StackFull IT Runbook

This runbook documents the IT Pre-onboarding process for setting up a new machine for new employees at StackFull. This setup ensures each machine is secure, compliant with IT policies, and ready for use immediately. It will go over the procedures on how to connect your workstation to the correct domain, create new users and groups for different departments, how to create and change group policies, search logs through Event Viewer, and write scripts on Powershell.

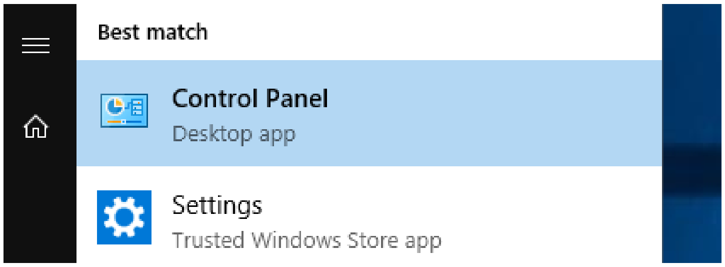
Name: John Doe

Role: Sales Associate

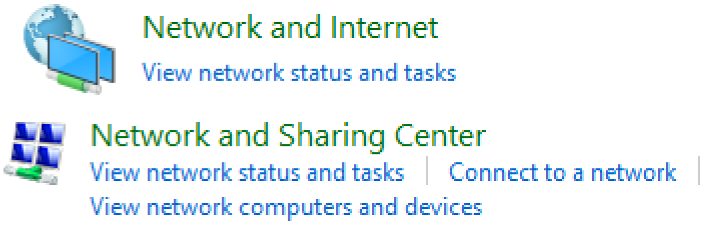
Department: Sales

1. Joining a Domain

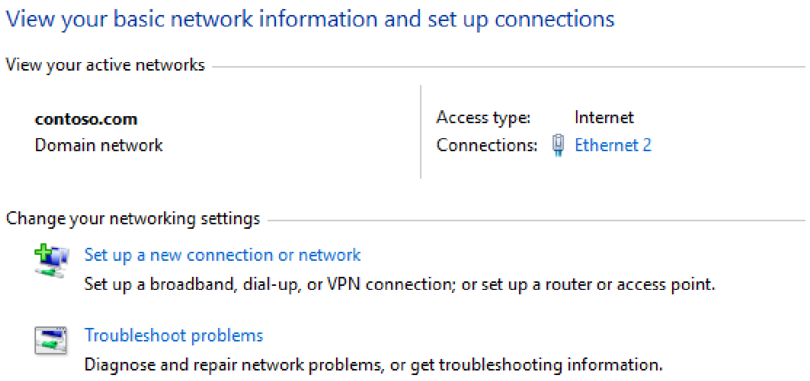
Log into the computer using the username and password administrator/Pa$$w0rd. Once you're logged in, you want to make your way to the Control Panel. Click the Windows button on the screen or on your keyboard, and search "Control Panel" and open it.



Once you're in the Control Panel, click on "Network and Internet" and then "Network and Sharing Center."


Network and Internet
View network status and tasks
Network and Sharing Center
View network status and tasks
Connect to a network
View network computers and devices

Within the Network and Sharing Center, click on the blue "Ethernet 2" and click on Properties so you can edit the IPv4 Address. Within Properties, double click Internet Protocol Version 4 (TCP/IPv4).



View your basic network information and set up connections

View your active networks

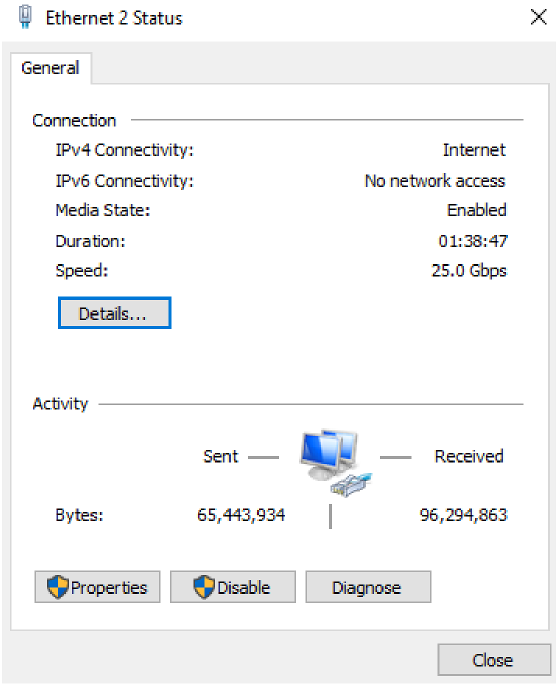
contoso.com
Domain network

Access type: Internet
Connections: Ethernet 2

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.



