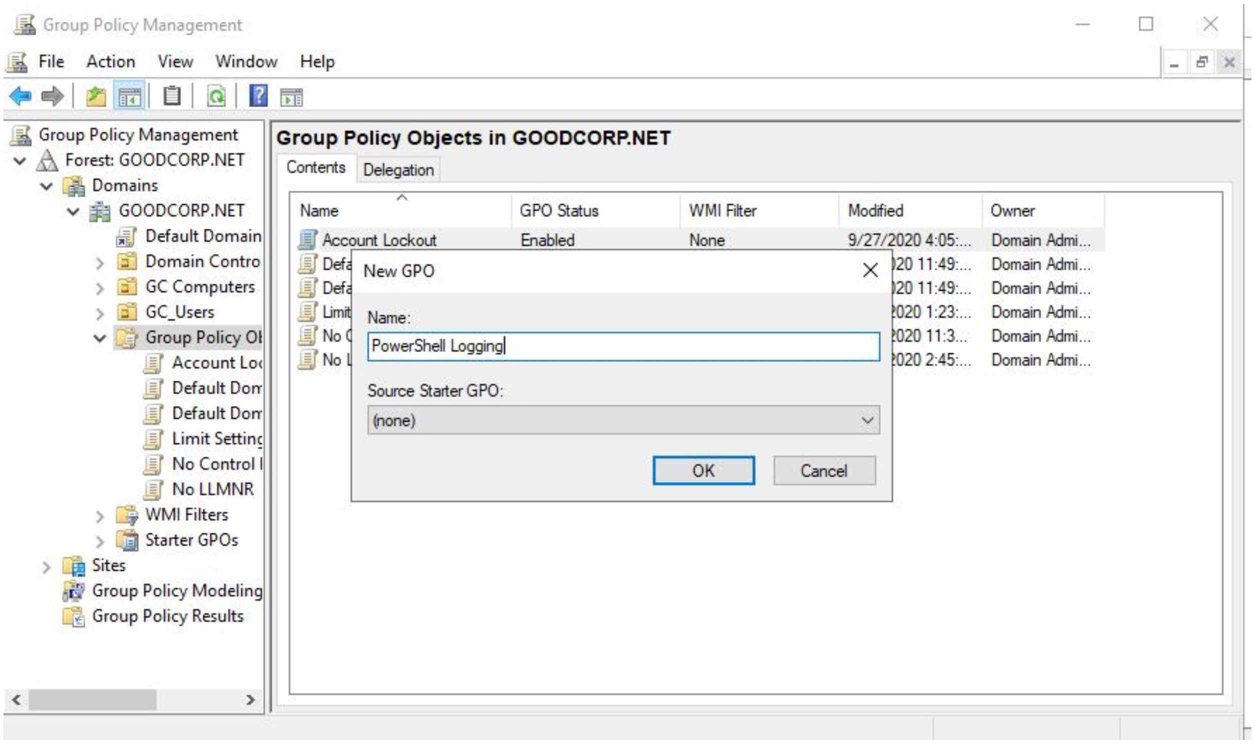
Task 3: Create a GPO: Enabling Verbose PowerShell Logging and Transcription

Solution:

This GPO will combine multiple policies into one.

Name the Group Policy Object **PowerShell Logging**.



