Assigning rights and permissions using Active Directory and Group Policy

Overview

This guide will explain how to create and link a Group Policy in Active Directory. In the example to be shown we are applying **Principle of Least Privilege**. This principle establishes that users, devices, and applications be given only the minimum amount of privilege necessary for them to complete their task.

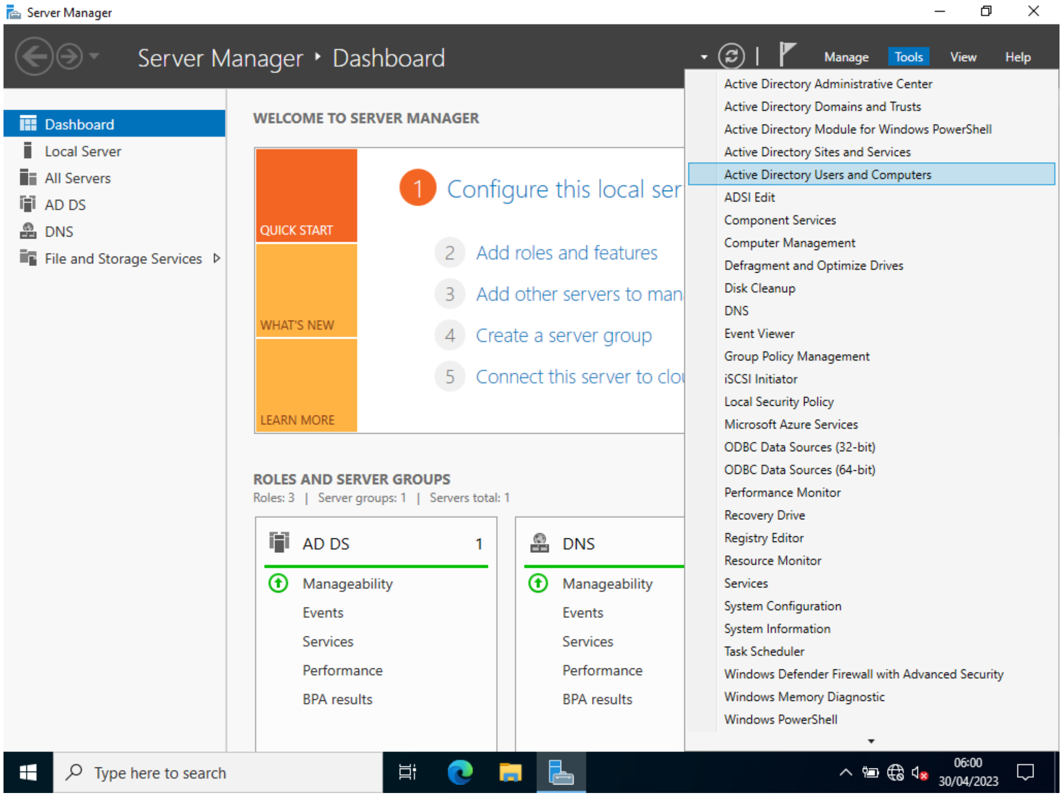
In a Windows Domain, privileges are handled from the Domain Controller server using Active Directory and Group Policy. In a Windows Workgroup, privileges are handled from Local Users and Groups, which is used in smaller networks but requires permissions to be assigned to each system the user needs access to - there’s no central console to configure all systems at once.

