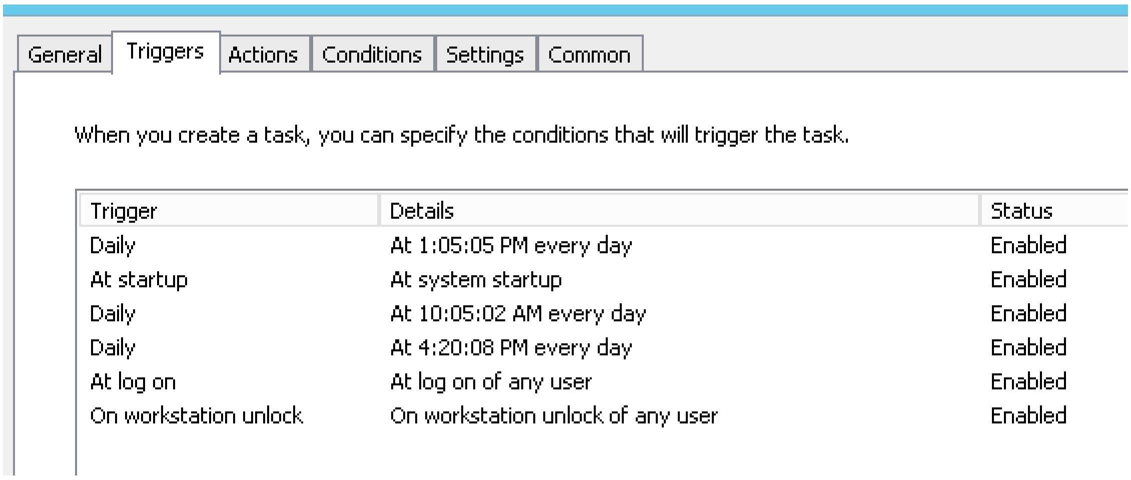


New Task (At least Windows 7) Properties

When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status
Daily	At 12:30:10 PM every day	Enabled

Create more triggers as desired. Example:



When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status
Daily	At 1:05:05 PM every day	Enabled
At startup	At system startup	Enabled
Daily	At 10:05:02 AM every day	Enabled
Daily	At 4:20:08 PM every day	Enabled
At log on	At log on of any user	Enabled
On workstation unlock	On workstation unlock of any user	Enabled

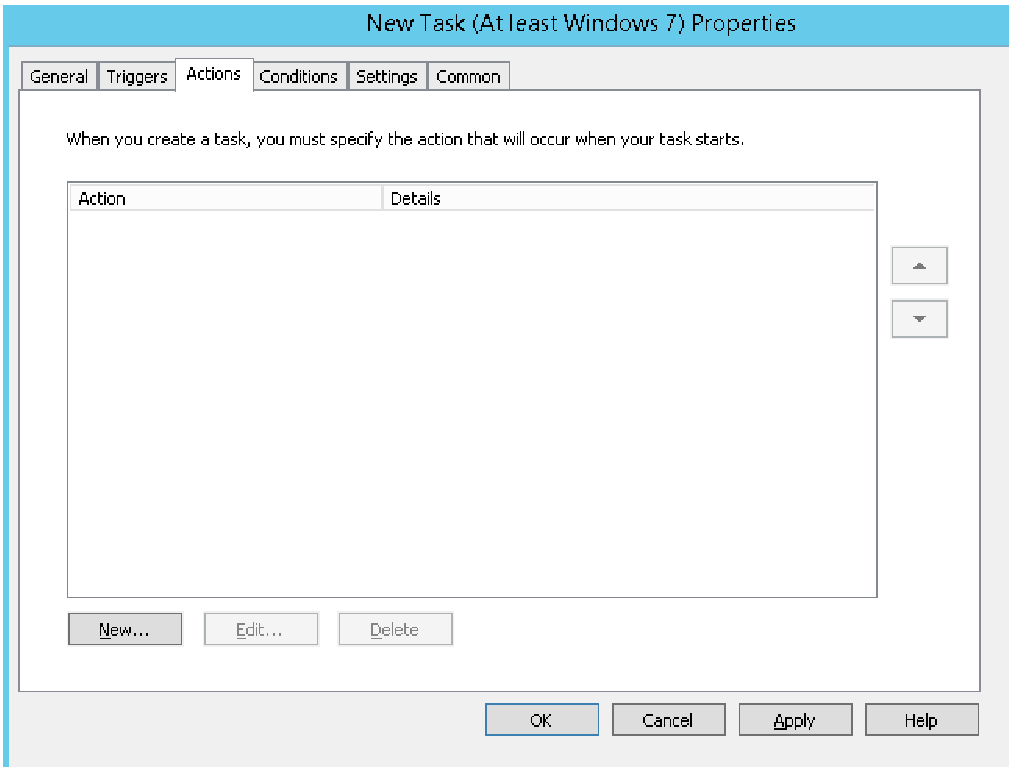
Some possible options:

- 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)

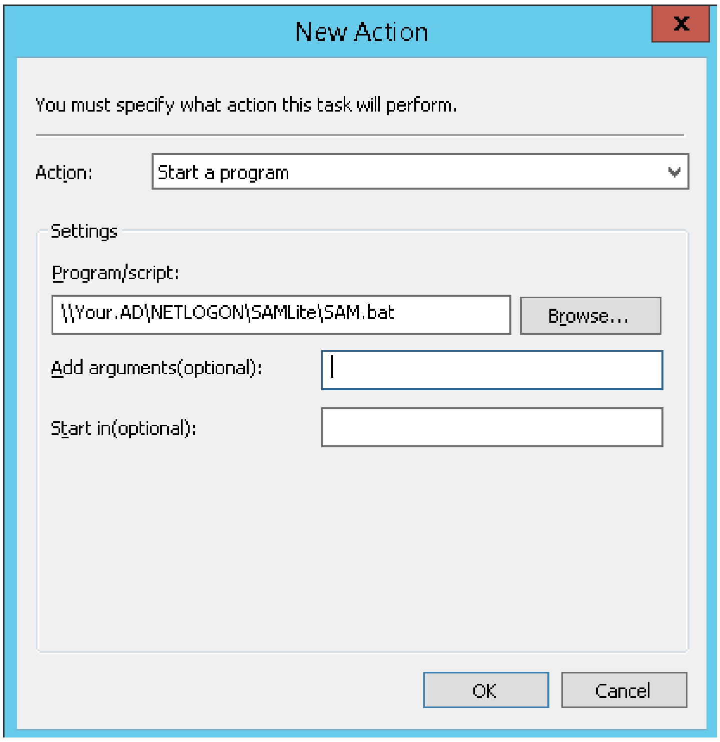
More than one trigger can be active. E.g. you can add “At log on” and “On workstation unlock”.

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 Task (At least Windows 7) Properties
General
Triggers
Actions
Conditions
Settings
Common
When you create a task, you must specify the action that will occur when your task starts.
Action
Details
New...
Edit...
Delete
OK
Cancel
Apply
Help

Click on New…



Action: Start a program

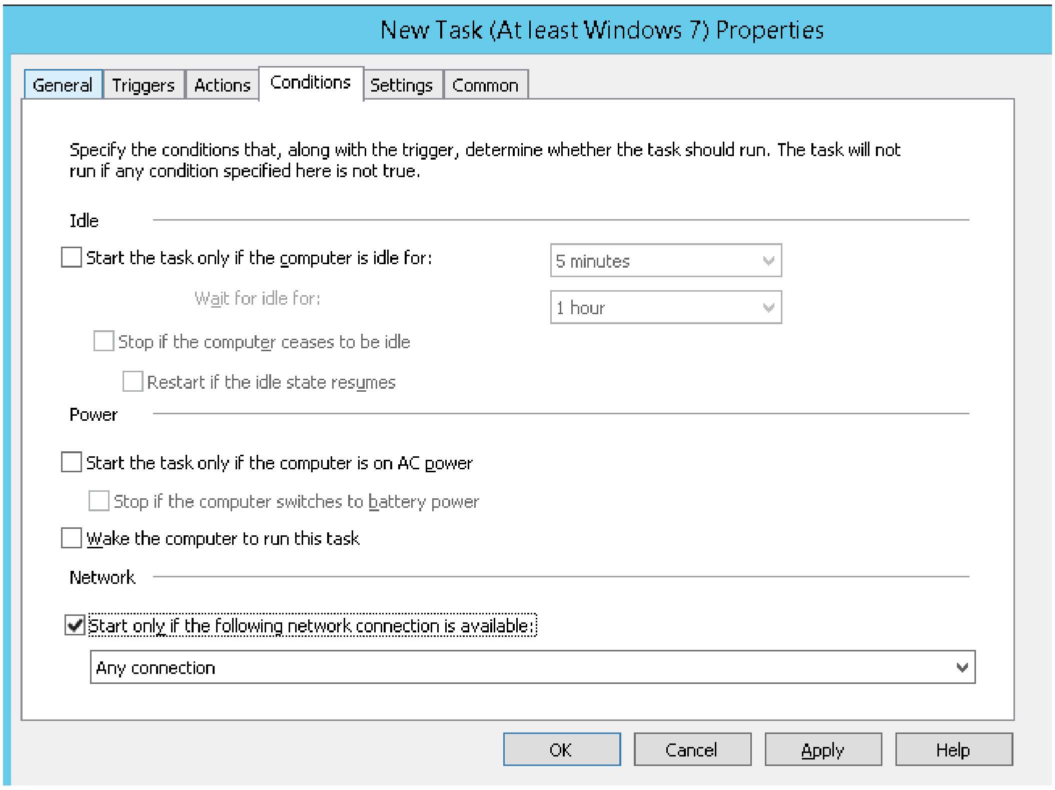
Program/script: \\Your.AD\NETLOGON\SAMLite\SAM.bat

Add arguments(optional):

Start in(optional):

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

Click on the Conditions tab.



New Task (At least Windows 7) Properties

Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true.

