Implementing Privileged Access Workstation – part 1

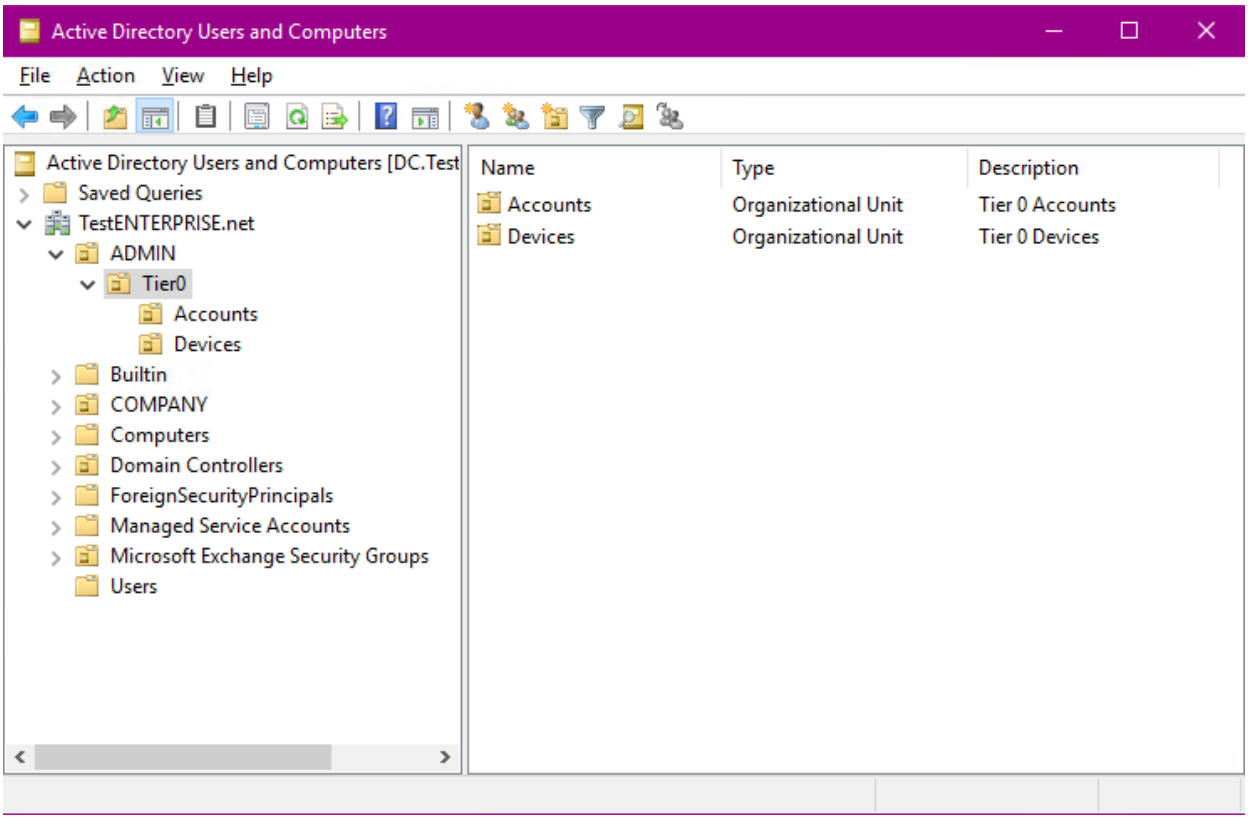

michaelfirsov.wordpress.com/implementing-privileged-access-workstation-part-1

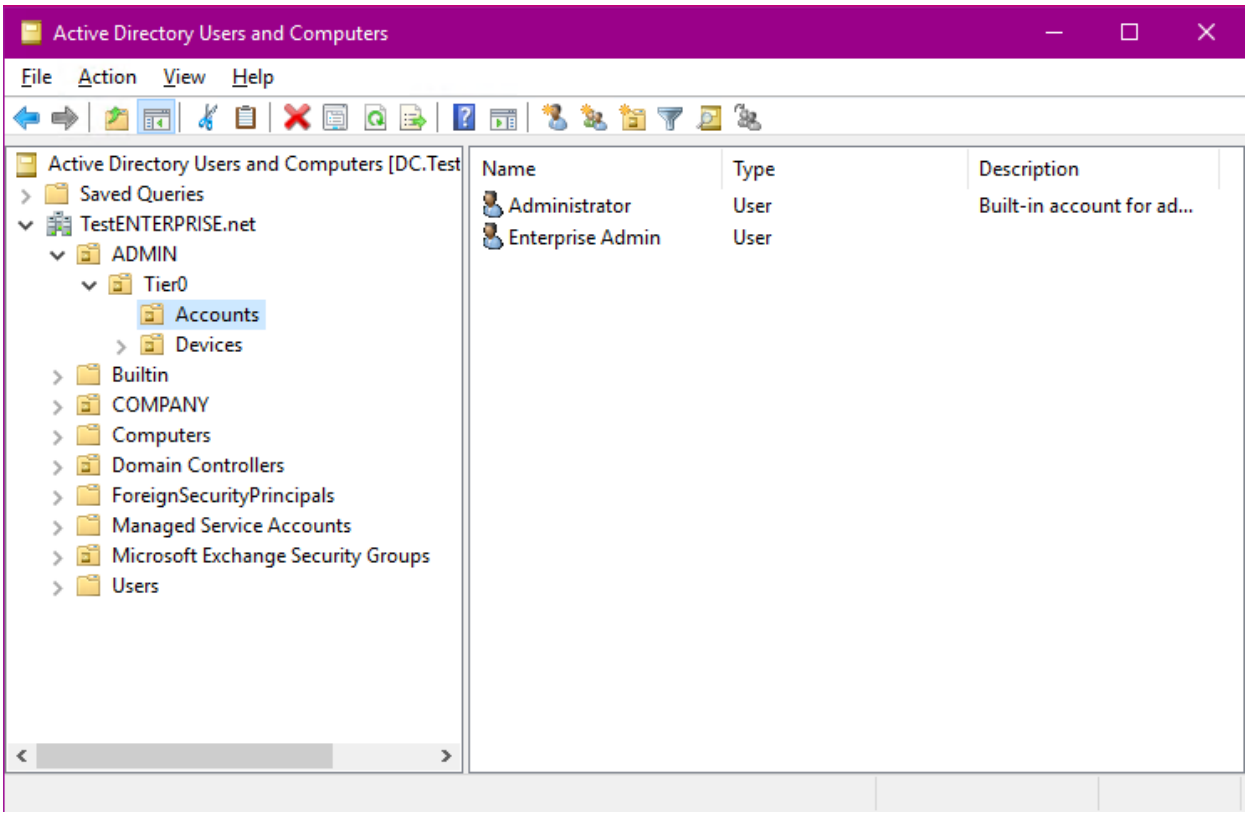
October 25, 2018

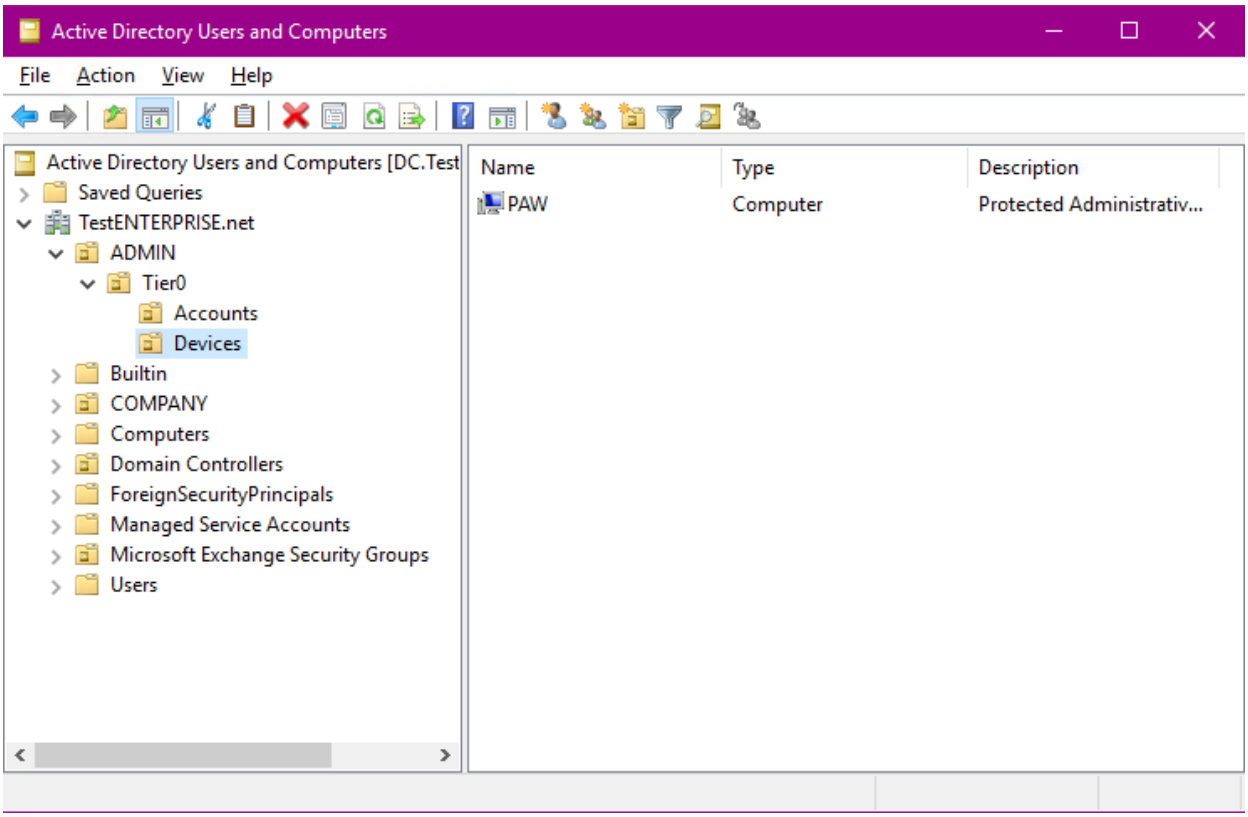
In this blog post I'd like to share the results of my Privileged Access Workstation (PAW) implementation – this implementation will be based on this MS document. Although I didn't follow MS guide in its enterity (because my network cannot be divided to so many tiers as MS prescribes), the main steps of the paw configuration will be illustrated along with the results to which these steps lead.

Phase 1

The first step in the PAW configuration is creating the corresponding AD infrastructure: I'm not planning to use MS's scripts which create all required OUs and groups and will create only those ones which I think will be sufficient for the PAW deployment. The upper-level OU to host the paw devices and users is ADMIN:

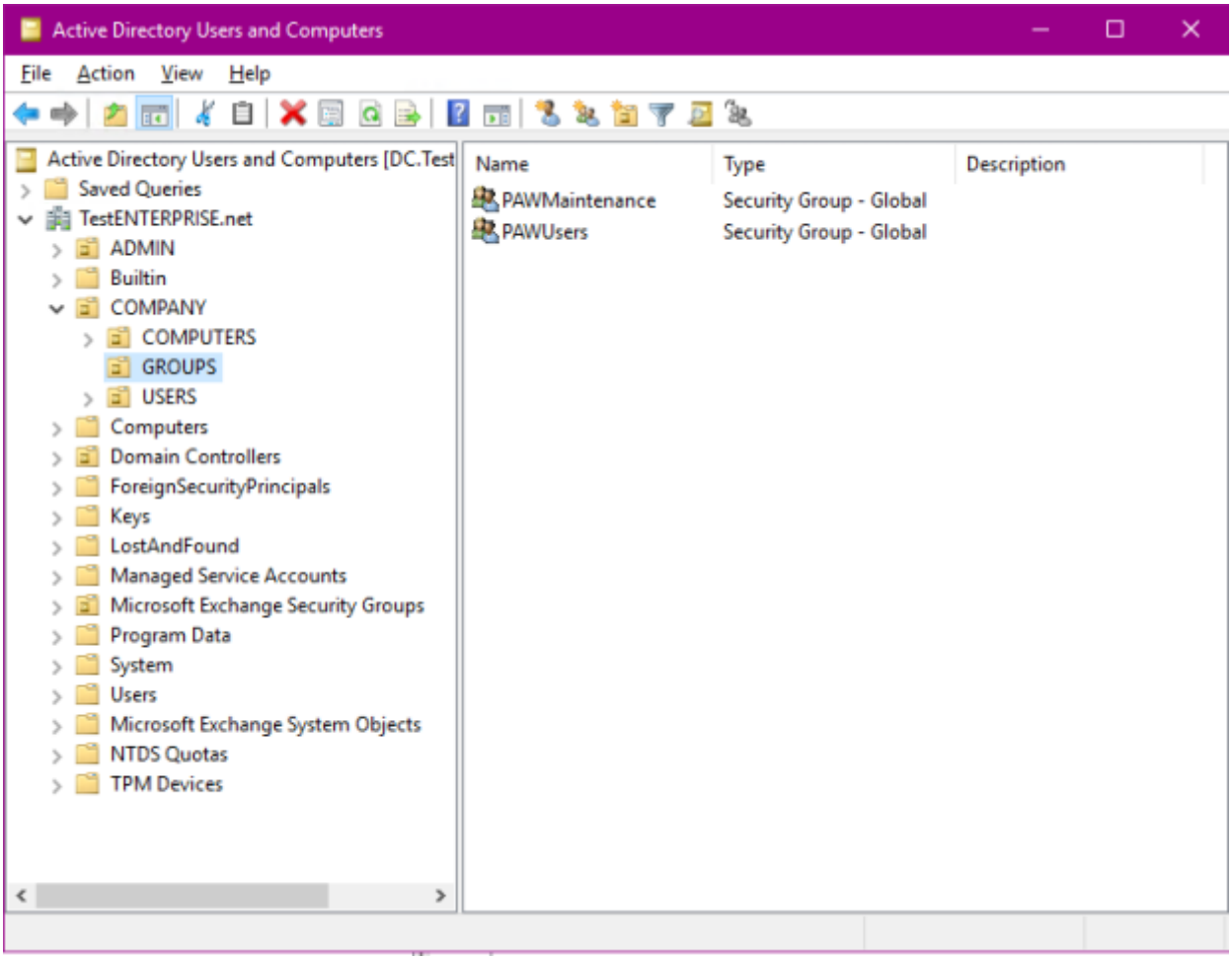


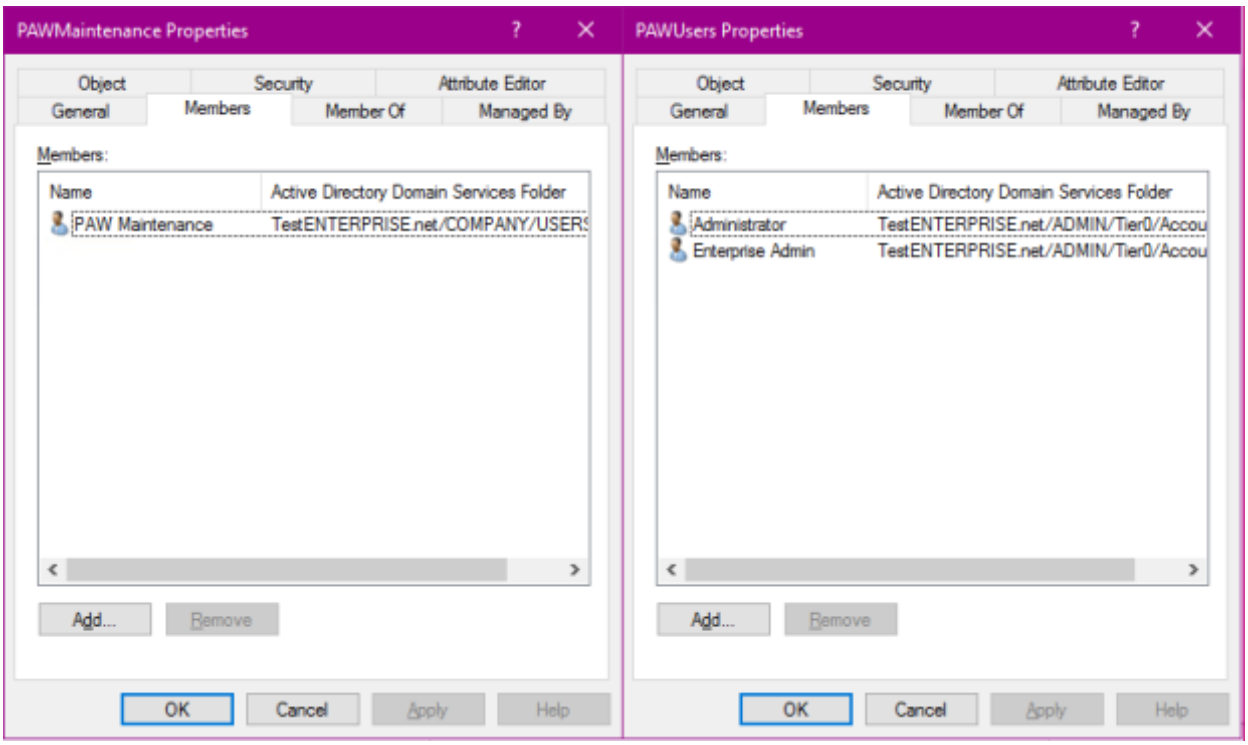




As you see the Tier0 accounts which will be allowed to log onto the PAW (which is placed into Devices OU) are Enterprise Admin (*EntAdmin*) and built-in *Administrator*.

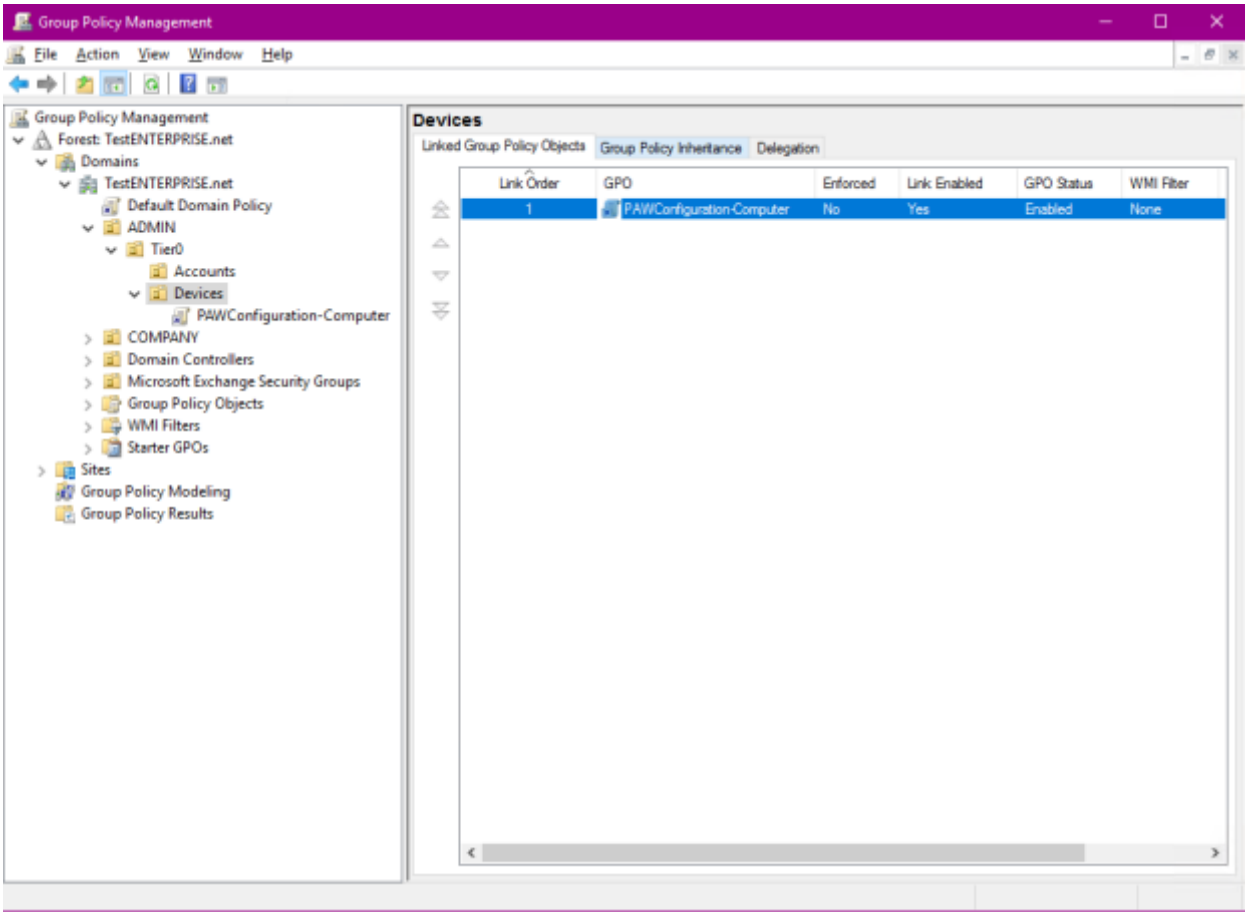
Two groups must be created to separate access to PAW: PAWMaintenance group (with the single member PAW Maintenance – *pawm* which was created beforehand) will be used only for the paw maintenance while the other – PAWUsers will contain the Tier0 user accounts –*Administrator* and Enterprise Admin(*EntAdmin*).





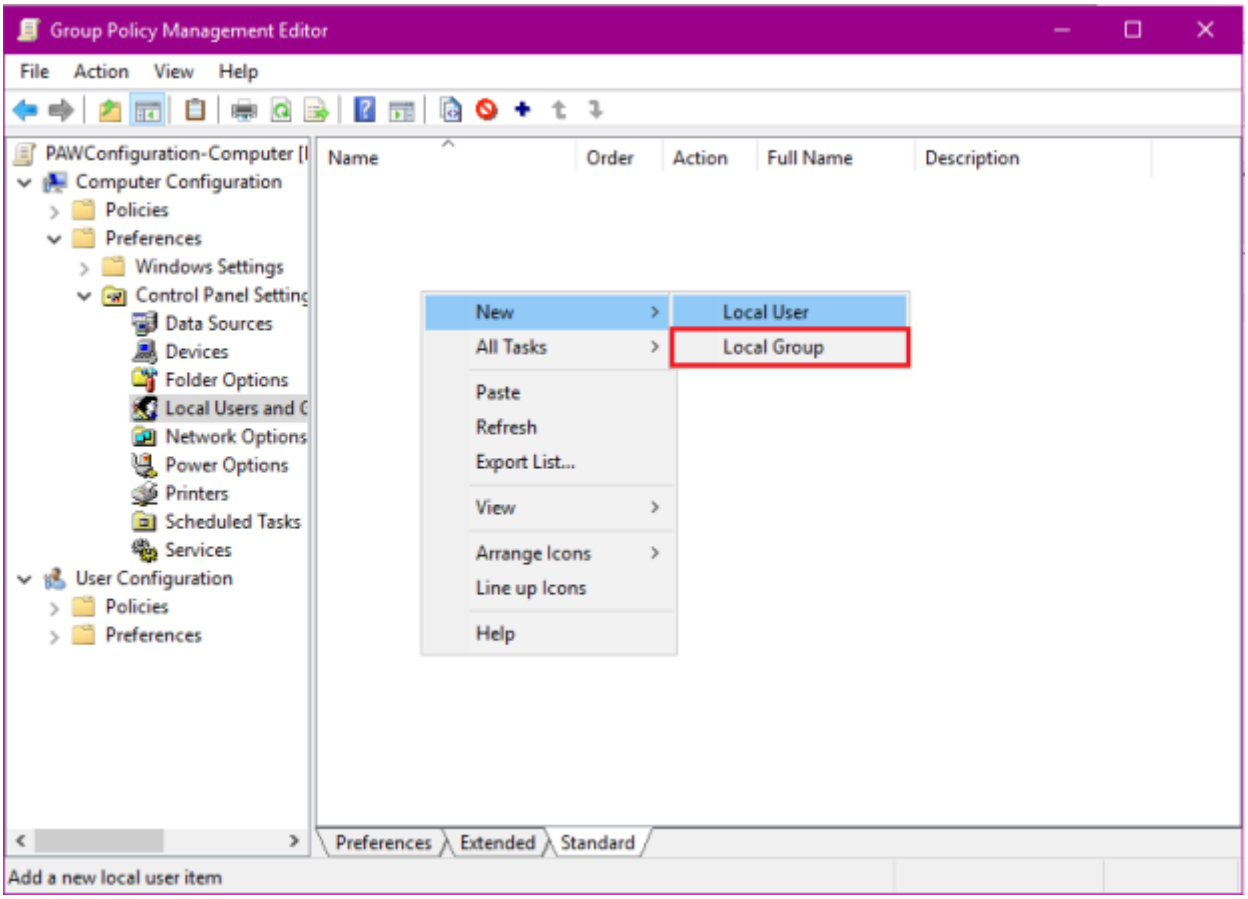
Next a couple of GPOs must be created and linked to the Admin\Tier0\Accounts and Admin\Tier0\Devices OUs.