Managing permissions using Active Directory and Group Policy

Task 1: Creating a Security Group

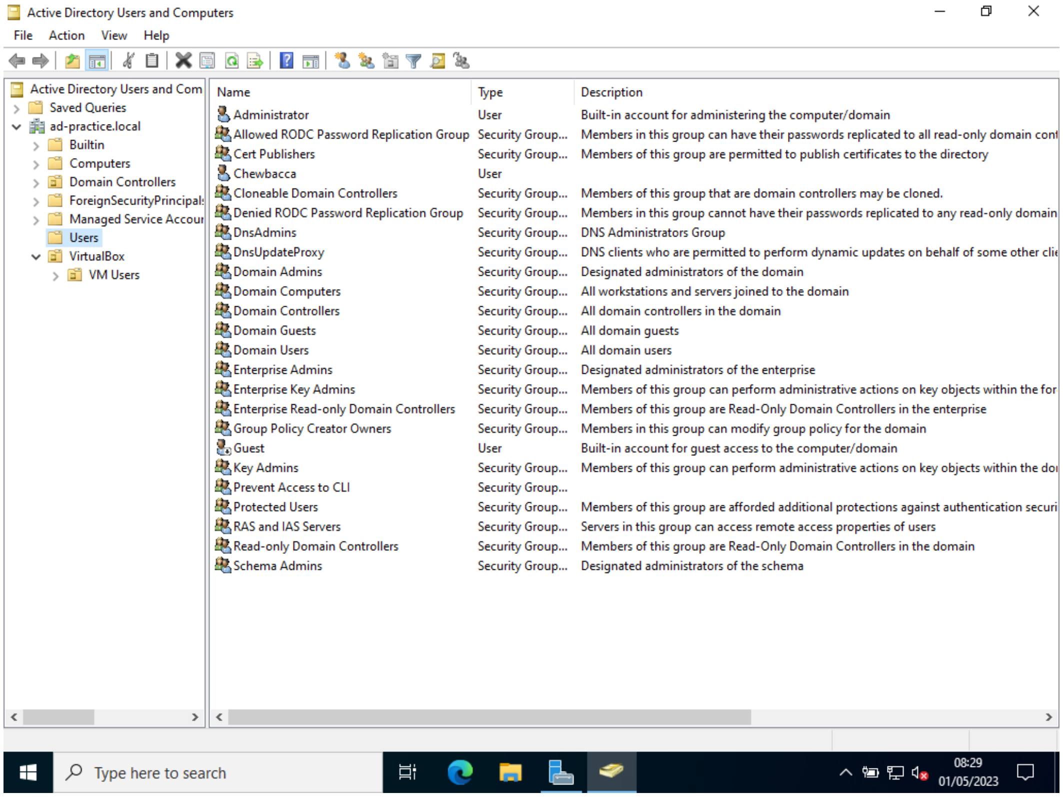
In this scenario, we will be applying certain rights and permissions which prevent users from accessing the command prompt.

1. Inside your chosen hypervisor (e.g. VirtualBox) connect to your Domain Controller VM and login. The Server Manager should open automatically. From the Server Manager window, click **Tools** > **Active Directory Users and Computers**.



Accessing AD Users and Computers via Server Manager

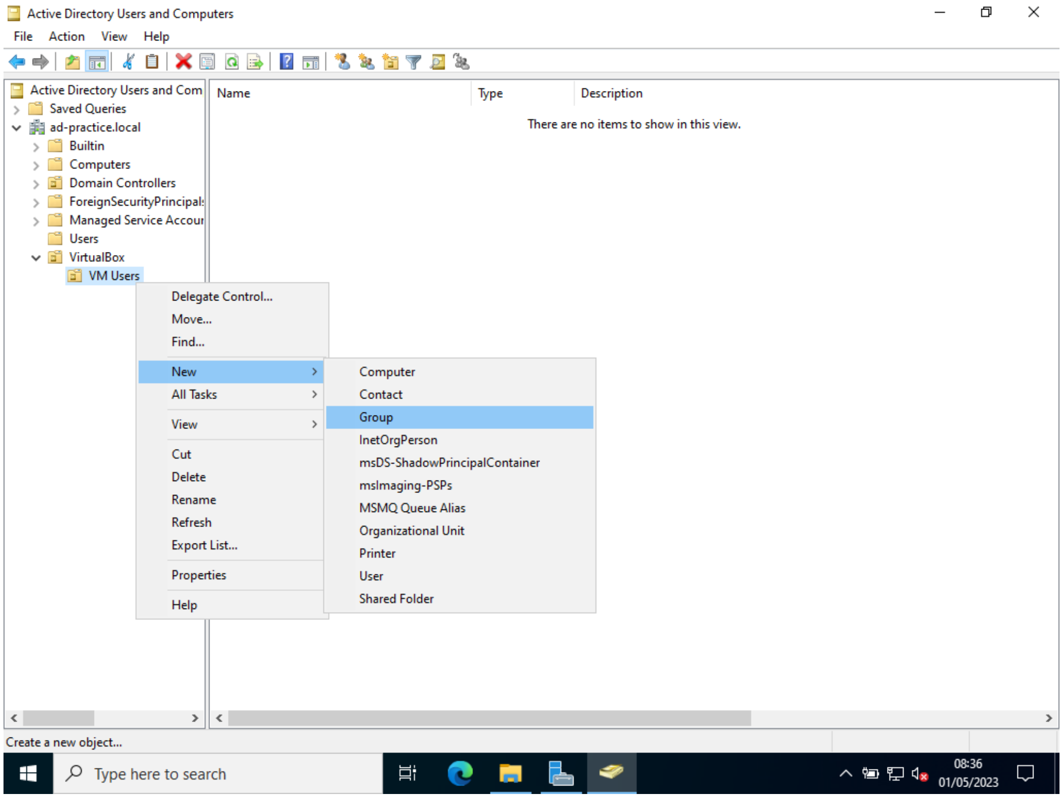
2. We are first going to create an **Organisational Unit (OU)** to organise our users and groups. **Right-click your domain on the left pane** (e.g. ad-practice.local) > **New** > **Organizational Unit**. Give it a relevant name for our purposes, in my case I called the OU “VirtualBox” and then created an OU inside it called “VM Users”.