Idle

☐ Start the task only if the computer is idle for: 5 minutes

Wait for idle for: 1 hour

☐ Stop if the computer ceases to be idle

☐ Restart if the idle state resumes

Power

☐ Start the task only if the computer is on AC power

☐ Stop if the computer switches to battery power

☐ Wake the computer to run this task

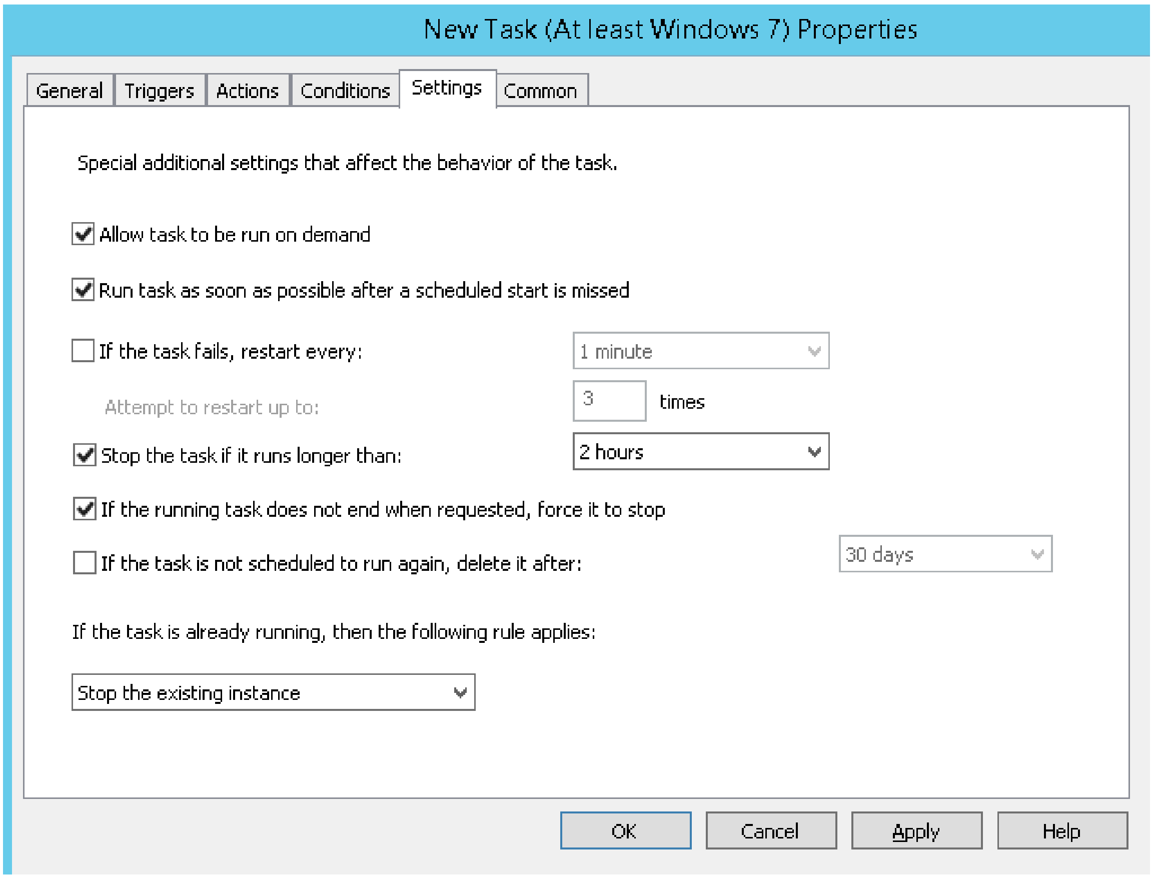
Network

☑ Start only if the following network connection is available:

Any connection

Start only if the computer might have network connectivity.

Click on the Settings tab.



New Task (At least Windows 7) Properties

Special additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

☑ Run task as soon as possible after a scheduled start is missed

☐ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

☑ Stop the task if it runs longer than: 2 hours

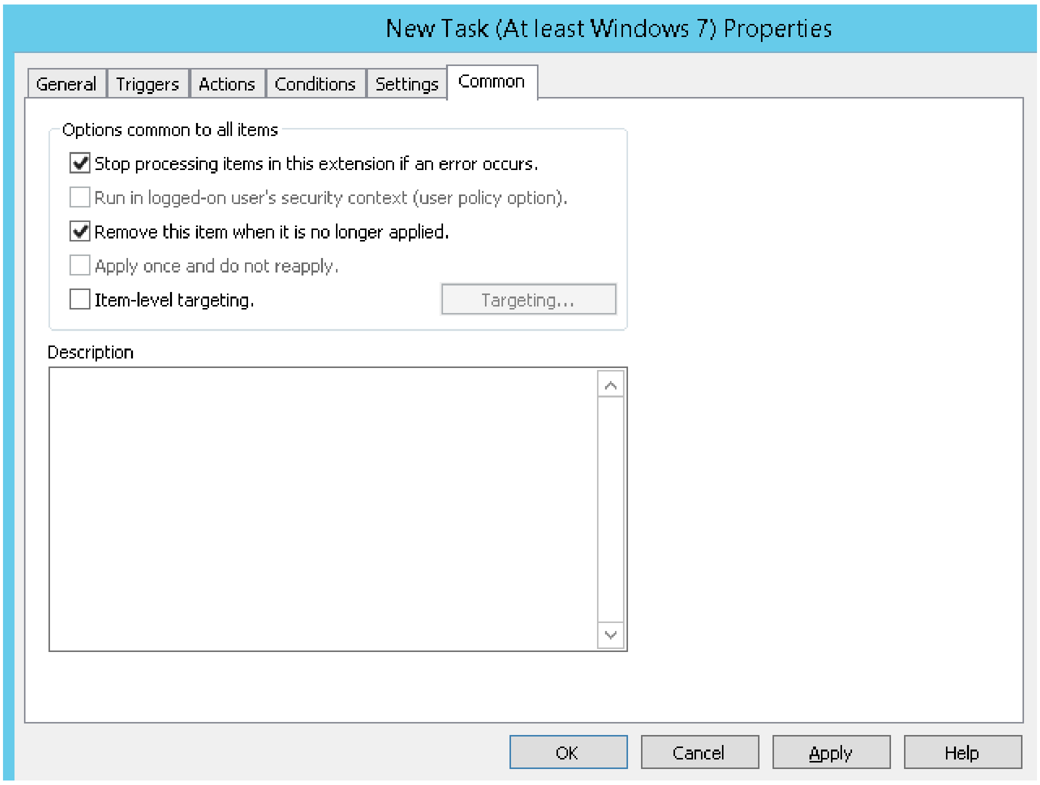
☑ If the running task does not end when requested, force it to stop

☐ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Stop the existing instance

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



New Task (At least Windows 7) Properties

Options common to all items

☑ Stop processing items in this extension if an error occurs.

□ Run in logged-on user's security context (user policy option).

☑ Remove this item when it is no longer applied.

□ Apply once and do not reapply.

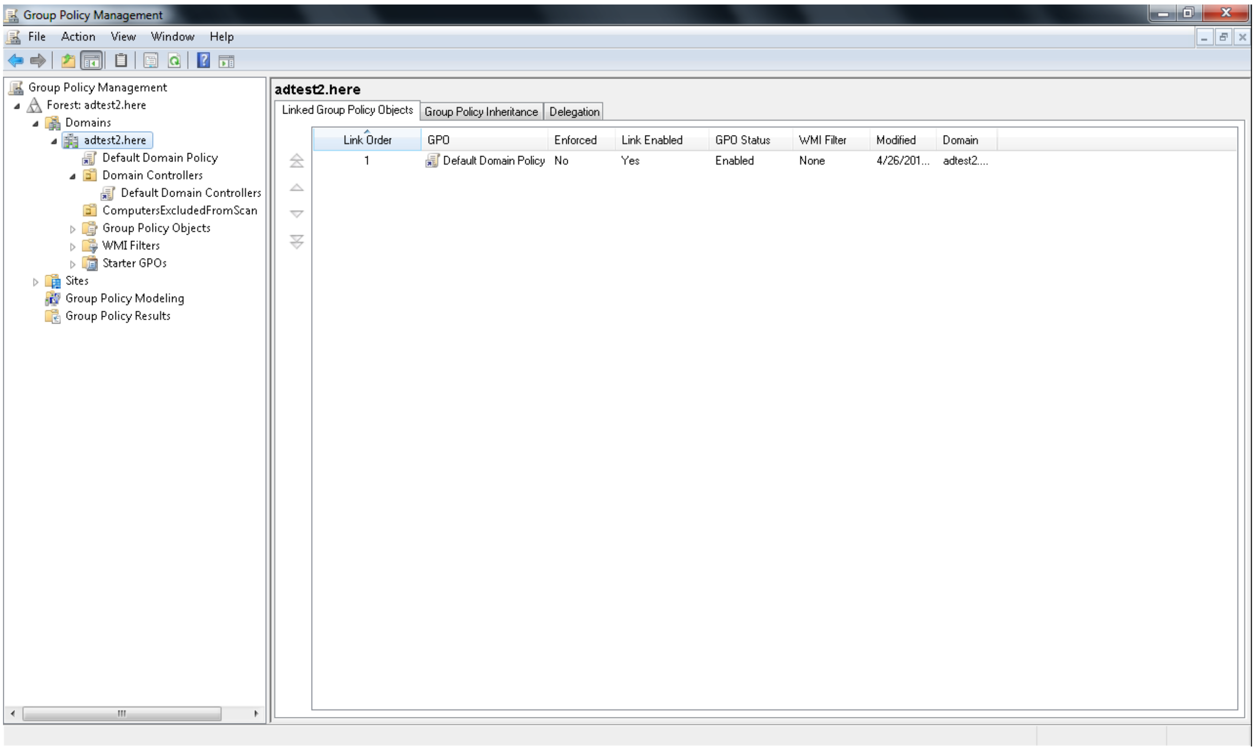
□ Item-level targeting.

Recommended settings as above. Click OK.

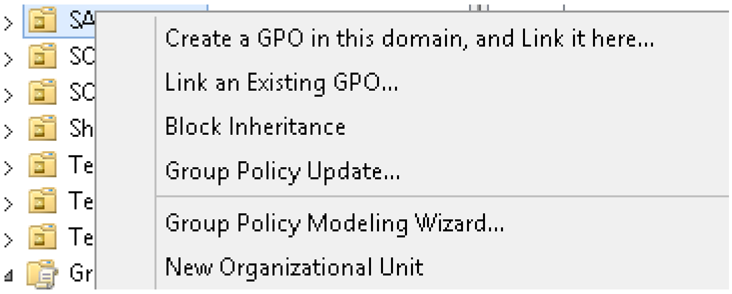
You now have created the SAMLiteScan group policy object.