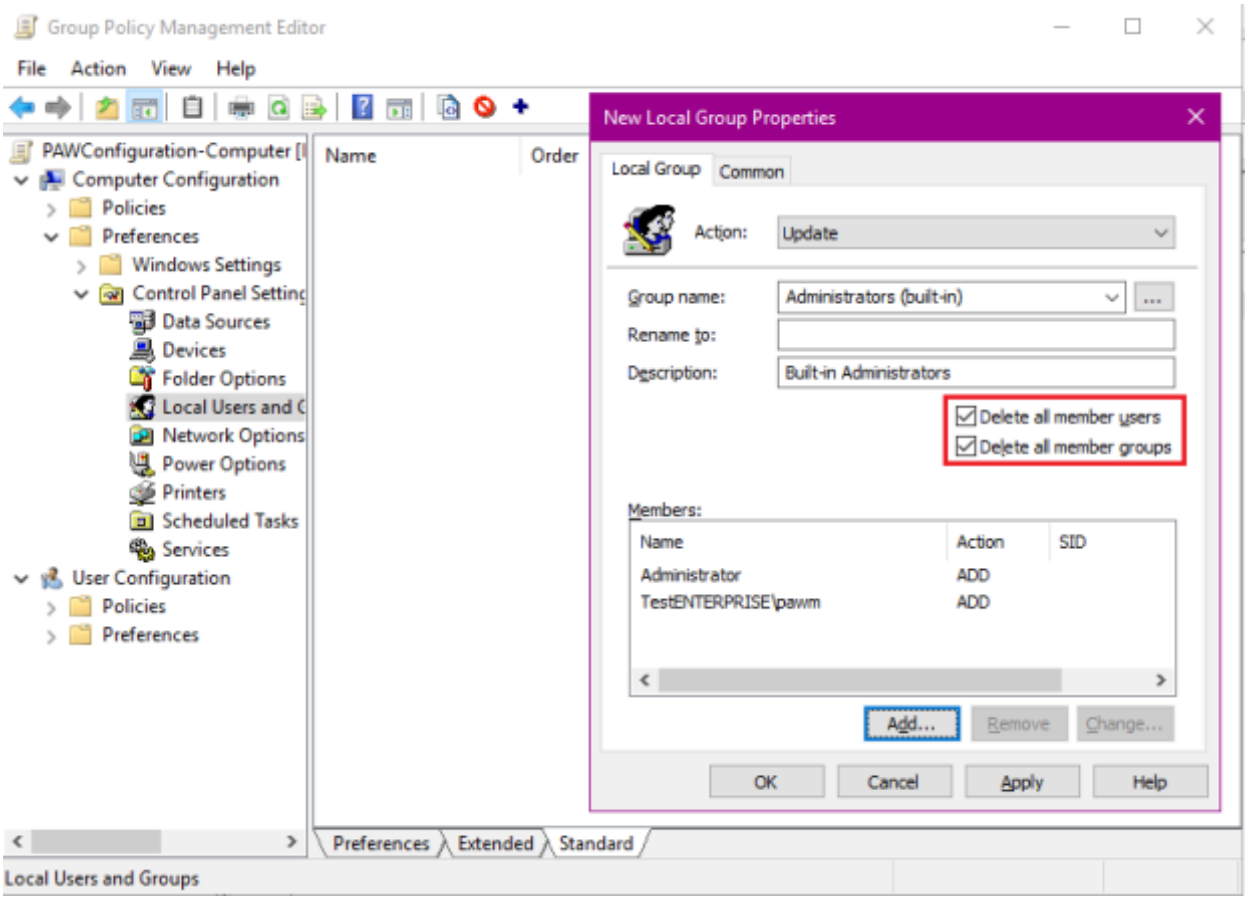
1) **PAWConfiguration-Computer** gpo will configure the paw device and thus must be linked to the Devices OU:

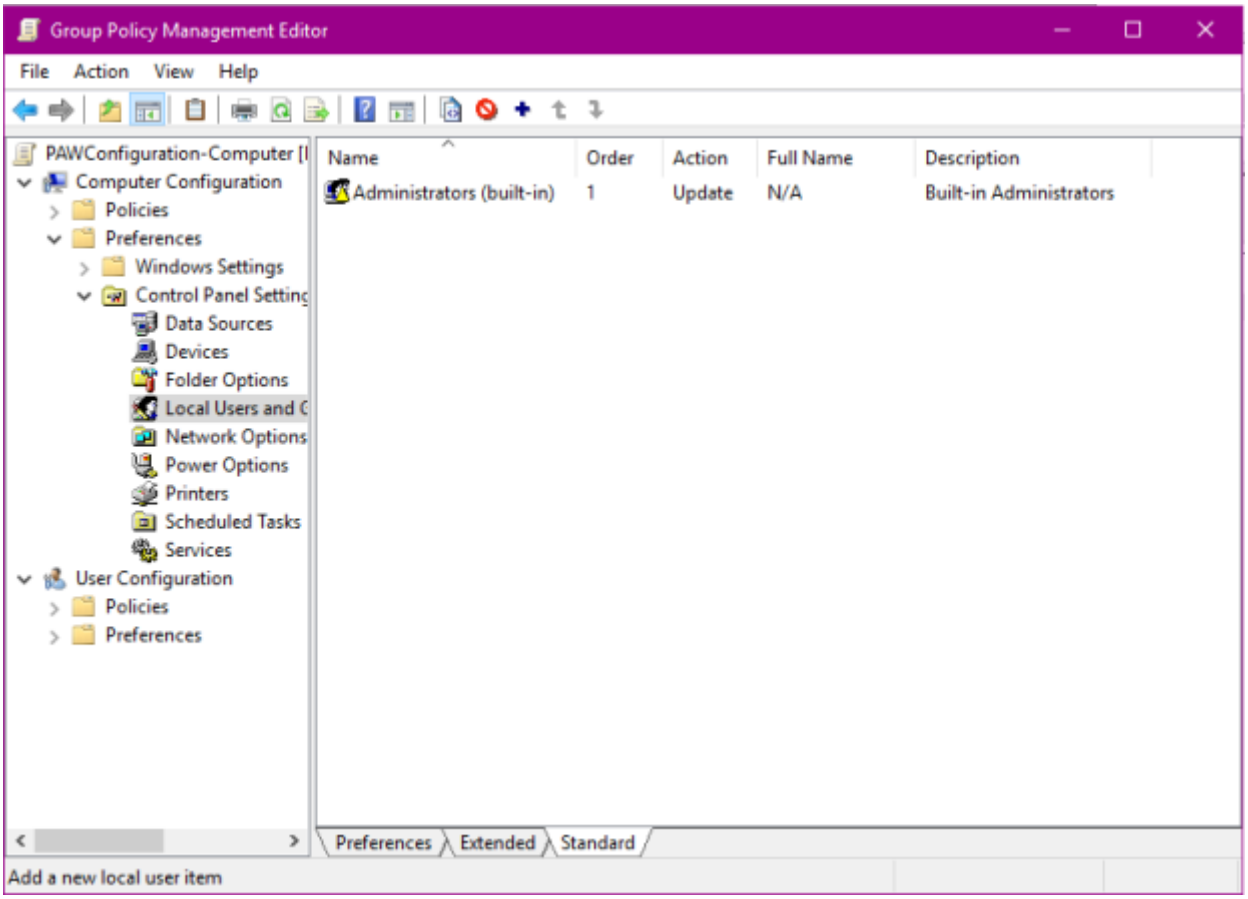


The primary goal of the **PAWConfiguration-Computer** gpo is to protect a paw device by different ways.

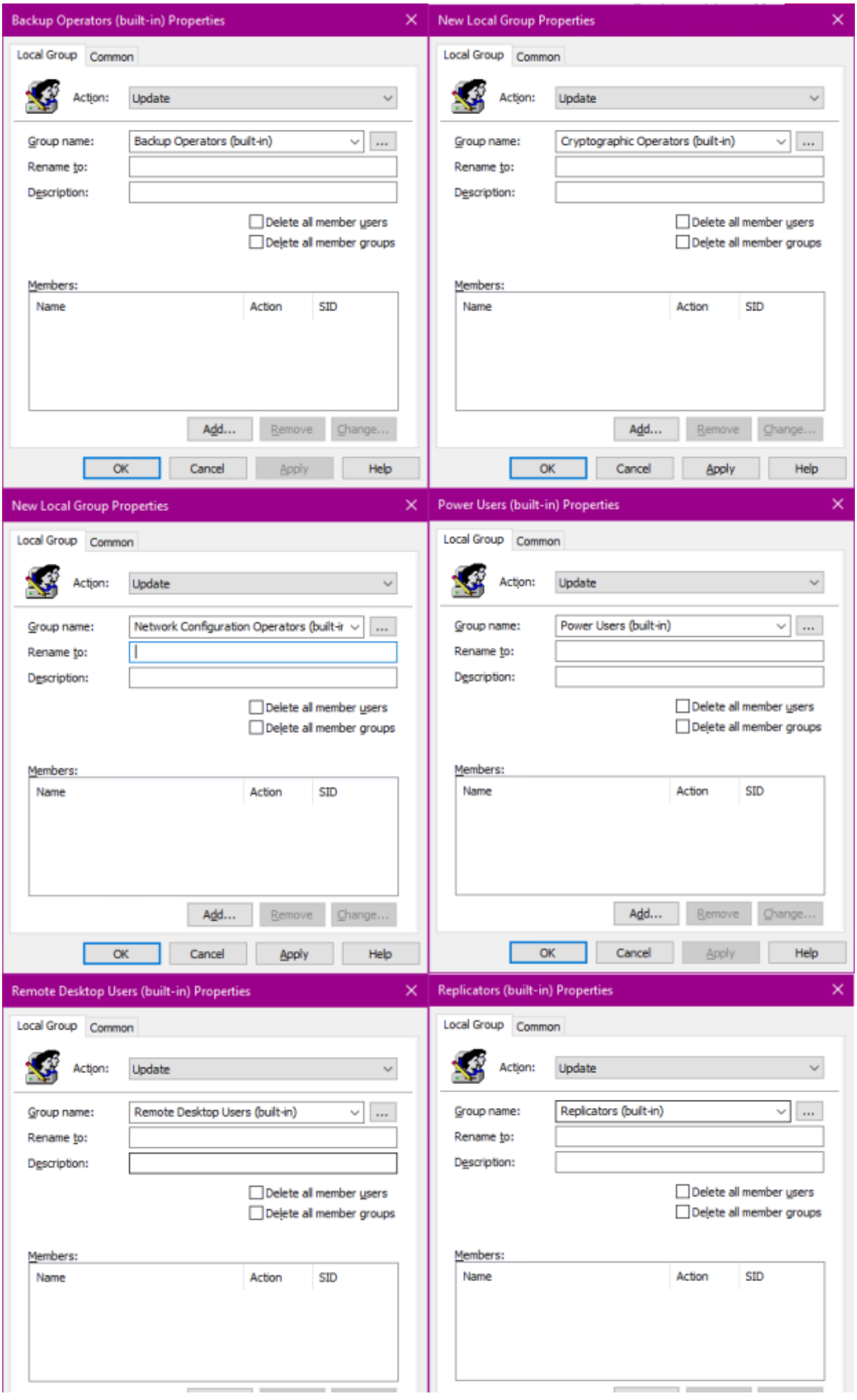
a) Local Administrators group membership should be as follows:

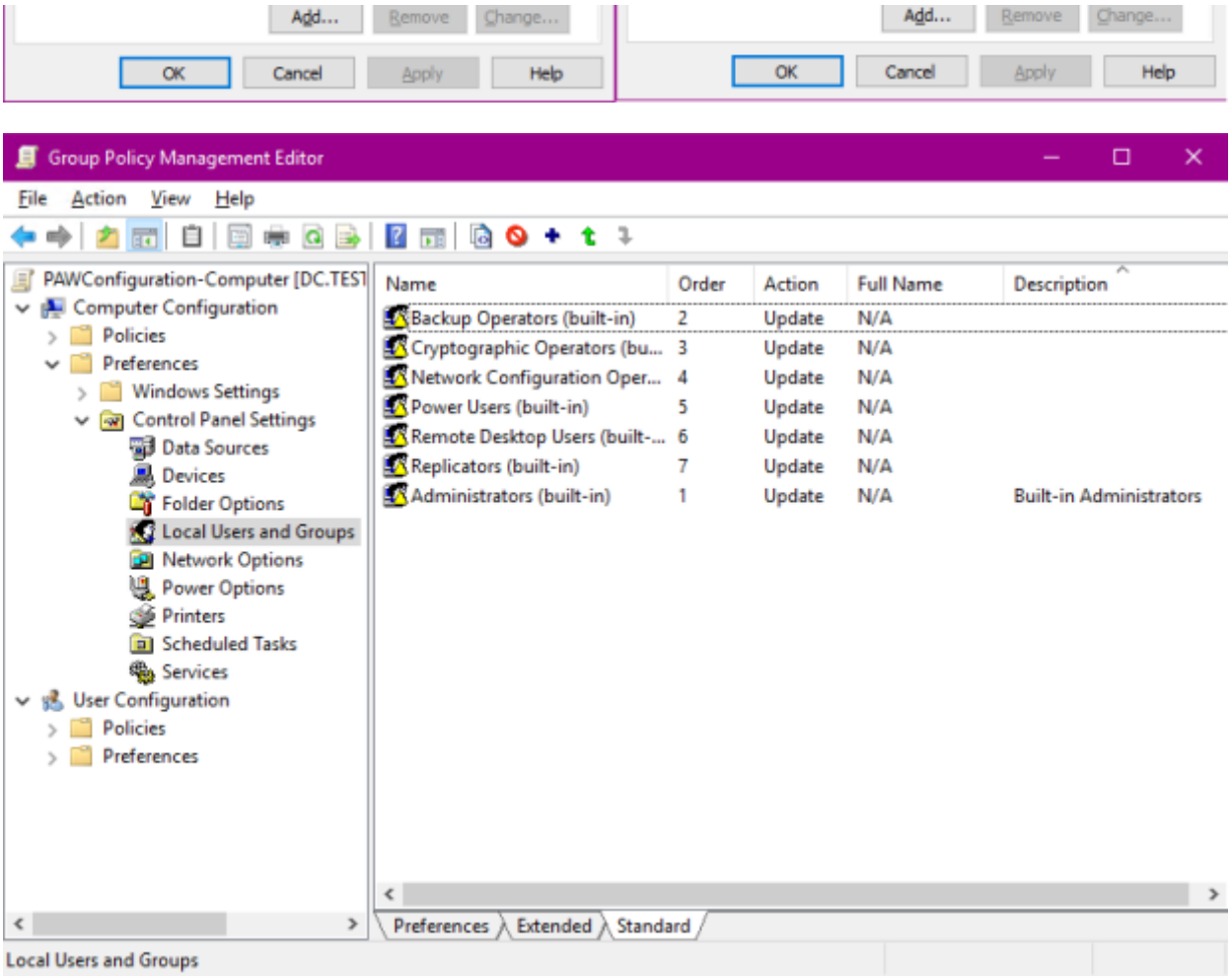

Group Policy Management Editor
File Action View Help
PAWConfiguration-Computer [I
Computer Configuration
Policies
Preferences
Windows Settings
Control Panel Setting
Data Sources
Devices
Folder Options
Local Users and G
Network Options
Power Options
Printers
Scheduled Tasks
Services
User Configuration
Policies
Preferences
Name
Order
Action
Full Name
Description
New
All Tasks
Paste
Refresh
Export List...
View
Arrange Icons
Line up Icons
Help
Local User
Local Group
Preferences
Extended
Standard
Add a new local user item


Group Policy Management Editor
File Action View Help
PAWConfiguration-Computer [I
Computer Configuration
Policies
Preferences
Windows Settings
Control Panel Setting
Data Sources
Devices
Folder Options
Local Users and G
Network Options
Power Options
Printers
Scheduled Tasks
Services
User Configuration
Policies
Preferences
Name
Order
New Local Group Properties
Local Group
Common
Action:
Update
Group name:
Administrators (built-in)
Rename to:
Description:
Built-in Administrators
Delete all member users
Delete all member groups
Members:
Name
Action
SID
Administrator
ADD
TestENTERPRISE\pawm
ADD
Add...
Remove
Change...
OK
Cancel
Apply
Help
Preferences
Extended
Standard
Local Users and Groups

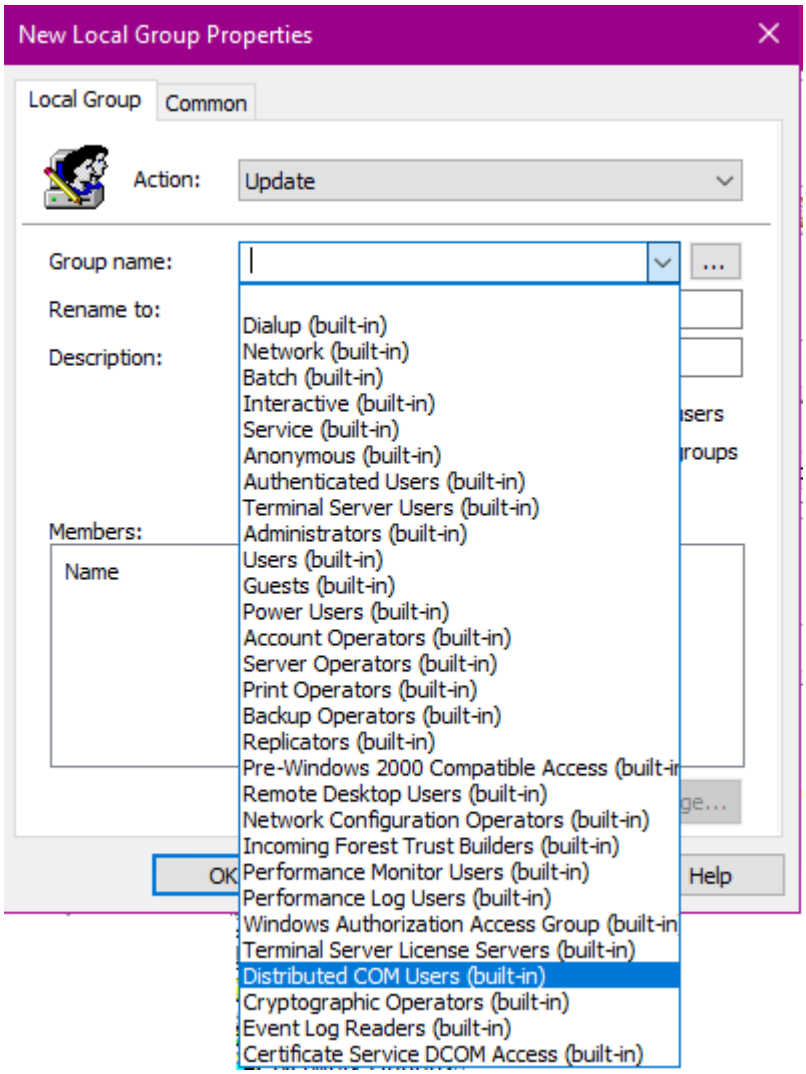


– on paw devices only built-in local *Administrator* account and the domain PAW Maintenance user account (*pawm* in this case) should be the members of the local Administrators group – all other members must be deleted.
All other privileged groups must always be empty:

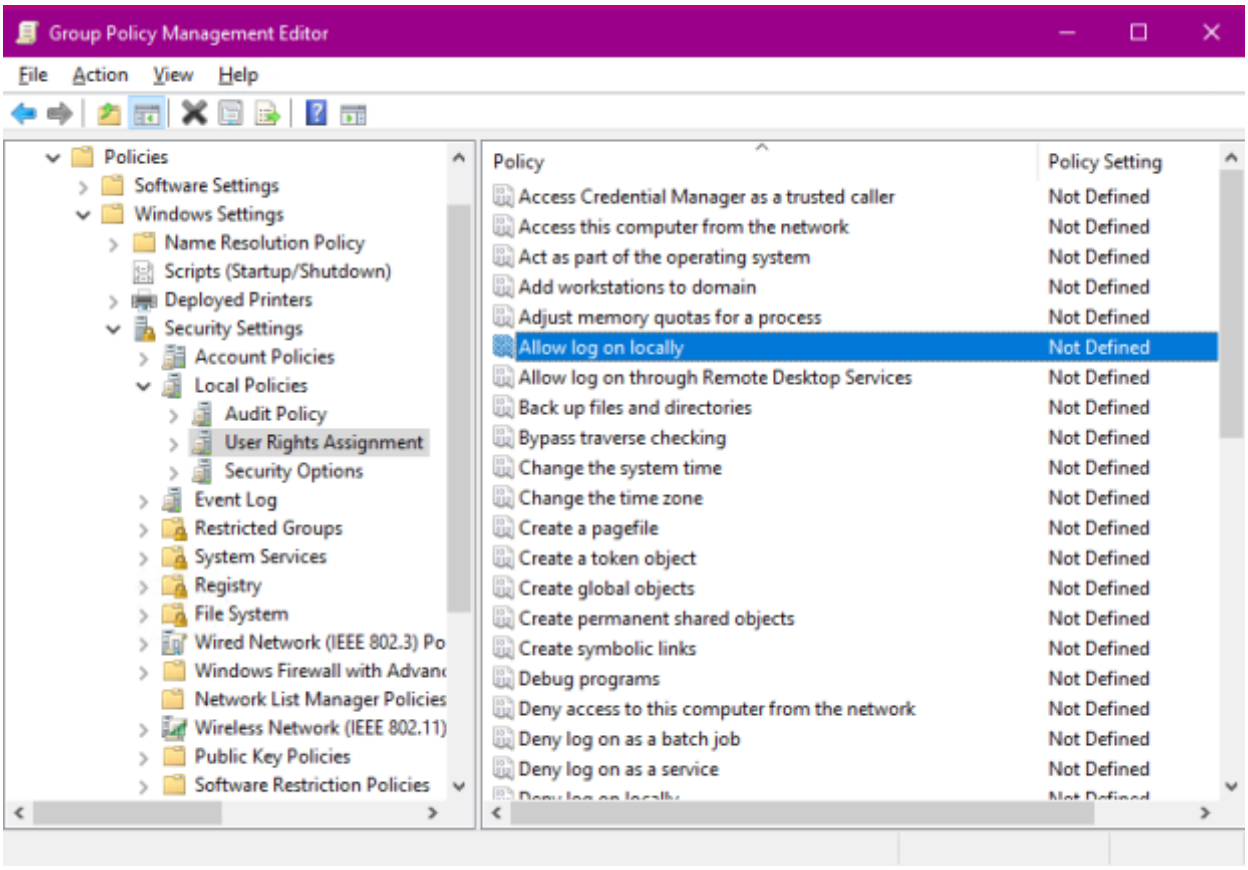

Backup Operators (built-in) Properties
Local Group
Common
Action:
Update
Group name:
Backup Operators (built-in)
Rename to:
Description:
Delete all member users
Delete all member groups
Members:
Name
Action
SID
Add...
Remove
Change...
OK
Cancel
Apply
Help
New Local Group Properties
Local Group
Common
Action:
Update
Group name:
Cryptographic Operators (built-in)
Rename to:
Description:
Delete all member users
Delete all member groups
Members:
Name
Action
SID
Add...
Remove
Change...
OK
Cancel
Apply
Help
New Local Group Properties
Local Group
Common
Action:
Update
Group name:
Network Configuration Operators (built-ir
Rename to:
Description:
Delete all member users
Delete all member groups
Members:
Name
Action
SID
Add...
Remove
Change...
OK
Cancel
Apply
Help
Power Users (built-in) Properties
Local Group
Common
Action:
Update
Group name:
Power Users (built-in)
Rename to:
Description:
Delete all member users
Delete all member groups
Members:
Name
Action
SID
Add...
Remove
Change...
OK
Cancel
Apply
Help
Remote Desktop Users (built-in) Properties
Local Group
Common
Action:
Update
Group name:
Remote Desktop Users (built-in)
Rename to:
Description:
Delete all member users
Delete all member groups
Members:
Name
Action
SID
Replicators (built-in) Properties
Local Group
Common
Action:
Update
Group name:
Replicators (built-in)
Rename to:
Description:
Delete all member users
Delete all member groups
Members:
Name
Action
SID

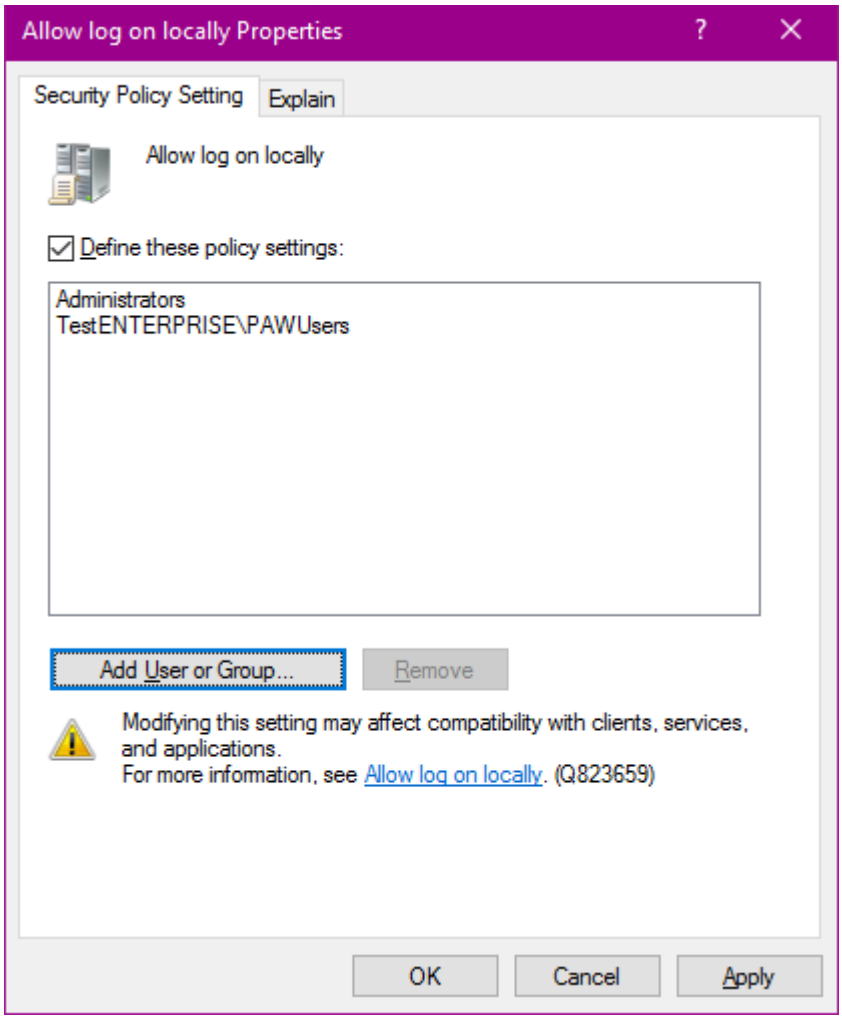


Here's where the first discrepancy between MS's documentation and the practice can be seen: MS says the Hyper-V Administrators group should be among the groups with empty membership but this group can't be added here – it just does not exist in the drop-down group list:



b) the next gpo setting will define which accounts are permitted to log on to the PAW:


Group Policy Management Editor
File Action View Help
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Po
Windows Firewall with Advanc
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Policy
Policy Setting
Access Credential Manager as a trusted caller Not Defined
Access this computer from the network Not Defined
Act as part of the operating system Not Defined
Add workstations to domain Not Defined
Adjust memory quotas for a process Not Defined
Allow log on locally Not Defined
Allow log on through Remote Desktop Services Not Defined
Back up files and directories Not Defined
Bypass traverse checking Not Defined
Change the system time Not Defined
Change the time zone Not Defined
Create a pagefile Not Defined
Create a token object Not Defined
Create global objects Not Defined
Create permanent shared objects Not Defined
Create symbolic links Not Defined
Debug programs Not Defined
Deny access to this computer from the network Not Defined
Deny log on as a batch job Not Defined
Deny log on as a service Not Defined


Allow log on locally Properties
Security Policy Setting
Explain
Allow log on locally
Define these policy settings:
Administrators
TestENTERPRISE\PAWUsers
Add User or Group...
Remove
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Allow log on locally. (Q823659)
OK
Cancel
Apply

Here I'd like to draw your attention once again to which account will have and which will have not the right to log on locally to the paw.