Name	Type	Description
Administrator	User	Built-in account for administering the computer/domain
Allowed RODC Password Replication Group	Security Group...	Members in this group can have their passwords replicated to all read-only domain cont
Cert Publishers	Security Group...	Members of this group are permitted to publish certificates to the directory
Chewbacca	User	
Cloneable Domain Controllers	Security Group...	Members of this group that are domain controllers may be cloned.
Denied RODC Password Replication Group	Security Group...	Members in this group cannot have their passwords replicated to any read-only domain
DnsAdmins	Security Group...	DNS Administrators Group
DnsUpdateProxy	Security Group...	DNS clients who are permitted to perform dynamic updates on behalf of some other clie
Domain Admins	Security Group...	Designated administrators of the domain
Domain Computers	Security Group...	All workstations and servers joined to the domain
Domain Controllers	Security Group...	All domain controllers in the domain
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrators of the enterprise
Enterprise Key Admins	Security Group...	Members of this group can perform administrative actions on key objects within the for
Enterprise Read-only Domain Controllers	Security Group...	Members of this group are Read-Only Domain Controllers in the enterprise
Group Policy Creator Owners	Security Group...	Members in this group can modify group policy for the domain
Guest	User	Built-in account for guest access to the computer/domain
Key Admins	Security Group...	Members of this group can perform administrative actions on key objects within the dor
Prevent Access to CLI	Security Group...	
Protected Users	Security Group...	Members of this group are afforded additional protections against authentication securi
RAS and IAS Servers	Security Group...	Servers in this group can access remote access properties of users
Read-only Domain Controllers	Security Group...	Members of this group are Read-Only Domain Controllers in the domain
Schema Admins	Security Group...	Designated administrators of the schema

Creating an OU

3. Inside our newly created OU(s) we will **create a Security group**: **right-click your OU** > **New** > **Group**.



There are no items to show in this view.

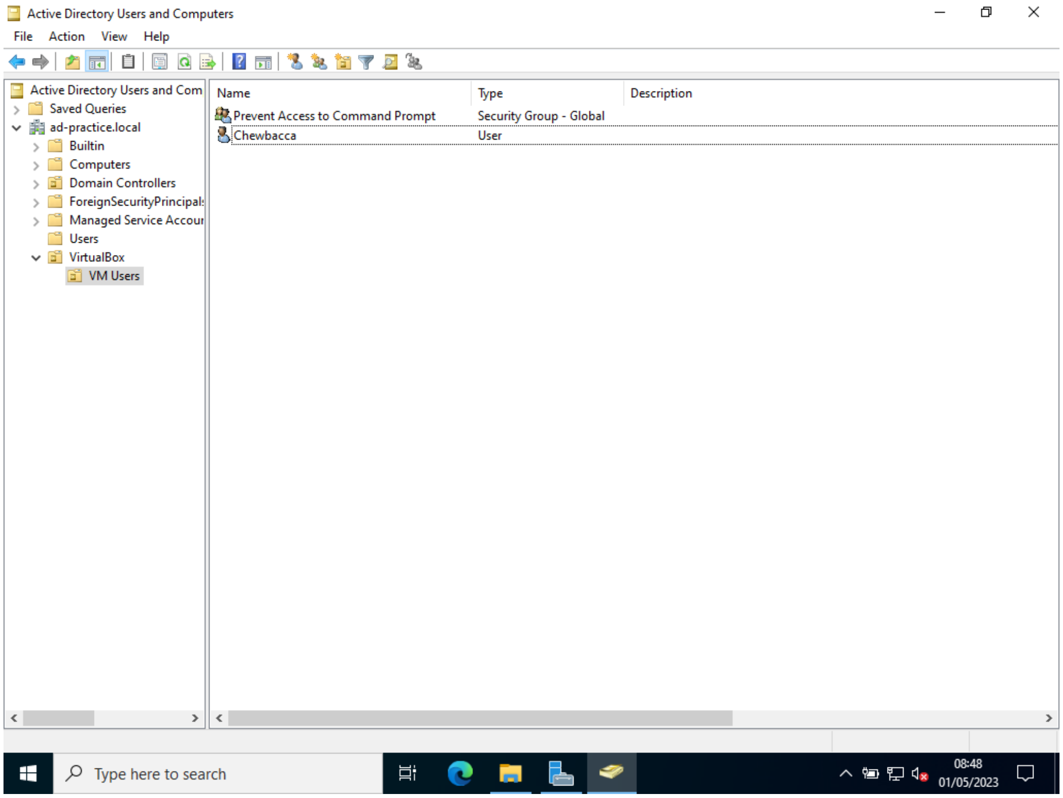
Create a new object...