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

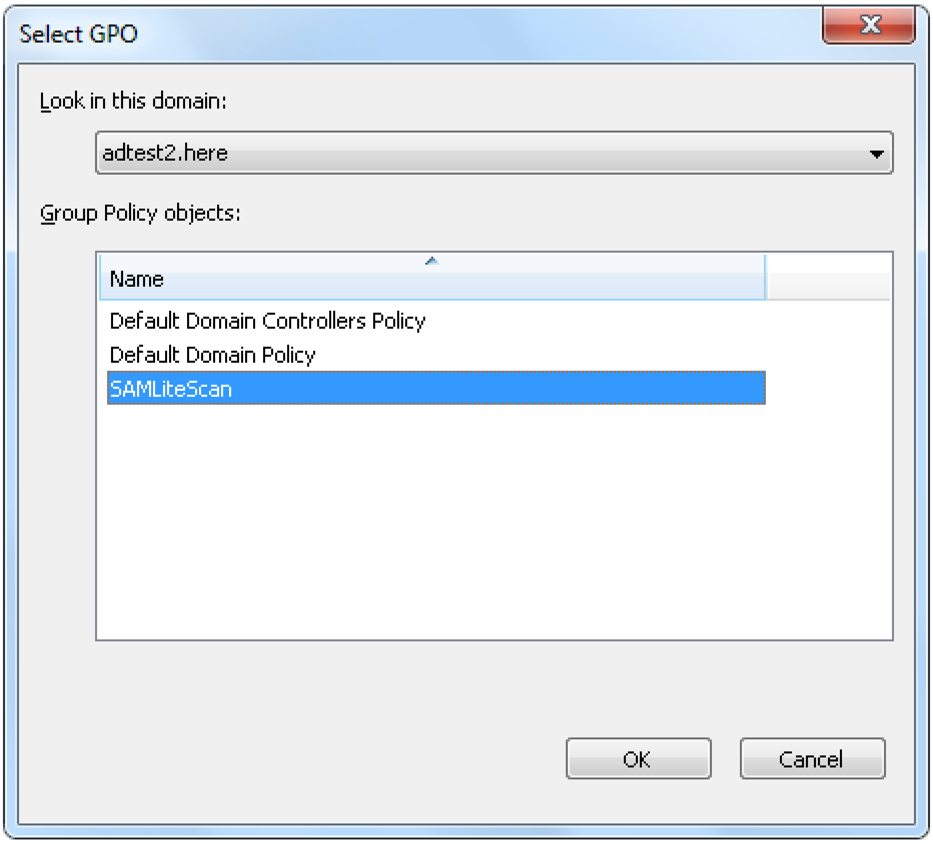
Right click on the target domain.



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Default Domain Policy	No	Yes	Enabled	None	4/26/201...	adtest2....



Select Link an Existing GPO.



Select GPO

Look in this domain: adtest2.here

Group Policy objects:

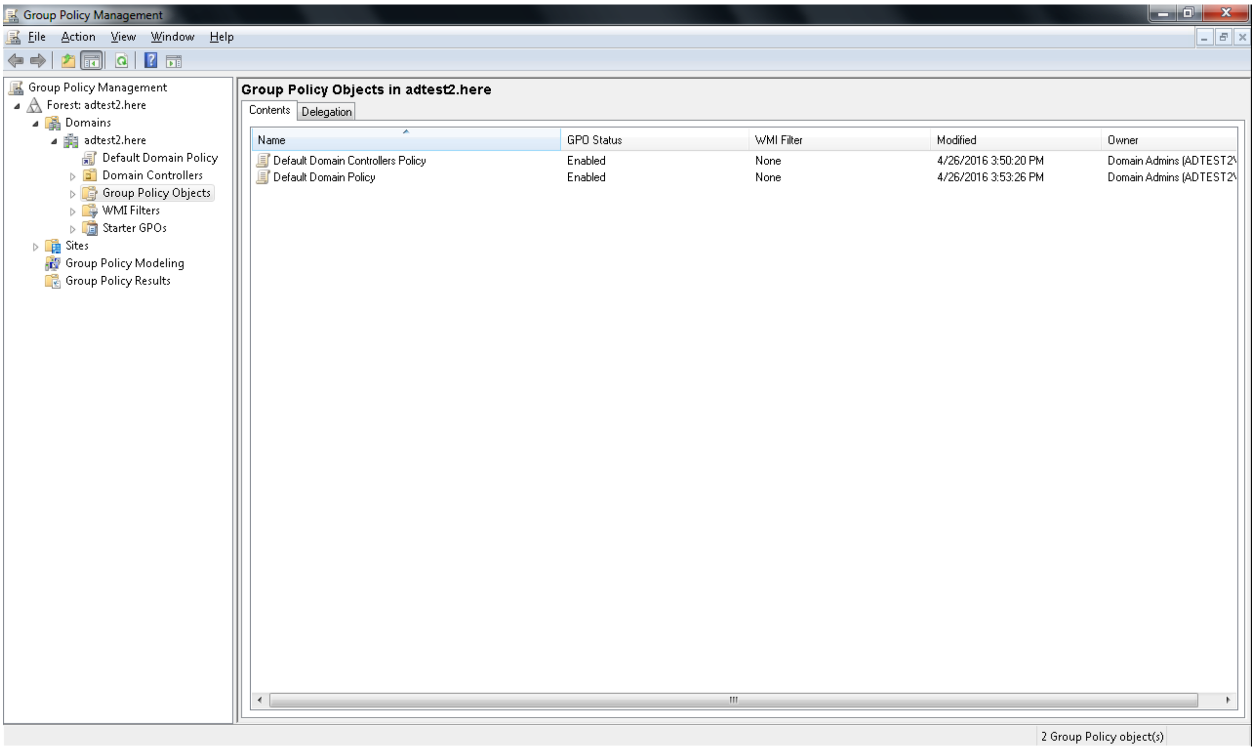
Name
Default Domain Controllers Policy
Default Domain Policy
SAMLiteScan

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.

3.1 Creating the SAMLiteLogonScan Group Policy Object

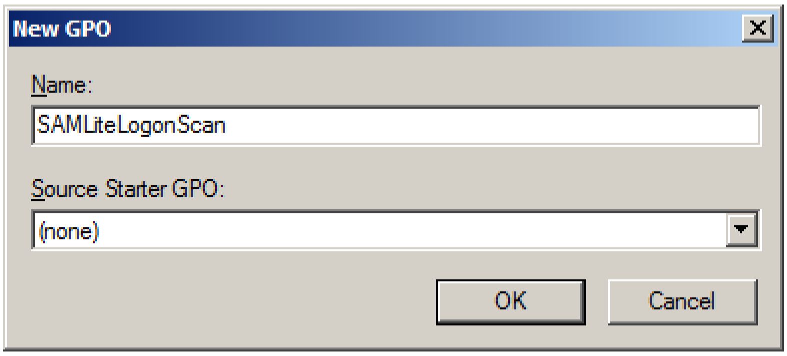


Group Policy Objects in adtest2.here

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controllers Policy	Enabled	None	4/26/2016 3:50:20 PM	Domain Admins (ADTEST2\
Default Domain Policy	Enabled	None	4/26/2016 3:53:26 PM	Domain Admins (ADTEST2\

Launch Group Policy Management and select Group Policy Objects

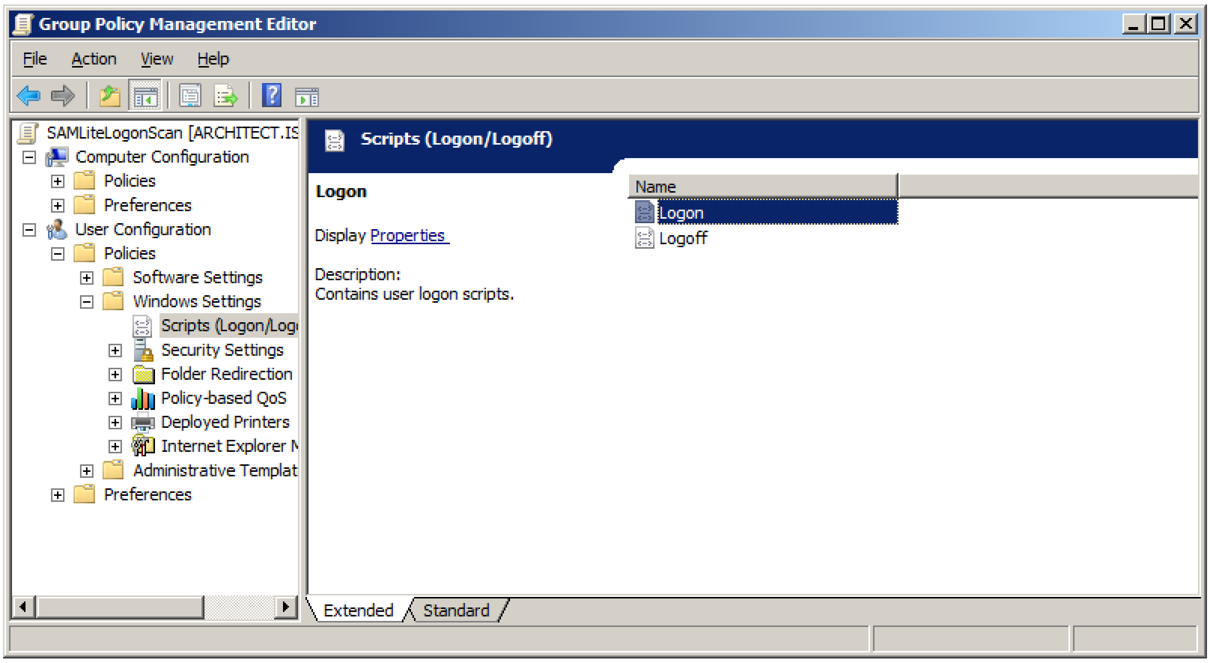
Right-click blank space and select New



Name:
SAMLiteLogonScan

Source Starter GPO:
(none)