These users/groups will have the right to log on:

i) TestENTERPRISE\PAWUsers – *TestENTERPRISE\Administrator* and *TestENTERPRISE\EntAdmin*

ii) Members of the LOCAL Administrators group on the PAW device

– as you remember the membership of the local Administrators group on paw devices is configured by the respective gpo setting which states that only the *LOCAL Administrator* and the *TestENTERPRISE\pawm* user accounts can be the members of the local Administrators group so in this case it means the *local built-in Administrator* (*PAW\Administrator*) and *TestENTERPRISE\pawm* user account WILL have the right to log on to PAW locally and

these users/groups will NOT have the right to log on locally:

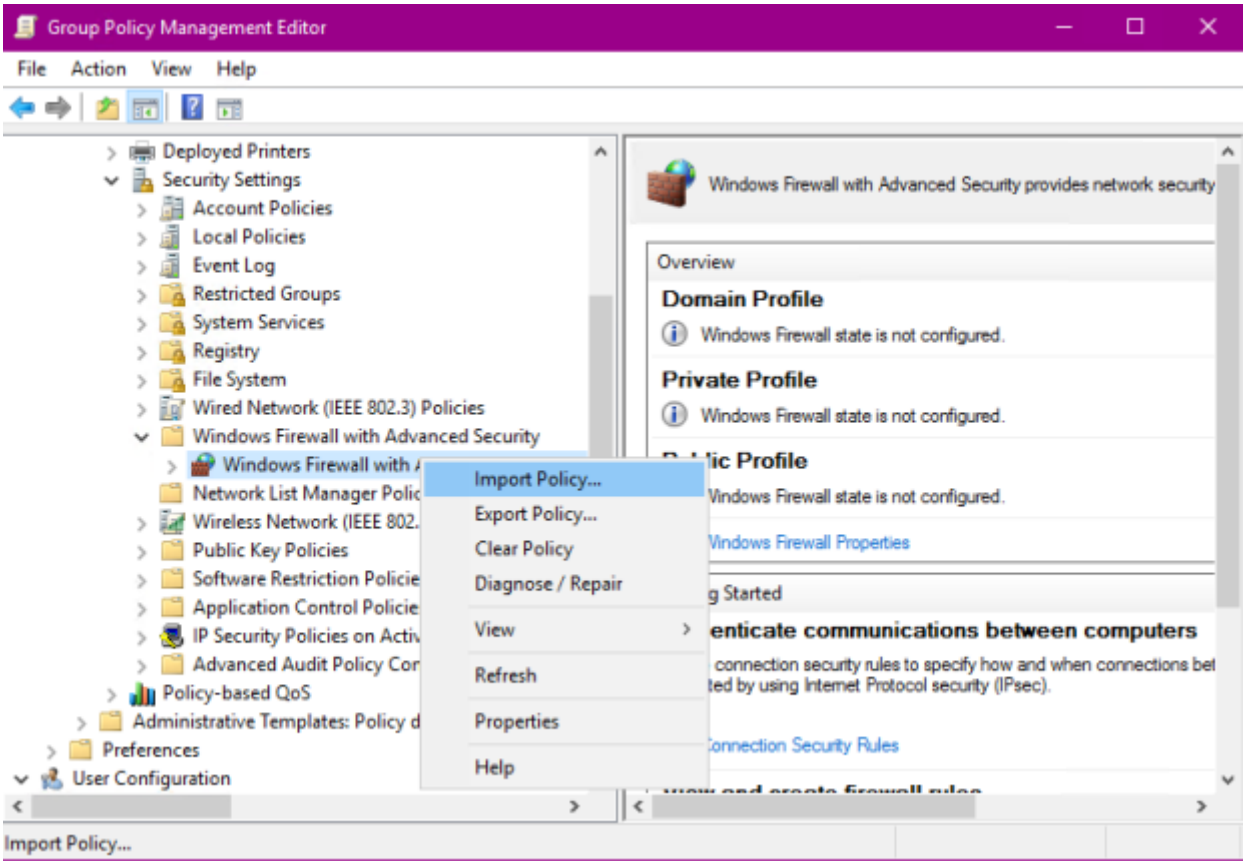
i) any other LOCAL user account which was added to the local Administrators group

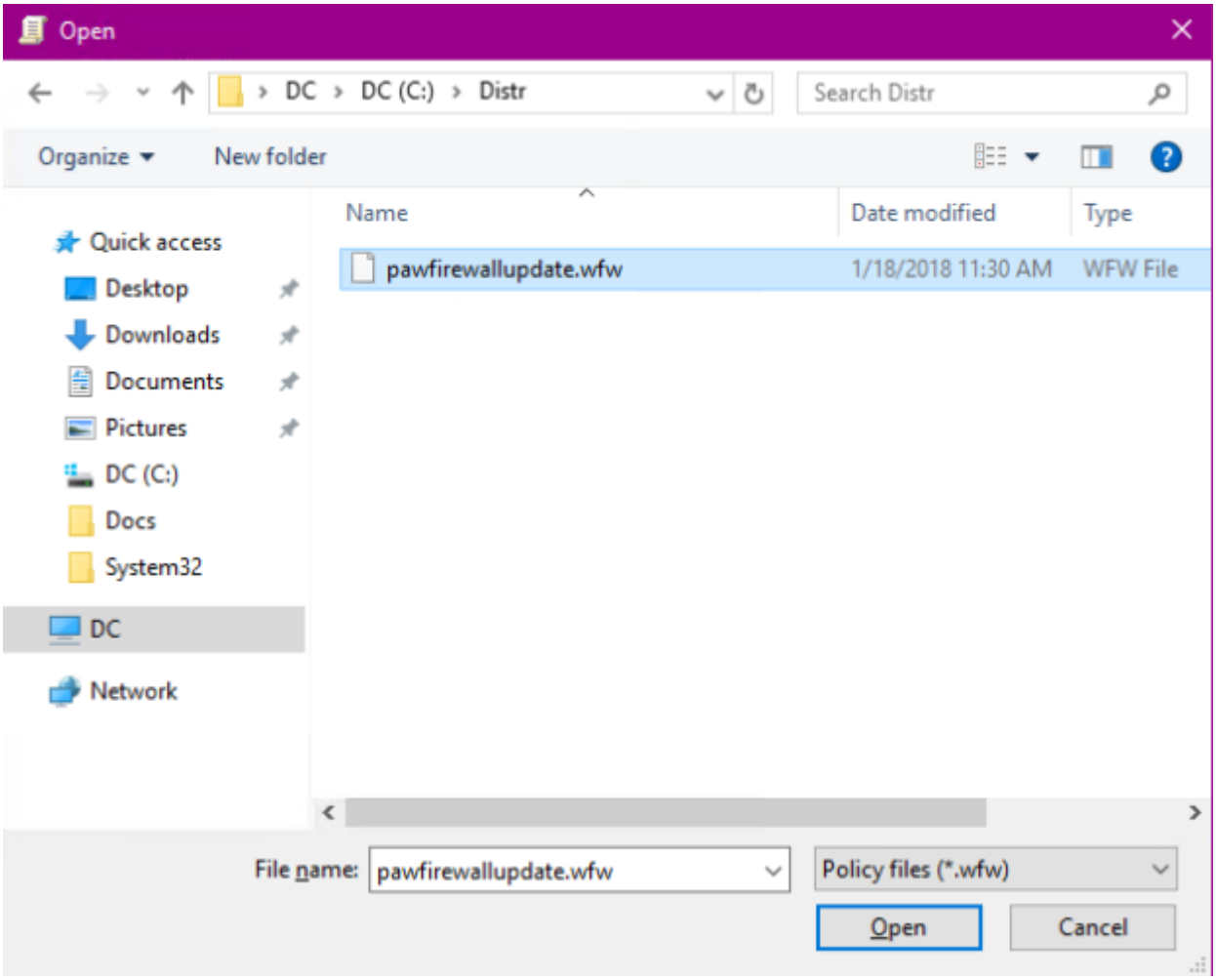
ii) any other domain user account(s)

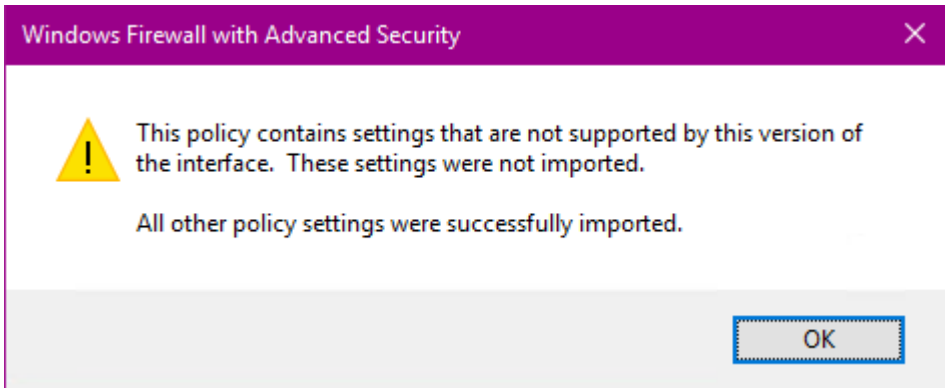
Once we have the paw configured, the *Allow to log on locally* user right will be the first setting to test.

One more thing to note here: Tier0 accounts (*TestENTERPRISE\Administrator* and *TestENTERPRISE\EntAdmin*) will NOT be the members of the local (PAW) Administrators group – this will be the second thing to check.

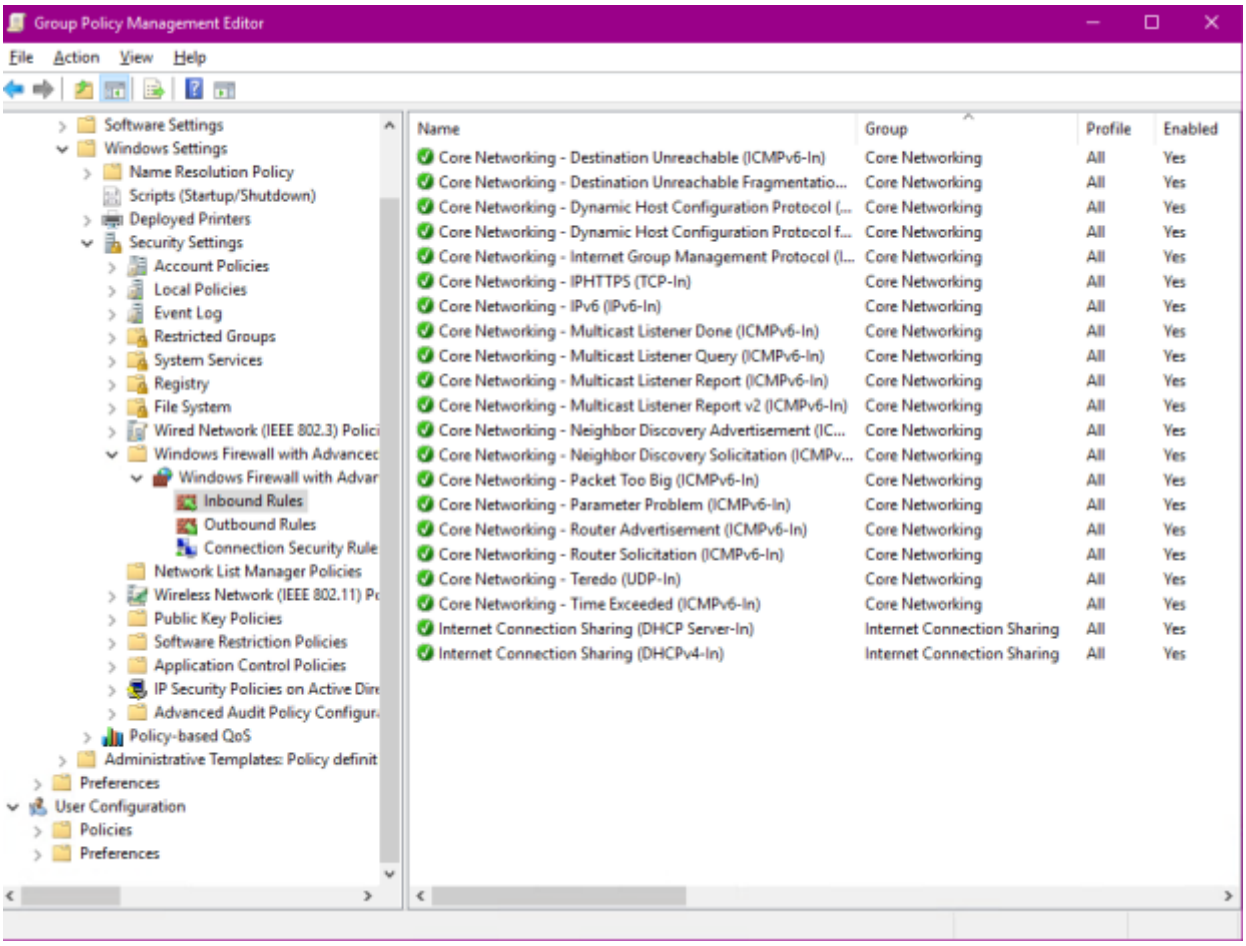
iii) MS offers to download the pawfirewallupdate.wfw file to configure the PAW's firewall in the most restrictive way:


Group Policy Management Editor
File Action View Help
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Polic
Wireless Network (IEEE 802.
Public Key Policies
Software Restriction Policie
Application Control Policie
IP Security Policies on Activ
Advanced Audit Policy Cor
Policy-based QoS
Administrative Templates: Policy d
Preferences
User Configuration
Import Policy...
Export Policy...
Clear Policy
Diagnose / Repair
View
Refresh
Properties
Help
Windows Firewall with Advanced Security provides network security
Overview
Domain Profile
Windows Firewall state is not configured.
Private Profile
Windows Firewall state is not configured.
Windows Firewall state is not configured.
Windows Firewall Properties
Started
enticate communications between computers
connection security rules to specify how and when connections bet
ted by using Internet Protocol security (IPsec).
Connection Security Rules
Import Policy...

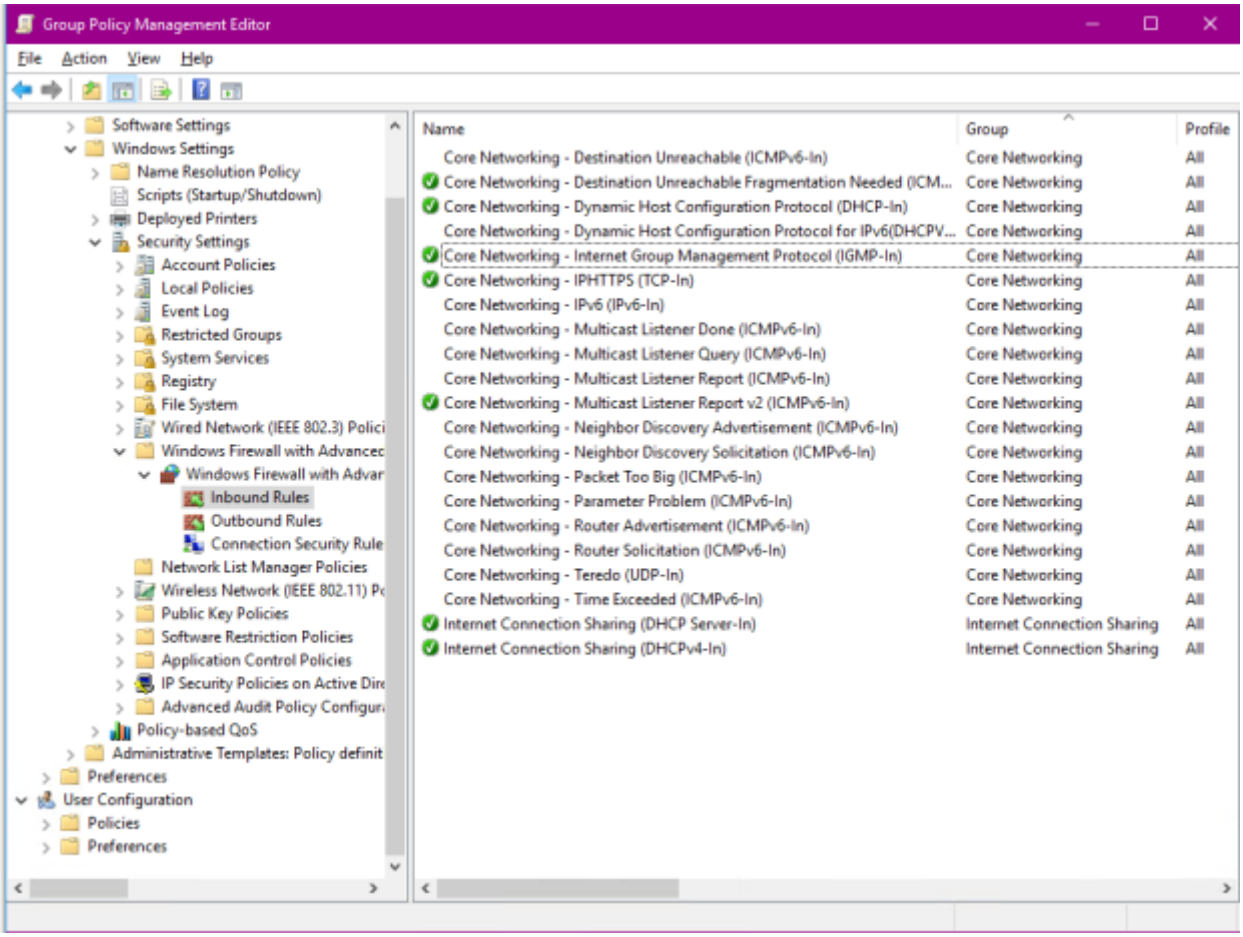

Open
DC › DC (C:) › Distr
Search Distr
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
DC (C:)
Docs
System32
DC
Network
Name
Date modified
Type
pawfirewallupdate.wfw
1/18/2018 11:30 AM
WFW File
File name:
pawfirewallupdate.wfw
Policy files (*.wfw)
Open
Cancel



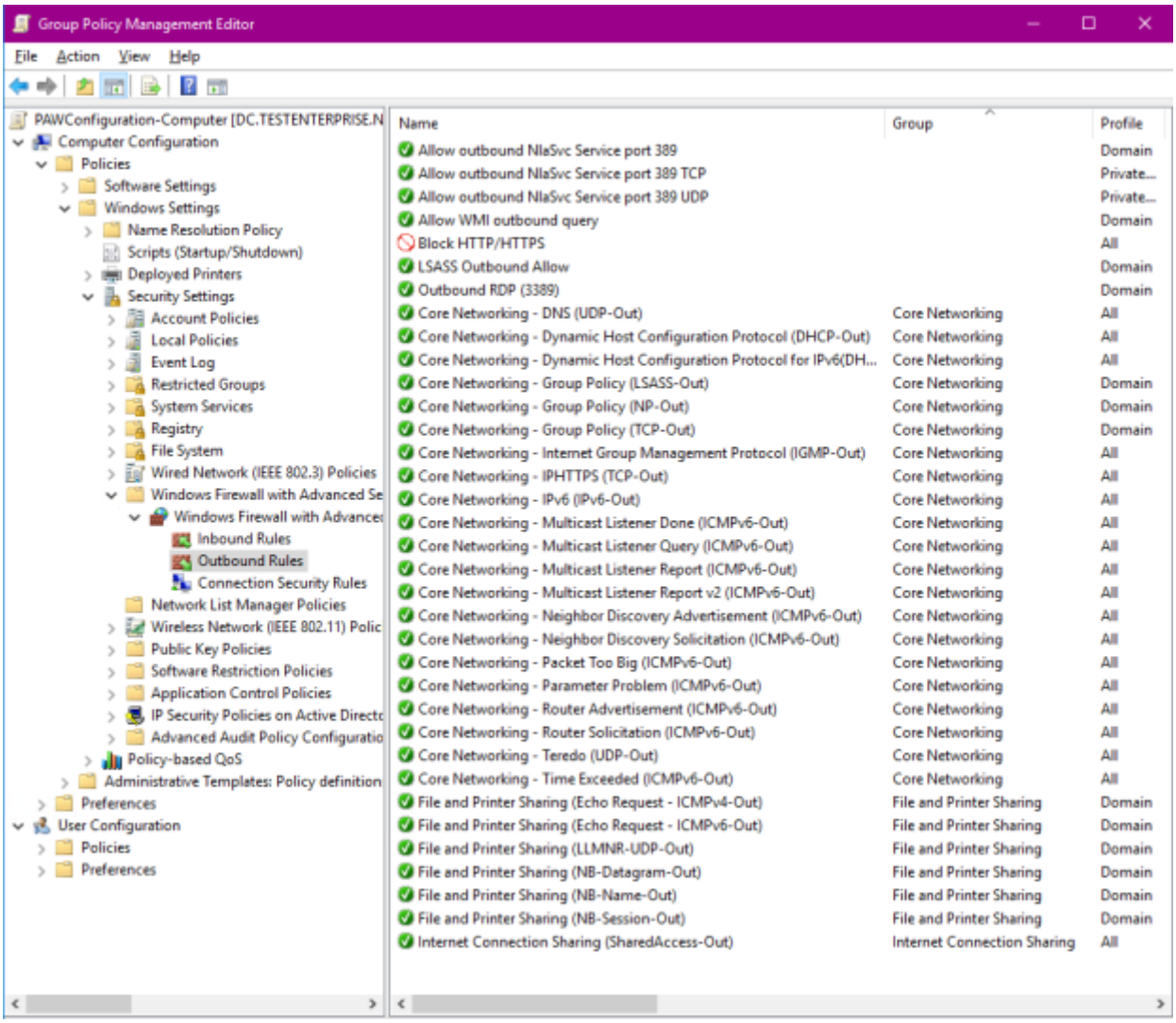
Here's the list of the inbound rules:



As I'm not going to use IPv6 I reduced the number of the enabled rules once again to rule out the IPv6-related rules:

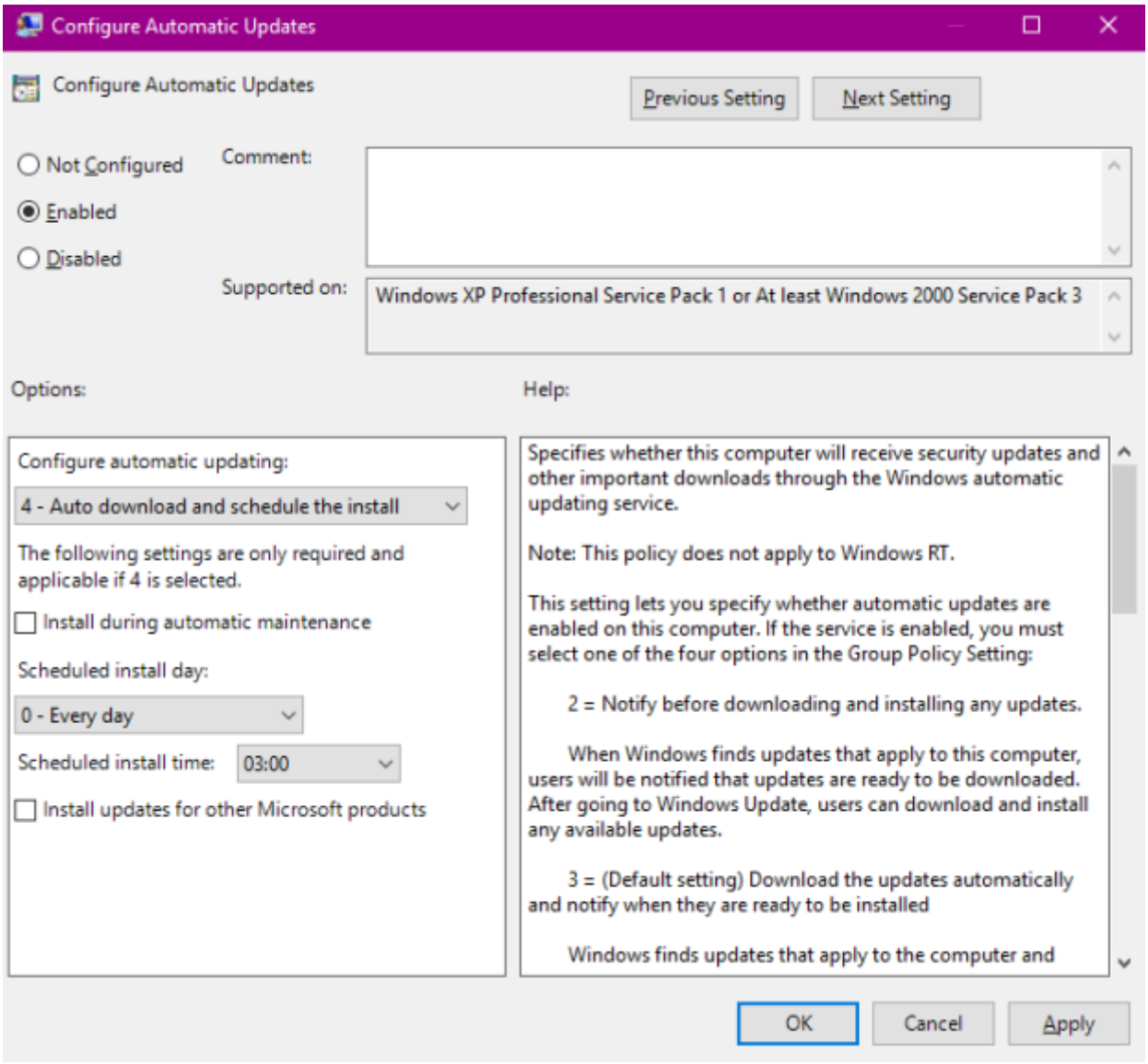


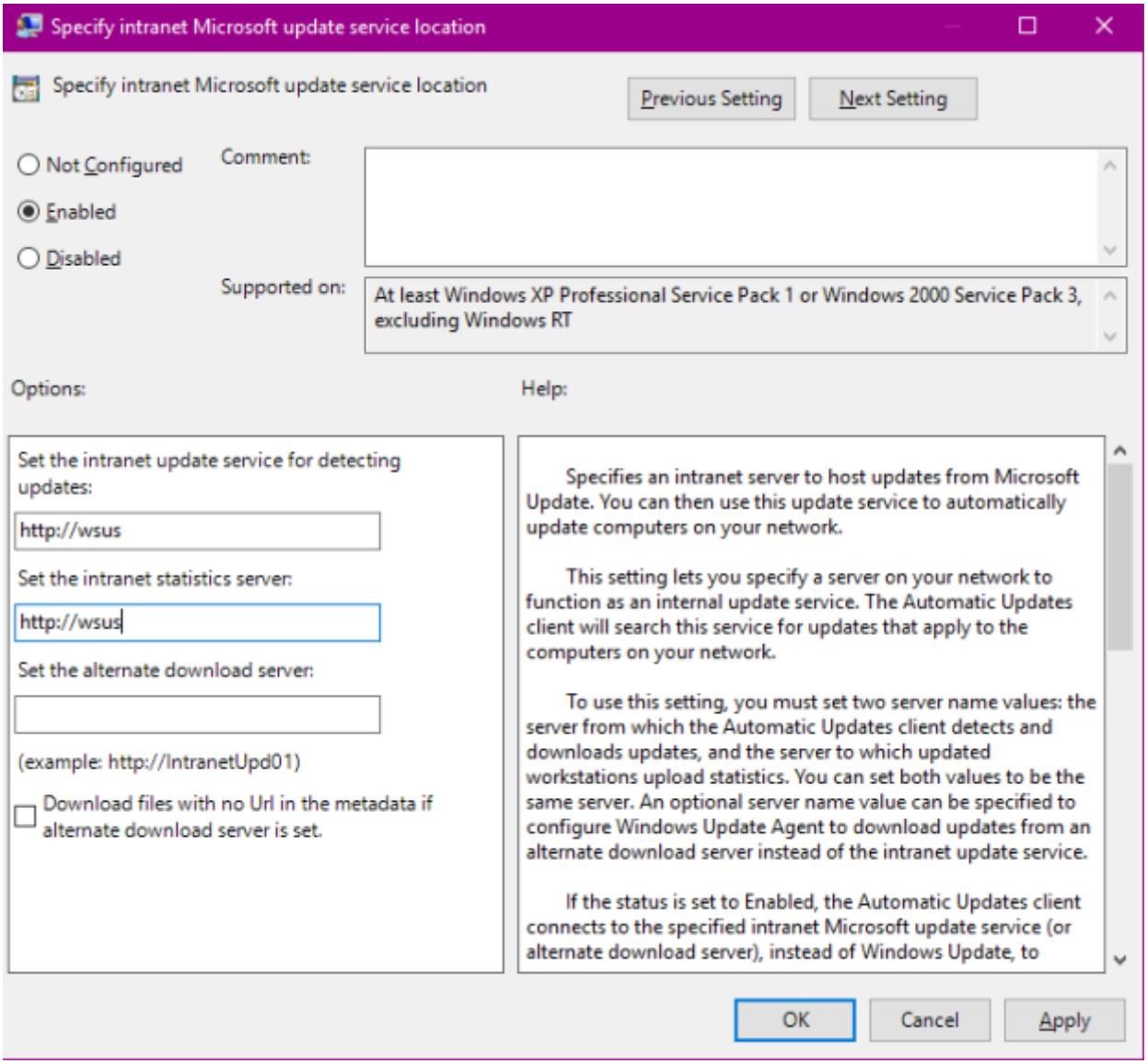
The list of the outboud rules after applying the .wfw file:



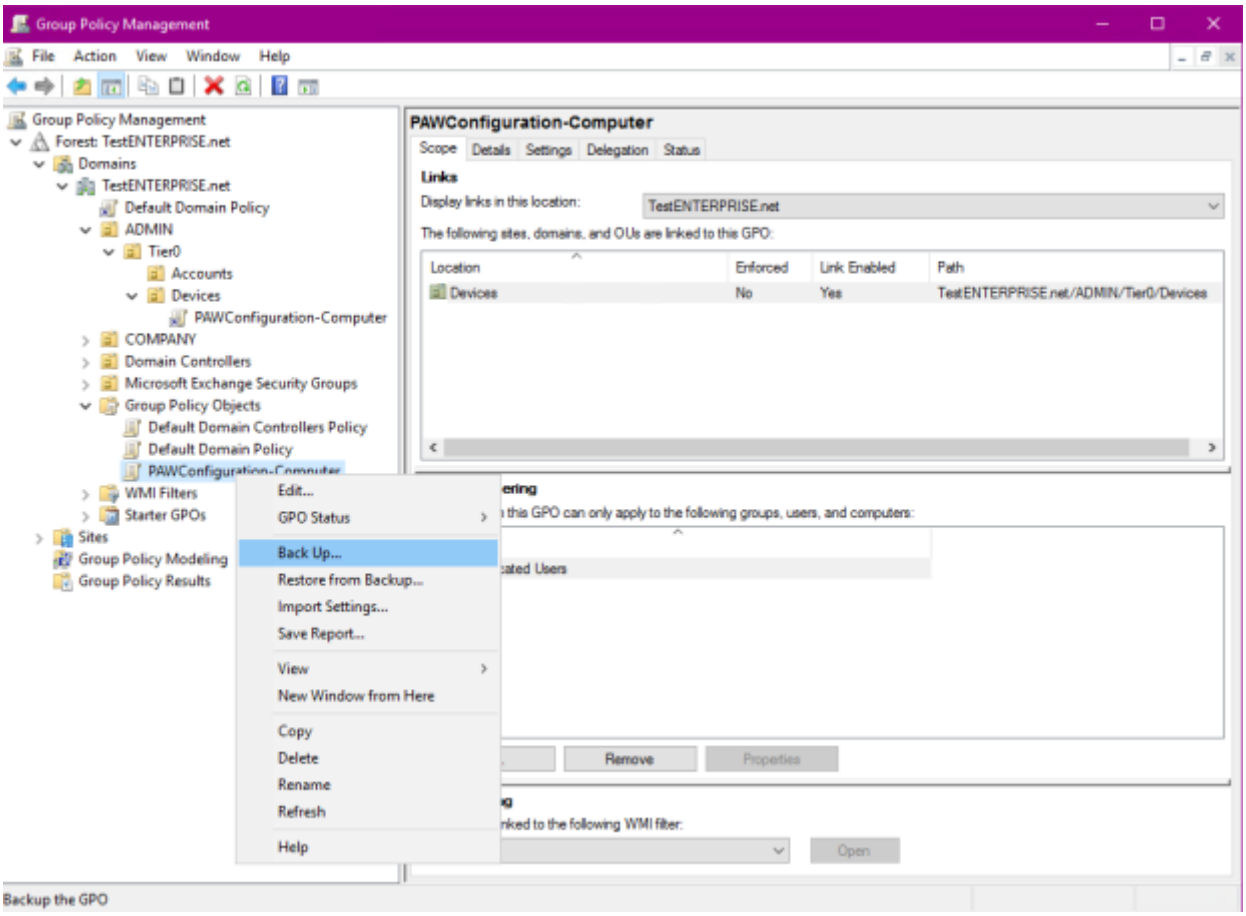
– of course IPv6 rules can be disabled here as well but given that my paw is not going to produce any IPv6 packets I won't do it now.

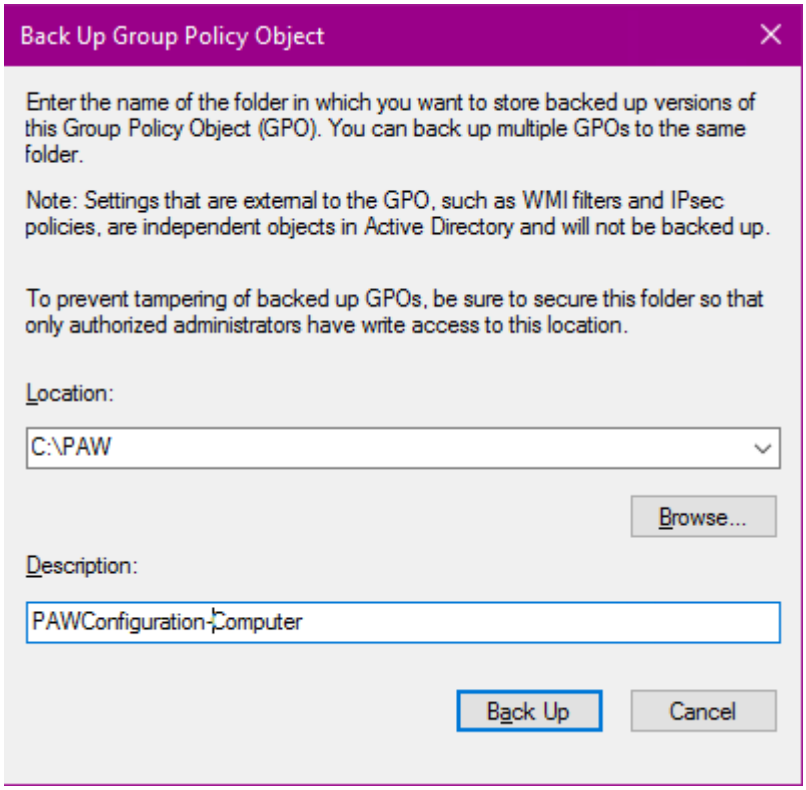
iv) the last gpo setting to configure is the Automatic Updates: the updates for the paw should be auto-aproved and installed daily:

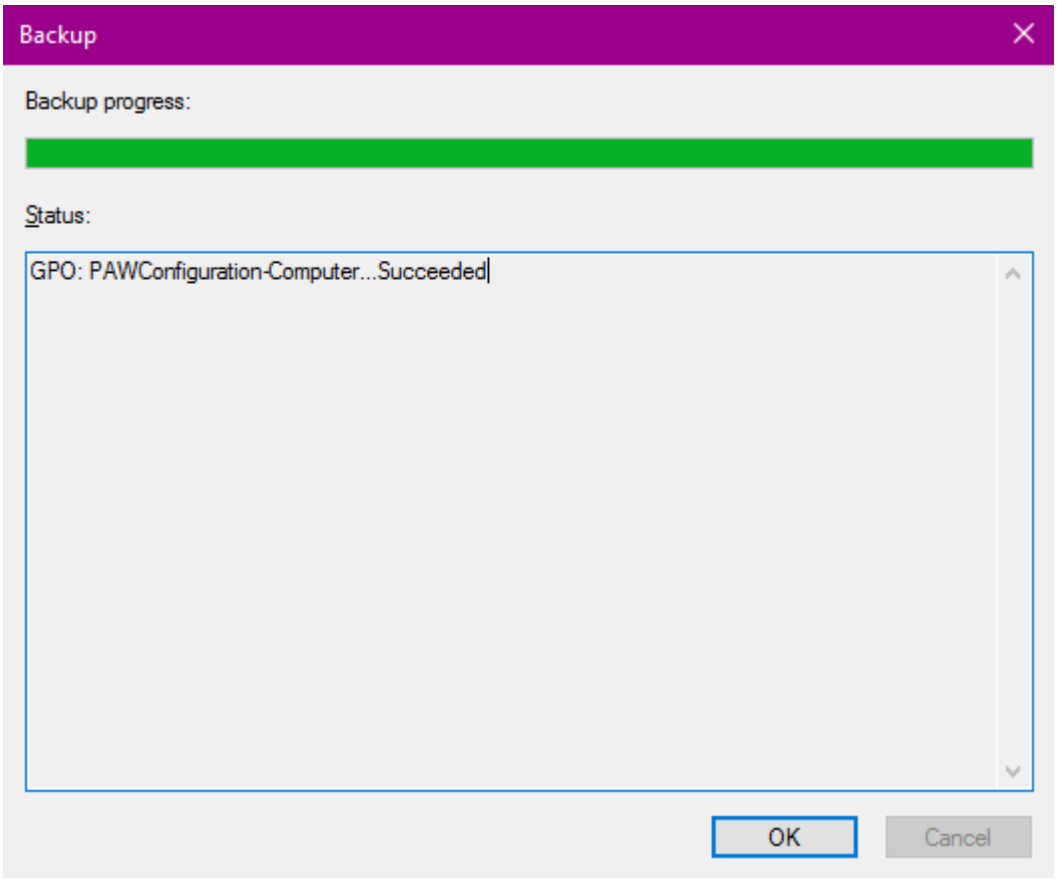

Configure Automatic Updates
Configure Automatic Updates
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3
Options:
Help:
Configure automatic updating:
4 - Auto download and schedule the install
The following settings are only required and applicable if 4 is selected.
Install during automatic maintenance
Scheduled install day:
0 - Every day
Scheduled install time:
03:00
Install updates for other Microsoft products
Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.
Note: This policy does not apply to Windows RT.
This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:
2 = Notify before downloading and installing any updates.
When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.
3 = (Default setting) Download the updates automatically and notify when they are ready to be installed
Windows finds updates that apply to the computer and
OK
Cancel
Apply

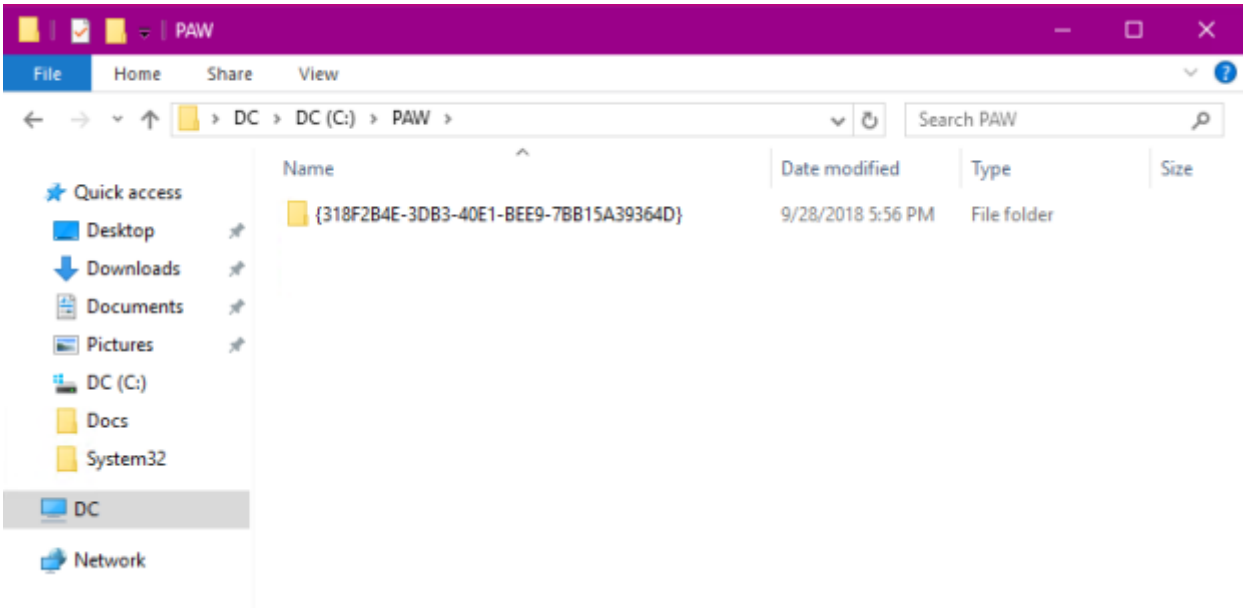


These are the all settings that should have been configured for the **PAWConfiguration-Computer gpo**. As a final step here I'd like to take the gpo backup:

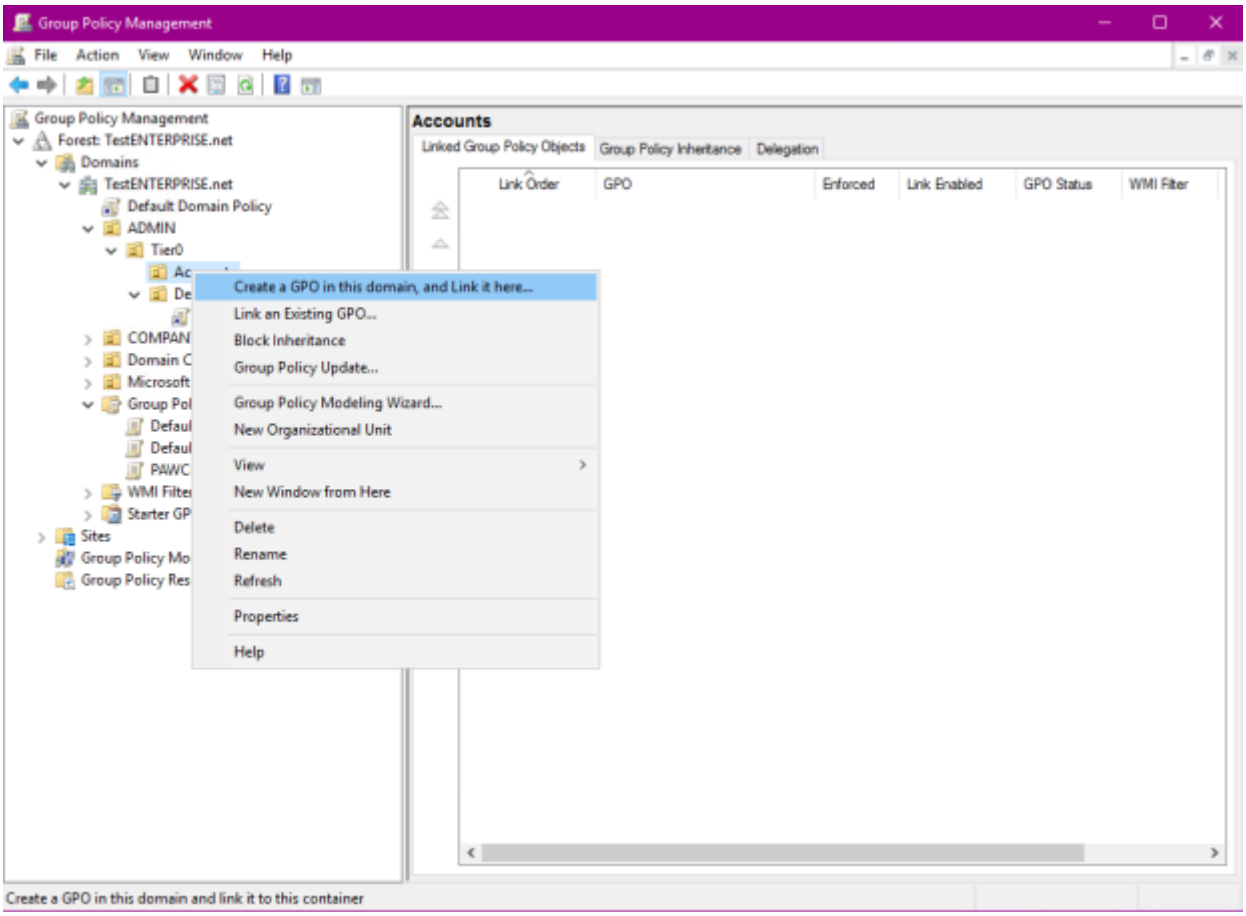

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: TestENTERPRISE.net
Domains
TestENTERPRISE.net
Default Domain Policy
ADMIN
Tier0
Accounts
Devices
PAWConfiguration-Computer
COMPANY
Domain Controllers
Microsoft Exchange Security Groups
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
PAWConfiguration-Computer
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
PAWConfiguration-Computer
Scope Details Settings Delegation Status
Links
Display links in this location:
TestENTERPRISE.net
The following sites, domains, and OUs are linked to this GPO:
Location Enforced Link Enabled Path
Devices No Yes TestENTERPRISE.net/ADMIN/Tier0/Devices
Edit...
GPO Status
Back Up...
Restore from Backup...
Import Settings...
Save Report...
View
New Window from Here
Copy
Delete
Rename
Refresh
Help
Remove
Properties
Open
Backup the GPO

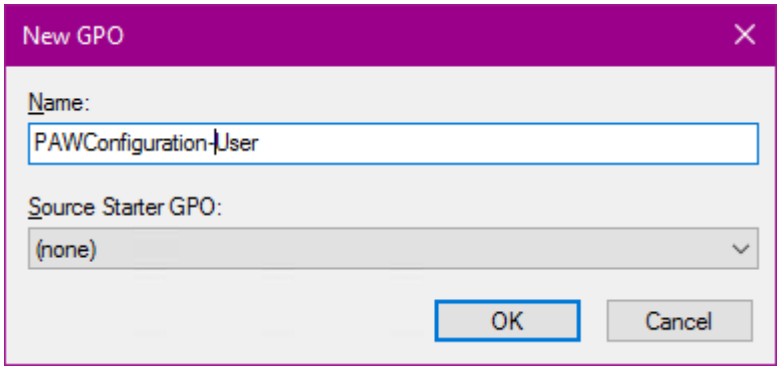

Back Up Group Policy Object
Enter the name of the folder in which you want to store backed up versions of this Group Policy Object (GPO). You can back up multiple GPOs to the same folder.
Note: Settings that are external to the GPO, such as WMI filters and IPsec policies, are independent objects in Active Directory and will not be backed up.
To prevent tampering of backed up GPOs, be sure to secure this folder so that only authorized administrators have write access to this location.
Location:
C:\PAW
Browse...
Description:
PAWConfiguration-Computer
Back Up
Cancel