💡 Active Directory works with Group Policy as follows: permissions are assigned to Groups, then users are added to one or more Groups. The User inherits their permissions from the Groups they belong to.

4. In the **New Object - Group** dialog box, create a **Group name**, then click **OK** - I have given the name “Prevent Access to Command Prompt”.

5. **Repeat step 3** again but instead of Group, click **User**. In the **New Object - User** dialog box, provide a **first name** (and a last name if you like) and the **User logon name** of the User Account you created for your Windows 10 Enterprise VM.

6. Click **Next**, provide a password, confirm it. To keep things simple for our homelab, tick the ***Password never expires*** checkbox. Click **Next,** review the details then click **Finish**.



Name	Type	Description
Prevent Access to Command Prompt	Security Group - Global	
Chewbacca	User	

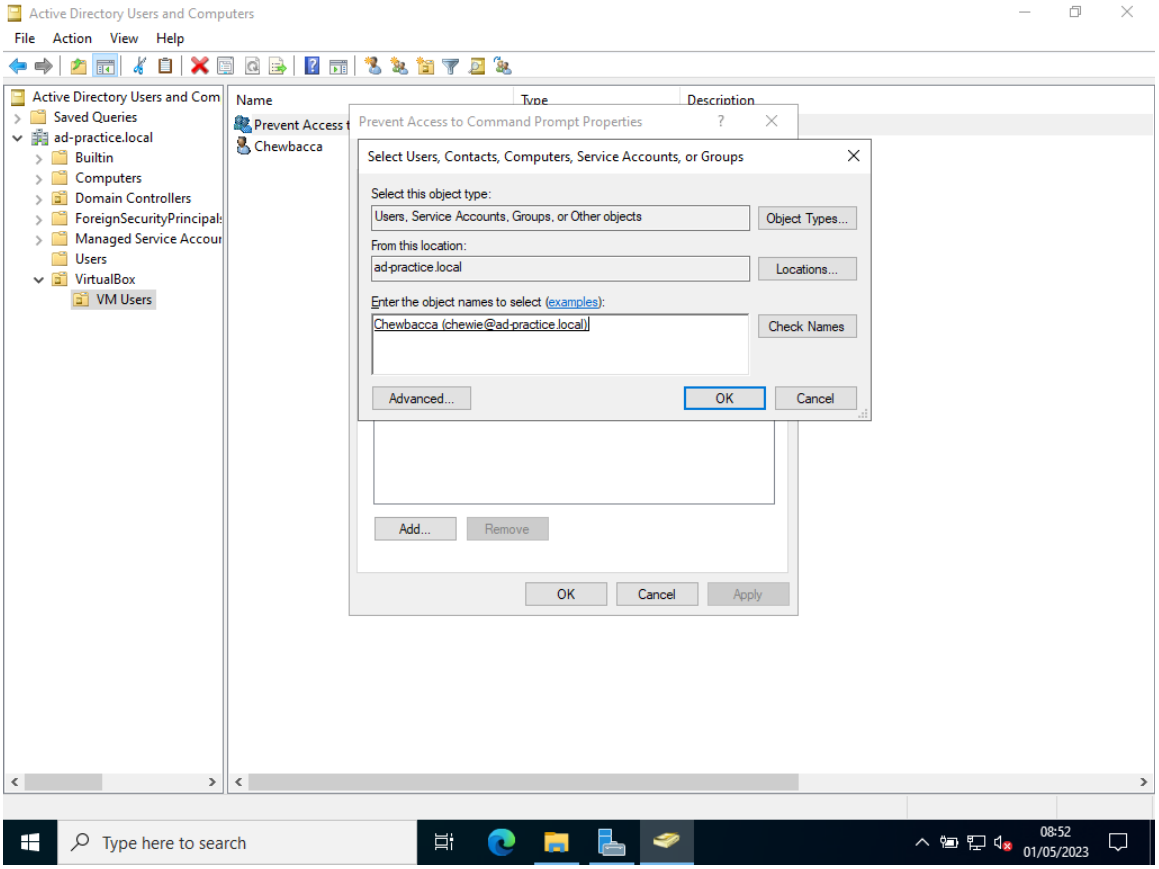
Populated OU with New User and Security group

7. **Right-click *Prevent Access to Command Prompt* > Properties**.