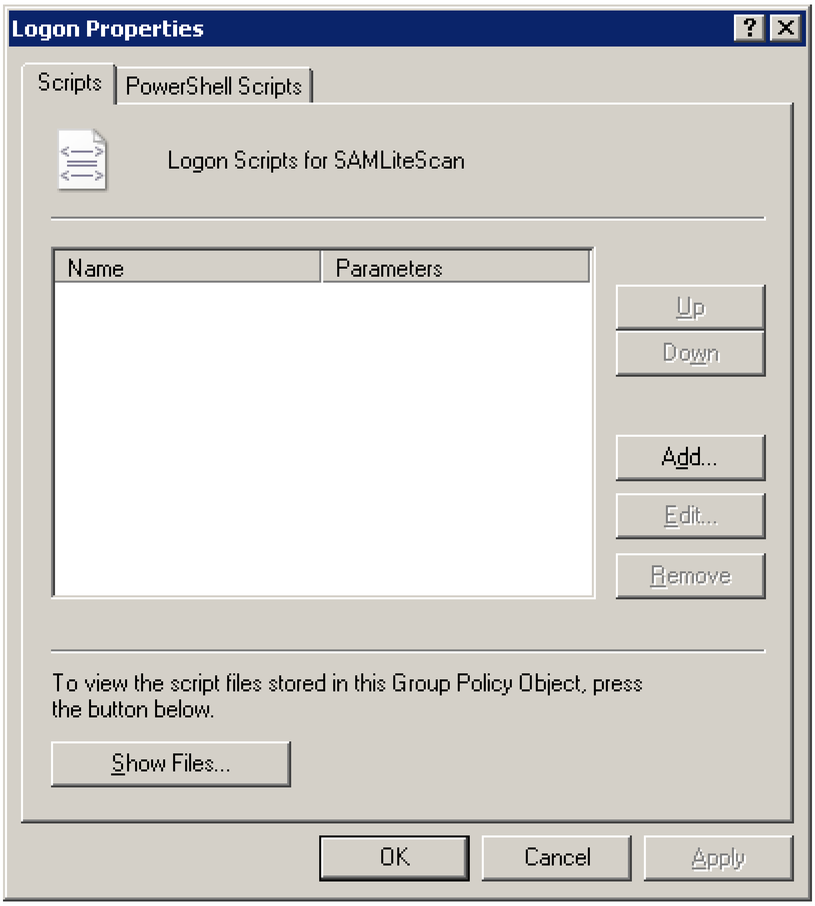
Click OK



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

Right click Logon, click Properties.

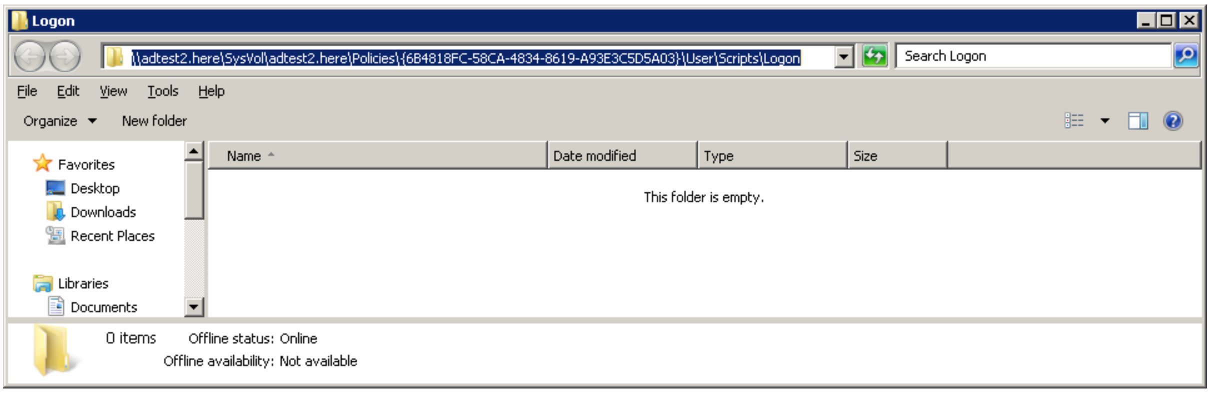
3.1.1 Copy Logon script files to the Group Policy Object



Logon Scripts for SAMLiteScan

To view the script files stored in this Group Policy Object, press the button below.

Click Show Files



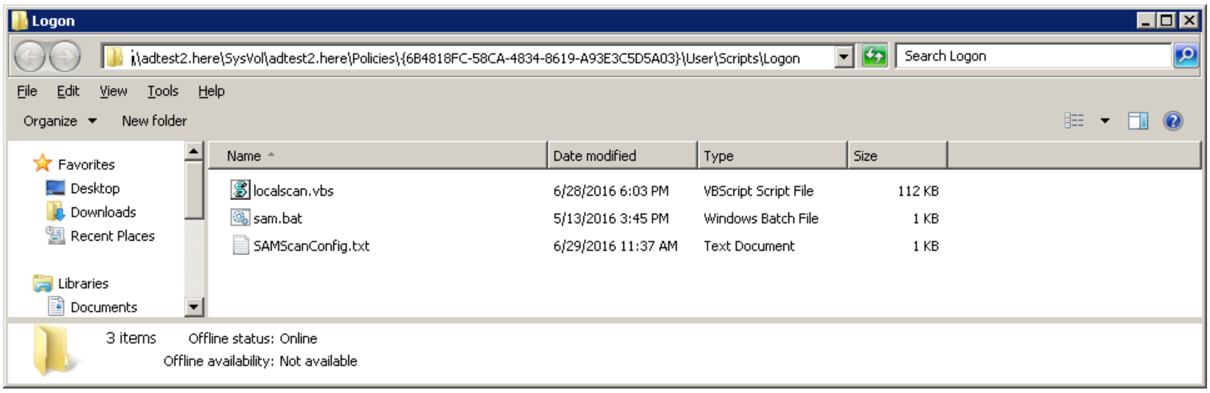
\\adtest2.here\SysVol\adtest2.here\Policies\{6B4818FC-58CA-4834-8619-A93E3C5D5A03}\User\Scripts\Logon

This folder is empty.

0 items Offline status: Online

Offline availability: Not available

Copy the scan script files into this folder from:
`C:\Windows\SYSVOL\sysvol\domain\scripts\SAMLite`



Logon

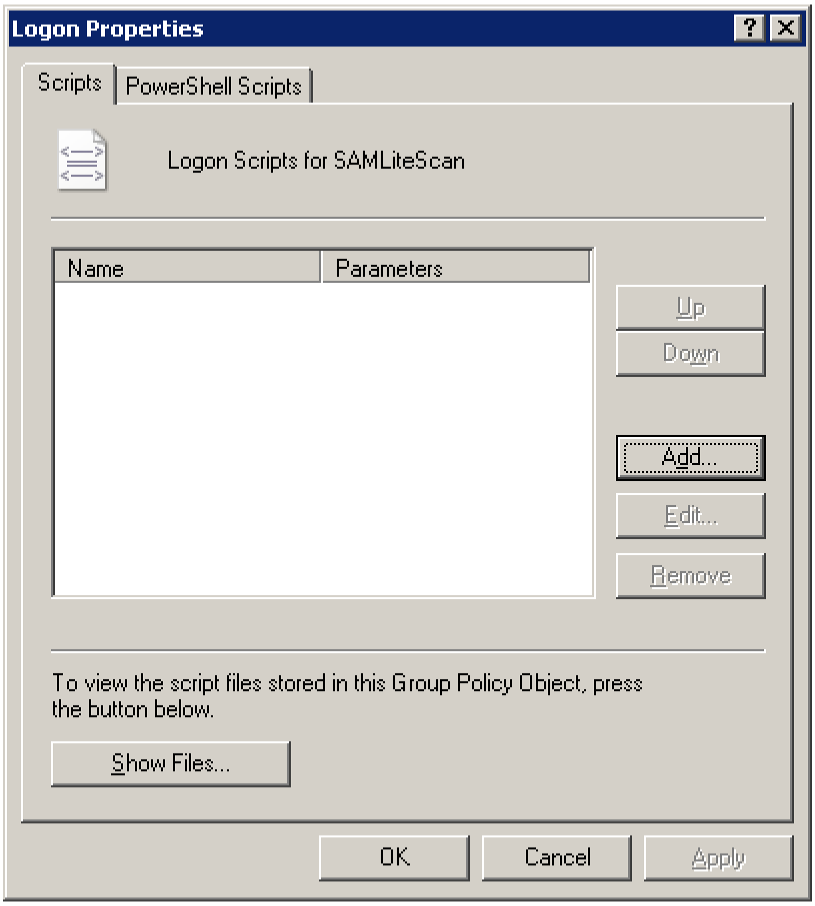
\\adtest2.here\SysVol\adtest2.here\Policies\{6B4818FC-58CA-4834-8619-A93E3C5D5A03}\User\Scripts\Logon

Name	Date modified	Type	Size
localscan.vbs	6/28/2016 6:03 PM	VBScript Script File	112 KB
sam.bat	5/13/2016 3:45 PM	Windows Batch File	1 KB
SAMScanConfig.txt	6/29/2016 11:37 AM	Text Document	1 KB

3 items Offline status: Online

Offline availability: Not available

Close the window.



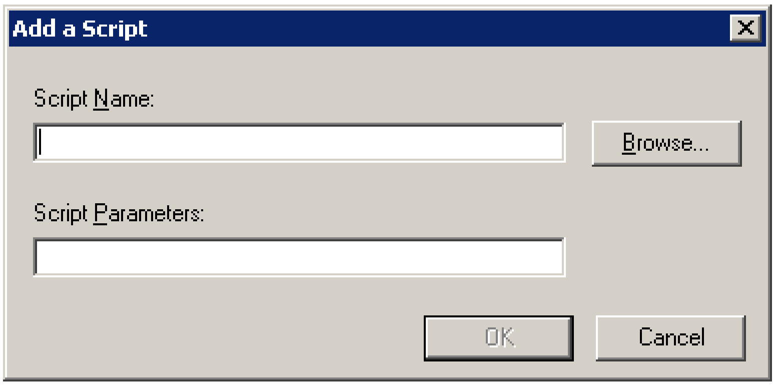
Logon Properties

Logon Scripts for SAMLiteScan

Name	Parameters

To view the script files stored in this Group Policy Object, press the button below.