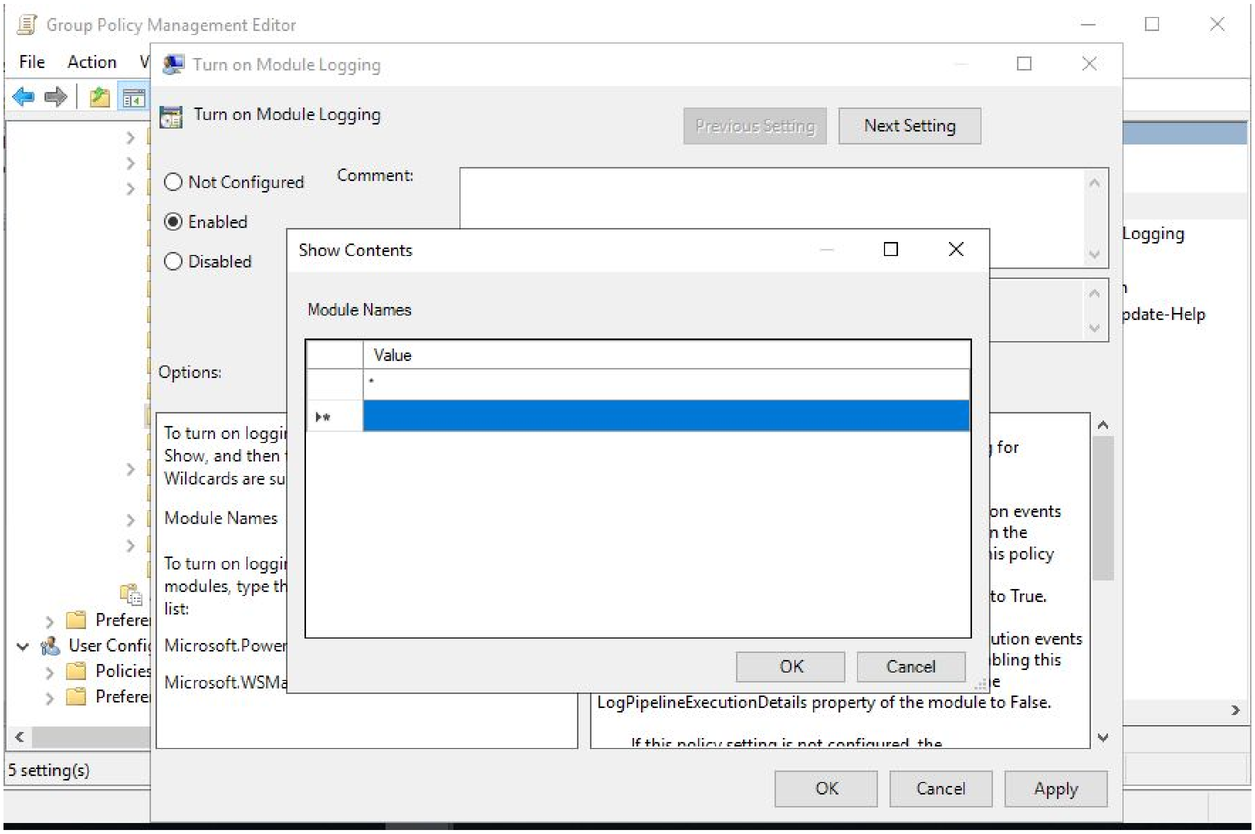
Name	GPO Status	WMI Filter	Modified	Owner
Account Lockout	Enabled	None	9/27/2020 4:05:...	Domain Admi...
Defa			20 11:49:...	Domain Admi...
Defa			20 11:49:...	Domain Admi...
Limit			2020 1:23:...	Domain Admi...
No C			2020 11:3...	Domain Admi...
No L			2020 2:45:...	Domain Admi...

Name: PowerShell Logging

Source Starter GPO: (none)

To find the Windows Powershell policy in Group Policy Management Editor, you check out the computer configuration, administrative templates, and Windows component directories.

Enable the Turn on Module Logging, click **Show** next to **Module Names**, enter asterisk *, and then click **OK.** This will log all PowerShell modules.



Turn on Module Logging

○ Not Configured
● Enabled
○ Disabled

Show Contents

Module Names

	Value
	*
▸*	

To turn on loggi
Show, and then
Wildcards are su

Module Names

To turn on loggi
modules, type th
list:

Microsoft.Power

Microsoft.WSMa

for

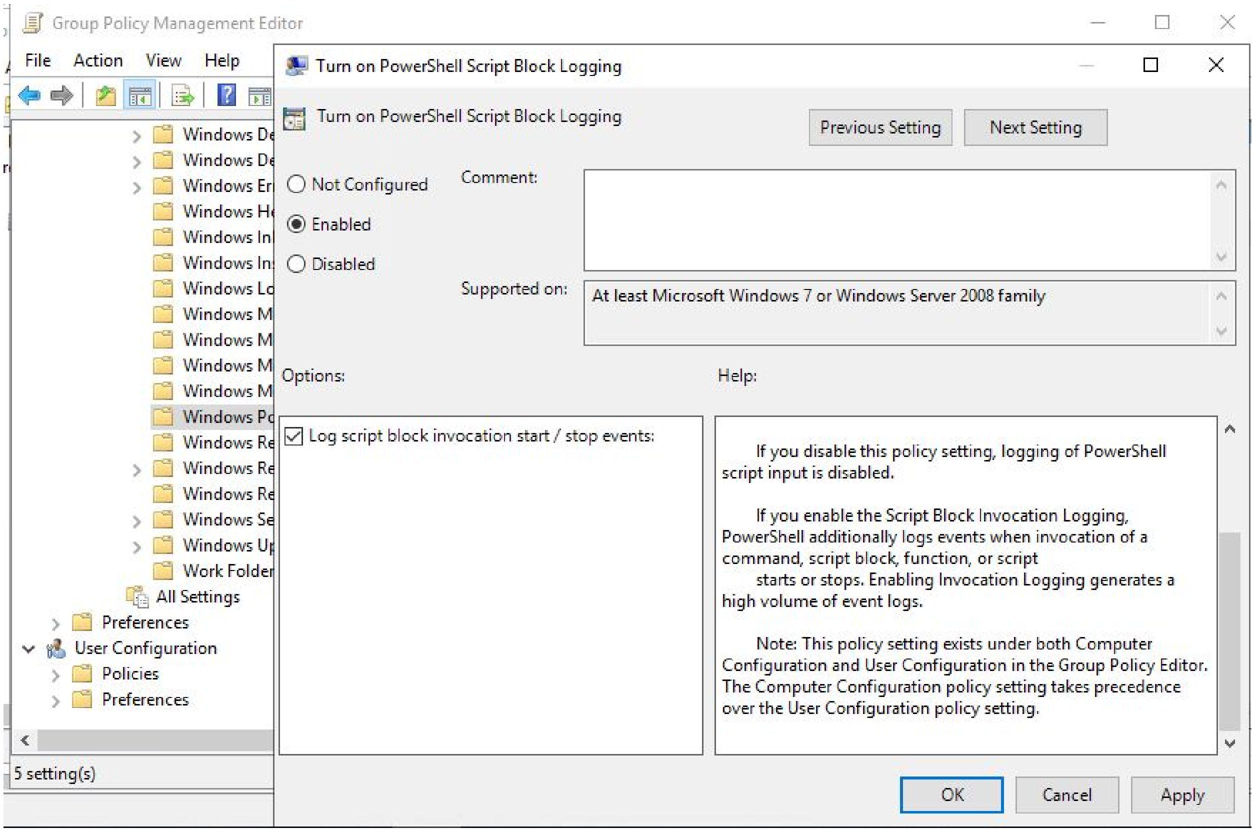
on events
n the
is policy

to True.

ution events
bling this
e
LogPipelineExecutionDetails property of the module to False.

If this policy setting is not configured, the

Enable the **Turn on PowerShell Script Block Logging** policy, and check the **Log script block invocation start/stop events** option



Turn on PowerShell Script Block Logging

Turn on PowerShell Script Block Logging

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Options:

☑ Log script block invocation start / stop events:

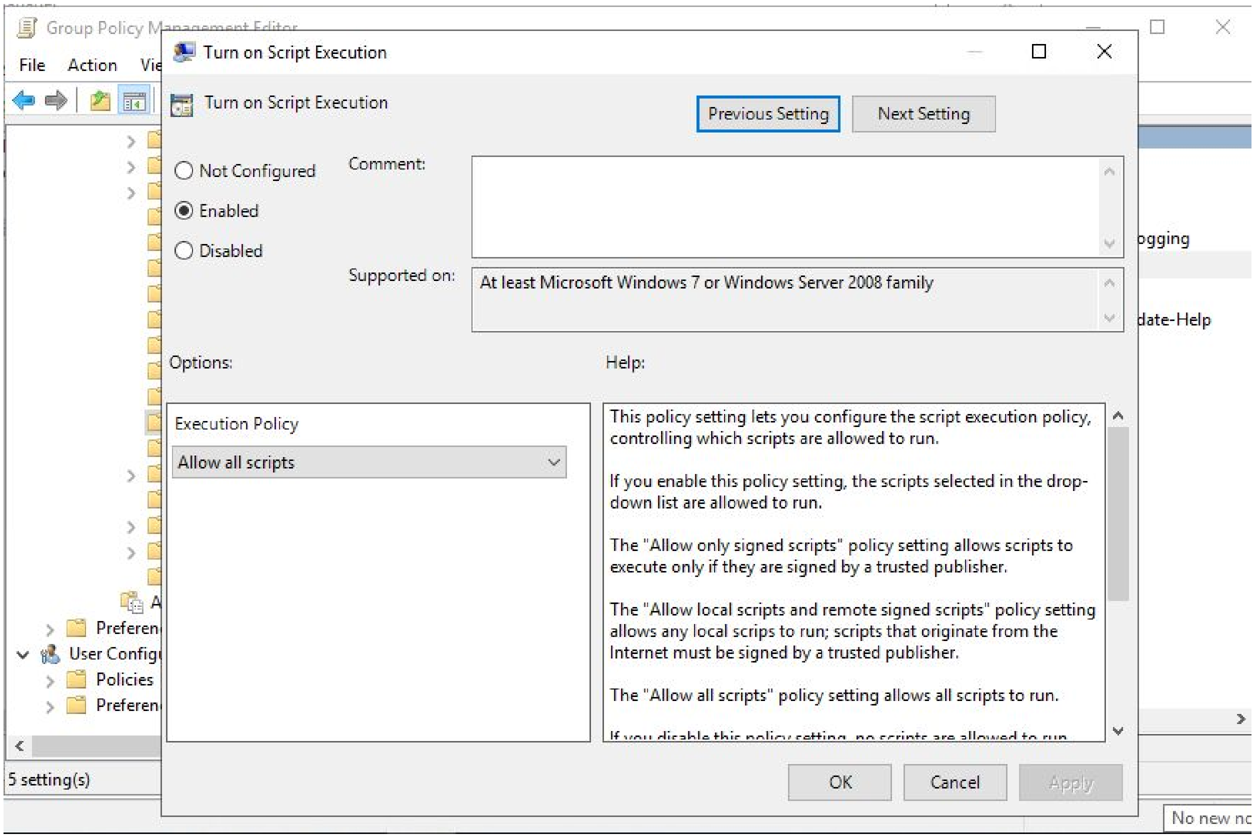
Help:

If you disable this policy setting, logging of PowerShell script input is disabled.

If you enable the Script Block Invocation Logging, PowerShell additionally logs events when invocation of a command, script block, function, or script starts or stops. Enabling Invocation Logging generates a high volume of event logs.

Note: This policy setting exists under both Computer Configuration and User Configuration in the Group Policy Editor. The Computer Configuration policy setting takes precedence over the User Configuration policy setting.

Enable the **Turn on Script Execution** policy, and set **Execution Policy** option to **Allow all scripts**.



Turn on Script Execution

Turn on Script Execution

○ Not Configured

● Enabled

○ Disabled

Comment:

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Options:

Execution Policy

Allow all scripts

Help:

This policy setting lets you configure the script execution policy, controlling which scripts are allowed to run.

If you enable this policy setting, the scripts selected in the drop-down list are allowed to run.

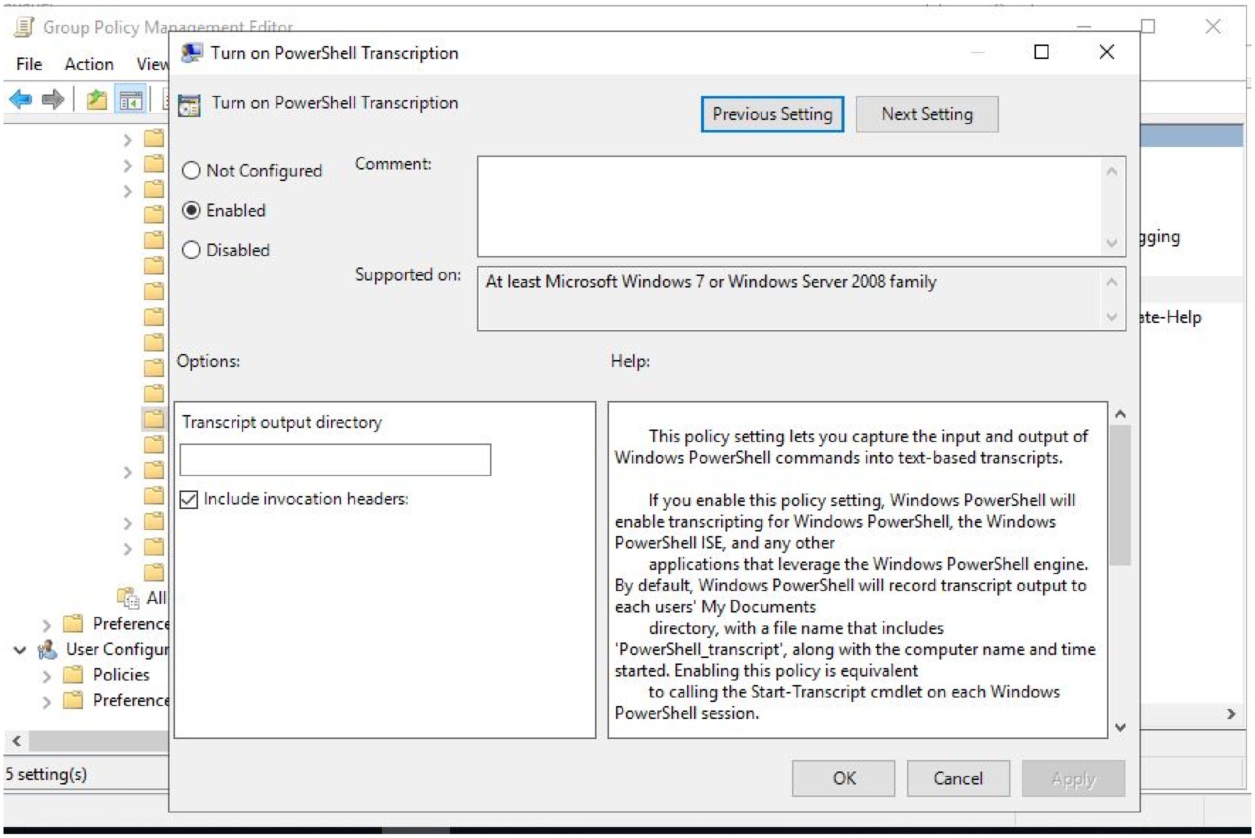
The "Allow only signed scripts" policy setting allows scripts to execute only if they are signed by a trusted publisher.