5. From the ***Prevent Access to Command Prompt* Properties** dialog box, select the **Members** tab then click **Add**.

6. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, type in the username of the user we created in our OU, then click **Check Names**.

7. Click **OK** and **OK** again in the ***Prevent Access to Command Prompt* Properties** dialog box. The user is now a member of this newly created Security group, inside our OU, inside our Domain.



Select this object type: Users, Service Accounts, Groups, or Other objects

From this location: ad-practice.local

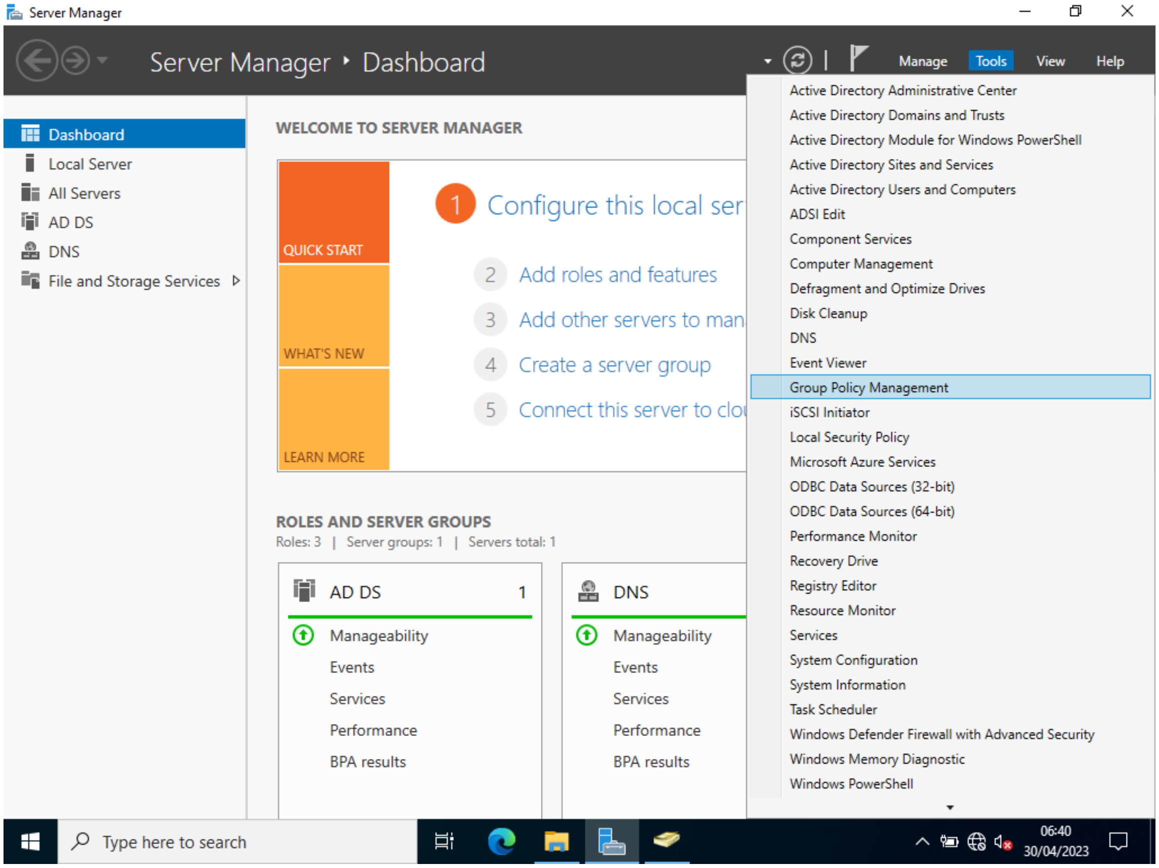
Enter the object names to select (examples): Chewbacca (chewie@ad-practice.local)

Adding the User to our Security group

Task 2: Setting Group Policy for the Security Group

After we have created the Security group and added the relevant members, we can now apply permissions to the group using **Group Policy**.

