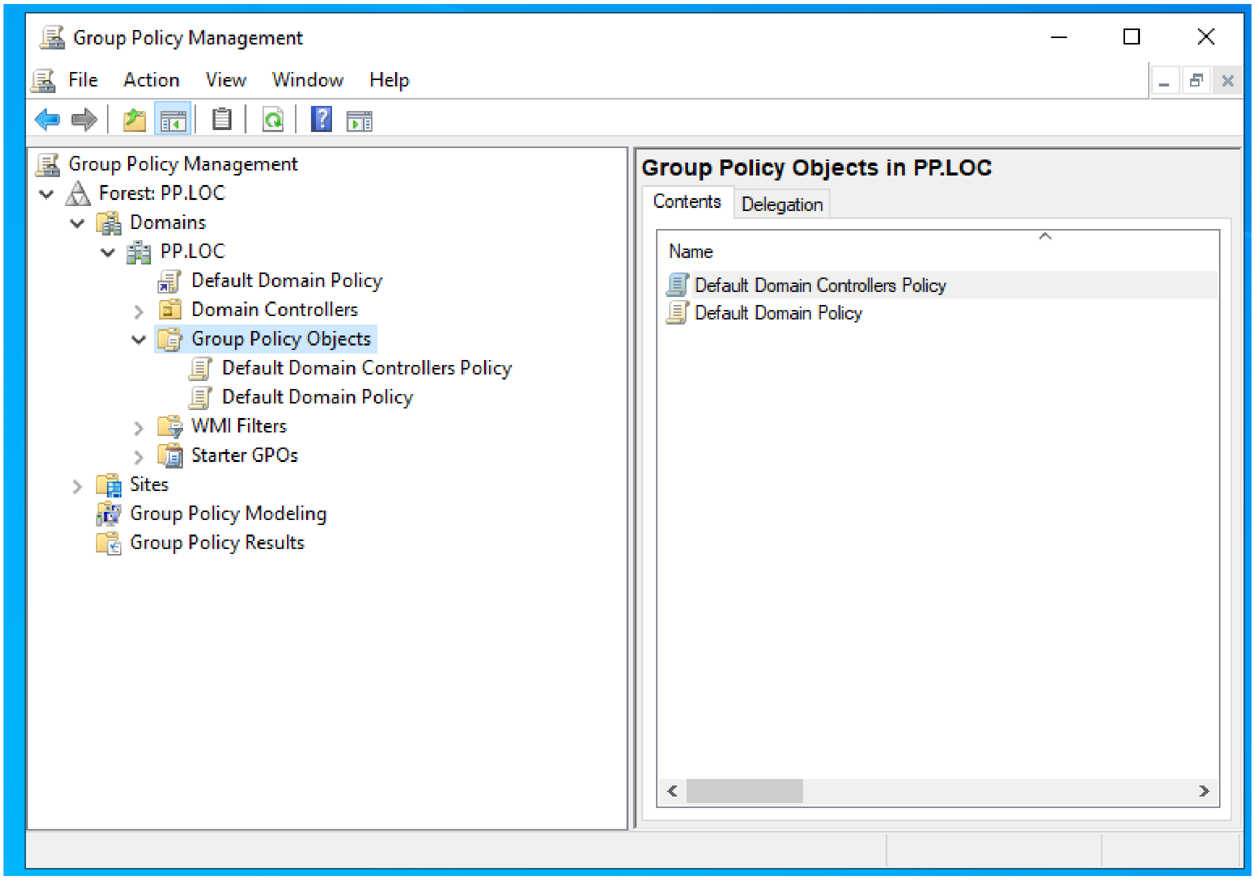
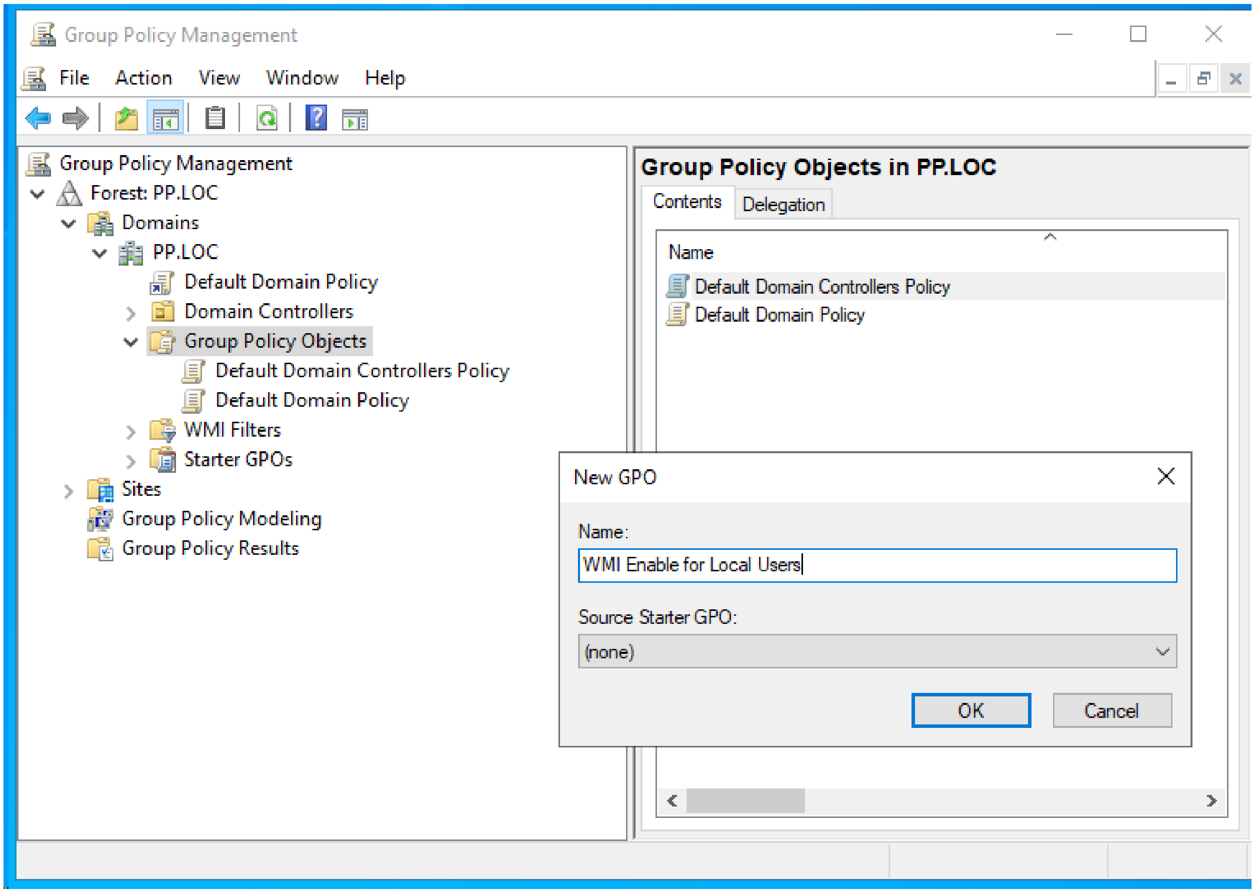
WMI Access For All Users

This document outlines giving WMI access to domain member local users for Securden through GPO. It includes the following steps,

Step 1: Open ‘Group Policy Management’ (gpmc.msc)



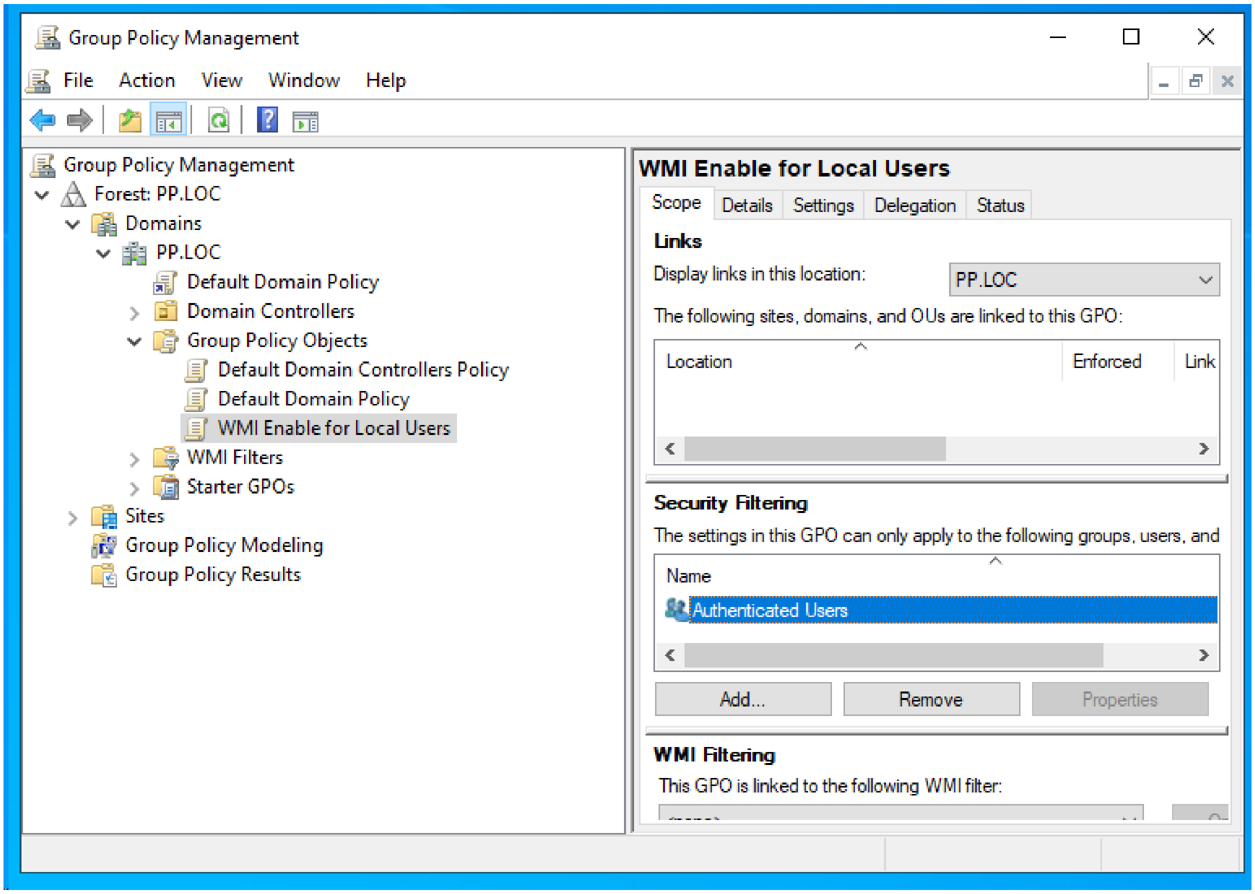
Step 2: Right-Click on ‘Group Policy Objects’ and select ‘New’. ‘New GPO’ popup will open, give a name for the new GPO.