Go back to Logon Properties and click Add…

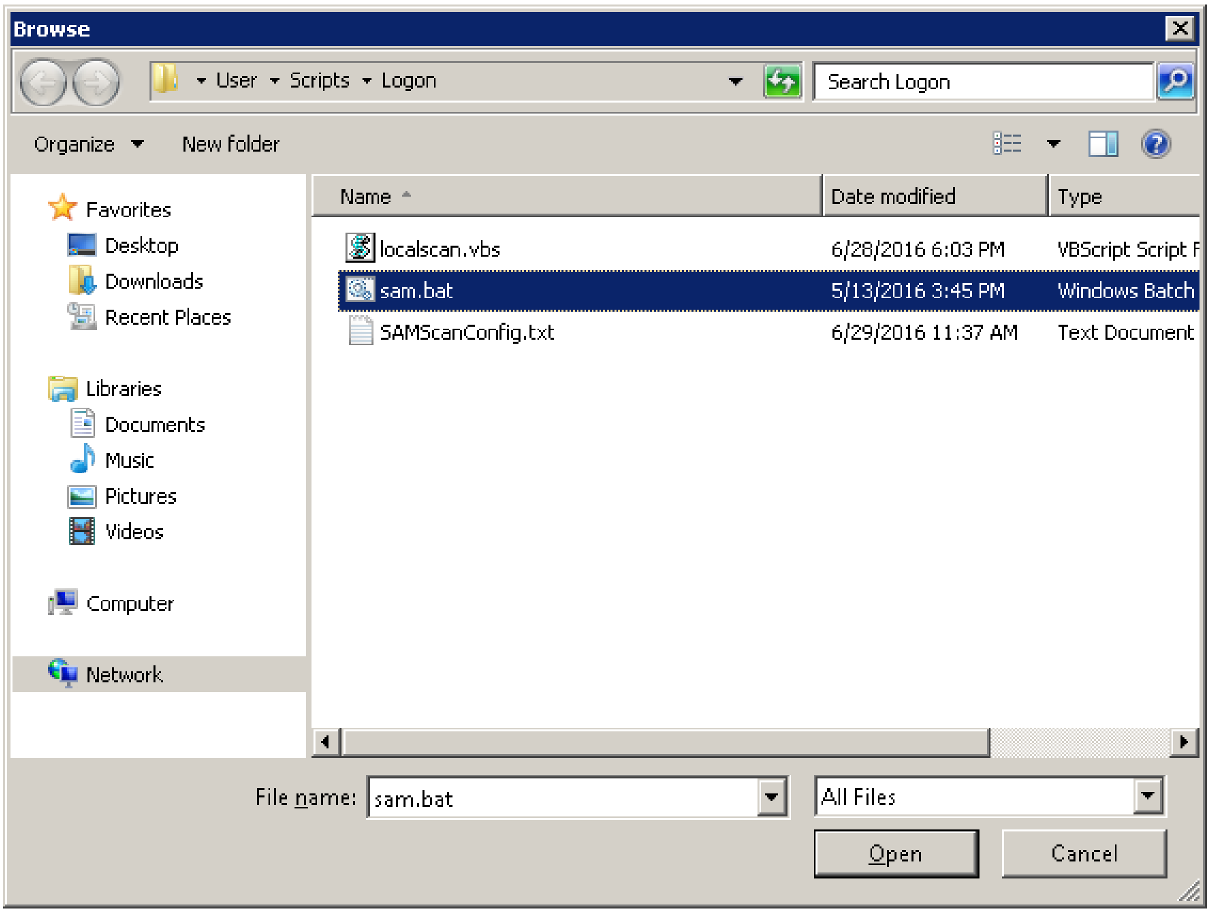


Add a Script

Script Name:

Script Parameters:

Click Browse.

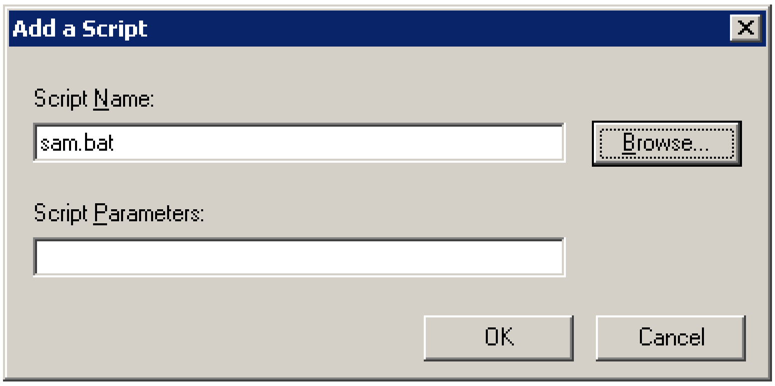


Name	Date modified	Type
localscan.vbs	6/28/2016 6:03 PM	VBScript Script F
sam.bat	5/13/2016 3:45 PM	Windows Batch
SAMScanConfig.txt	6/29/2016 11:37 AM	Text Document

File name: sam.bat

All Files

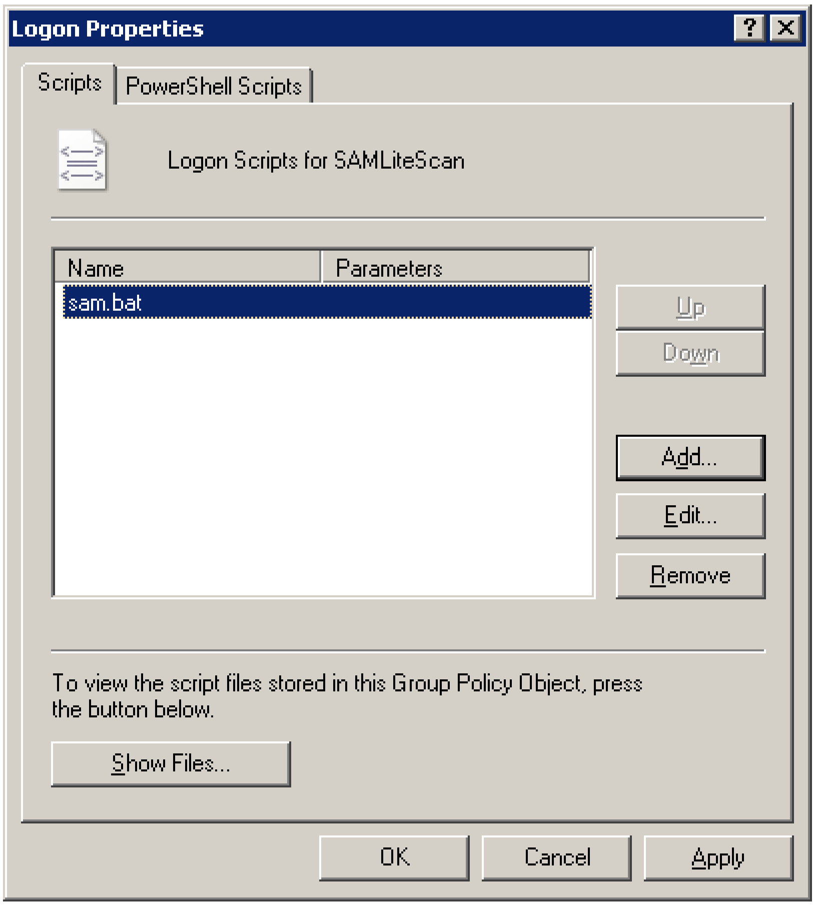
Select sam.bat and Open.



Script Name: sam.bat

Script Parameters:

Click OK.



Logon Scripts for SAMLiteScan

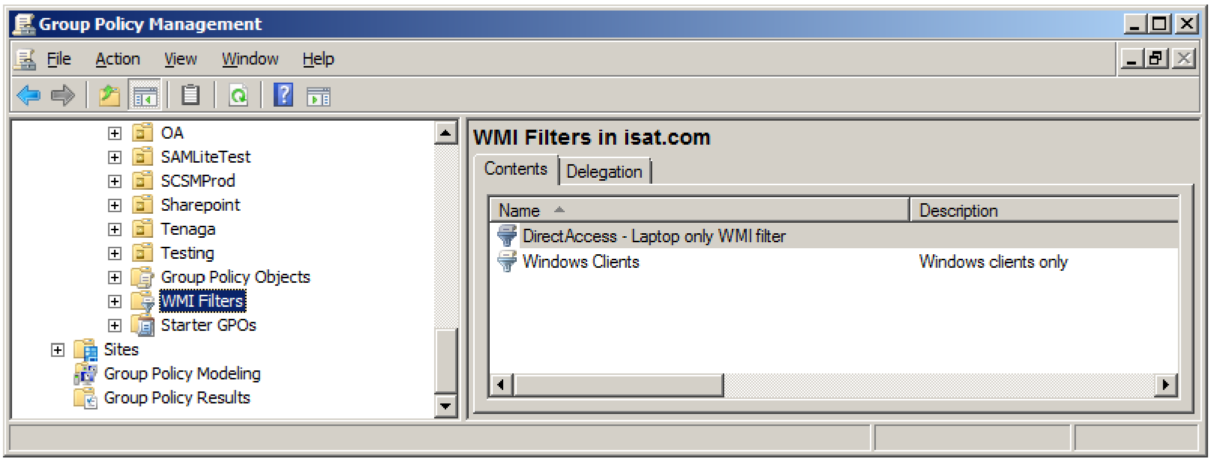
Name	Parameters
sam.bat	

To view the script files stored in this Group Policy Object, press the button below.