11. In Server Manager, click **Tools** > **Group Policy Management**.



Accessing Group Policy Management via Server Manager

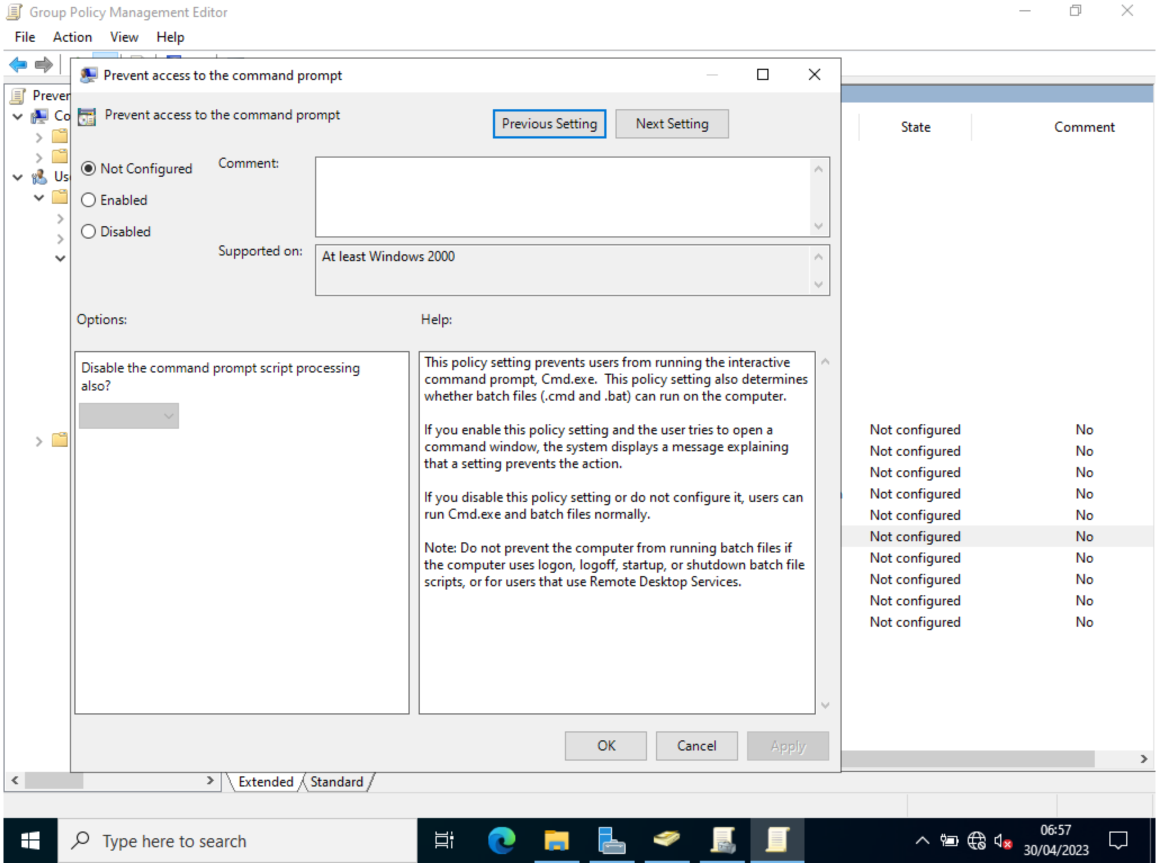
12. In the **Group Policy Management** window, find the OU we created, **right-click the OU** > **Create a GPO in this domain, and Link it here…**

13. In the **New GPO** dialog box, type in the same name you gave your Security group in Active Directory Users and Computers (e.g. *Prevent Access to Command Prompt*), then click **OK**. The new GPO will populate under the OU on the left pane.

11. Now **right-click your new GPO** > click **Edit**. A **Group Policy Management Editor** window will open and it is from here that we can apply the policies we need for our Security group.

12. Expand the following nodes: **User Configuration** > **Policies** > **Administrative Templates** > **System**.

13. On the right pane, **right-click Prevent access to the command prompt** > **Edit**.



Prevent access to the command prompt

● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Disable the command prompt script processing also?

Help:

This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.

If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.

Note: Do not prevent the computer from running batch files if the computer uses logon, logoff, startup, or shutdown batch file scripts, or for users that use Remote Desktop Services.

State	Comment
Not configured	No
Not configured	No
Not configured	No
Not configured	No
Not configured	No
Not configured	No
Not configured	No
Not configured	No
Not configured	No
Not configured	No