Name: WMI Enable for Local Users

Source Starter GPO: (none)

Step 3: Once the GPO is created, go to ‘Security Filtering’



WMI Enable for Local Users

Links

Display links in this location: PP.LOC

The following sites, domains, and OUs are linked to this GPO:

Security Filtering

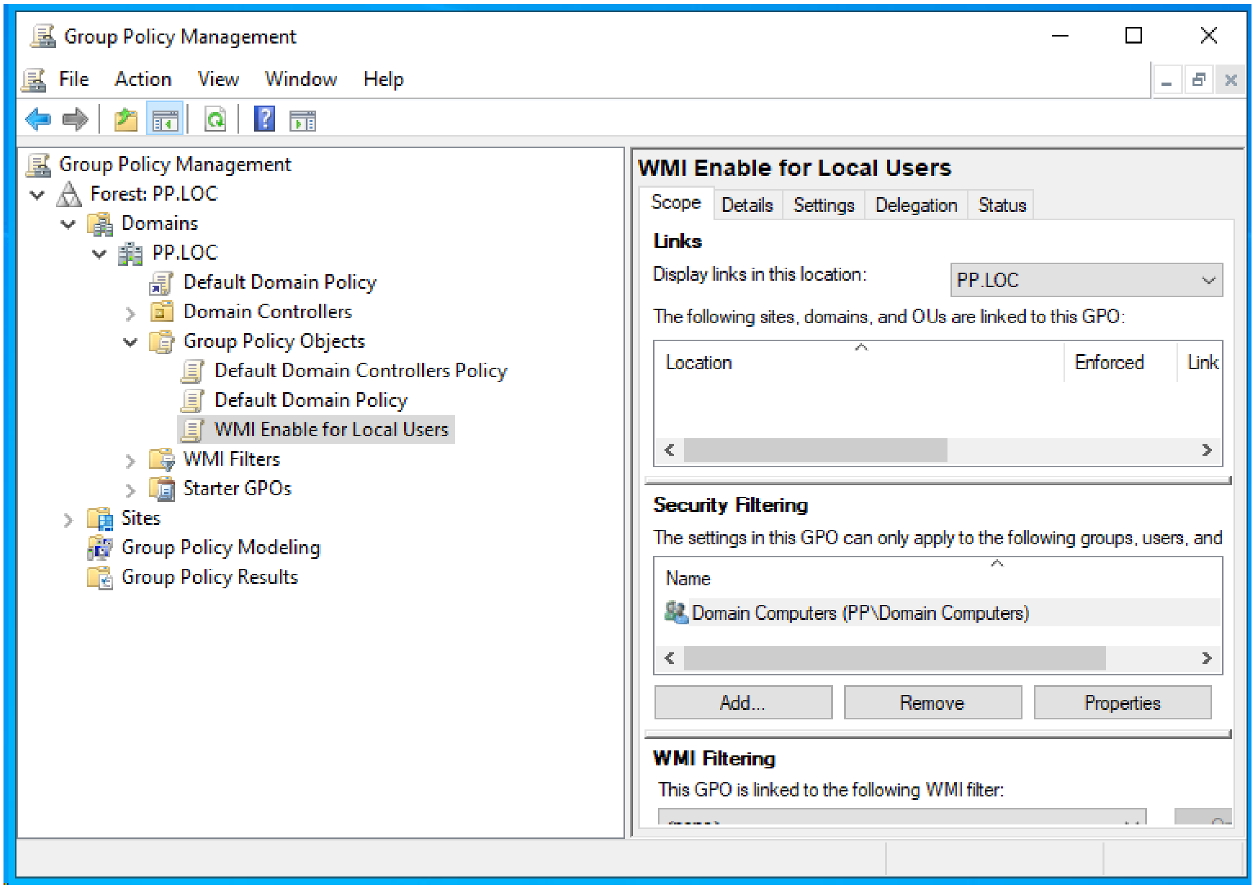
The settings in this GPO can only apply to the following groups, users, and

Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

Step 4: Remove 'Authenticated Users' and add 'Domain Computers' under 'Security Filtering'.



Display links in this location: PP.LOC

The following sites, domains, and OUs are linked to this GPO:

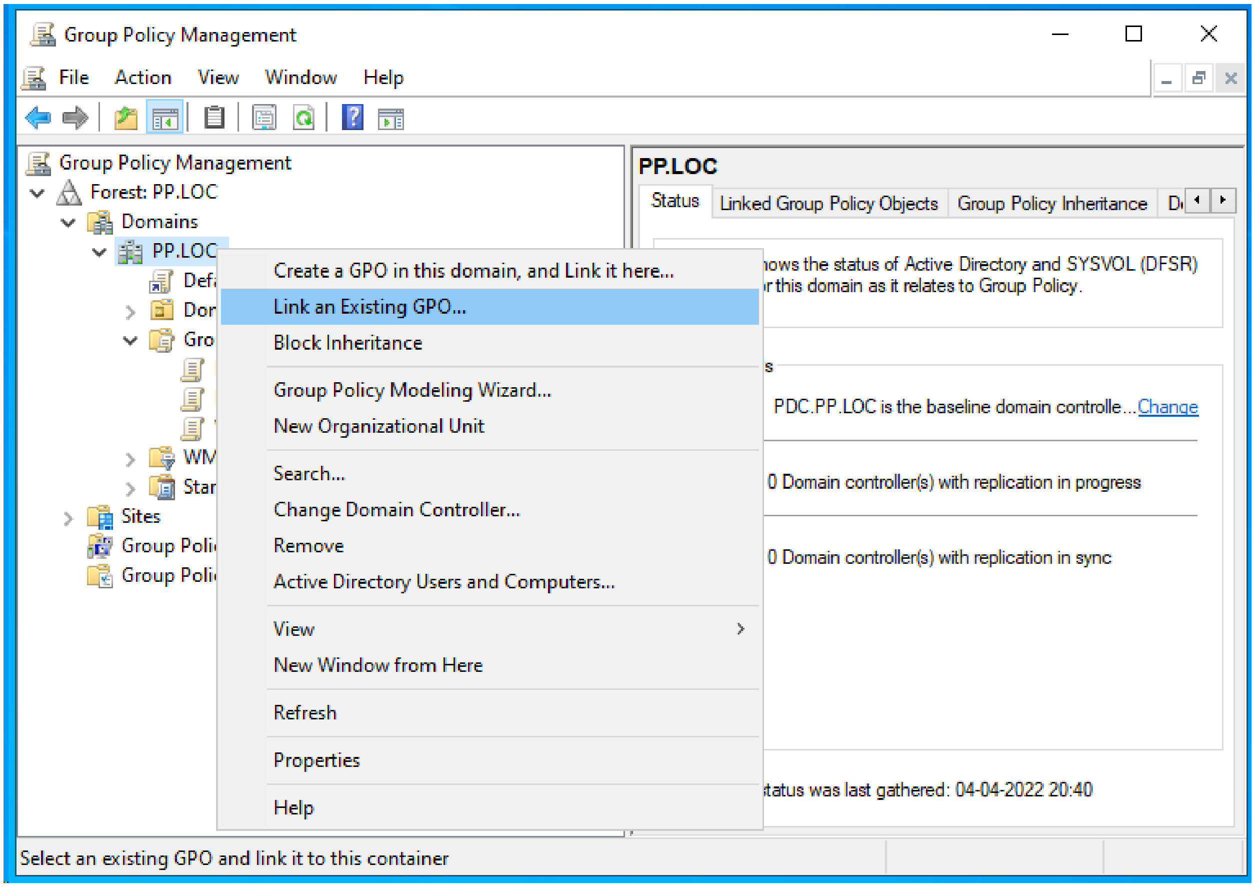
Security Filtering

The settings in this GPO can only apply to the following groups, users, and

Name
Domain Computers (PP\Domain Computers)

This GPO is linked to the following WMI filter:

Step 5: Right-Click on the domain and choose 'Link an Existing GPO'. In case if you would like to link specific to a particular OU, you can right-click on that OU and choose 'Link an Existing GPO'.



ows the status of Active Directory and SYSVOL (DFSR) r this domain as it relates to Group Policy.