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

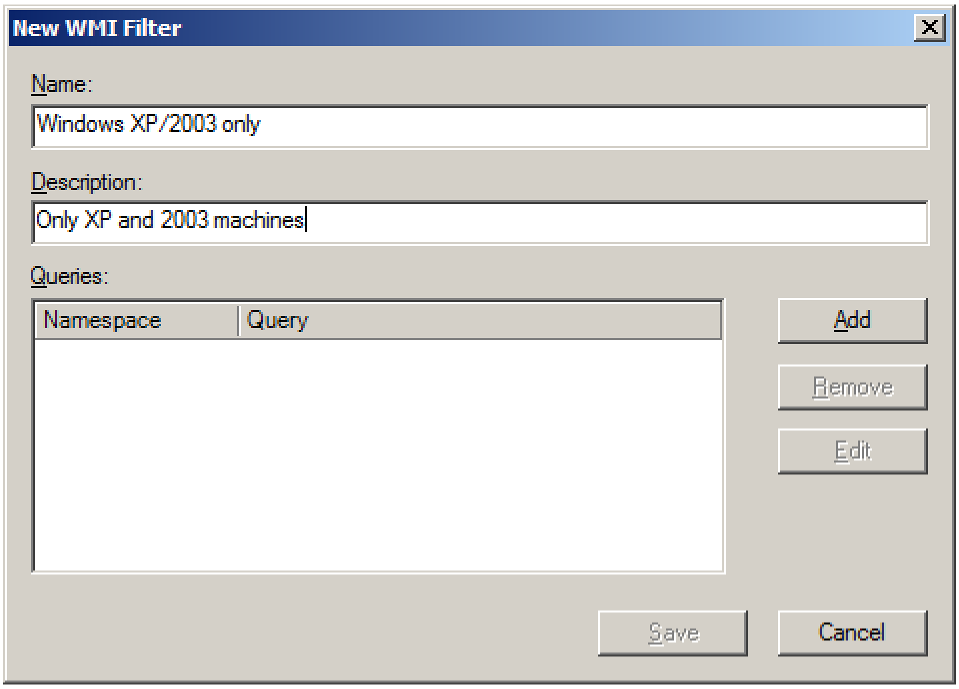
4 Creating a WMI Filter for Windows XP and 2003

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).



Name	Description
DirectAccess - Laptop only WMI filter	
Windows Clients	Windows clients only

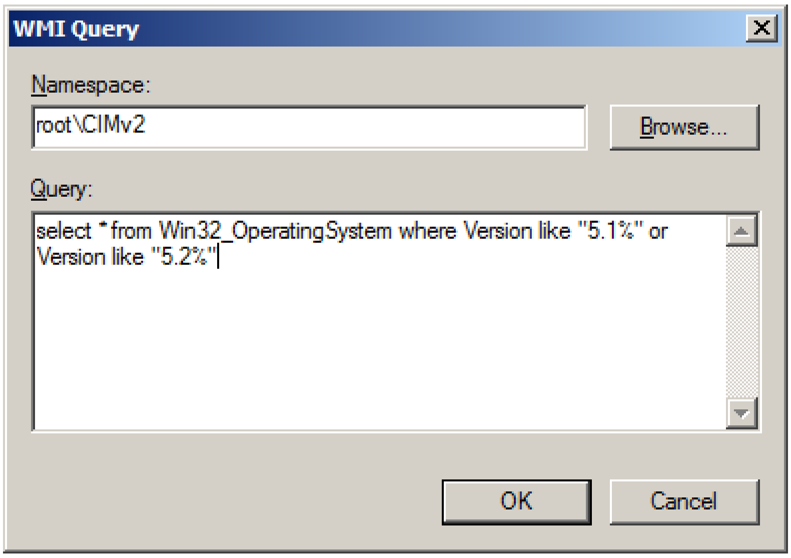
Right click in the blank space and select New…



Name: Windows XP/2003 only

Description: Only XP and 2003 machines

Click Add

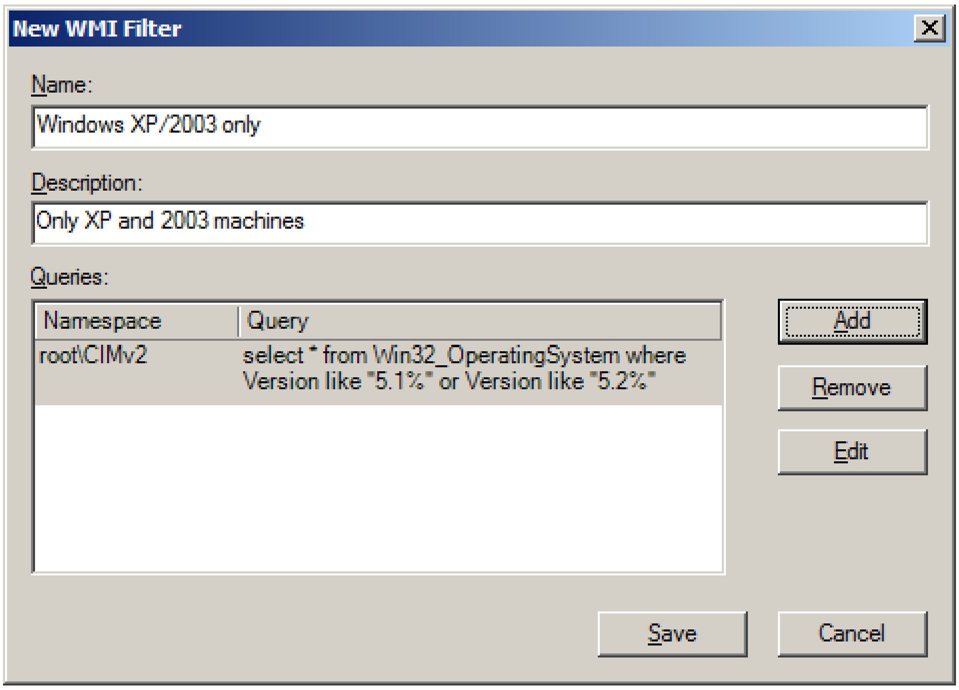


Namespace: root\CIMv2

Query:

```
select * from Win32_OperatingSystem where Version like "5.1%" or
Version like "5.2%"
```

Set the query accordingly. Click OK



Name: Windows XP/2003 only

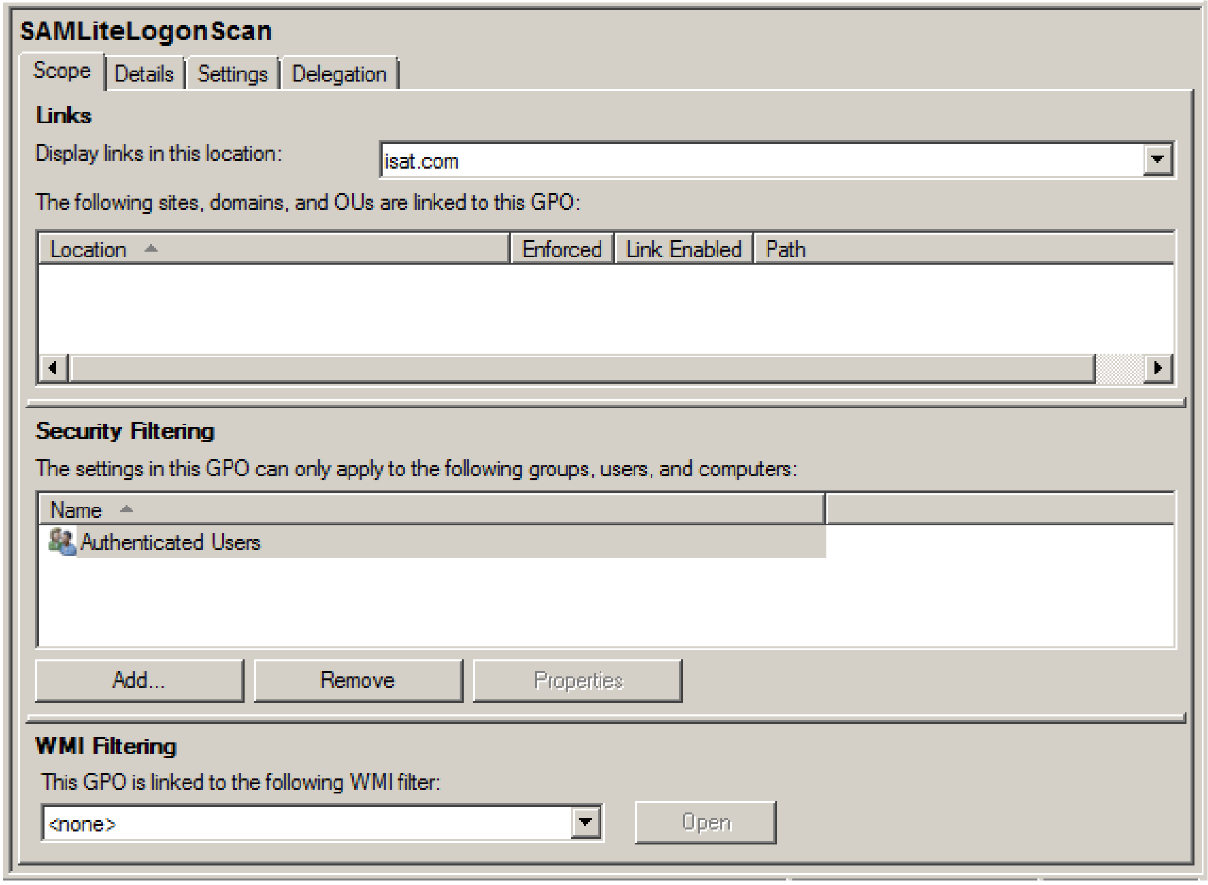
Description: Only XP and 2003 machines

Queries:

Namespace	Query
root\CIMv2	select * from Win32_OperatingSystem where Version like "5.1%" or Version like "5.2%"

Click Save.

4.1 Applying the WMI Filter to the SAMLiteLogonScan GPO



SAMLiteLogonScan

Links

Display links in this location: isat.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:

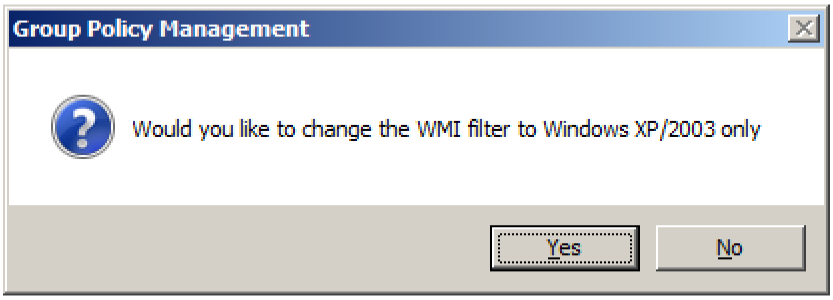
Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter: <none>

Select the SAMLiteLogonScan GPO.