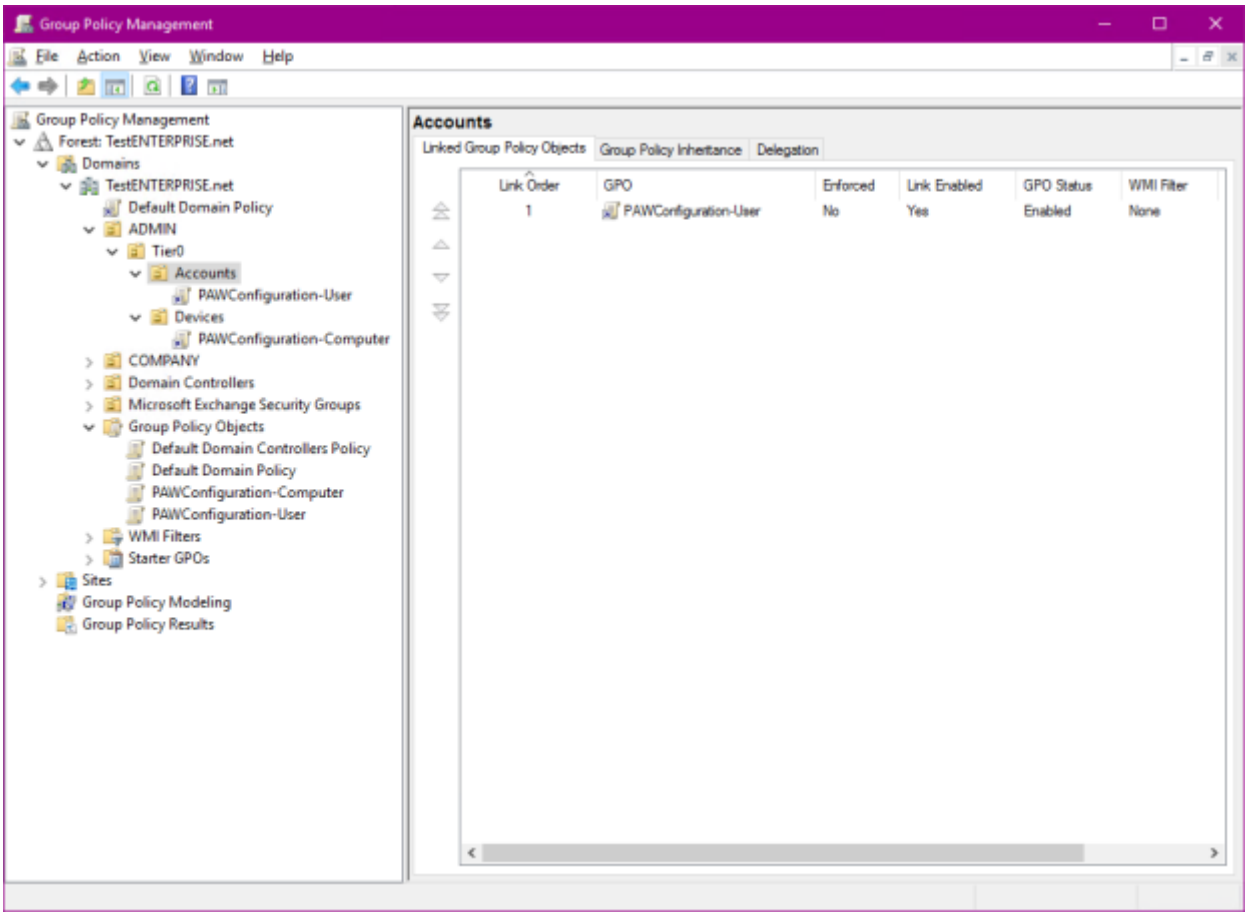




2) **PAWConfiguration-User** gpo will configure the tier0 user accounts – it must be linked to the Accounts OU:

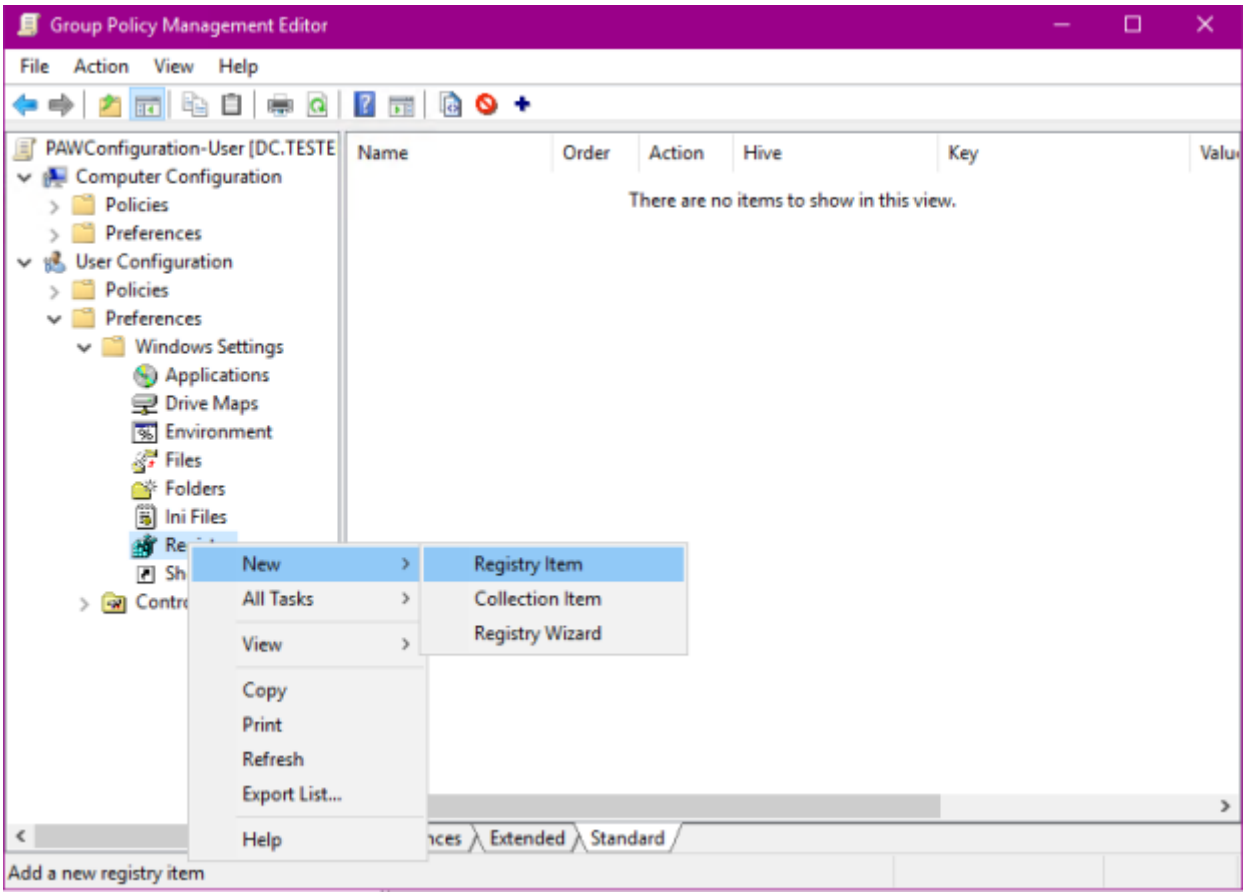

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: TestENTERPRISE.net
Domains
TestENTERPRISE.net
Default Domain Policy
ADMIN
Tier0
Accounts
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
WMI Filter
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Update...
Group Policy Modeling Wizard...
New Organizational Unit
View
New Window from Here
Delete
Rename
Refresh
Properties
Help
Sites
Create a GPO in this domain and link it to this container

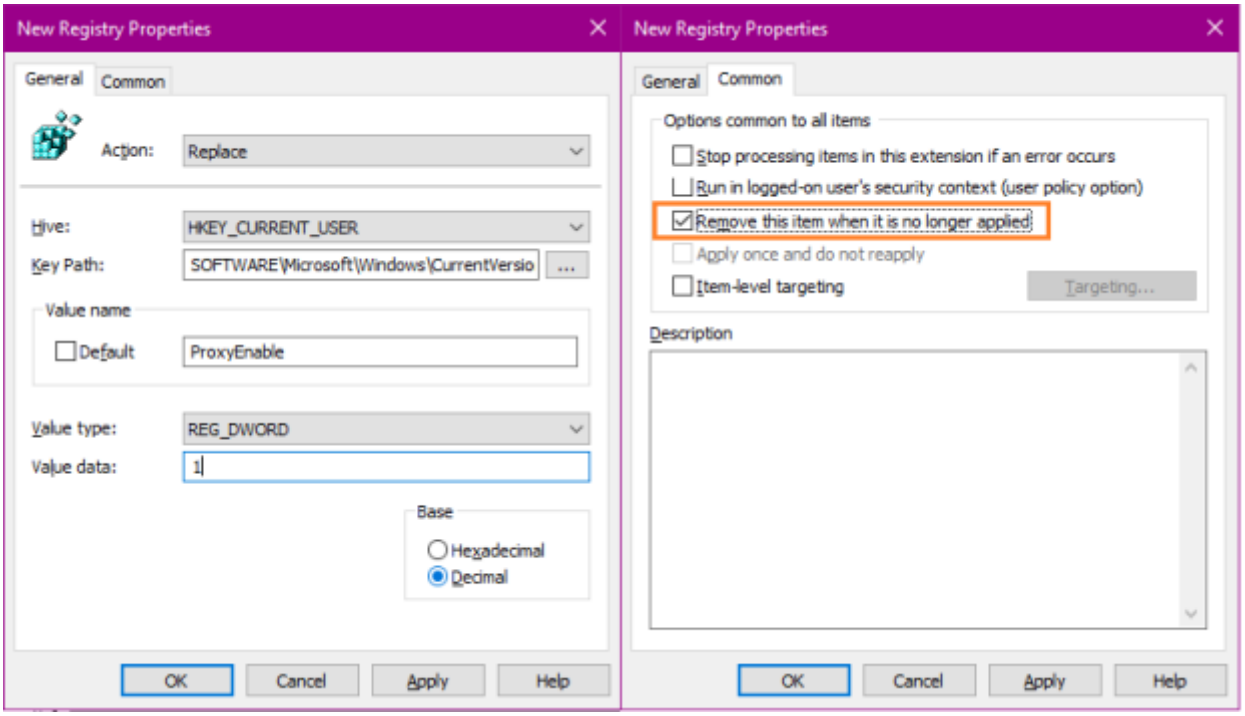

New GPO
Name:
PAWConfiguration-User
Source Starter GPO:
(none)
OK
Cancel



The **PAWConfiguration-User** gpo prevents tier0 users accounts from browsing Internet by enabling proxy and setting it to the non-existing ip – 127.0.0.1. If some user should have access to the Internet from this workstation we can create the special group – for example, CloudAdministrators as per MS's documentation – and prevent Internet browsing for all groups except CloudAdministrators:

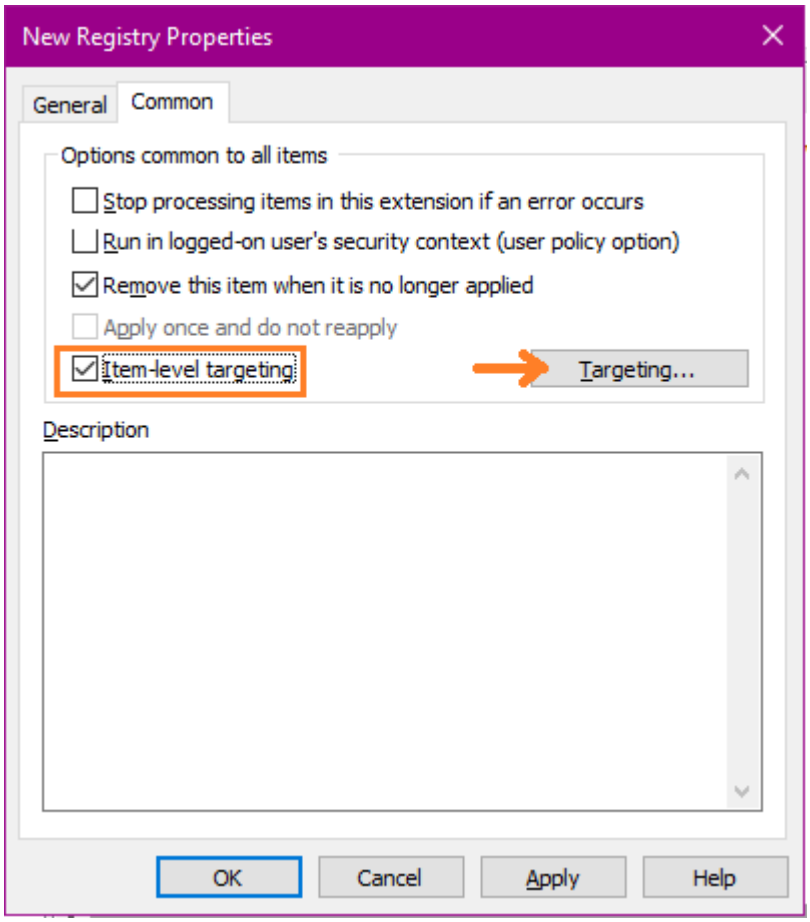
i) Software\Microsoft\Windows\CurrentVersion\Internet Settings – ProxyEnable

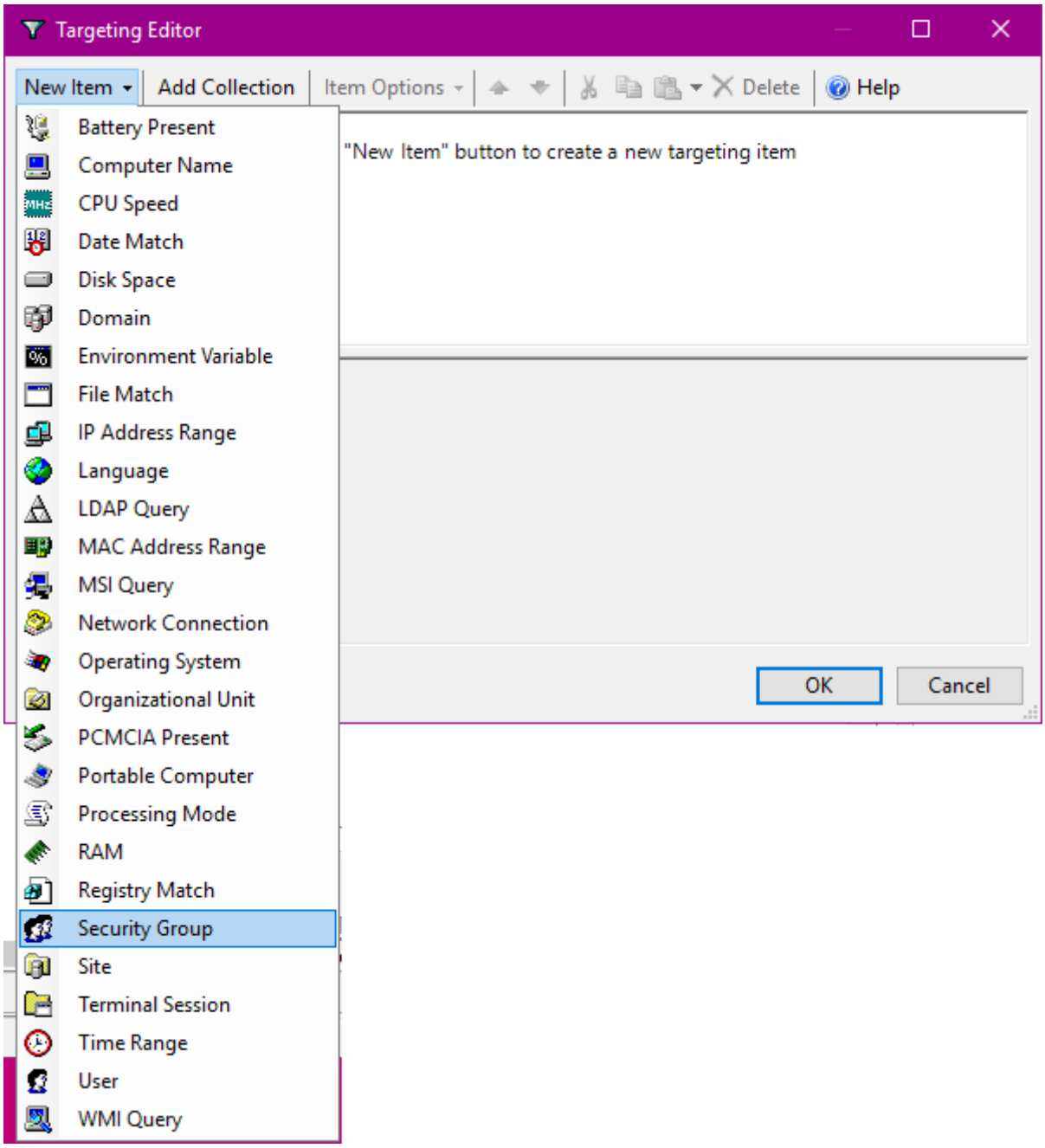


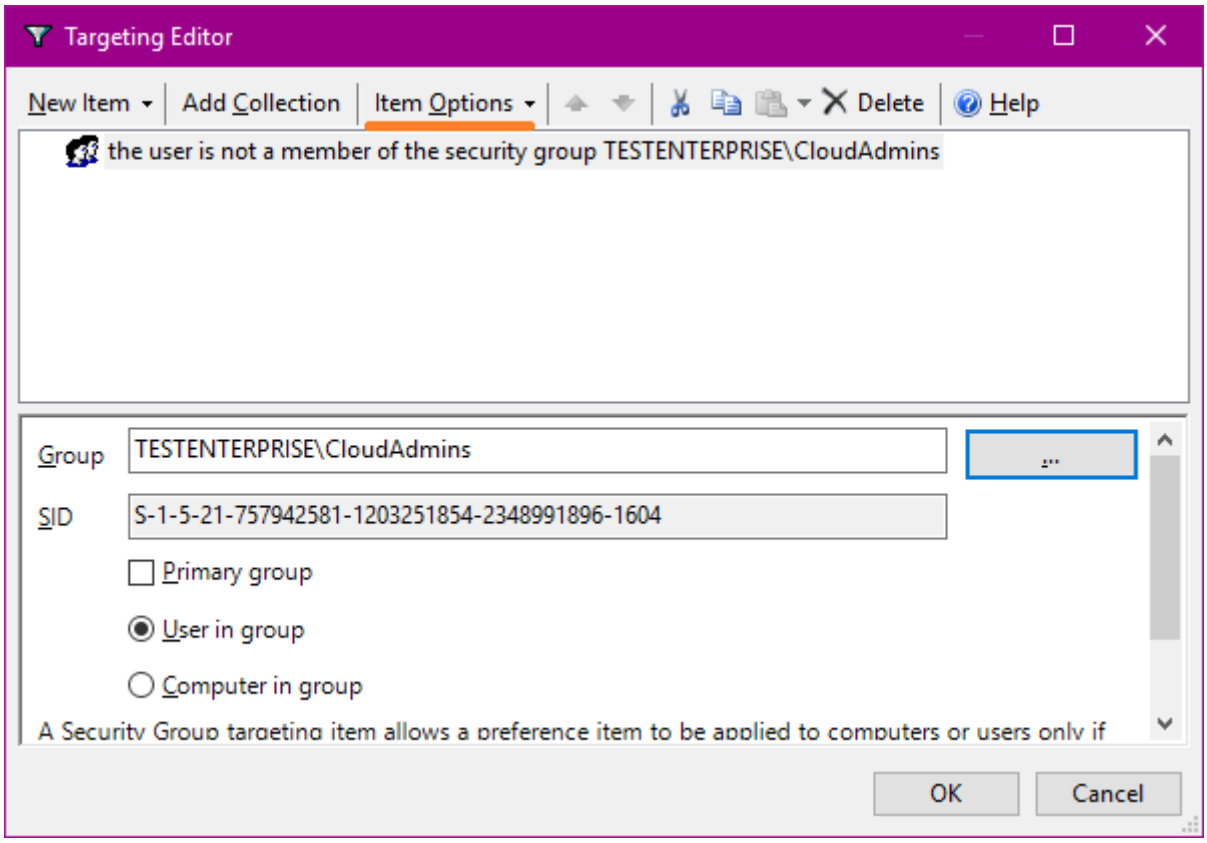


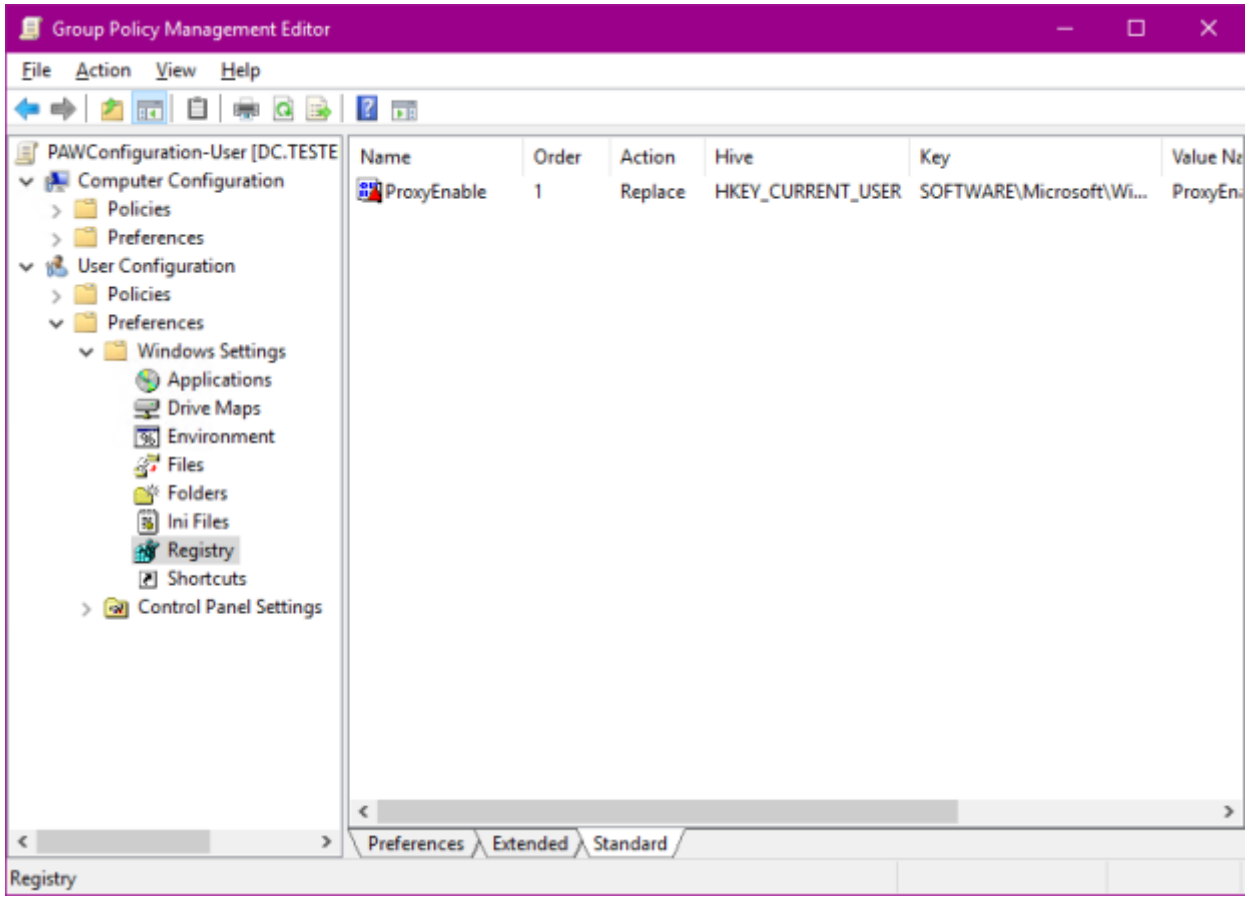
The key path mentioned above:
Software\Microsoft\Windows\CurrentVersion\Internet Settings

This setting must be applied to any account except CloudAdmins:

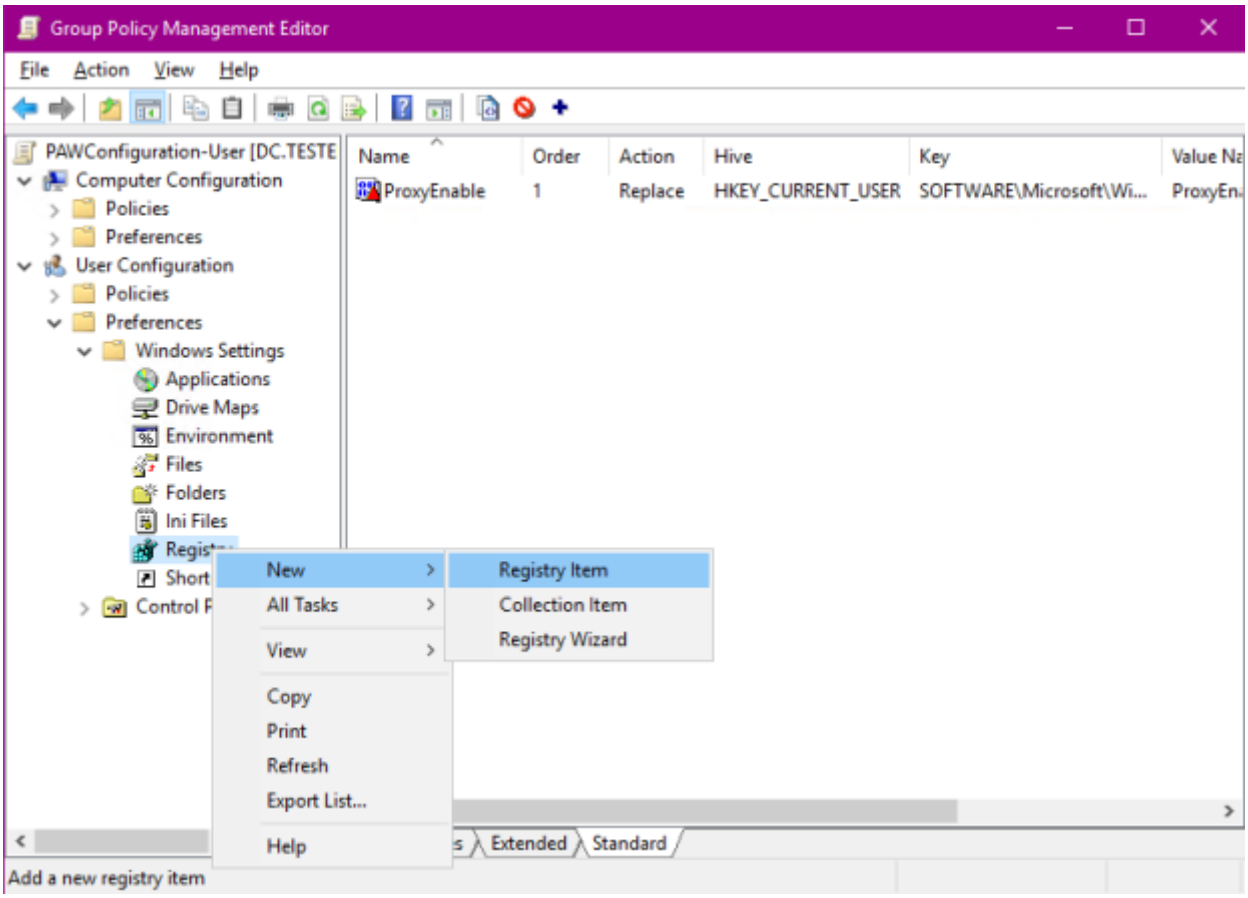

New Registry Properties
General
Common
Options common to all items
Stop processing items in this extension if an error occurs
Run in logged-on user's security context (user policy option)
Remove this item when it is no longer applied
Apply once and do not reapply
Item-level targeting
Targeting...
Description
OK
Cancel
Apply
Help

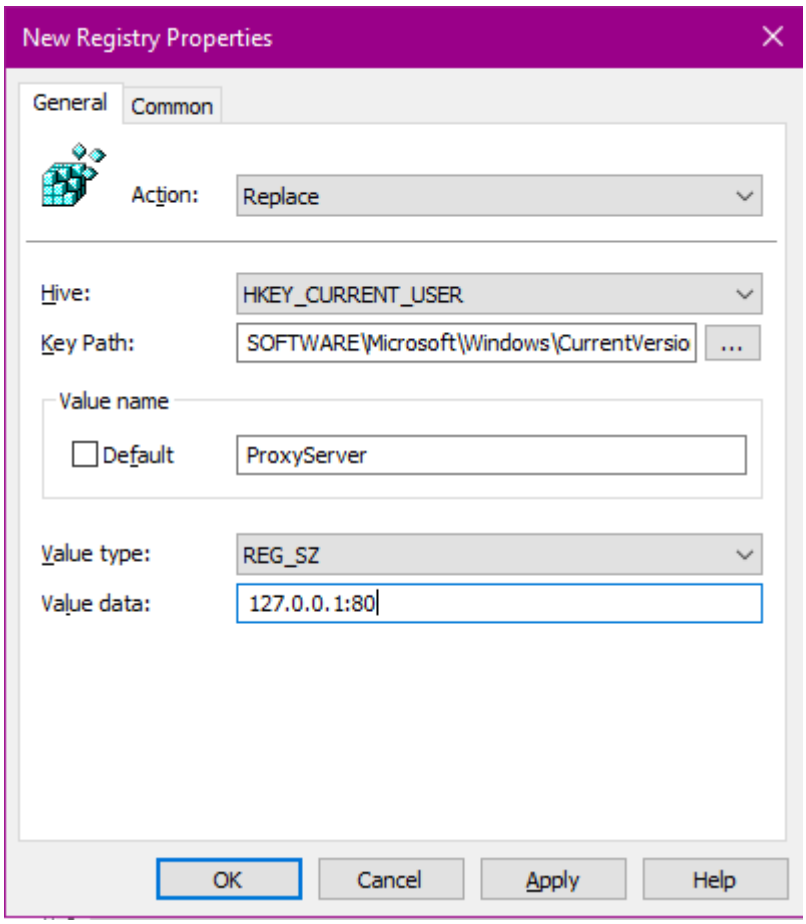

Targeting Editor
New Item
Add Collection
Item Options
Delete
Help
"New Item" button to create a new targeting item
OK
Cancel
Battery Present
Computer Name
CPU Speed
Date Match
Disk Space
Domain
Environment Variable
File Match
IP Address Range
Language
LDAP Query
MAC Address Range
MSI Query
Network Connection
Operating System
Organizational Unit
PCMCIA Present
Portable Computer
Processing Mode
RAM
Registry Match
Security Group
Site
Terminal Session
Time Range
User
WMI Query

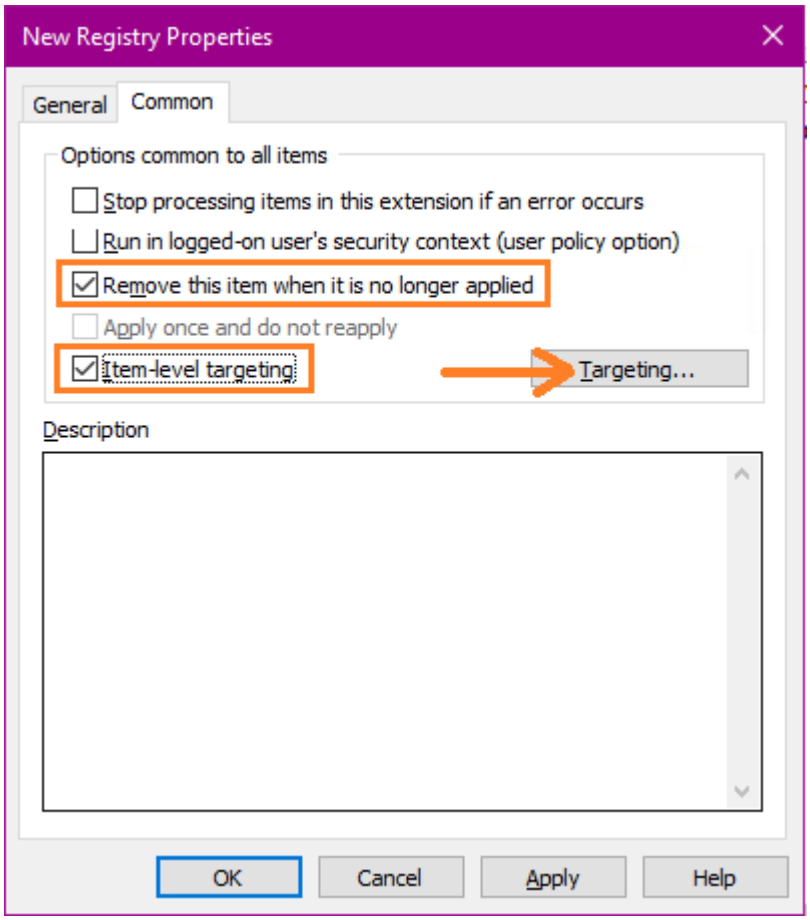


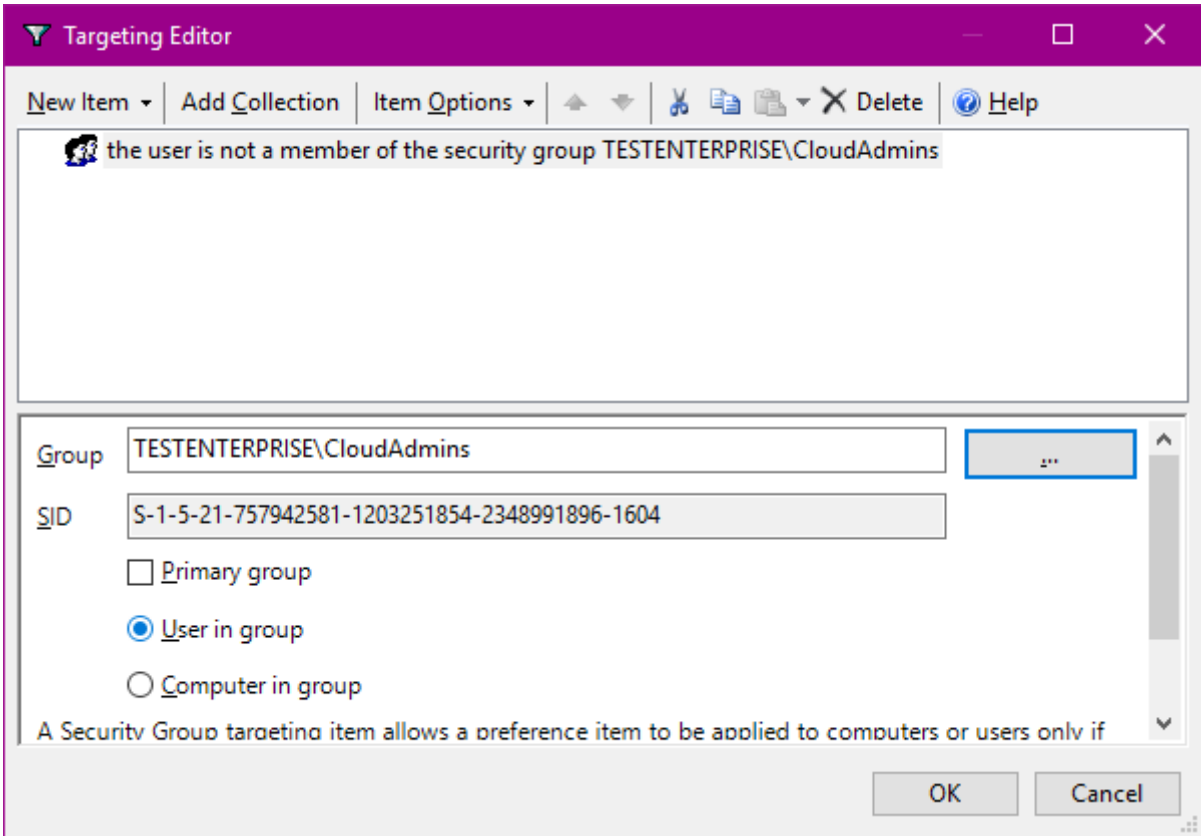


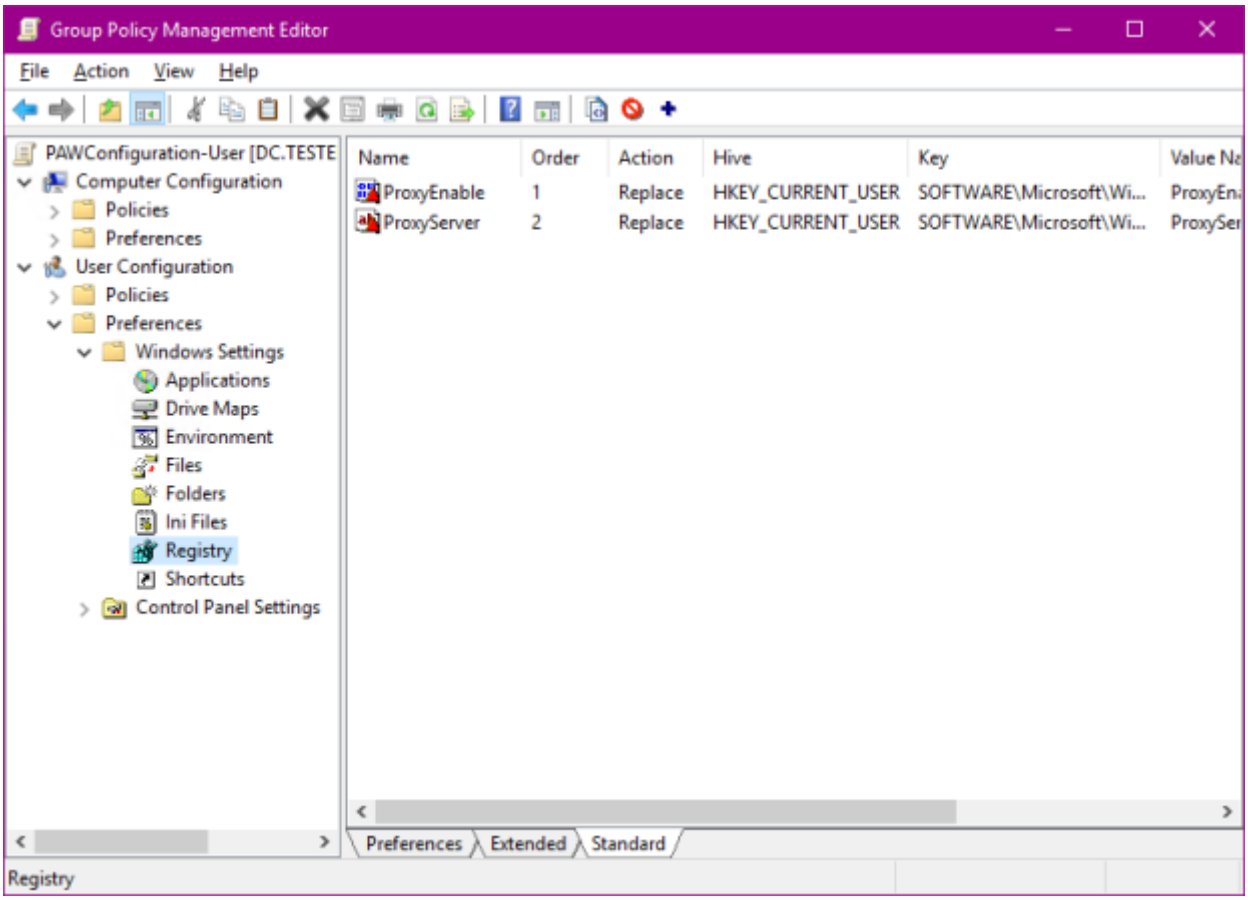
ii) i) Software\Microsoft\Windows\CurrentVersion\Internet Settings – ProxyServer


Group Policy Management Editor
File Action View Help
PAWConfiguration-User [DC.TESTE
Computer Configuration
Policies
Preferences
User Configuration
Policies
Preferences
Windows Settings
Applications
Drive Maps
Environment
Files
Folders
Ini Files
Regist...
Short...
Control P...
Name Order Action Hive Key Value Na
ProxyEnable 1 Replace HKEY_CURRENT_USER SOFTWARE\Microsoft\Wi... ProxyEn...
New
All Tasks
View
Copy
Print
Refresh
Export List...
Help
Registry Item
Collection Item
Registry Wizard
Extended Standard
Add a new registry item

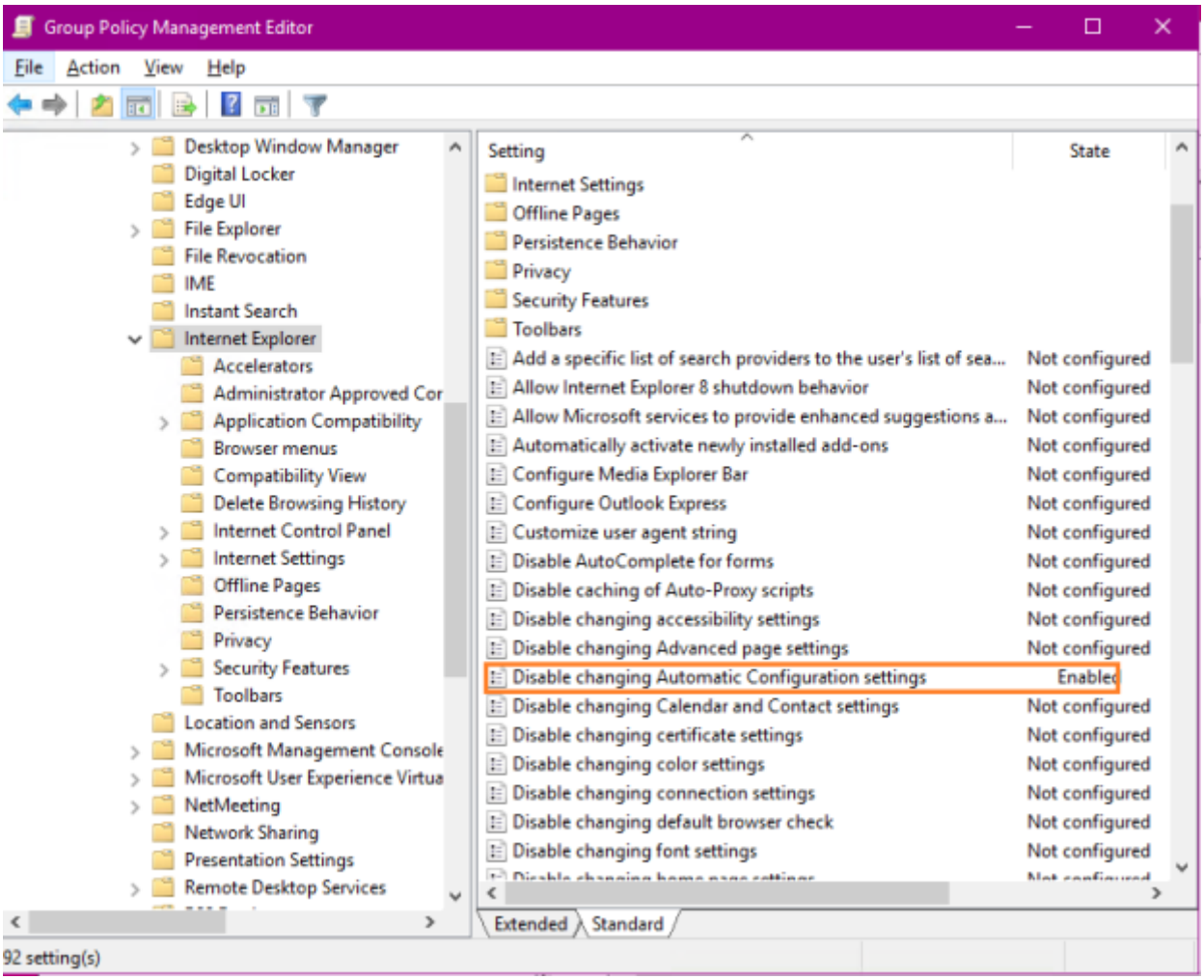

New Registry Properties
General Common
Action: Replace
Hive: HKEY_CURRENT_USER
Key Path: SOFTWARE\Microsoft\Windows\CurrentVersio ...
Value name
Default
ProxyServer
Value type: REG_SZ
Value data: 127.0.0.1:80
OK Cancel Apply Help

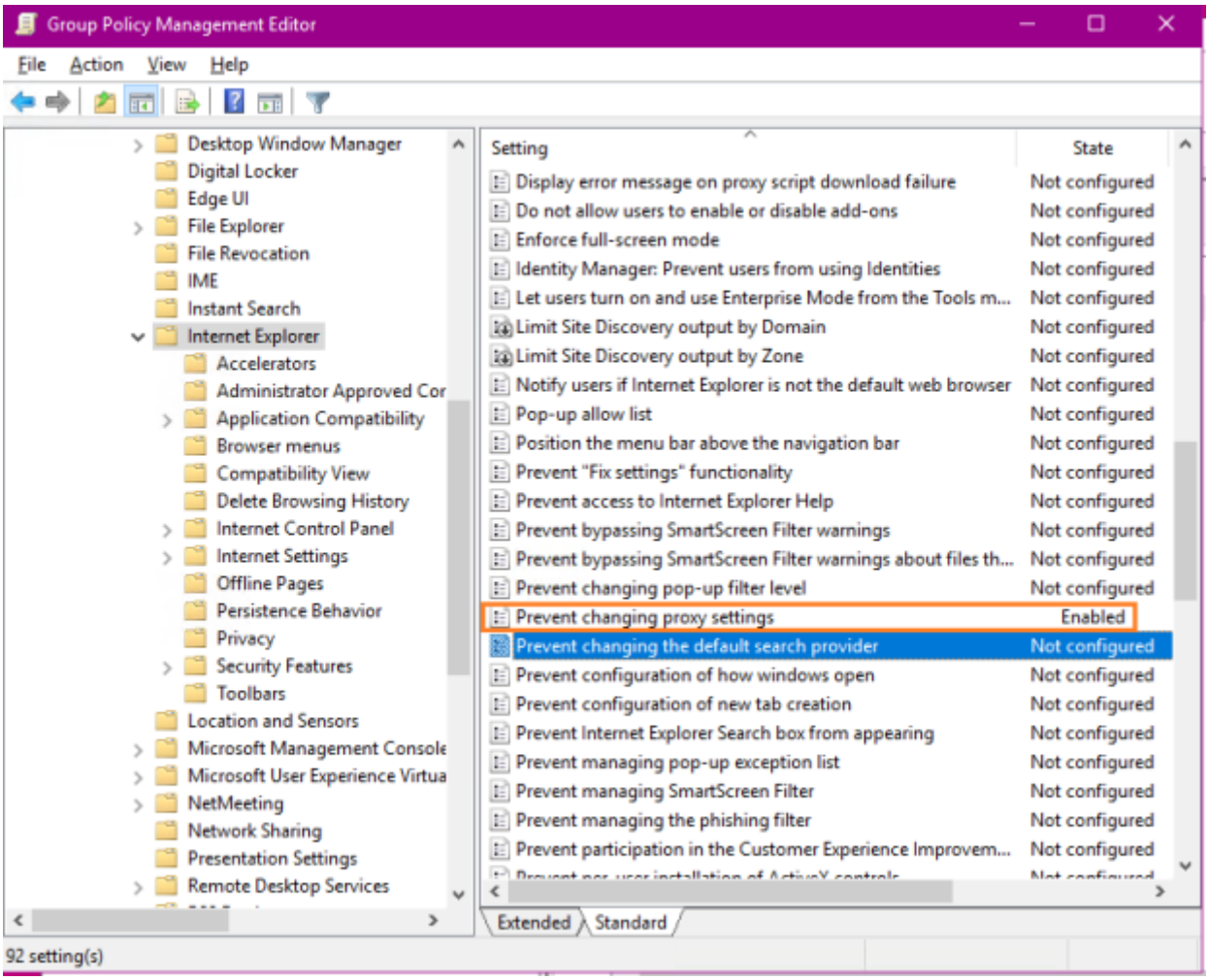

New Registry Properties
General
Common
Options common to all items
Stop processing items in this extension if an error occurs
Run in logged-on user's security context (user policy option)
Remove this item when it is no longer applied
Apply once and do not reapply
Item-level targeting
Targeting...
Description
OK
Cancel
Apply
Help


Targeting Editor
New Item
Add Collection
Item Options
Delete
Help
the user is not a member of the security group TESTENTERPRISE\CloudAdmins
Group
TESTENTERPRISE\CloudAdmins
SID
S-1-5-21-757942581-1203251854-2348991896-1604
Primary group
User in group
Computer in group
A Security Group targeting item allows a preference item to be applied to computers or users only if
OK
Cancel