PDC.PP.LOC is the baseline domain controlle...Change

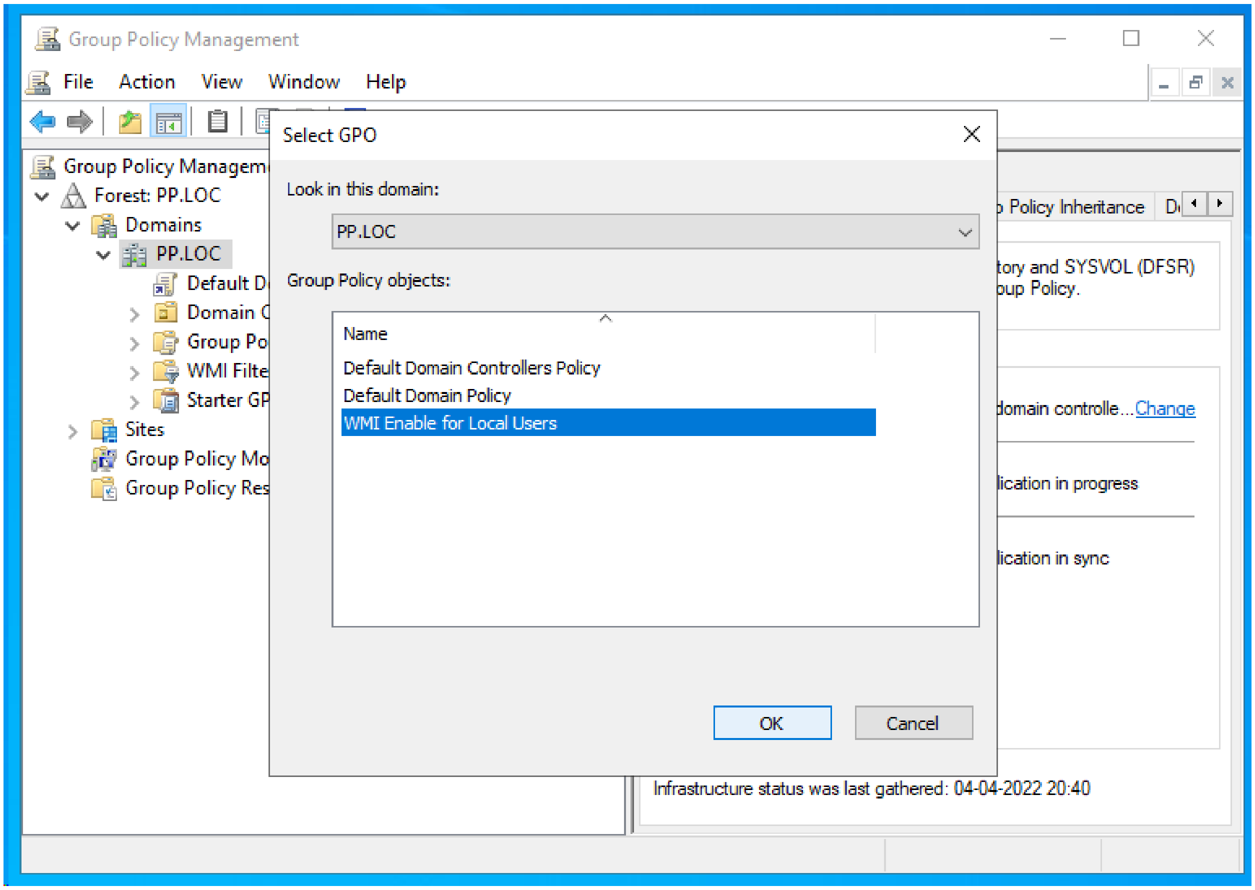
0 Domain controller(s) with replication in progress

0 Domain controller(s) with replication in sync

tatus was last gathered: 04-04-2022 20:40

Select an existing GPO and link it to this container

Step 6: Choose the newly created GPO.



Select GPO

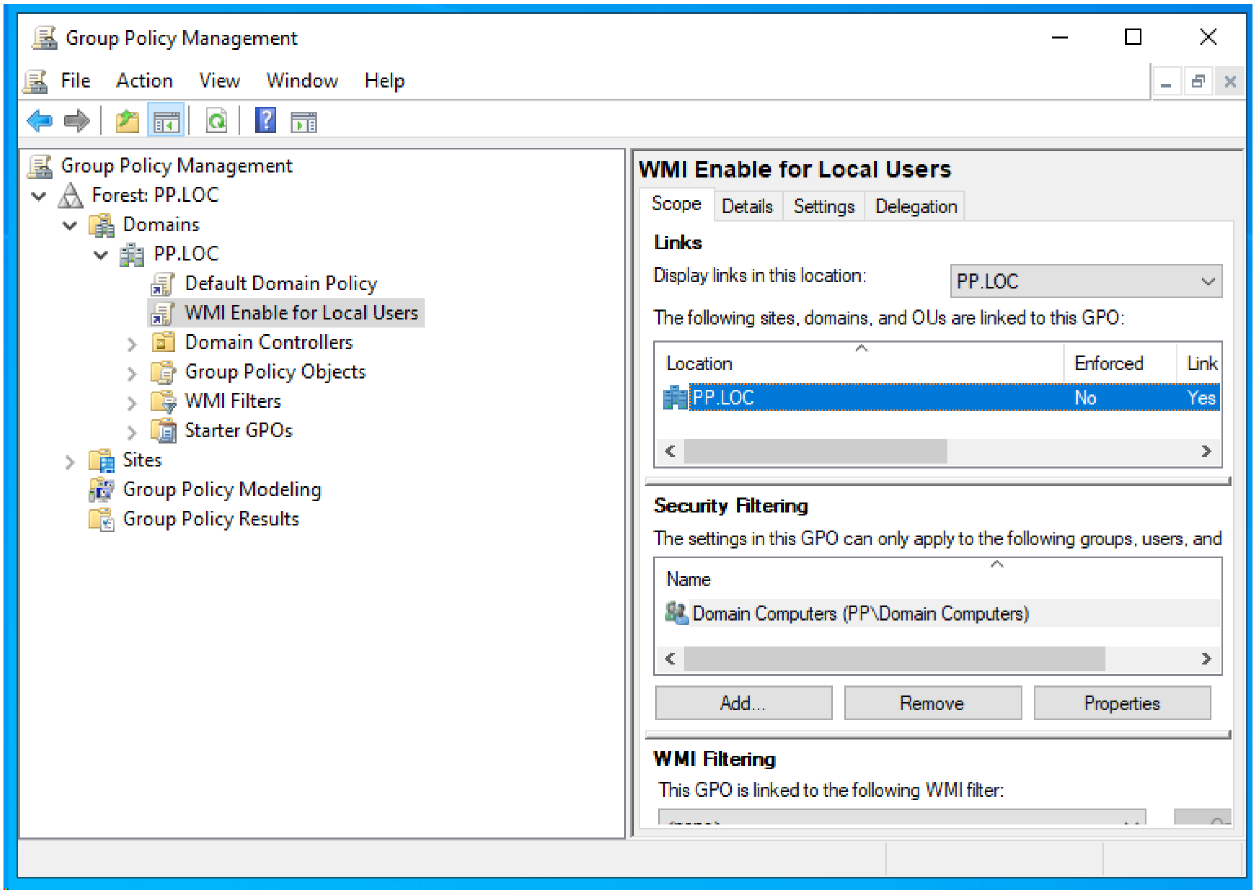
Look in this domain: PP.LOC

Group Policy objects:

Name
Default Domain Controllers Policy
Default Domain Policy
WMI Enable for Local Users

Infrastructure status was last gathered: 04-04-2022 20:40

Step 7: Go to the ‘Links’ column of the created GPO.



WMI Enable for Local Users

Links

Display links in this location: PP.LOC

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link
PP.LOC	No	Yes

Security Filtering

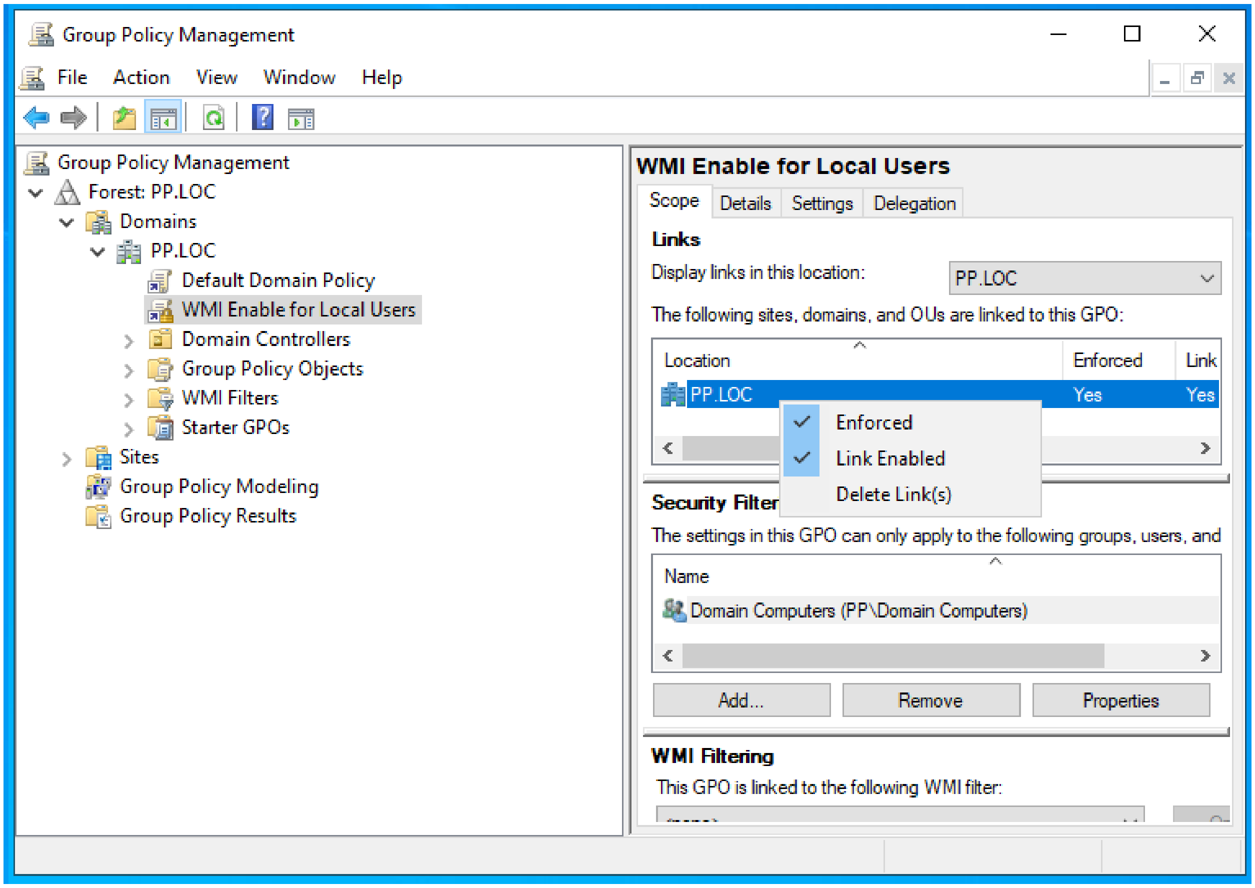
The settings in this GPO can only apply to the following groups, users, and

Name
Domain Computers (PP\Domain Computers)

WMI Filtering

This GPO is linked to the following WMI filter:

Step 8: Right-click on the link created and choose ‘Enforced’.