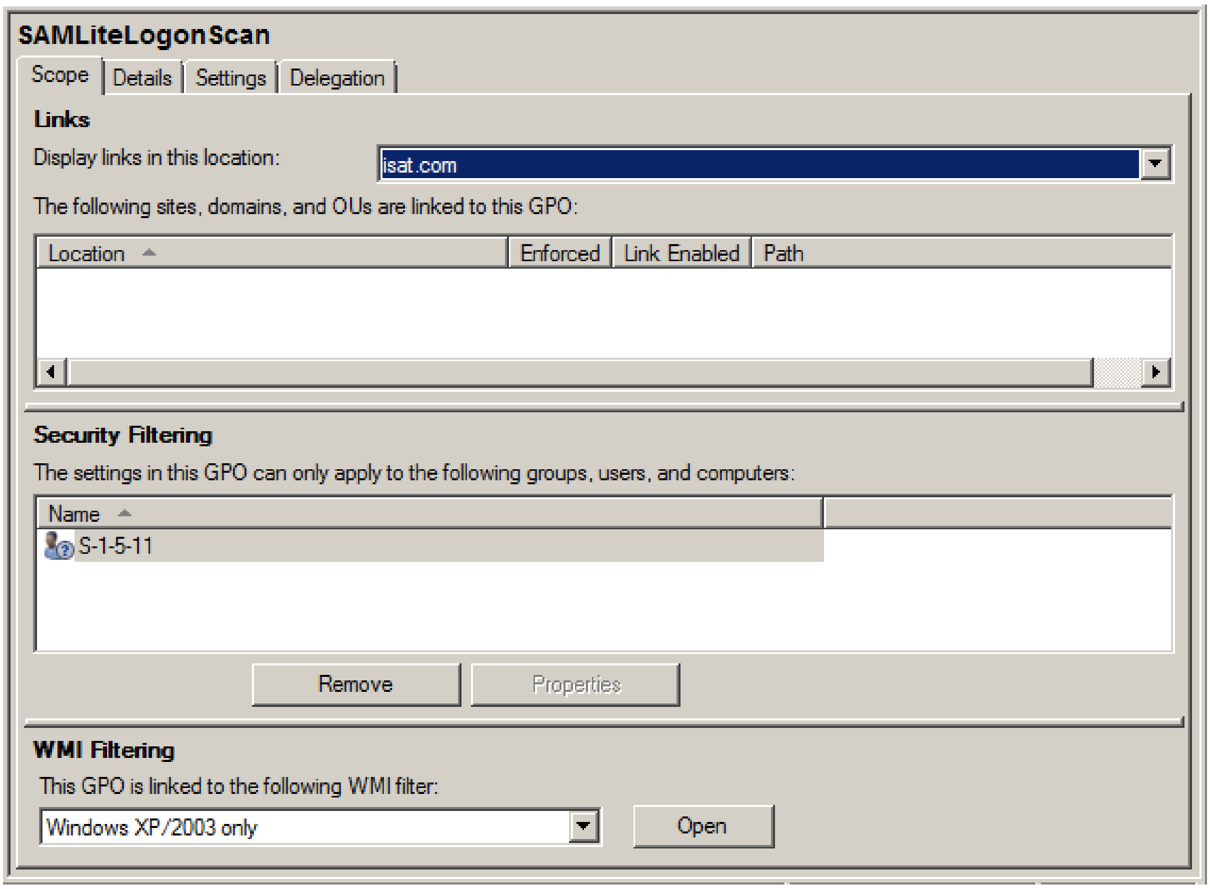
Click on the drop-down in WMI Filtering and select “Windows XP/2003 only”



Group Policy Management

Would you like to change the WMI filter to Windows XP/2003 only

Click Yes.



SAMLiteLogonScan

Links

Display links in this location: isat.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:

Name
S-1-5-11

WMI Filtering

This GPO is linked to the following WMI filter: Windows XP/2003 only

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

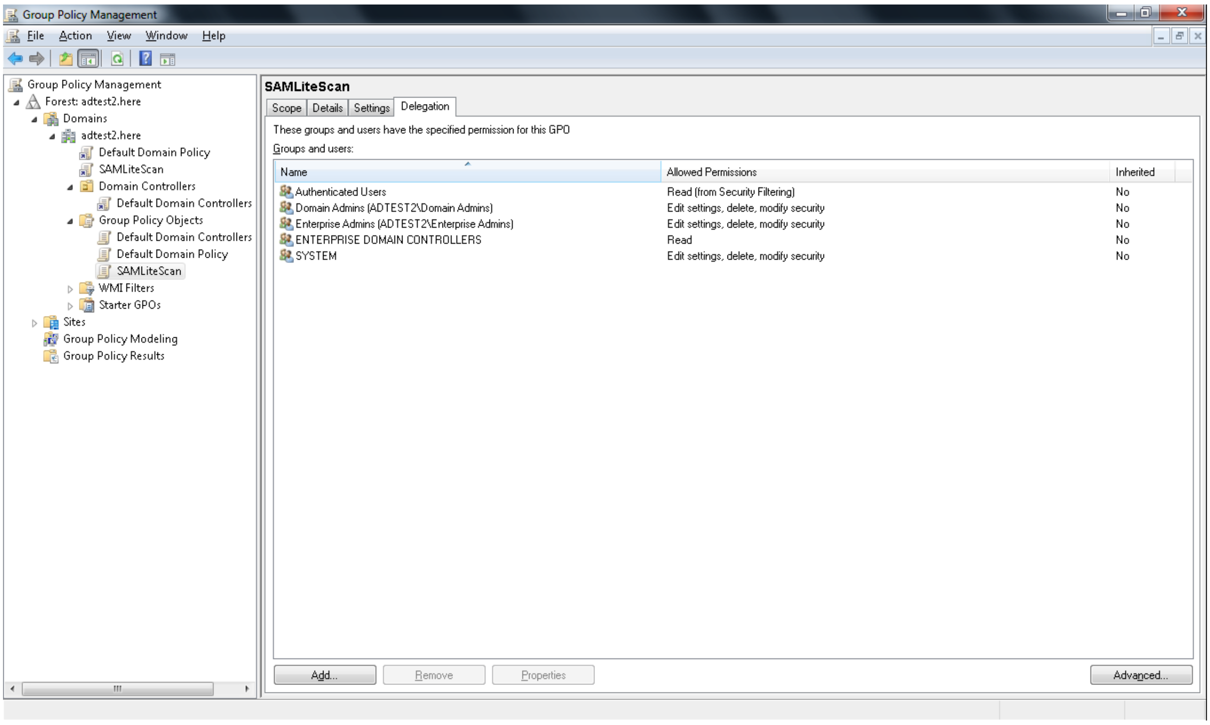
You may also wish to add the Software Restriction policies to this group policy object. To do that refer to Section 2 “Adding Software Restriction Policies.”

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)



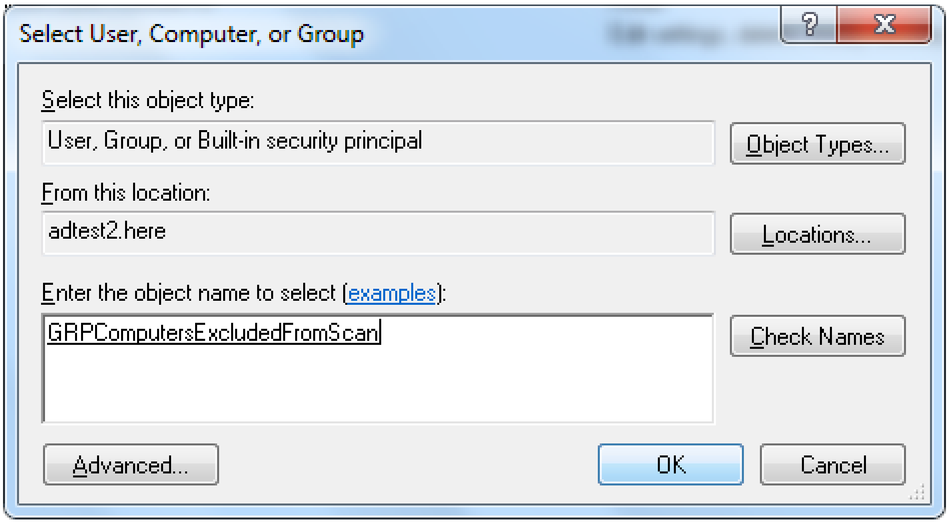
SAMLiteScan

These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (ADTEST2\Domain Admins)	Edit settings, delete, modify security	No
Enterprise Admins (ADTEST2\Enterprise Admins)	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
SYSTEM	Edit settings, delete, modify security	No

Click on Add…

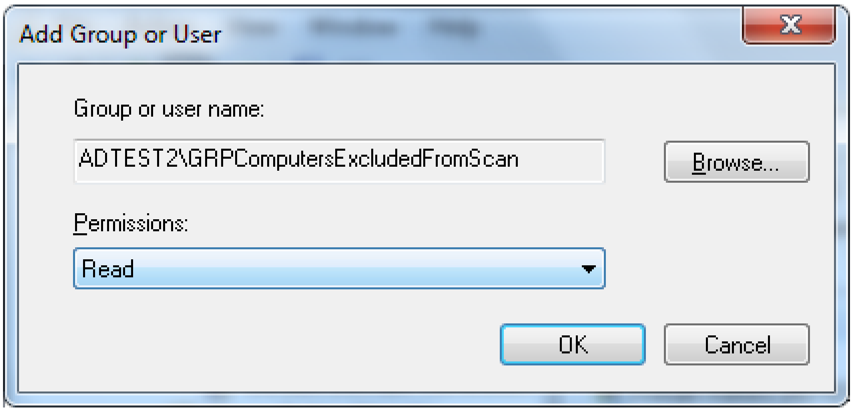


Select this object type:
User, Group, or Built-in security principal

From this location:
adtest2.here

Enter the object name to select (examples):
GRPComputersExcludedFromScan

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



Group or user name:

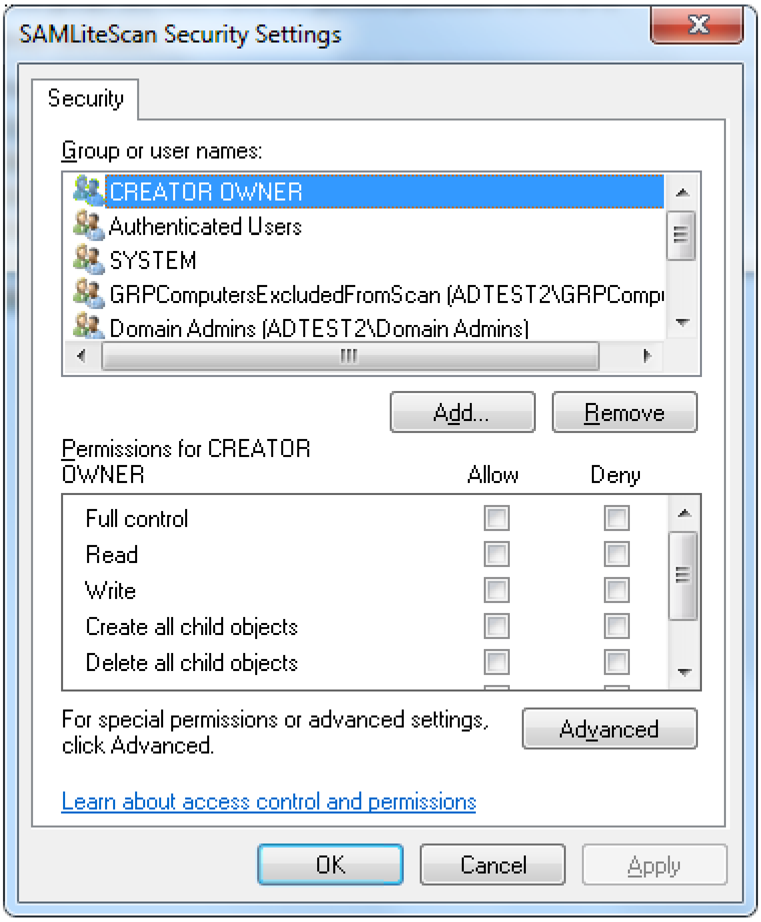
ADTEST2\GRPComputersExcludedFromScan

Permissions:

Read

Click OK.

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



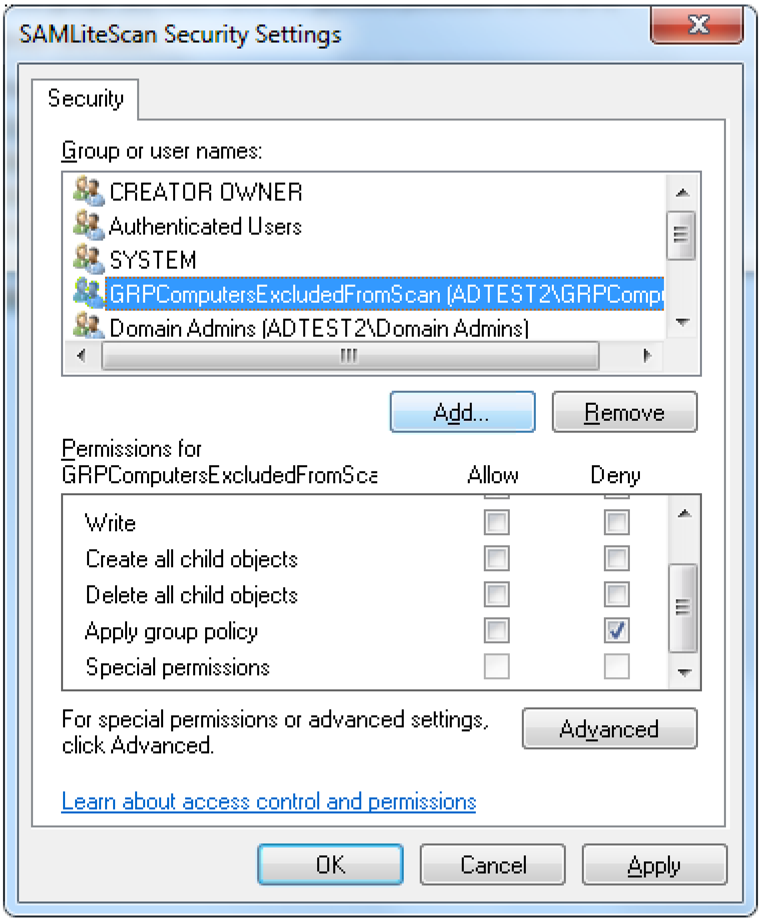
Group or user names:

- CREATOR OWNER
- Authenticated Users
- SYSTEM
- GRPComputersExcludedFromScan (ADTEST2\GRPComp
- Domain Admins (ADTEST2\Domain Admins)

Permissions for CREATOR OWNER	Allow	Deny
Full control	□	□
Read	□	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions



SAMLiteScan Security Settings

Group or user names:

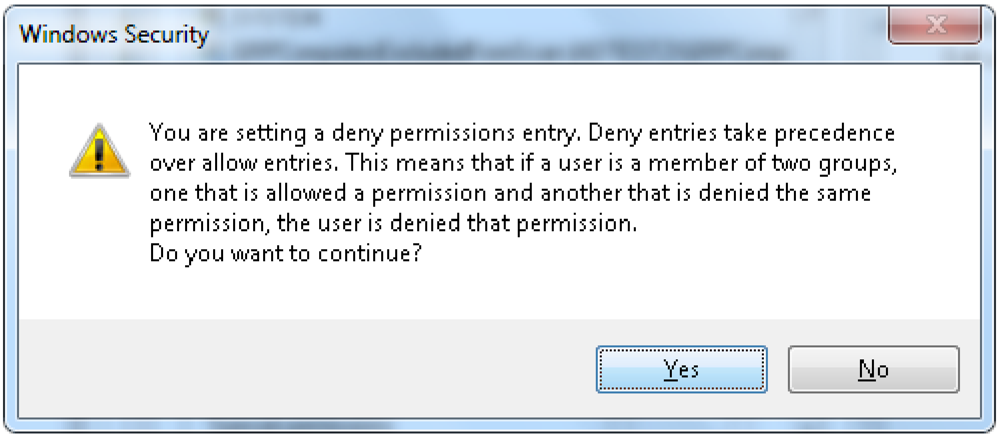
- CREATOR OWNER
- Authenticated Users
- SYSTEM
- GRPComputersExcludedFromScan (ADTEST2\GRPComp
- Domain Admins (ADTEST2\Domain Admins)

Permissions for GRPComputersExcludedFromSca	Allow	Deny
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Apply group policy	□	☑
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

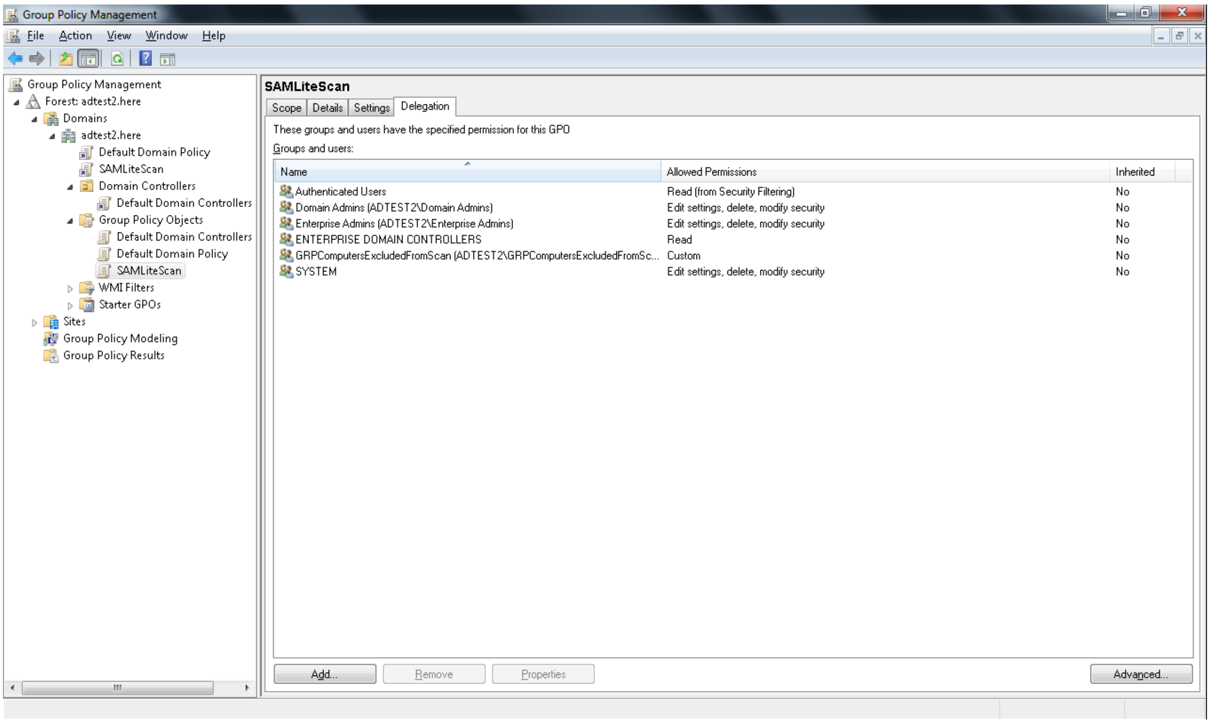
Select the object/group and scroll down in the permissions and click on Deny for “Apply group policy”



Windows Security

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?

Click Yes



These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (ADTEST2\Domain Admins)	Edit settings, delete, modify security	No
Enterprise Admins (ADTEST2\Enterprise Admins)	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
GRPComputersExcludedFromScan (ADTEST2\GRPComputersExcludedFromSc...	Custom	No
SYSTEM	Edit settings, delete, modify security	No

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