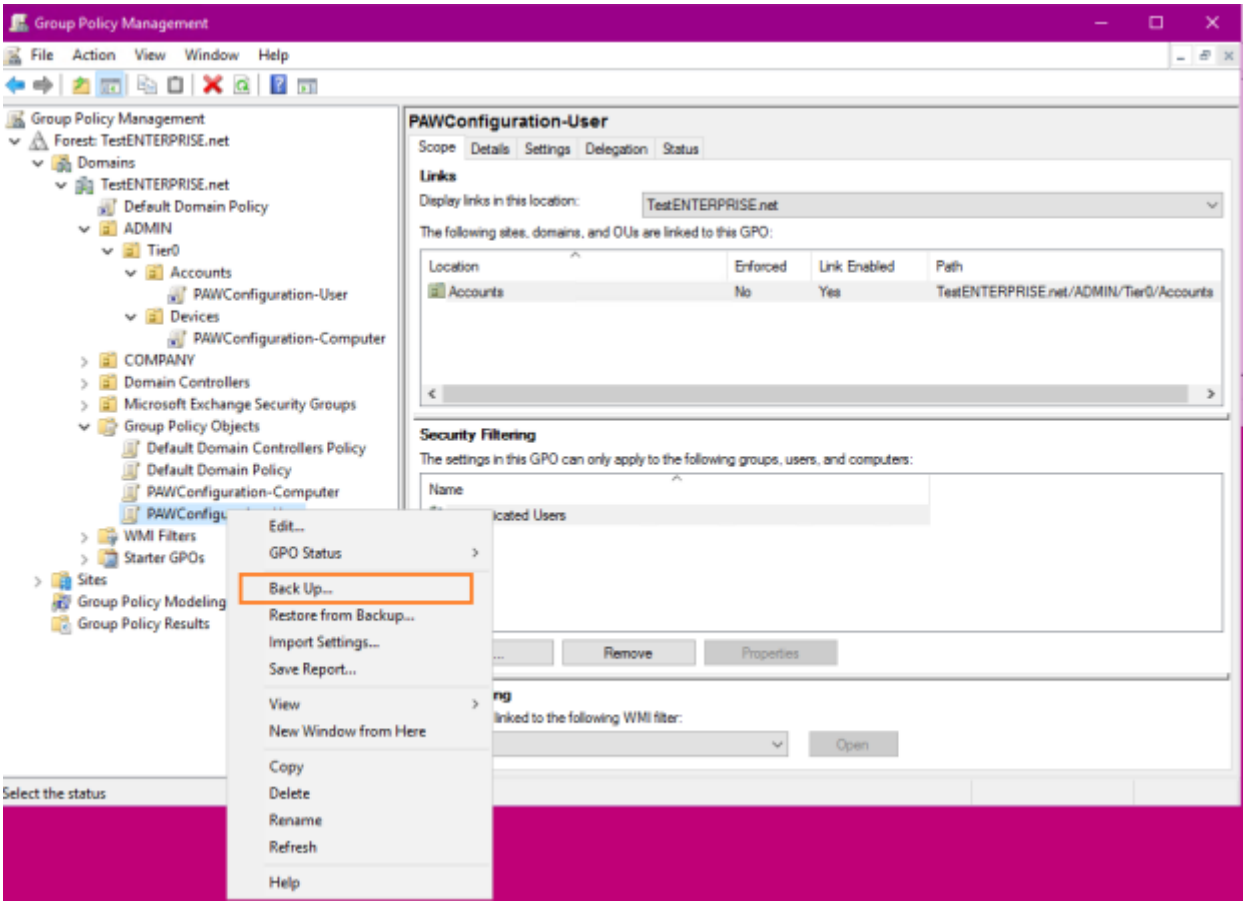


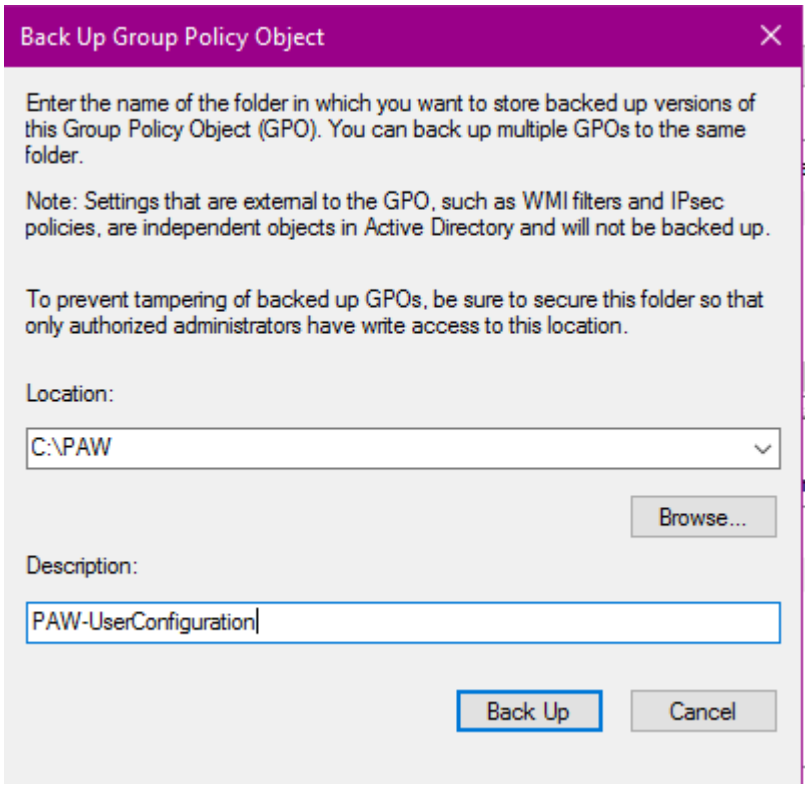
iii) and no one (except CloudeAdmins) should have the ability to overwrite the settings configured above (that would be the third test):
User Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer

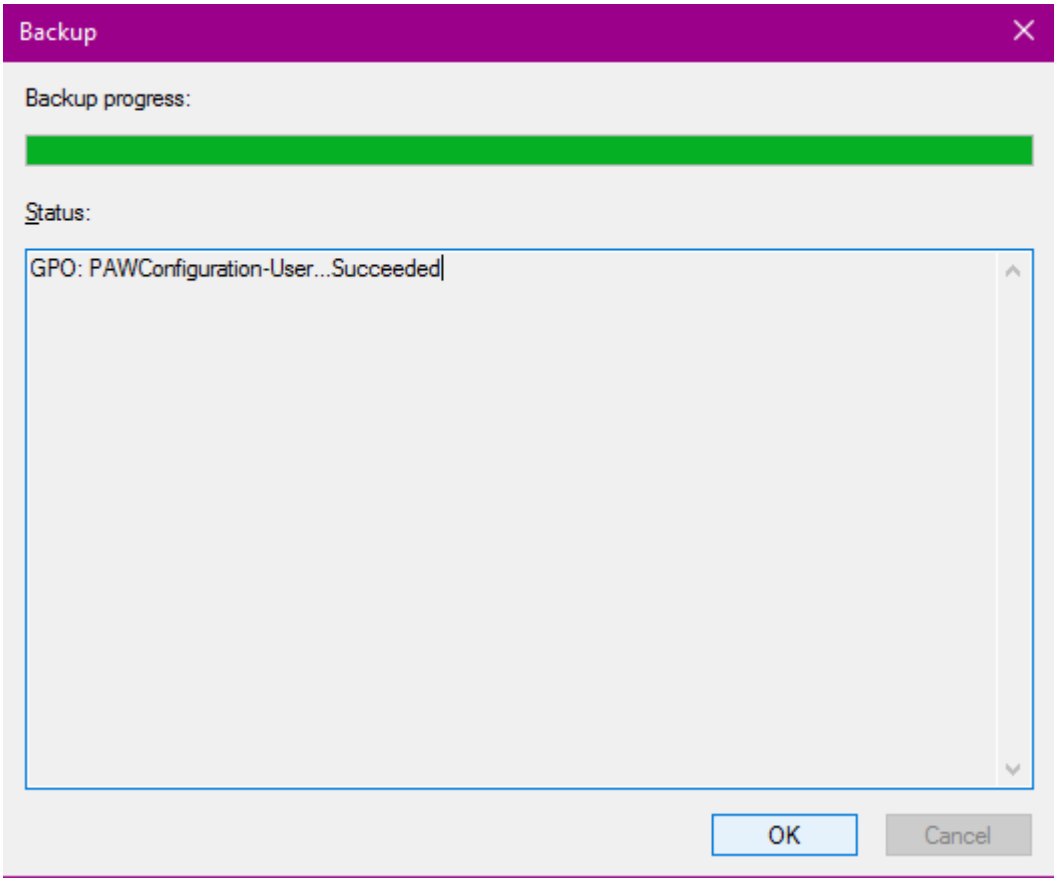

Group Policy Management Editor
File Action View Help
Desktop Window Manager
Digital Locker
Edge UI
File Explorer
File Revocation
IME
Instant Search
Internet Explorer
Accelerators
Administrator Approved Cor
Application Compatibility
Browser menus
Compatibility View
Delete Browsing History
Internet Control Panel
Internet Settings
Offline Pages
Persistence Behavior
Privacy
Security Features
Toolbars
Location and Sensors
Microsoft Management Console
Microsoft User Experience Virtua
NetMeeting
Network Sharing
Presentation Settings
Remote Desktop Services
Setting
State
Internet Settings
Offline Pages
Persistence Behavior
Privacy
Security Features
Toolbars
Add a specific list of search providers to the user's list of sea... Not configured
Allow Internet Explorer 8 shutdown behavior Not configured
Allow Microsoft services to provide enhanced suggestions a... Not configured
Automatically activate newly installed add-ons Not configured
Configure Media Explorer Bar Not configured
Configure Outlook Express Not configured
Customize user agent string Not configured
Disable AutoComplete for forms Not configured
Disable caching of Auto-Proxy scripts Not configured
Disable changing accessibility settings Not configured
Disable changing Advanced page settings Not configured
Disable changing Automatic Configuration settings Enable
Disable changing Calendar and Contact settings Not configured
Disable changing certificate settings Not configured
Disable changing color settings Not configured
Disable changing connection settings Not configured
Disable changing default browser check Not configured
Disable changing font settings Not configured
Extended
Standard
92 setting(s)

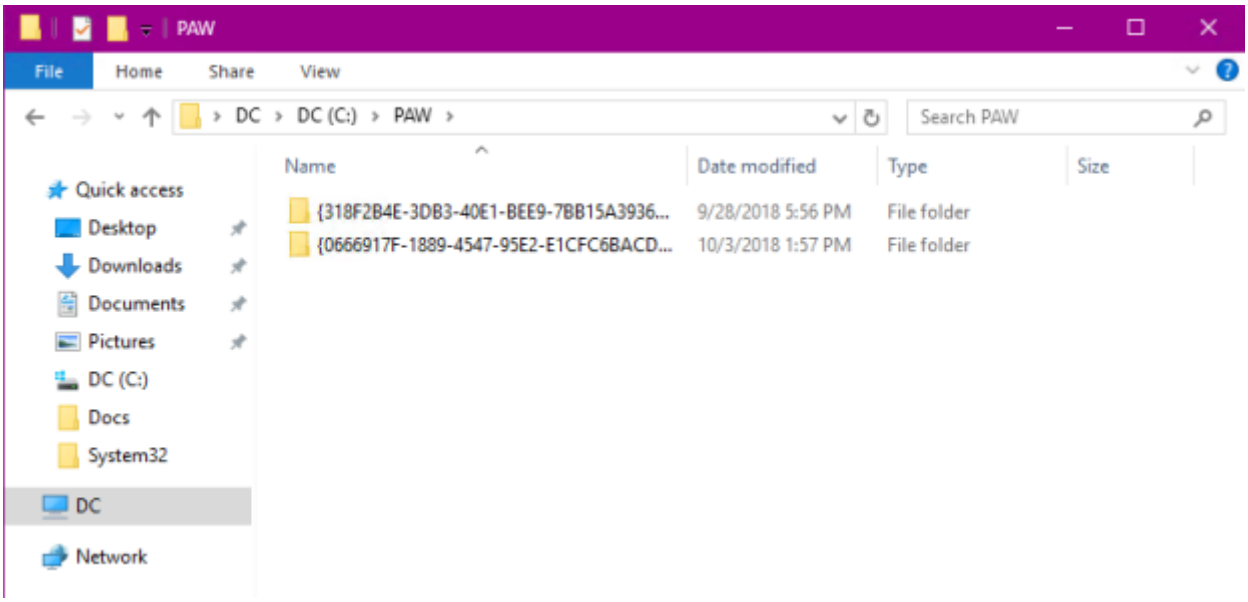

Group Policy Management Editor
File Action View Help
Desktop Window Manager
Digital Locker
Edge UI
File Explorer
File Revocation
IME
Instant Search
Internet Explorer
Accelerators
Administrator Approved Cor
Application Compatibility
Browser menus
Compatibility View
Delete Browsing History
Internet Control Panel
Internet Settings
Offline Pages
Persistence Behavior
Privacy
Security Features
Toolbars
Location and Sensors
Microsoft Management Console
Microsoft User Experience Virtua
NetMeeting
Network Sharing
Presentation Settings
Remote Desktop Services
Setting
State
Display error message on proxy script download failure Not configured
Do not allow users to enable or disable add-ons Not configured
Enforce full-screen mode Not configured
Identity Manager: Prevent users from using Identities Not configured
Let users turn on and use Enterprise Mode from the Tools m... Not configured
Limit Site Discovery output by Domain Not configured
Limit Site Discovery output by Zone Not configured
Notify users if Internet Explorer is not the default web browser Not configured
Pop-up allow list Not configured
Position the menu bar above the navigation bar Not configured
Prevent "Fix settings" functionality Not configured
Prevent access to Internet Explorer Help Not configured
Prevent bypassing SmartScreen Filter warnings Not configured
Prevent bypassing SmartScreen Filter warnings about files th... Not configured
Prevent changing pop-up filter level Not configured
Prevent changing proxy settings Enabled
Prevent changing the default search provider Not configured
Prevent configuration of how windows open Not configured
Prevent configuration of new tab creation Not configured
Prevent Internet Explorer Search box from appearing Not configured
Prevent managing pop-up exception list Not configured
Prevent managing SmartScreen Filter Not configured
Prevent managing the phishing filter Not configured
Prevent participation in the Customer Experience Improvem... Not configured
Extended Standard
92 setting(s)

Backup GPO:


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: TestENTERPRISE.net
Domains
TestENTERPRISE.net
Default Domain Policy
ADMIN
Tier0
Accounts
PAWConfiguration-User
Devices
PAWConfiguration-Computer
COMPANY
Domain Controllers
Microsoft Exchange Security Groups
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
PAWConfiguration-Computer
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
PAWConfiguration-User
Scope Details Settings Delegation Status
Links
Display links in this location: TestENTERPRISE.net
The following sites, domains, and OUs are linked to this GPO:
Location Enforced Link Enabled Path
Accounts No Yes TestENTERPRISE.net/ADMIN/Tier0/Accounts
Security Filtering
The settings in this GPO can only apply to the following groups, users, and computers:
Name
Edit...
GPO Status
Back Up...
Restore from Backup...
Import Settings...
Save Report...
View
New Window from Here
Copy
Delete
Rename
Refresh
Help
Remove
Properties
Open
Select the status


Back Up Group Policy Object
Enter the name of the folder in which you want to store backed up versions of this Group Policy Object (GPO). You can back up multiple GPOs to the same folder.
Note: Settings that are external to the GPO, such as WMI filters and IPsec policies, are independent objects in Active Directory and will not be backed up.
To prevent tampering of backed up GPOs, be sure to secure this folder so that only authorized administrators have write access to this location.
Location:
C:\PAW
Browse...
Description:
PAW-UserConfiguration
Back Up
Cancel

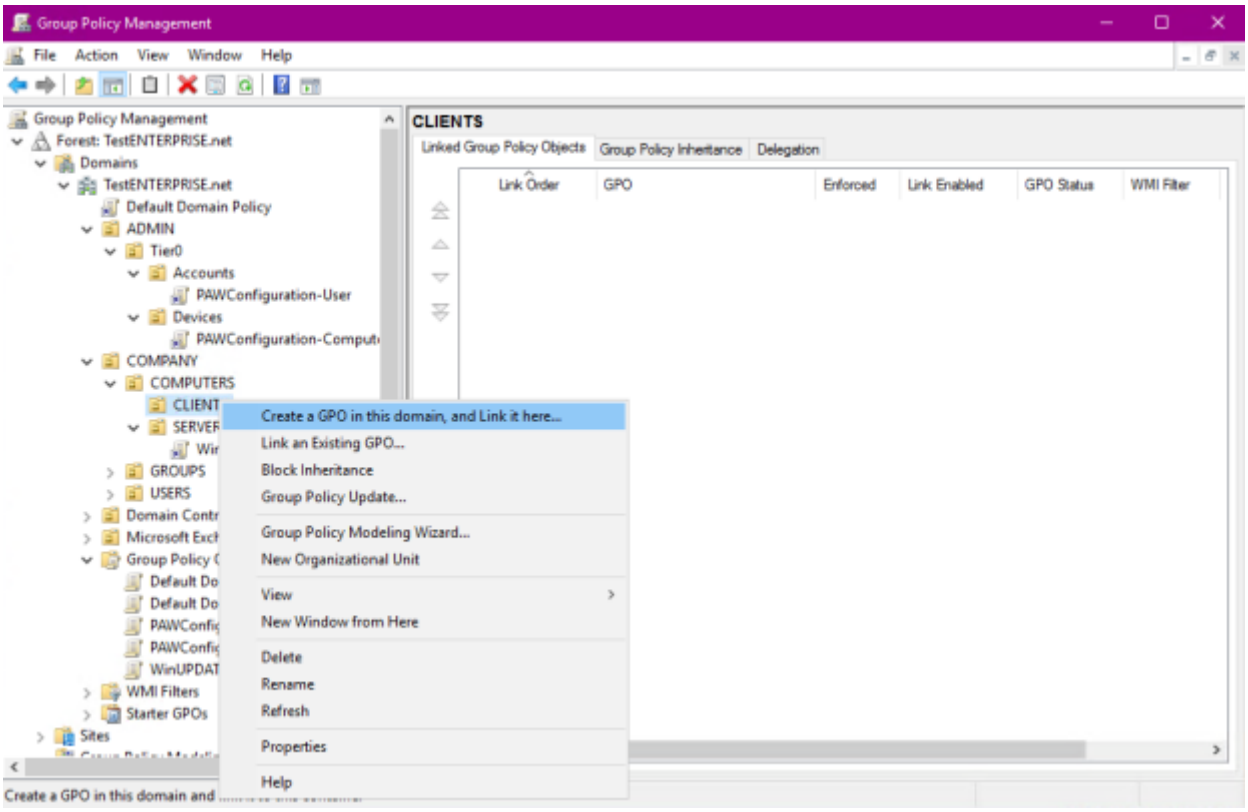

Backup
Backup progress:
Status:
GPO: PAWConfiguration-User...Succeeded
OK
Cancel

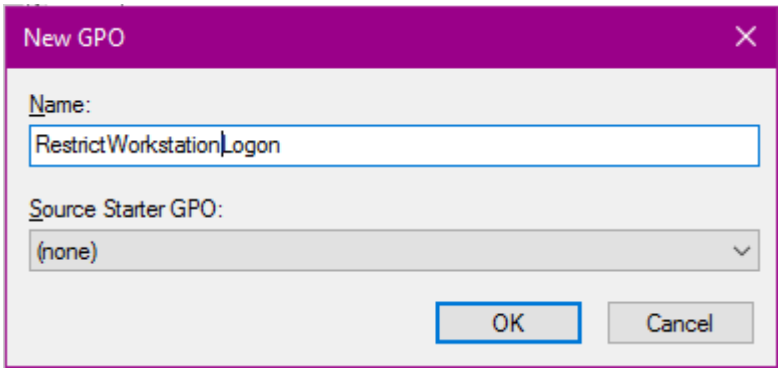


Aside from these two GPOs, at least one more GPO should be created – **RestrictWorkstationLogon** GPO. According to MS it must restrict tier0 accounts from logging onto users' workstations.

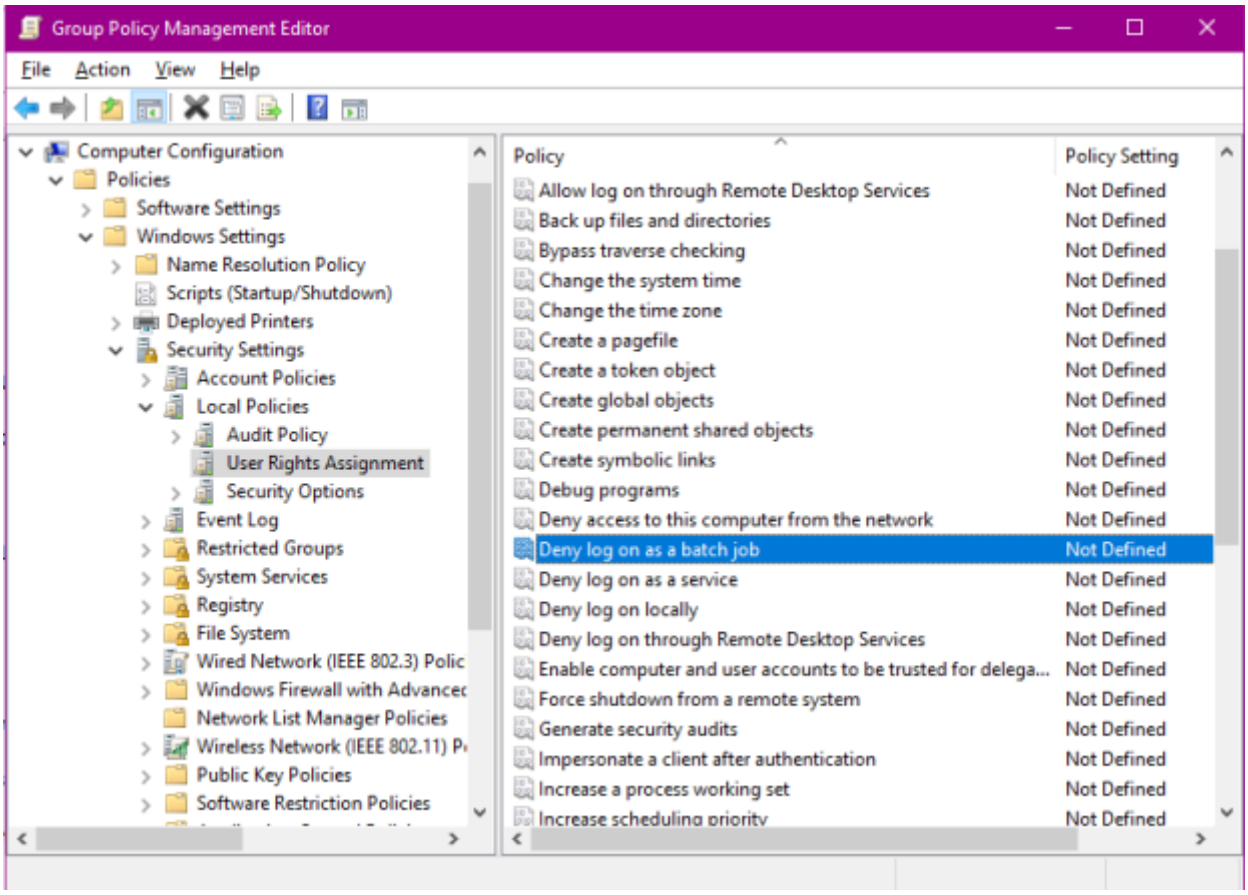
I won't create the **RestrictServerLogon** GPO as decribed in the MS's article because I'm not going to administer different servers with different accounts in the TestENTERPRISE network – if you're planning to deploy a paw in the production network and want to maximize its security level then the **RestrictServerLogon** GPO should be created and linked to the Tier1-Servers OU to which according to MS all other servers must be moved. In fact the **Restrict Server Logon** GPO is the same as the **RestrictWorkstationLogon** GPO – you just link it to another OU. However, for testing purposes I will link RestrictWorkstationLogon to the OU with server computer accounts to show how the whole paw infrastructure should look like.