06:57
30/04/2023

Prevent access to the command prompt window accessed via GPM Editor

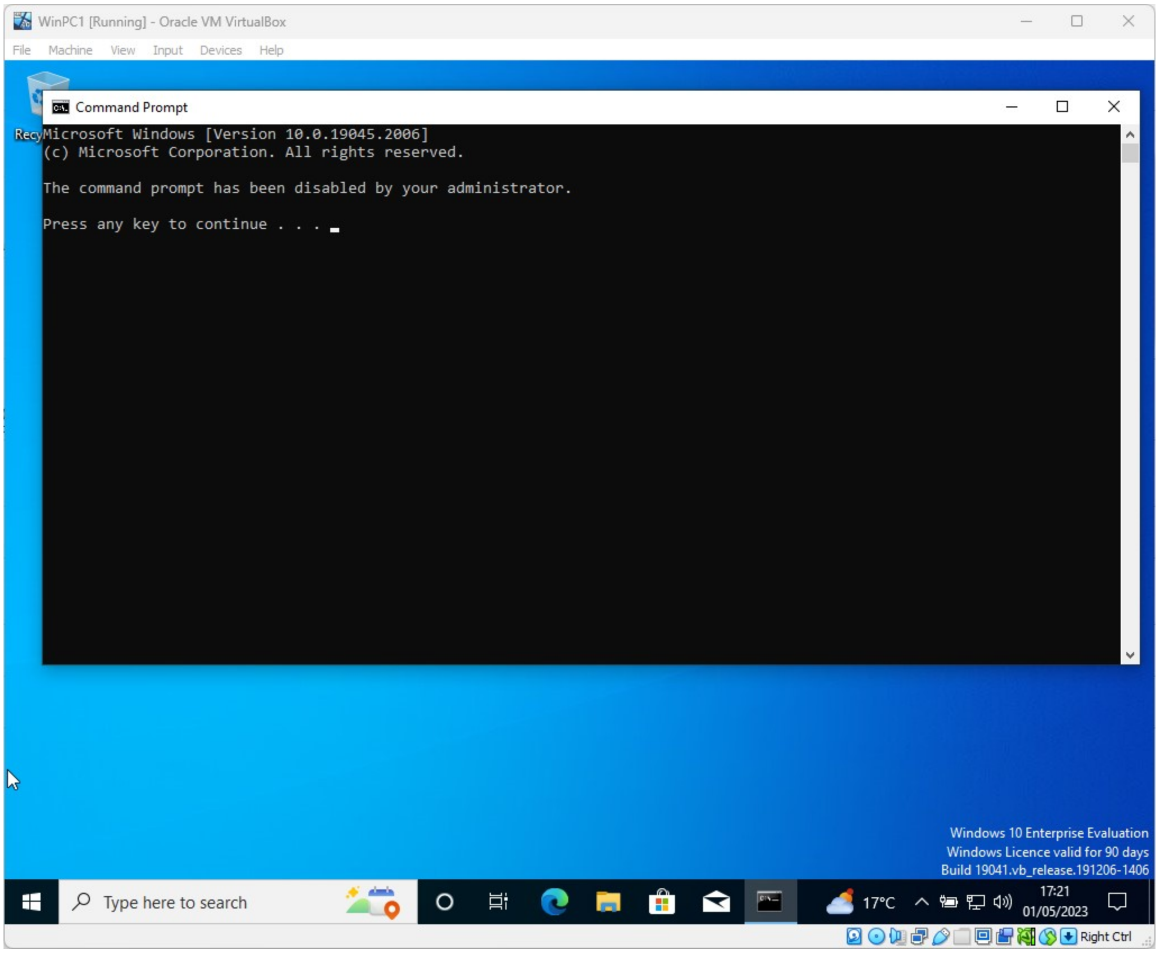
17. Inside the **Prevent access to the command prompt** window, click the **Enabled** radio button > click **OK**. Close the **Group Policy Management Editor** window.
18. In the **Group Policy Management** window you will see that our GPO is now linked to the OU. The permissions we applied to the **Prevent Access to Command Prompt GPO** can now begin to apply to the users listed in the OU.

> 💡 Please note that GPO can take a while for it to be applied to users but there are ways to force the update if necessary. The users may also need to log off and log back in for it to take effect.

Task 3: Test the Group Policy for your created User Account

We will now test to see if the GPO we applied to our OU has taken effect for the User Account.

19. Connect to your VM where we installed Windows 10 Enterprise and logon with the User Account we added to the OU.
20. Type in "**cmd**" into the search bar to open the command prompt, you should find that the GPO has taken effect and you will not be able to perform commands at the command prompt as a Standard User.