The "Allow local scripts and remote signed scripts" policy setting allows any local scrips to run; scripts that originate from the Internet must be signed by a trusted publisher.

The "Allow all scripts" policy setting allows all scripts to run.

If you disable this policy setting, no scripts are allowed to run.

Enable the **Turn on PowerShell Transcription** policy, leave the **Transcript output directory** blank (this defaults to the user's ~\Documents directory), and check the **Include invocation headers** option to add timestamps to the command transcriptions.



Turn on PowerShell Transcription

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Microsoft Windows 7 or Windows Server 2008 family

Options:

Transcript output directory

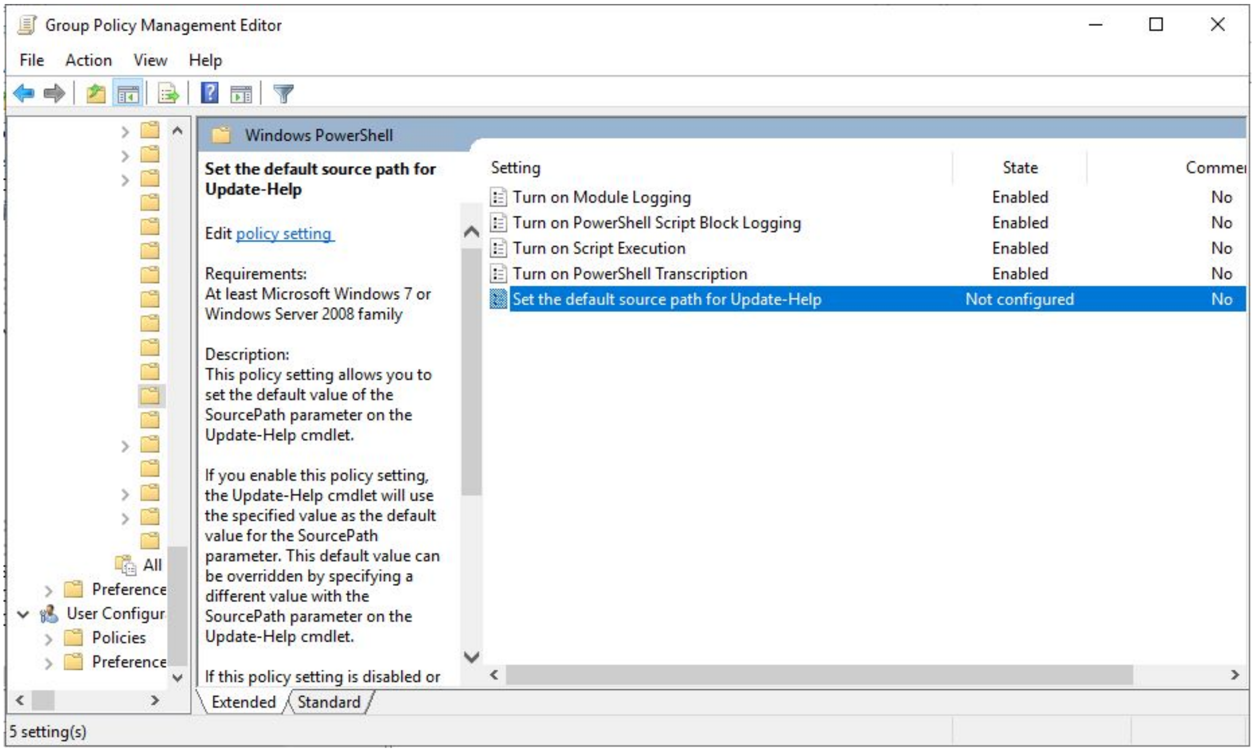
☑ Include invocation headers:

Help:

This policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts.

If you enable this policy setting, Windows PowerShell will enable transcripting for Windows PowerShell, the Windows PowerShell ISE, and any other applications that leverage the Windows PowerShell engine. By default, Windows PowerShell will record transcript output to each users' My Documents directory, with a file name that includes 'PowerShell_transcript', along with the computer name and time started. Enabling this policy is equivalent to calling the Start-Transcript cmdlet on each Windows PowerShell session.

Leave the **Set the default source path for Update-Help** policy as **Not configured**



Set the default source path for Update-Help

Edit policy setting

Requirements:
At least Microsoft Windows 7 or Windows Server 2008 family

Description:
This policy setting allows you to set the default value of the SourcePath parameter on the Update-Help cmdlet.

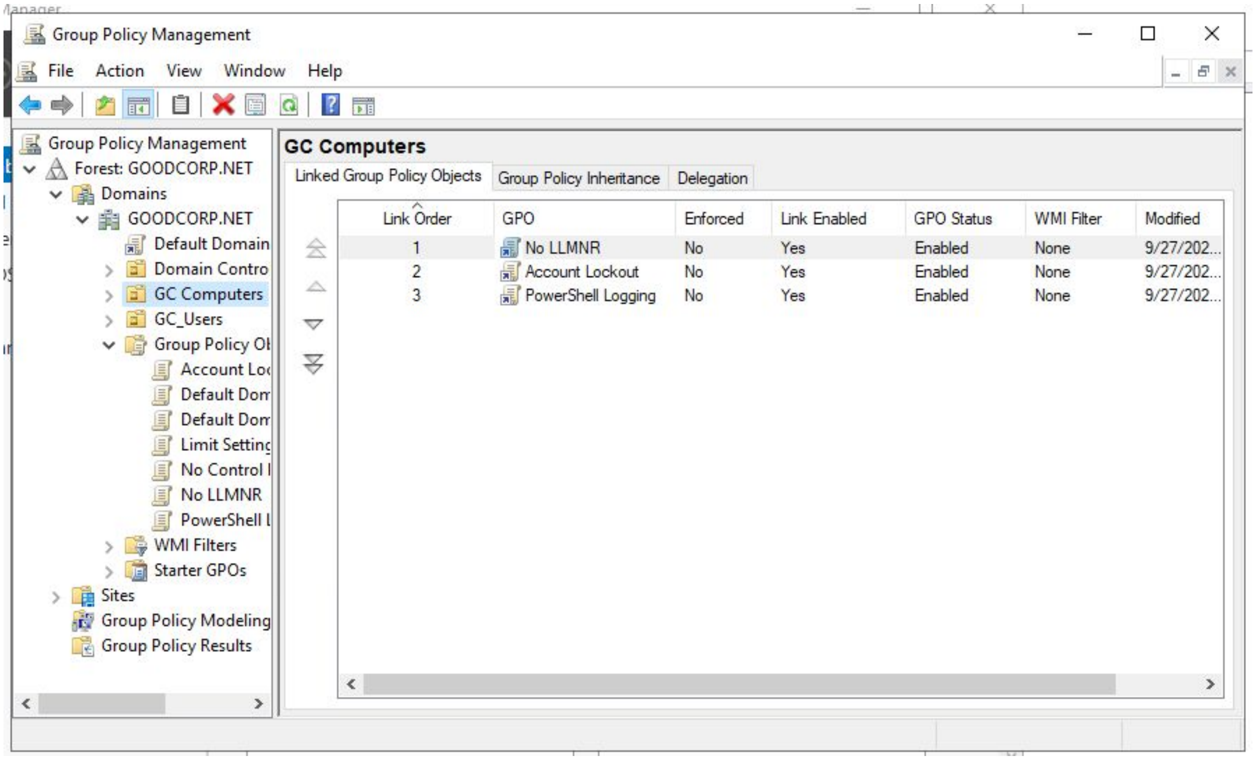
If you enable this policy setting, the Update-Help cmdlet will use the specified value as the default value for the SourcePath parameter. This default value can be overridden by specifying a different value with the SourcePath parameter on the Update-Help cmdlet.