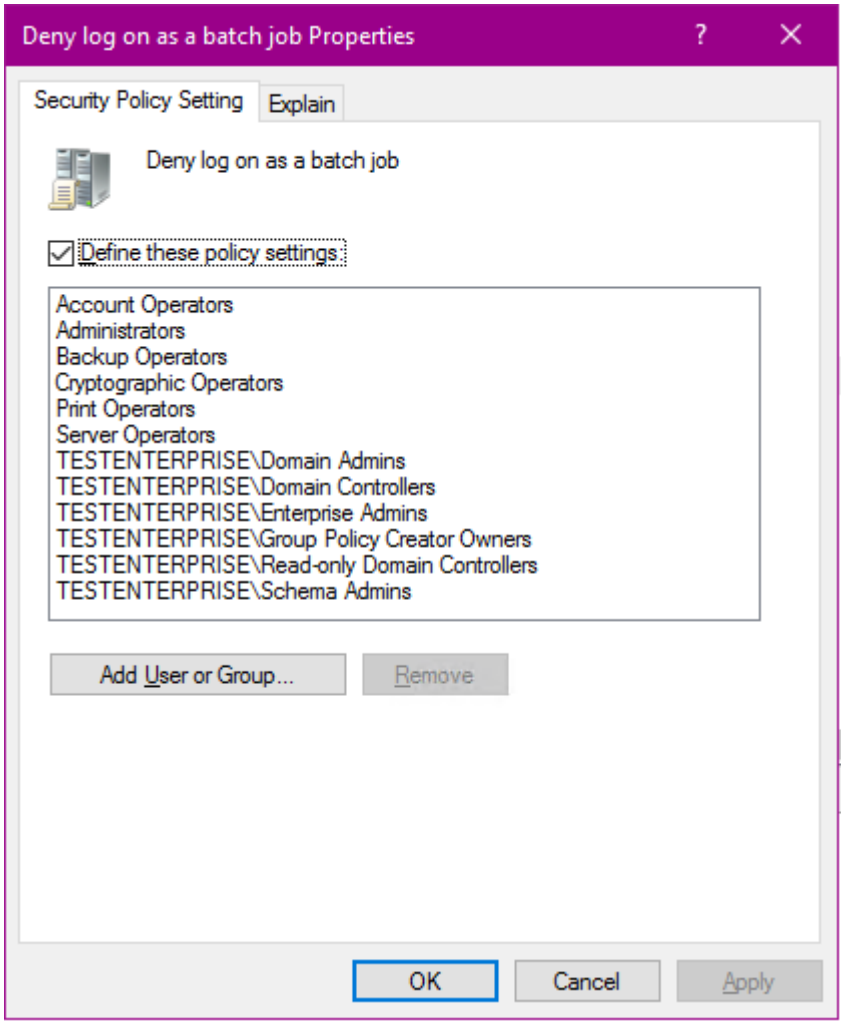
So let's create the **RestrictWorkstationLogon** GPO and link it to the OU which contains domain's client computer accounts – in my domain it is the COMPANY\COMPUTERS\Clients OU:



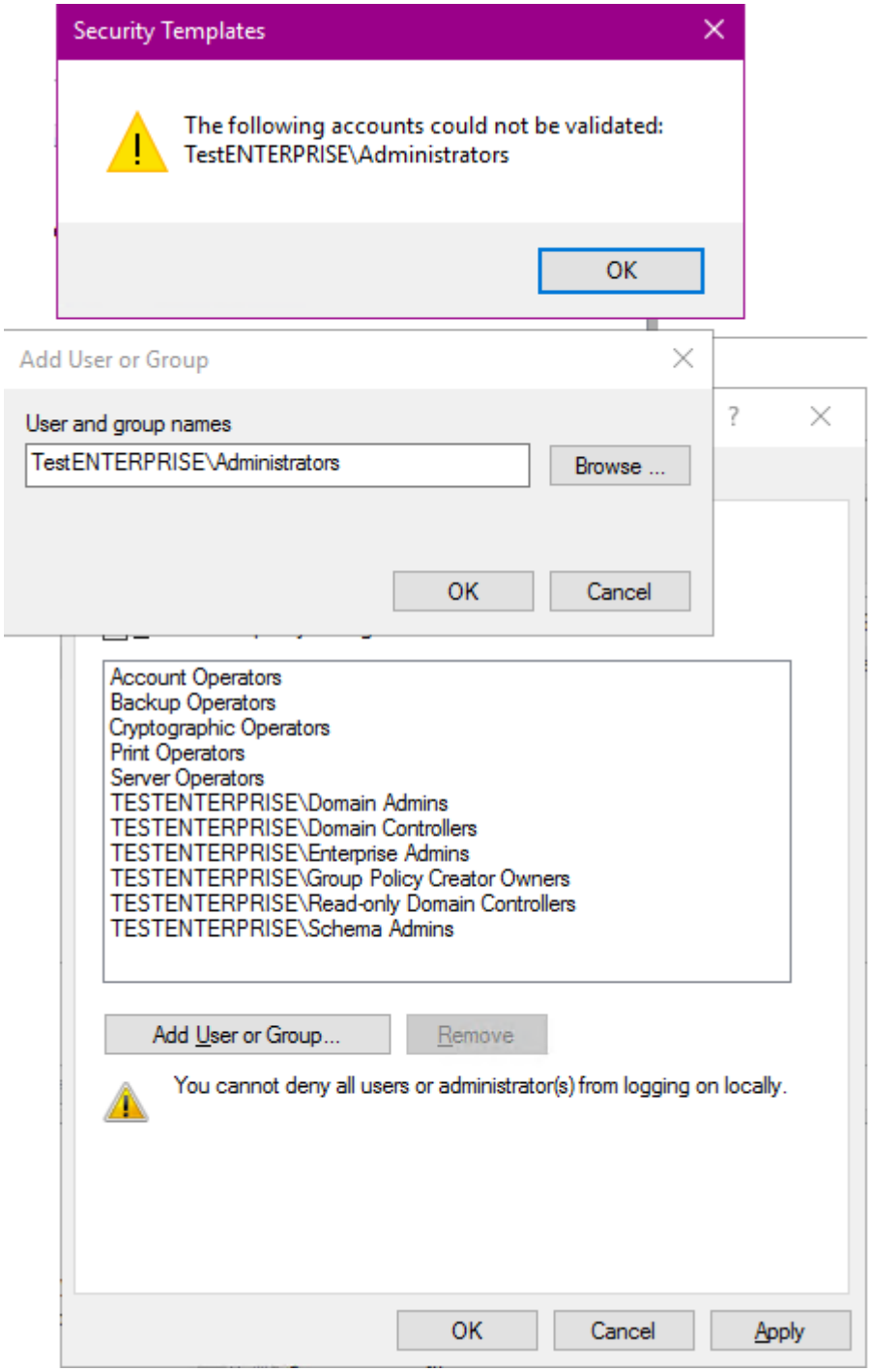


i) Deny Log on as a batch job for the following groups:

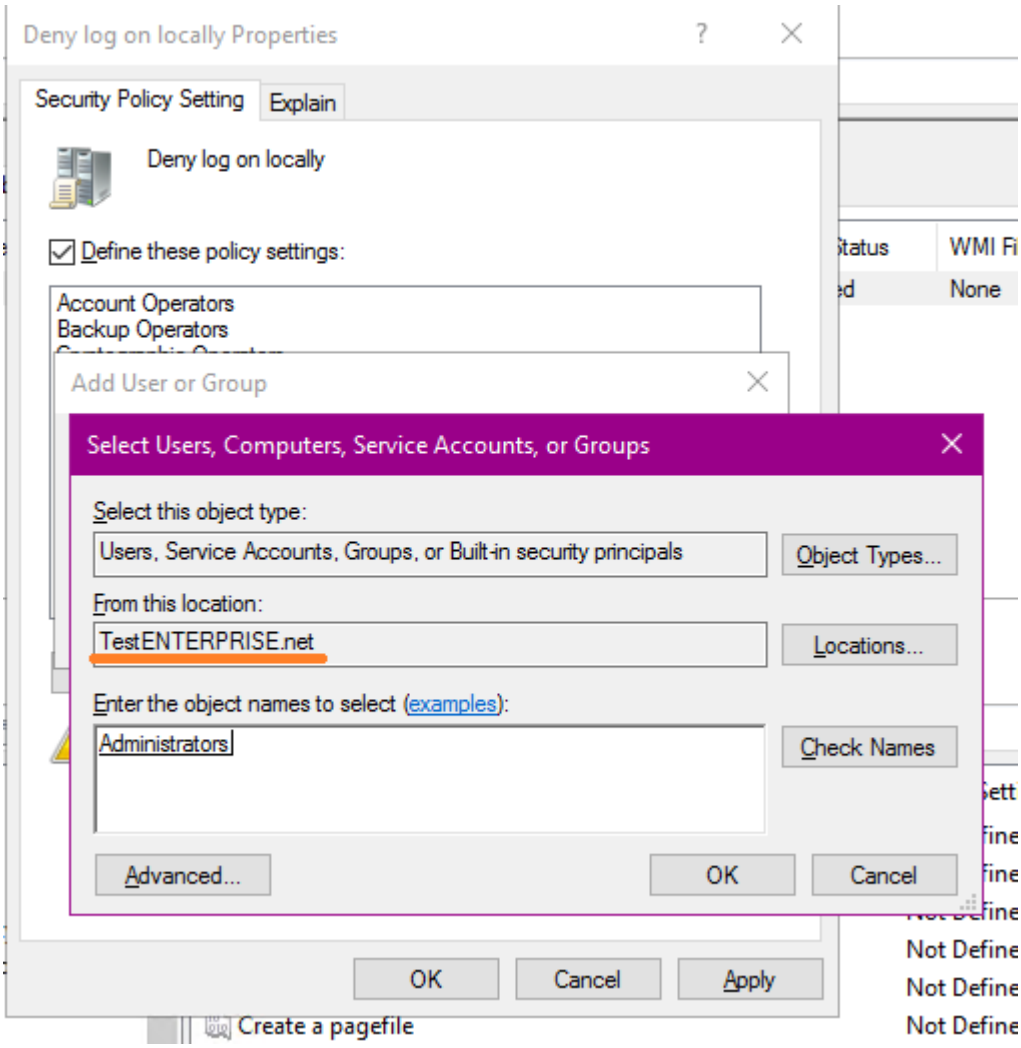

Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Polic
Windows Firewall with Advanced
Network List Manager Policies
Wireless Network (IEEE 802.11) P
Public Key Policies
Software Restriction Policies
Policy
Policy Setting
Allow log on through Remote Desktop Services Not Defined
Back up files and directories Not Defined
Bypass traverse checking Not Defined
Change the system time Not Defined
Change the time zone Not Defined
Create a pagefile Not Defined
Create a token object Not Defined
Create global objects Not Defined
Create permanent shared objects Not Defined
Create symbolic links Not Defined
Debug programs Not Defined
Deny access to this computer from the network Not Defined
Deny log on as a batch job Not Defined
Deny log on as a service Not Defined
Deny log on locally Not Defined
Deny log on through Remote Desktop Services Not Defined
Enable computer and user accounts to be trusted for delega... Not Defined
Force shutdown from a remote system Not Defined
Generate security audits Not Defined
Impersonate a client after authentication Not Defined
Increase a process working set Not Defined
Increase scheduling priority Not Defined


Deny log on as a batch job Properties
Security Policy Setting
Explain
Deny log on as a batch job
Define these policy settings:
Account Operators
Administrators
Backup Operators
Cryptographic Operators
Print Operators
Server Operators
TESTENTERPRISE\Domain Admins
TESTENTERPRISE\Domain Controllers
TESTENTERPRISE\Enterprise Admins
TESTENTERPRISE\Group Policy Creator Owners
TESTENTERPRISE\Read-only Domain Controllers
TESTENTERPRISE\Schema Admins
Add User or Group...
Remove
OK
Cancel
Apply

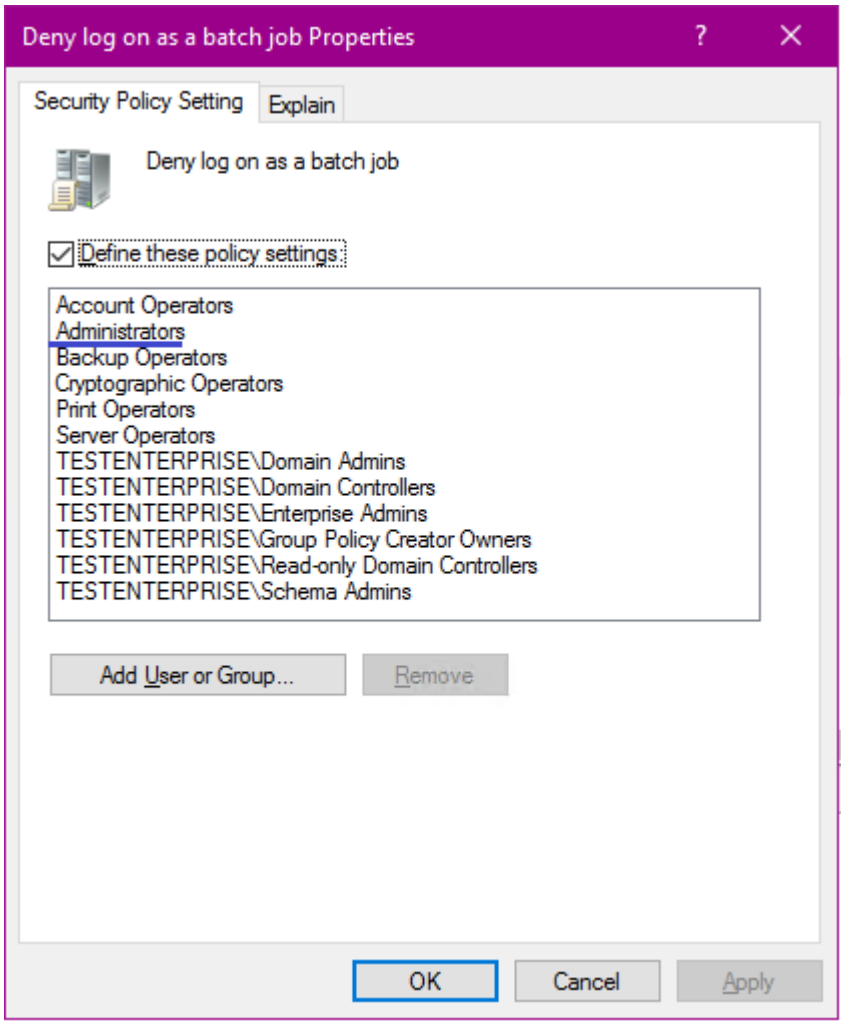
Attention! MS's article states that we must add "DOMAIN\Administrators" group (TestENTERPRISE\Administrators) to this policy setting – but I failed to do it: if I type the TestENTERPRISE\Administrators and press OK I get the following error:



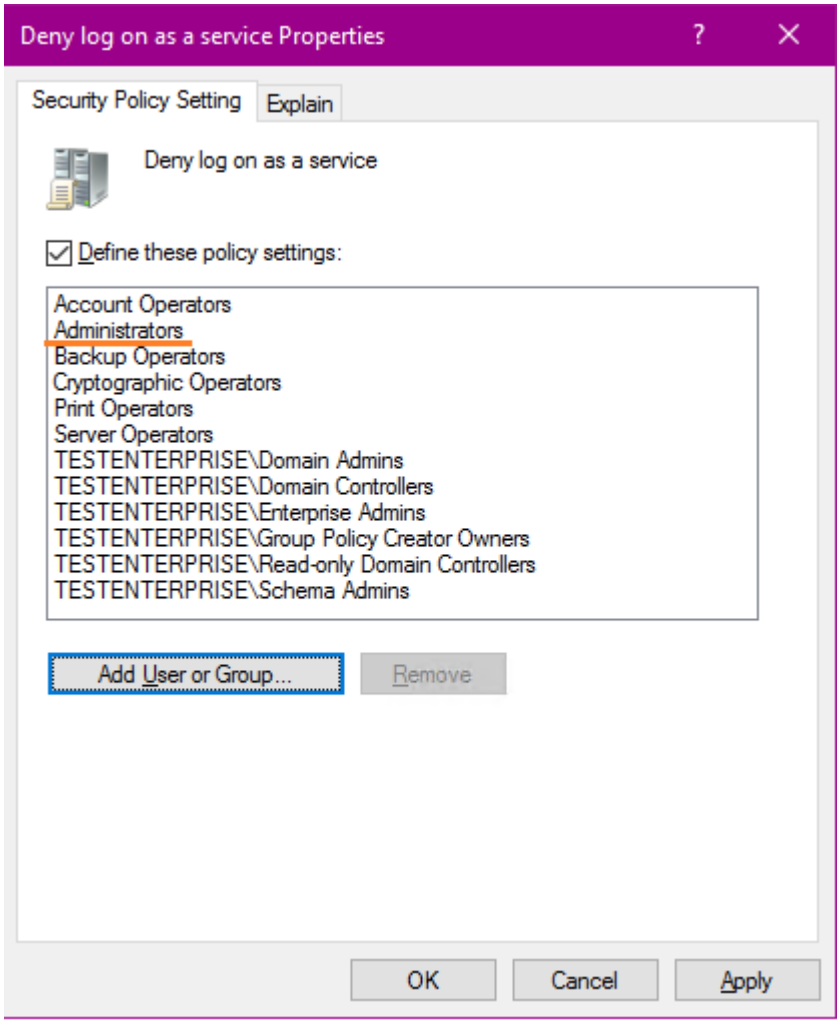
– if I search for the Administrators group IN THE TestNTERPRISE domain I see that it is the LOCAL Administrators group which gets added to the gpo once I click OK:



In fact many other groups (Server Operators, Backup Operators…) are being added in the same way: you search for them in the domain but after adding they look as the local groups: the problem is that for these particular groups the goal is to add exactly these LOCAL groups and only one group – DOMAIN\Administrators – must be added as the domain group and I don't know how to do it… I've asked this question on github.com but as of this writing no answers have been published yet there so in this situation I see only two possible "workarounds": 1) simply to omit DOMAIN\Administrators from this and in the next gpo setting (*Deny log on as a service*) or 2) add the local Administrators group to the list – the latter can (and I think will) lead to negative consequences because a) some services may need to be running under administrative user accounts and/or a scheduled task may require administrative credentials (as was discussed on github). Let's try the second option and see how it will work. Here's the final list of groups:



ii) Deny log on as a service



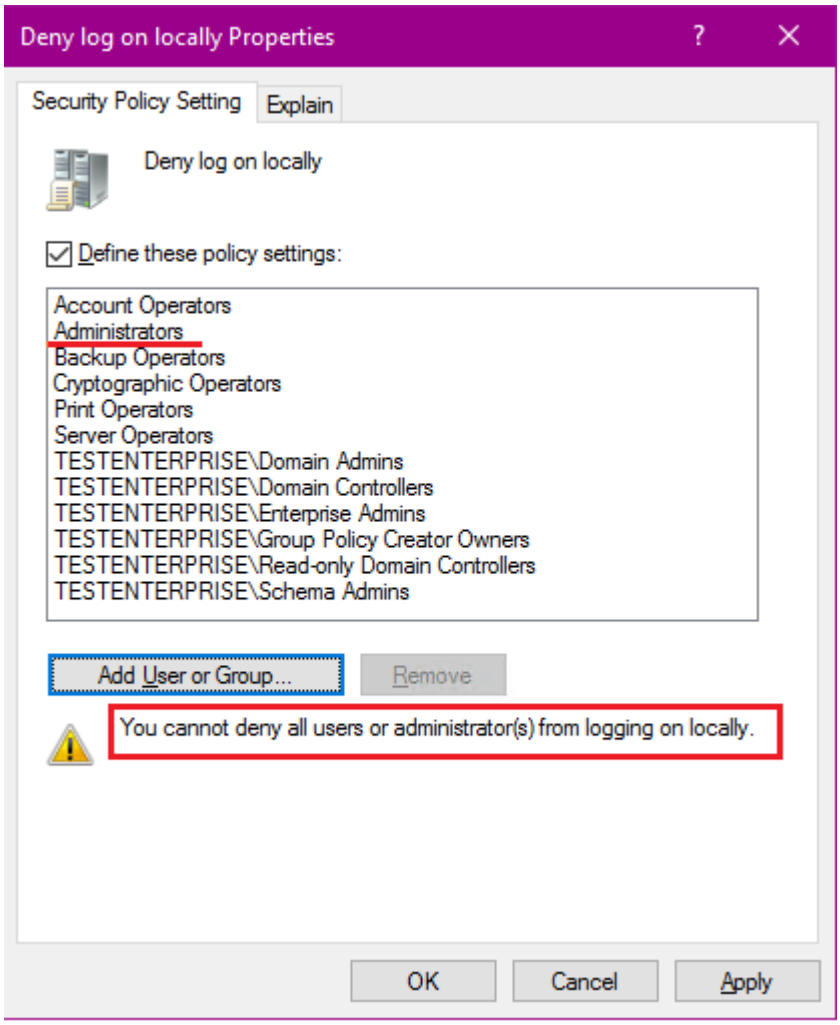
There's no more settings to configure in the **RestrictWorkstationLogon GPO** – let's now see whether the requested goal has been achieved. MS documentation states:

"*7.* ***Restrict Administrators from logging onto lower tier hosts****. In this section, we will configure group policies to prevent privileged administrative accounts from logging onto lower tier hosts.*"

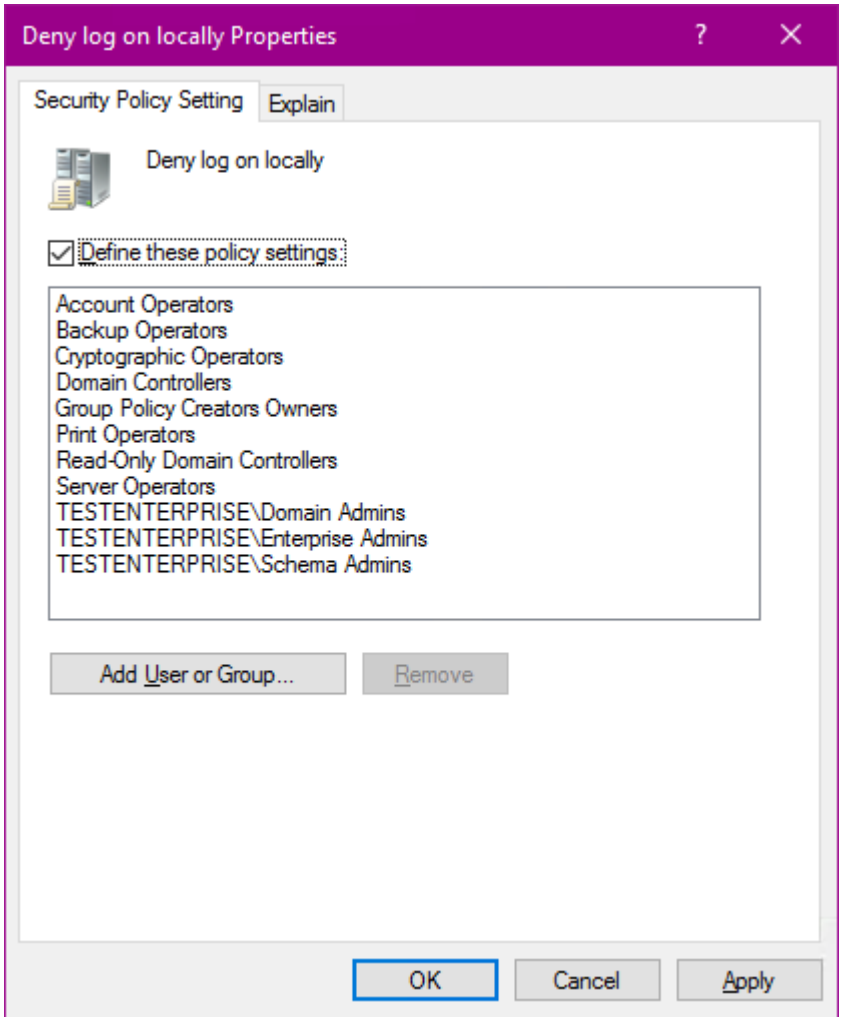
Obviously this goal can not be met by configuring (even with the LOCAL Administrators group added!) only the *Deny log on as a batch job* and *Deny log on as a service* policy settings: it is the ***Deny log on localy*** policy setting that really controls who can or can not log onto workstations! I'm definitely going to have to take the additional step:

I advise to add only domain accounts on the tab below as these are domain accounts that must be protected – NOT the local ones!!!

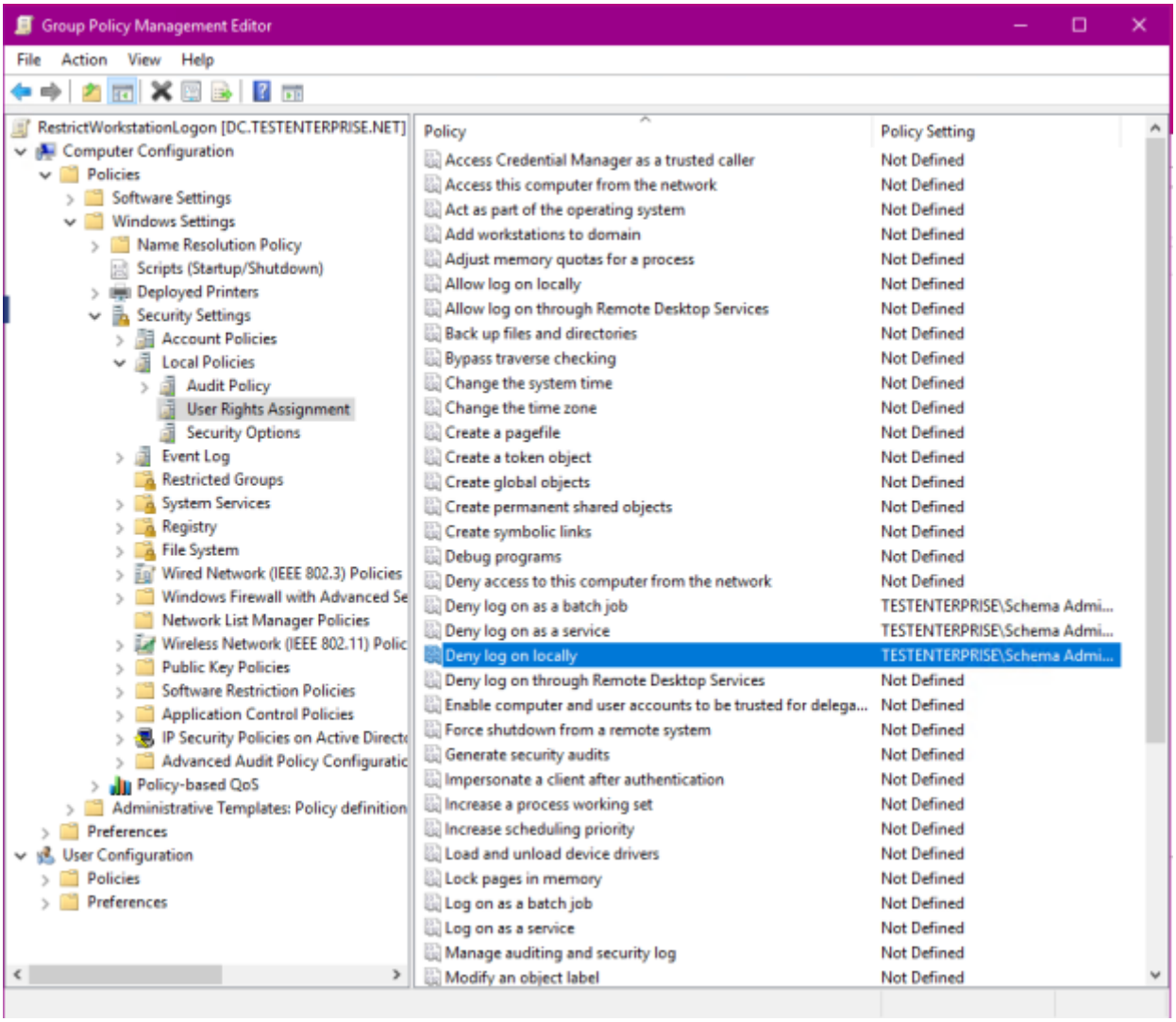
iii) Deny log on locally



As you see it's not possible to configure *Deny log on locally* policy setting the same way as the previous two settings so I'm left with the other option (the first option discussed earlier) – to omit local Administrators group from the group list:



Here’re the all configured policy settings:



In the next part we'll see how the newly installed privileged access workstation work using such custom configuration.