WinPC1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Command Prompt
Type here to search
17°C
17:21
01/05/2023
Windows 10 Enterprise Evaluation
Windows Licence valid for 90 days
Build 19041.vb_release.191206-1406
Right Ctrl

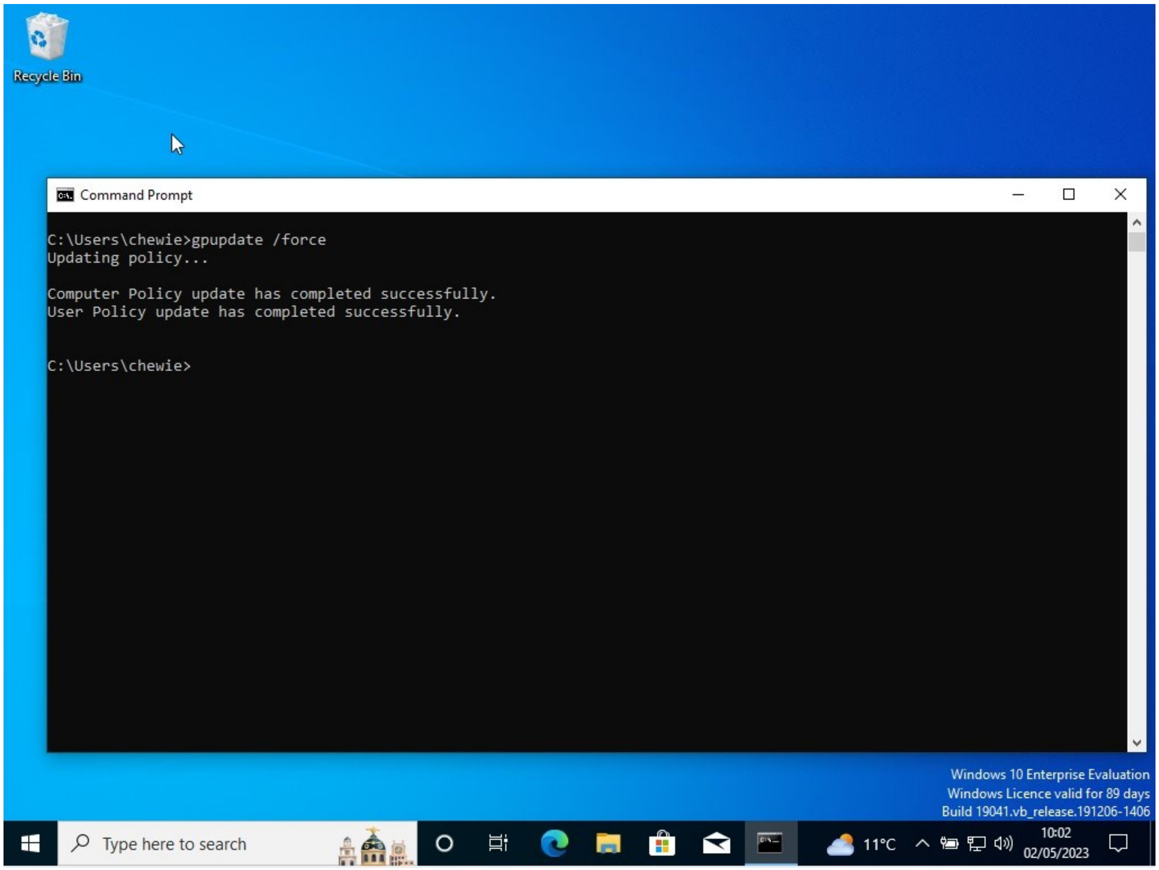
```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

The command prompt has been disabled by your administrator.

Press any key to continue . . .
```

GPO taken effect for users in the OU - no access to command prompt

21. If the GPO has yet to take effect for the user, you can have the update take effect immediately. In the command prompt type **gpupdate /force** then press **enter**.



Recycle Bin
Command Prompt
Windows 10 Enterprise Evaluation
Windows Licence valid for 89 days
Build 19041.vb_release.191206-1406
Type here to search
11°C
10:02
02/05/2023

```
C:\Users\chewie>gpupdate /force
Updating policy...

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


C:\Users\chewie>
```

Forcing GPO update via the ***gpupdate /force*** command

22. Close the Command Prompt window, reopen it, you should then see the same output in the previous screenshot indicating “The command prompt has been disabled by your administrator”.

> 💡 **As you’re likely to want to use the command prompt on your Windows 10 host machine going forward, it’s best to disable this GPO inside Active Directory.**

Task 4: Disabling the Prevent Access to Command Prompt GPO

23. Back in your Domain Controller machine, navigate to **Server Manager** > **Tools** > **Group Policy Management**.

24. From the Group Policy Management console, **navigate to the domain you created** > expand the **OU** > **repeat steps 14-16** > in the Prevent Access to Command Prompt window, click the **Disabled** radio button > click **Apply** then **OK**. Close the **Group Policy Management Editor** window.

25. From here we can now log back in to our Windows 10 host machine, and see if these changes have taken effect.