WMI Enable for Local Users

Links

Display links in this location: PP.LOC

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link
PP.LOC	Yes	Yes

Security Filter

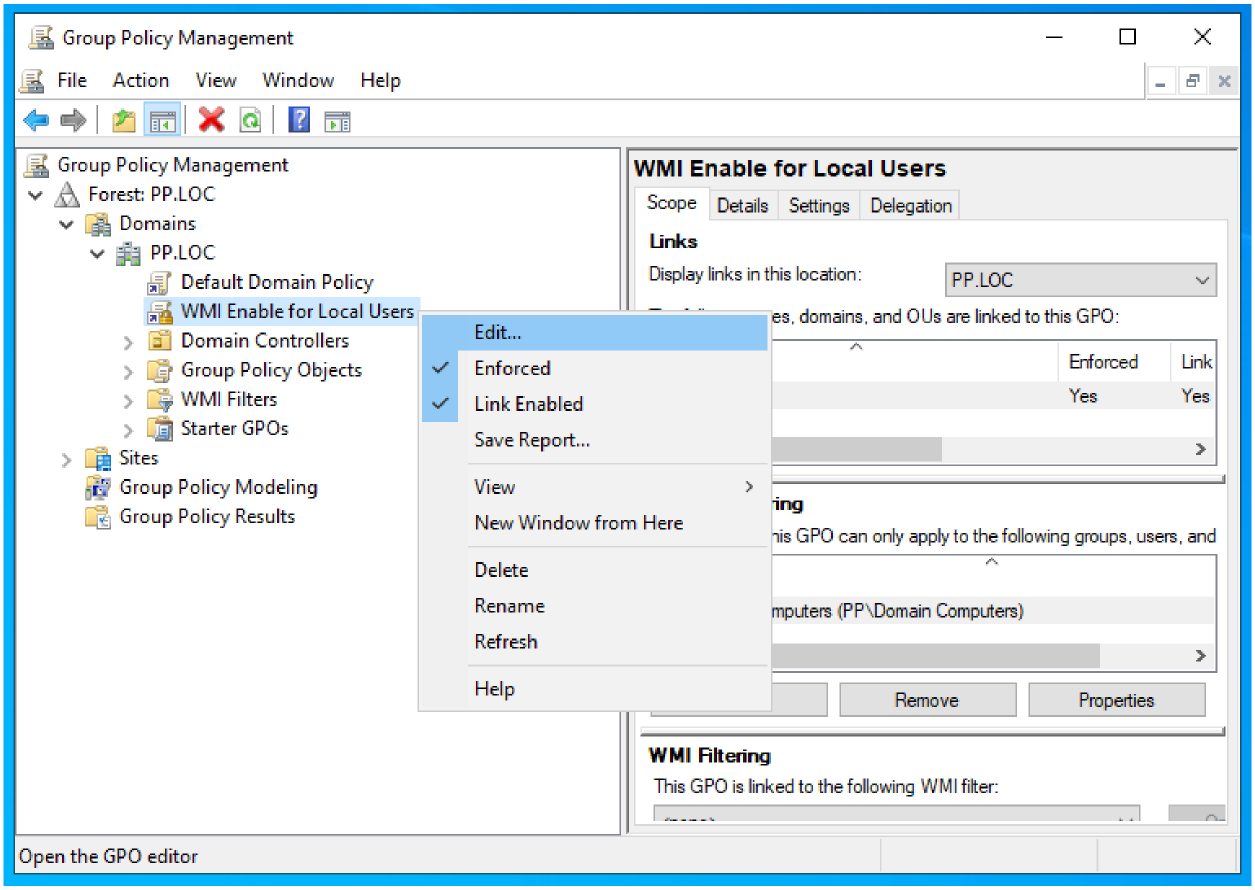
The settings in this GPO can only apply to the following groups, users, and

Name
Domain Computers (PP\Domain Computers)

WMI Filtering

This GPO is linked to the following WMI filter:

Step 9: Right-click on the link created and choose ‘Edit’.



WMI Enable for Local Users

Links

Display links in this location: PP.LOC

es, domains, and OUs are linked to this GPO:

	Enforced	Link
	Yes	Yes

ing

his GPO can only apply to the following groups, users, and

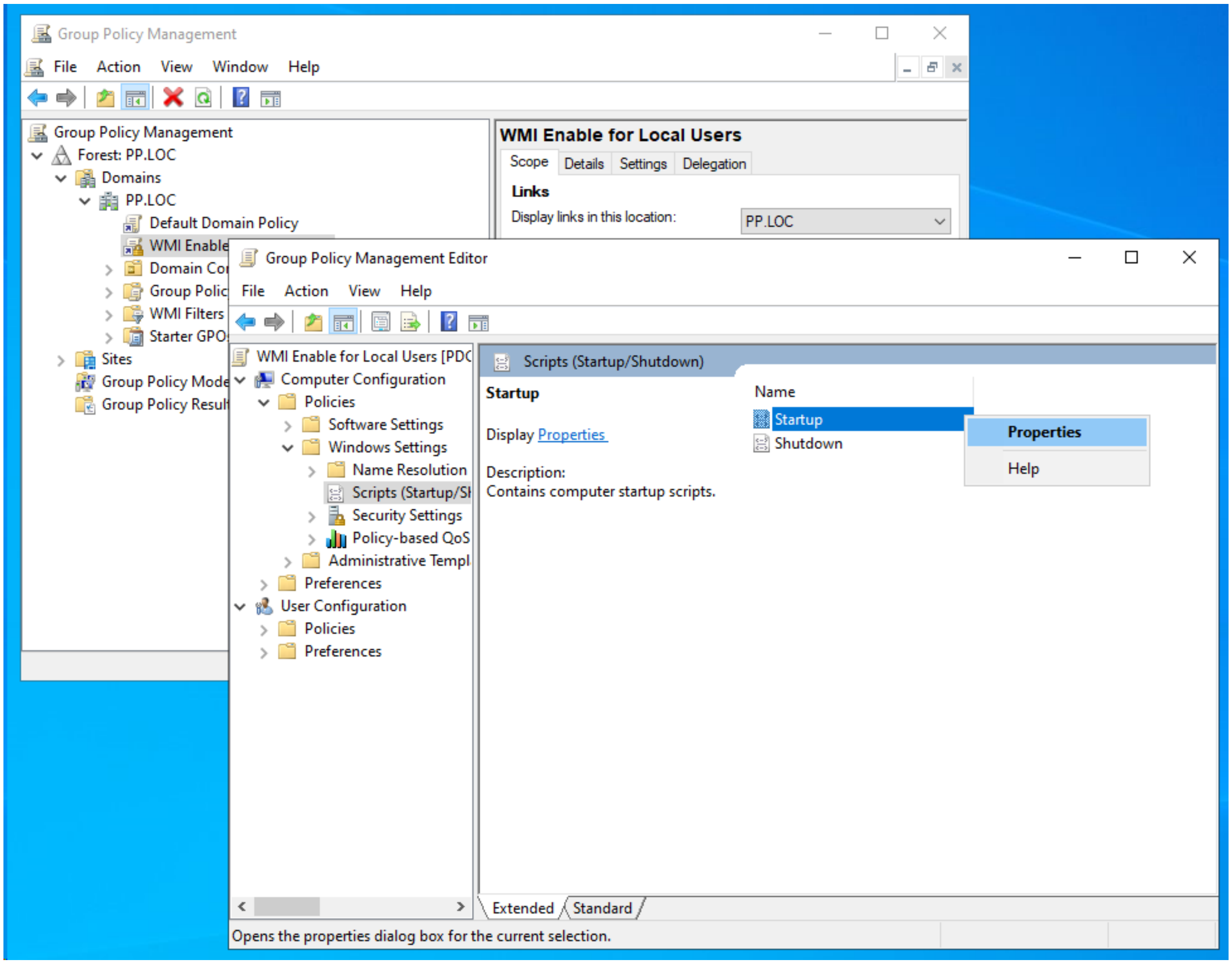
mputers (PP\Domain Computers)

WMI Filtering

This GPO is linked to the following WMI filter:

Open the GPO editor

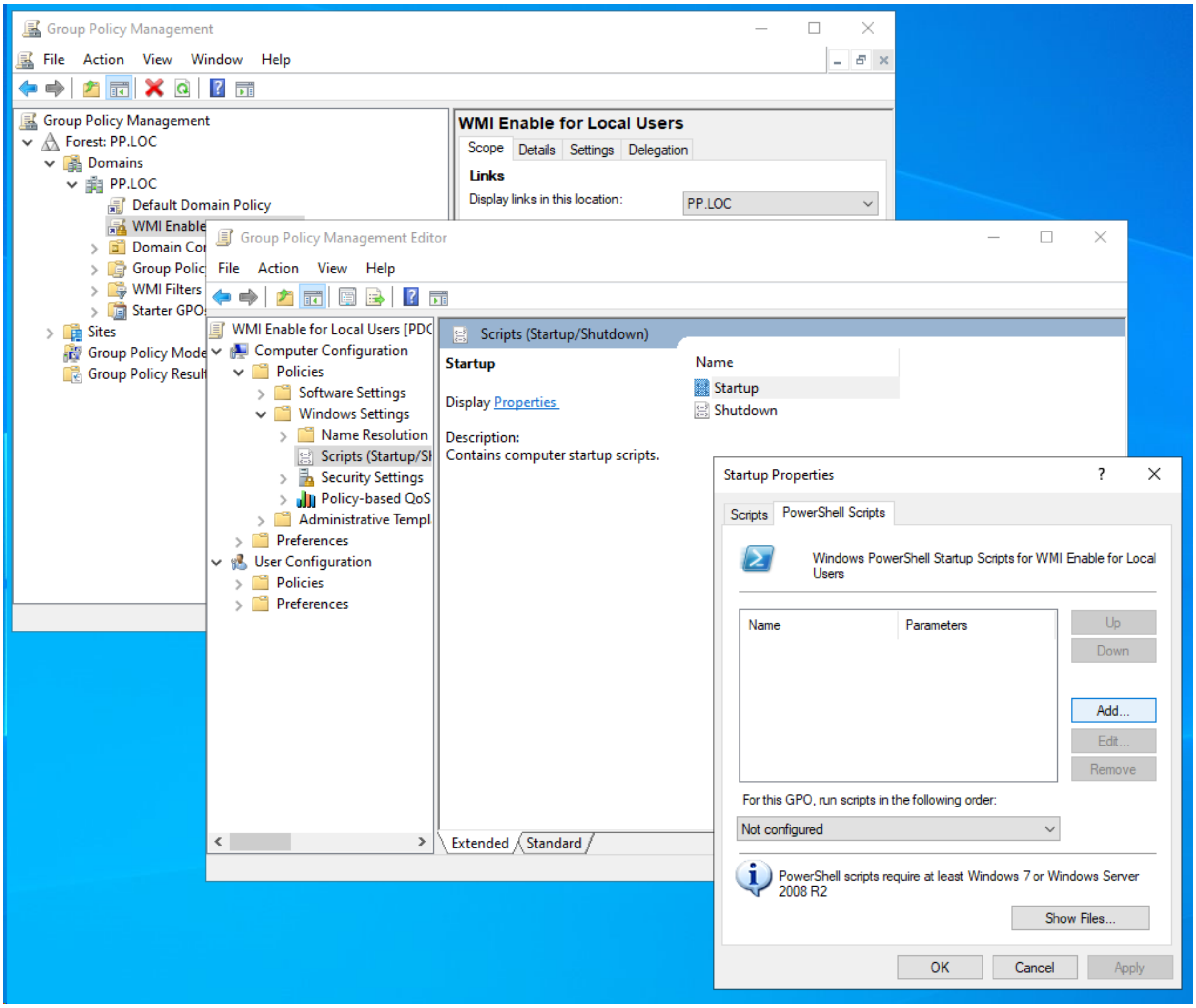
Step 10: Navigate to ‘Computer Configuration >> Policies >> Windows Settings >> Scripts(Startup/Shutdown) >> Startup’ and choose properties.



Description:
Contains computer startup scripts.

Opens the properties dialog box for the current selection.

Step 11: Go to ‘Powershell Scripts’ tab and choose ‘Add’.



Display links in this location: PP.LOC

Display Properties

Description:
Contains computer startup scripts.

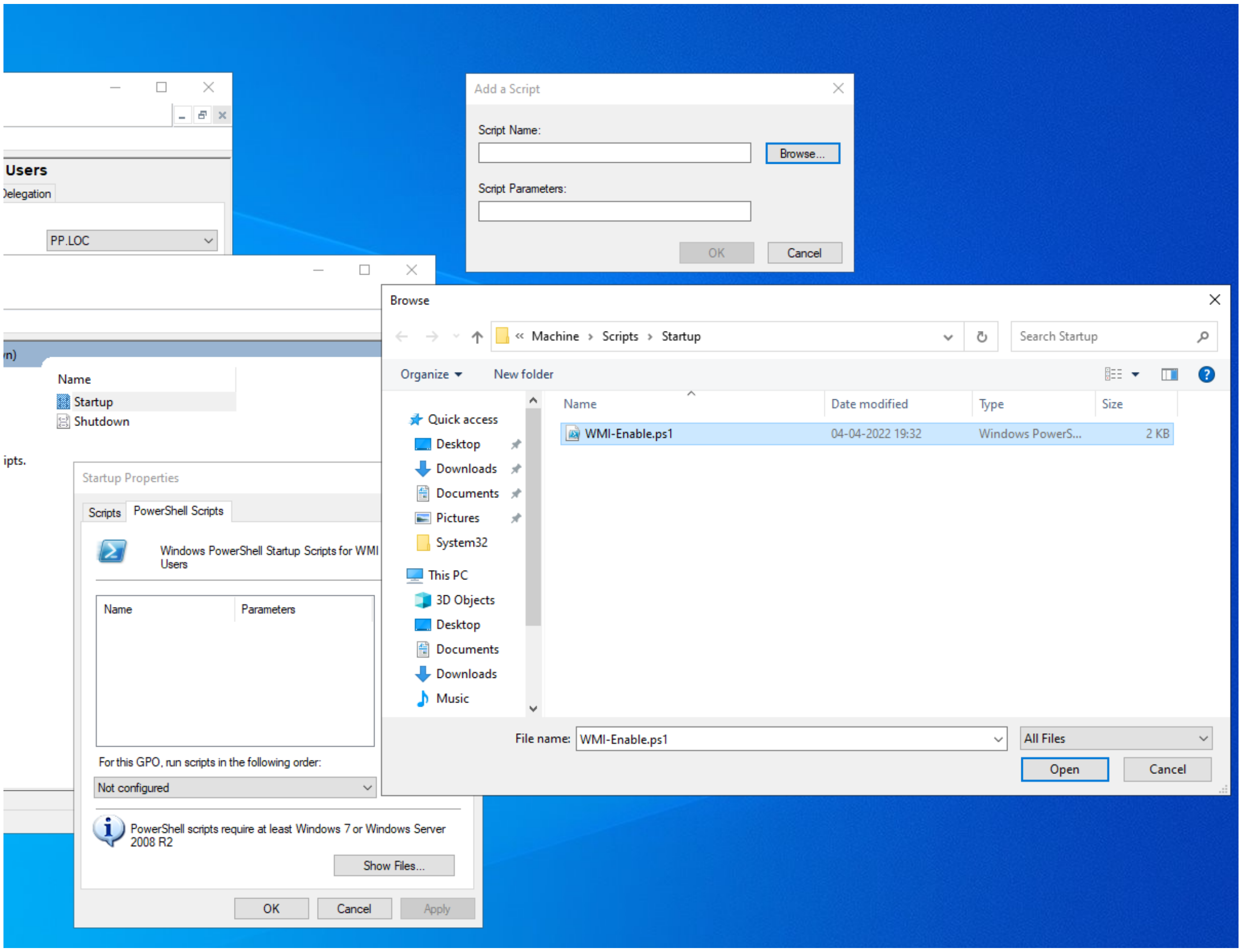
Windows PowerShell Startup Scripts for WMI Enable for Local Users

For this GPO, run scripts in the following order: Not configured

PowerShell scripts require at least Windows 7 or Windows Server 2008 R2

Step 12: Download wmi-enable.txt from the below link and **rename it with the extension (wmi-enable.ps1)**

https://drive.google.com/file/d/10bMt27b5FI6RNt5uBhhWcm5nTe79MjJE/view?usp=sharing



Add a Script

Script Name:

Script Parameters:

Startup Properties

Windows PowerShell Startup Scripts for WMI Users

For this GPO, run scripts in the following order: Not configured

PowerShell scripts require at least Windows 7 or Windows Server 2008 R2

Browse

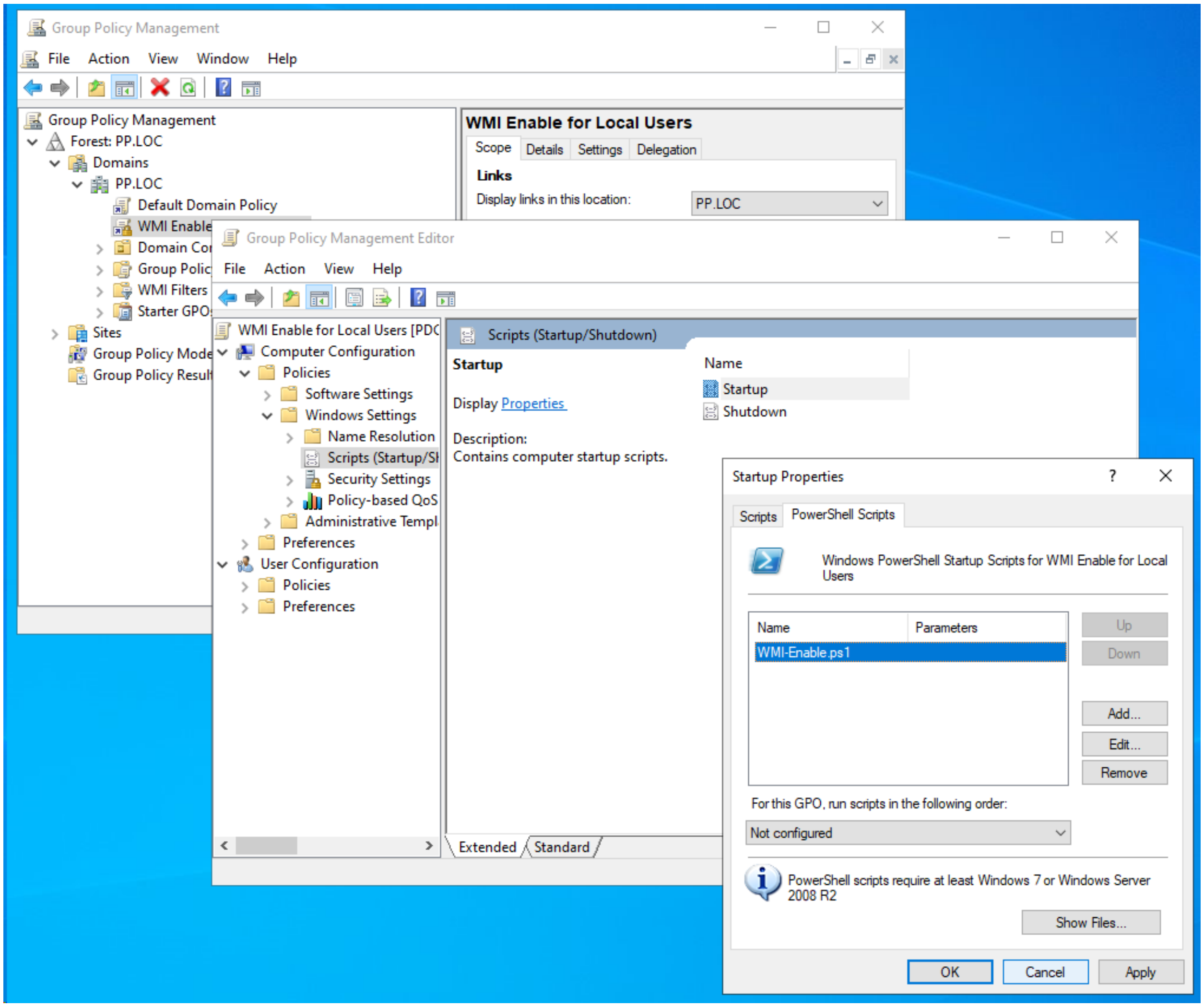
Machine › Scripts › Startup

Name	Date modified	Type	Size
WMI-Enable.ps1	04-04-2022 19:32	Windows PowerS...	2 KB

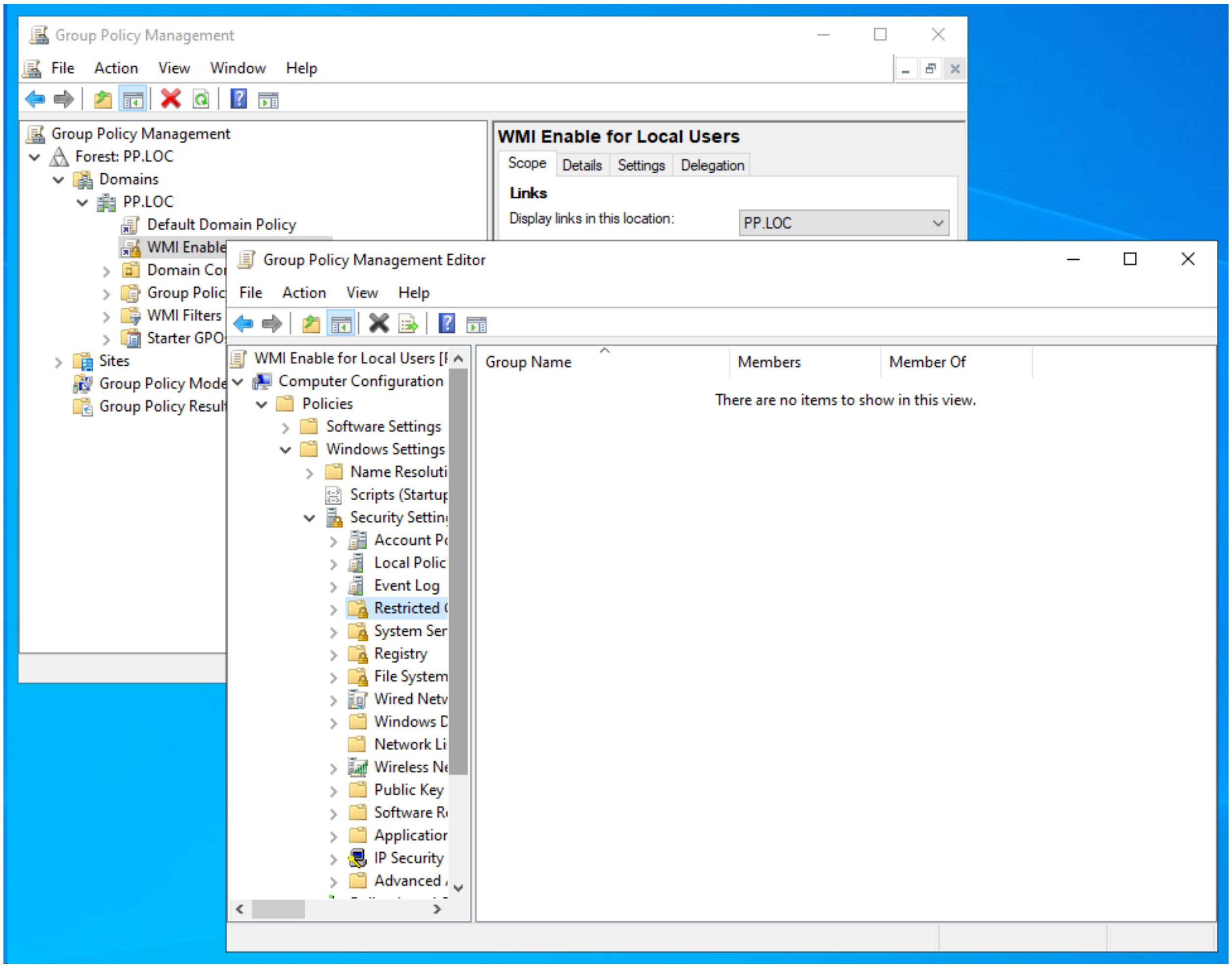
File name: WMI-Enable.ps1

All Files

Step 13: Save the 'Startup Properties' window.

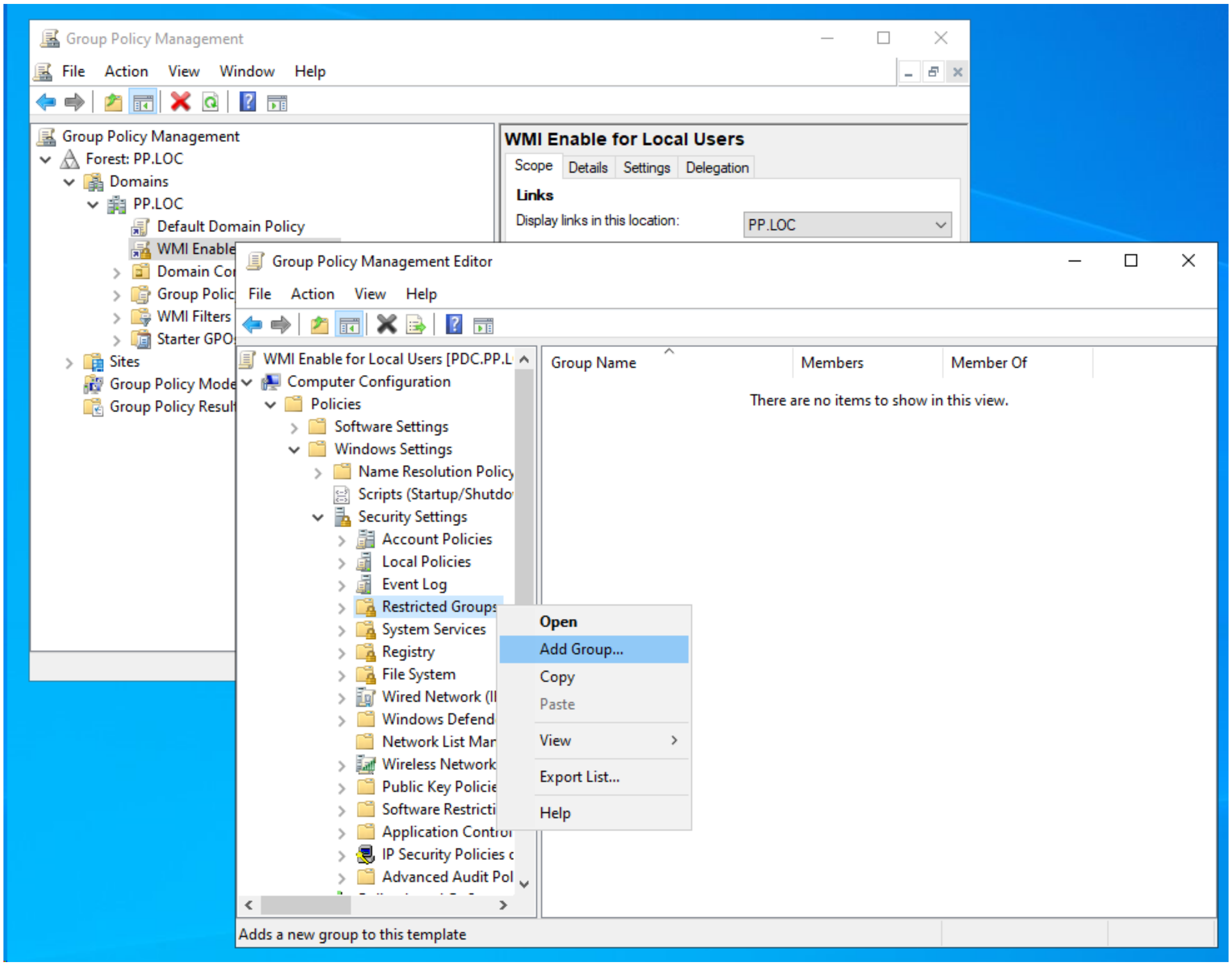


Step 14: Navigate to ‘Computer Configuration >> Windows Settings >> Security Settings >> Restricted Groups’.