If this policy setting is disabled or

Setting	State	Commer
Turn on Module Logging	Enabled	No
Turn on PowerShell Script Block Logging	Enabled	No
Turn on Script Execution	Enabled	No
Turn on PowerShell Transcription	Enabled	No
Set the default source path for Update-Help	Not configured	No

5 setting(s)

Then, link this new PowerShell Logging GPO to the GC Computers OU

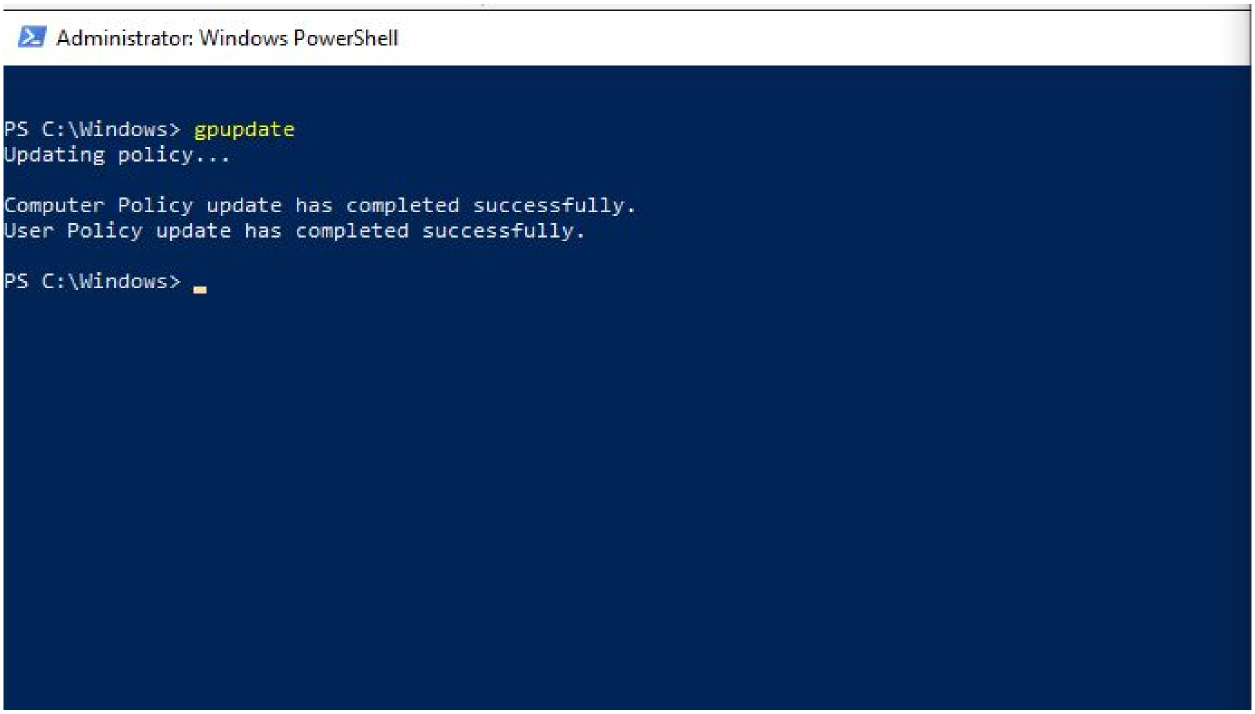


GC Computers

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified
1	No LLMNR	No	Yes	Enabled	None	9/27/202...
2	Account Lockout	No	Yes	Enabled	None	9/27/202...
3	PowerShell Logging	No	Yes	Enabled	None	9/27/202...

Finally, log into the nested Windows 10 machine, run gpupdate from PowerShell, bash, or cmd, to update the group policies in Windows operating system Domain.

PS > gpupdate



```
PS C:\Windows> gpupdate
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Windows> _
```