There are no items to show in this view.

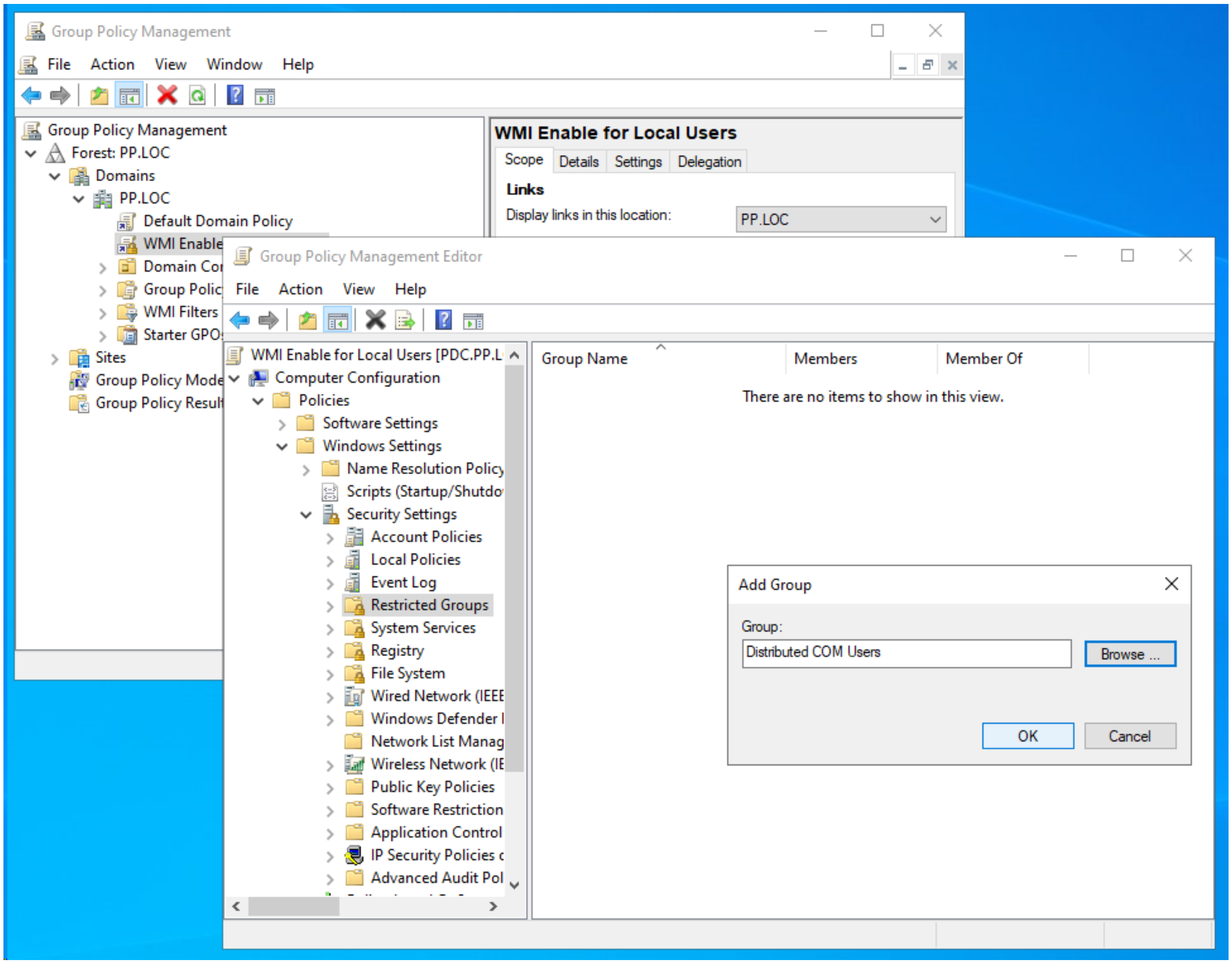
Step 15: Right-click on ‘Restricted Groups’ and click ‘Add Group’.



There are no items to show in this view.

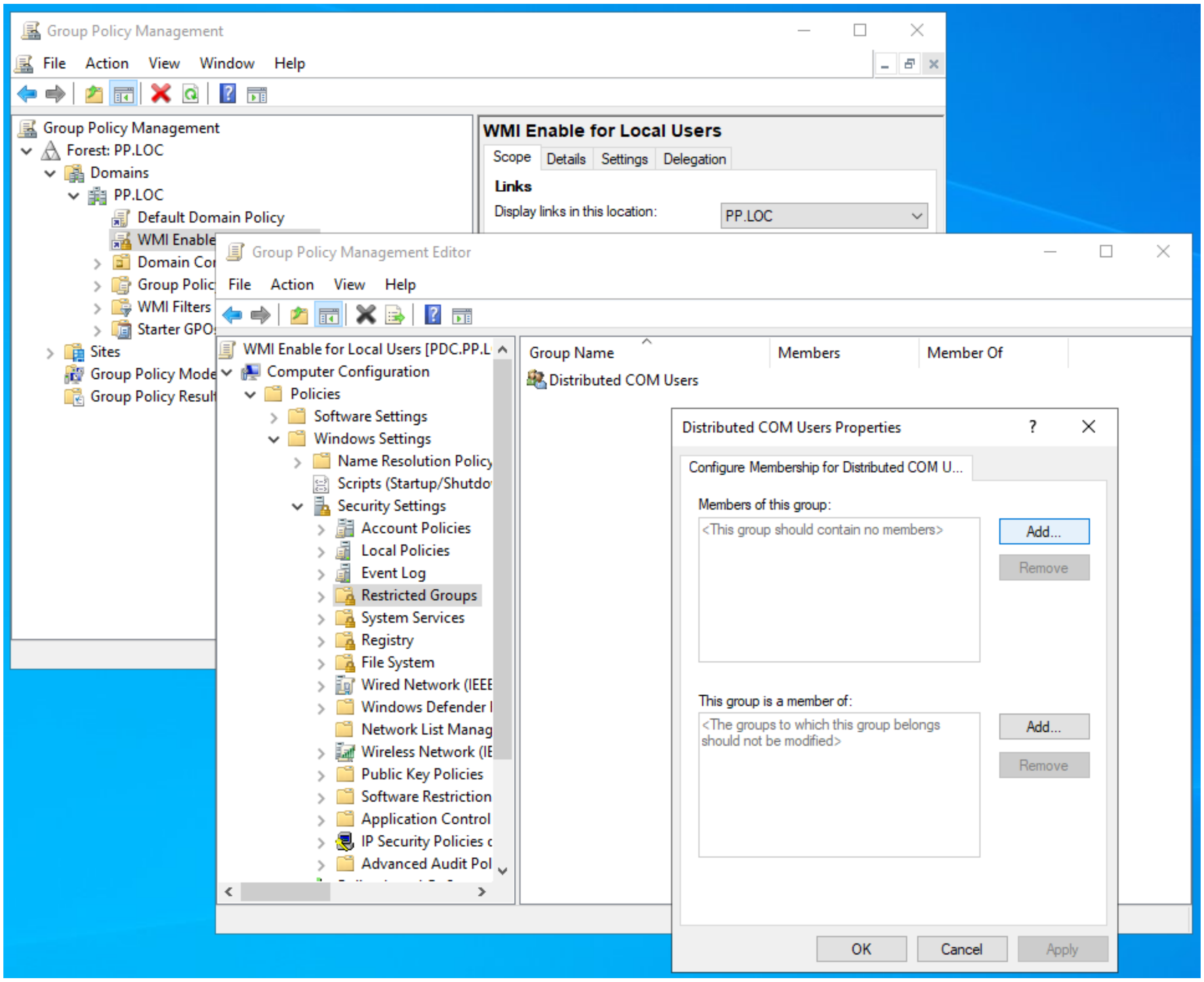
Adds a new group to this template

Step 16: Give the group name as ‘Distributed COM Users’.


Add Group

Group: Distributed COM Users

Step 17: Distributed COM Users Properties dialog will appear. Click ‘Add’ button under ‘Members of this group’

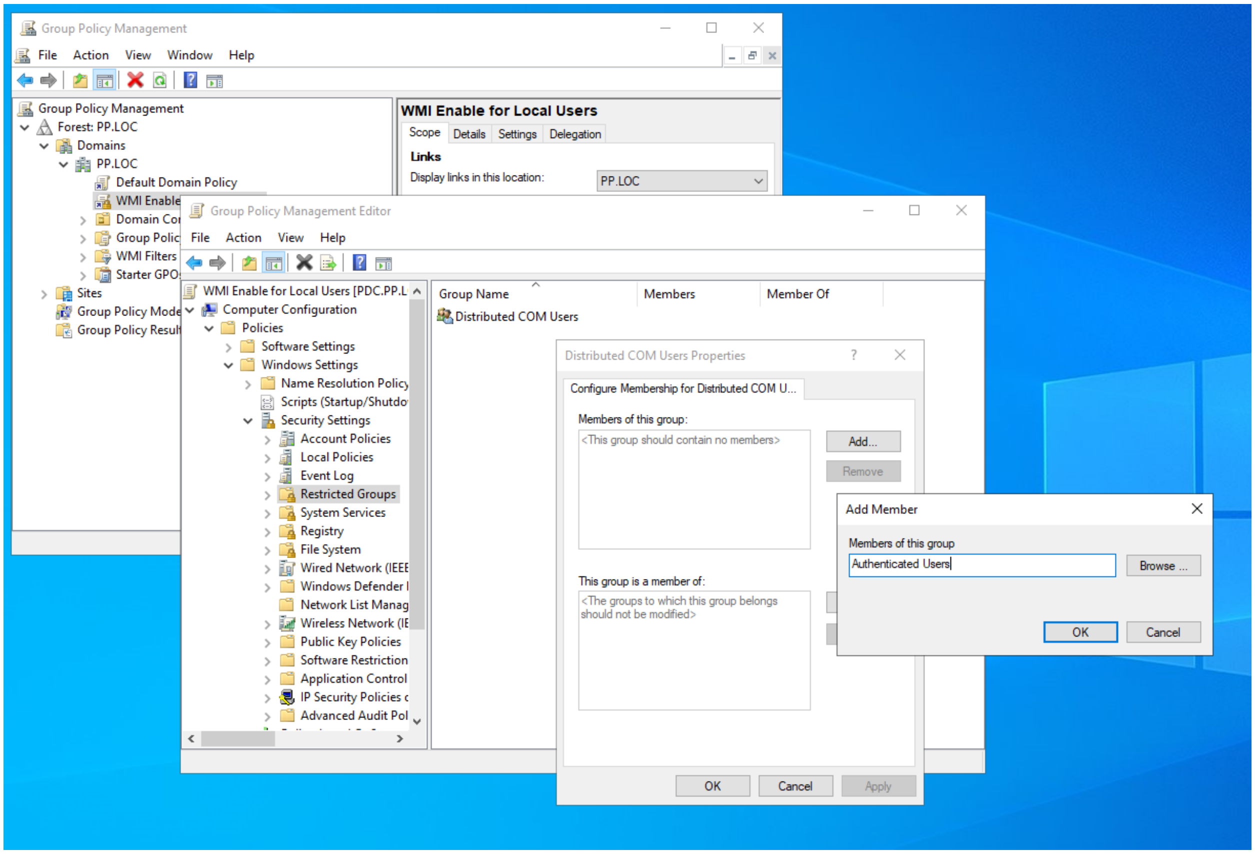


Display links in this location: PP.LOC

Members of this group:
<This group should contain no members>

This group is a member of:
<The groups to which this group belongs should not be modified>

Step 18: Give ‘Authenticated Users’ in the ‘Add Member’ dialog and save it.



Display links in this location: PP.LOC

Members of this group:

<This group should contain no members>

This group is a member of:

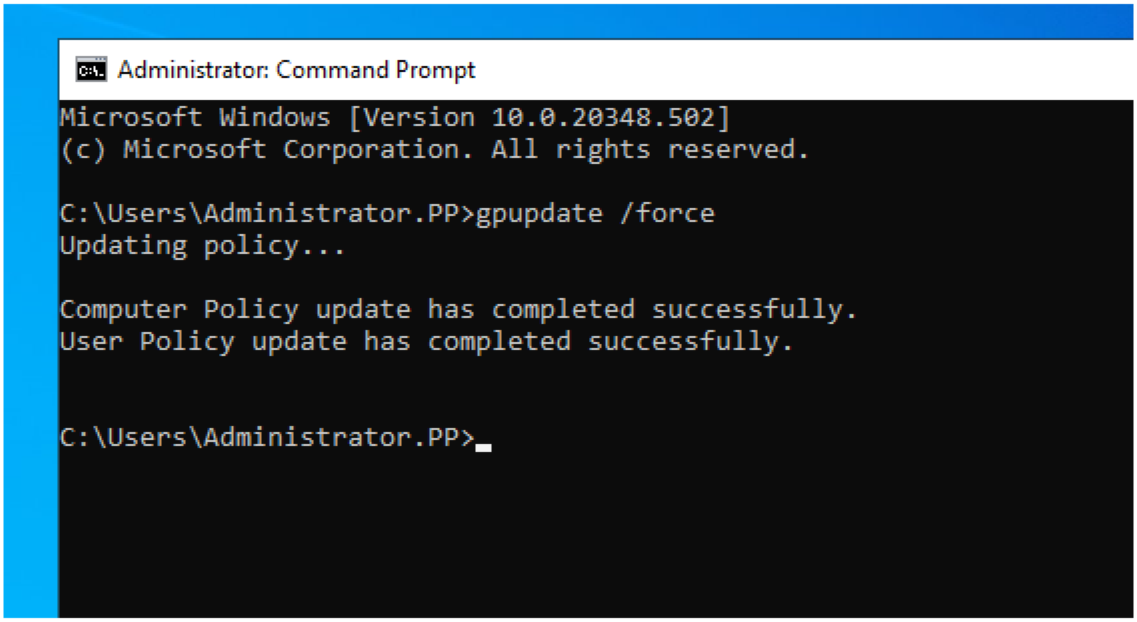
<The groups to which this group belongs should not be modified>

Add Member

Members of this group

Authenticated Users

Step 19: Changes related to GPO have been done. Steps 19 & 20 are optional, it explains that we can now check whether its' been propagated to the end machine. Open cmd as Administrator on the end machine and execute the command 'gpupdate /force'.



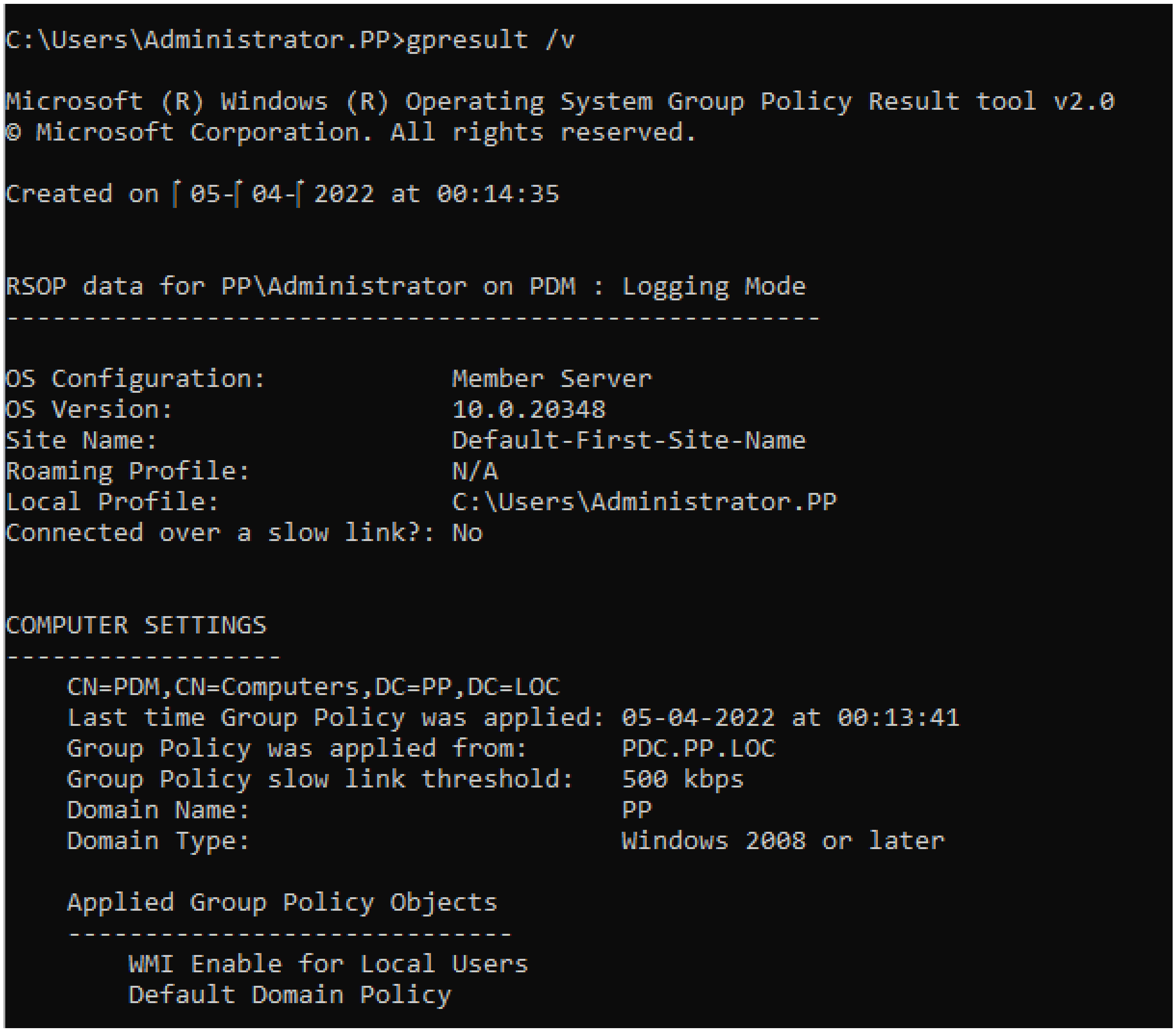
```
Microsoft Windows [Version 10.0.20348.502]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator.PP>gpupdate /force
Updating policy...

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


C:\Users\Administrator.PP>_
```

Step 20: Execute ‘gpresult /v’ to ensure GPO has been applied on the end machine.



```
C:\Users\Administrator.PP>gpresult /v

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.

Created on ⌈05-⌈04-⌈2022 at 00:14:35


RSOP data for PP\Administrator on PDM : Logging Mode
-----------------------------------------------------

OS Configuration:            Member Server
OS Version:                  10.0.20348
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\Administrator.PP
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
    CN=PDM,CN=Computers,DC=PP,DC=LOC
    Last time Group Policy was applied: 05-04-2022 at 00:13:41
    Group Policy was applied from:      PDC.PP.LOC
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        PP
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        WMI Enable for Local Users
        Default Domain Policy
```

Step 21: Once the GPO changes are pushed to the end machines, the ‘Authenticated Users’ addition to ‘Distributed COM Users’ will be applied but the Powershell script will be executed on the next startup of the end machines.

—---