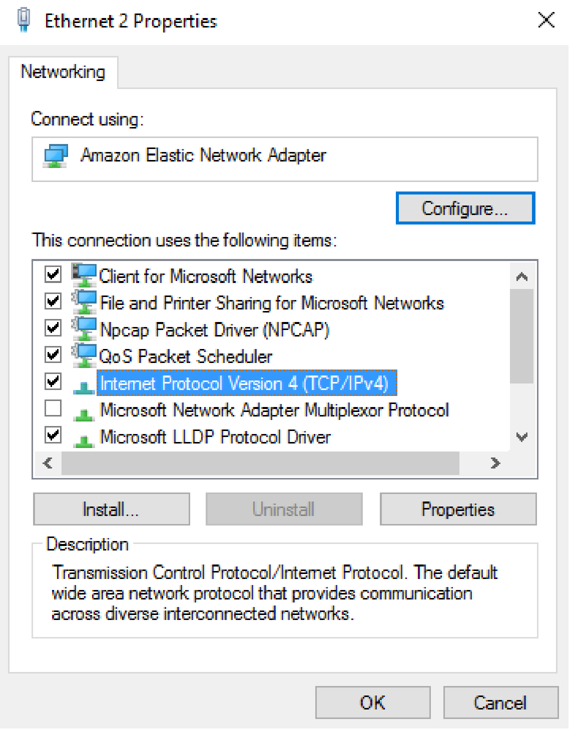
Ethernet 2 Status

Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	01:38:47
Speed:	25.0 Gbps

Activity

	Sent	Received
Bytes:	65,443,934	96,294,863



Connect using:

Amazon Elastic Network Adapter

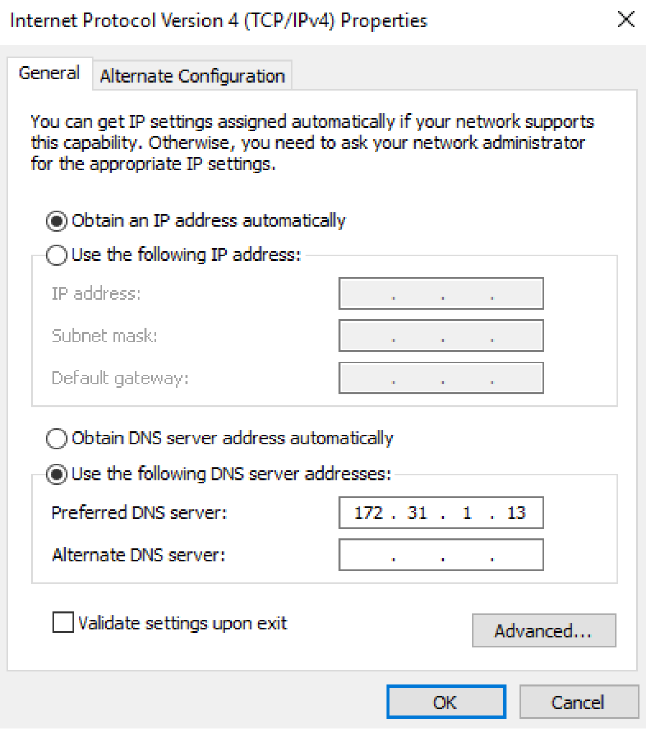
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Npcap Packet Driver (NPCAP)
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Within Internet Protocol Version 4 (TCP/IPv4), change the DNS server address to 172.31.1.13, which was retrieved through cmd.exe in the main server using the ipconfig command, then click apply and OK to confirm the change.

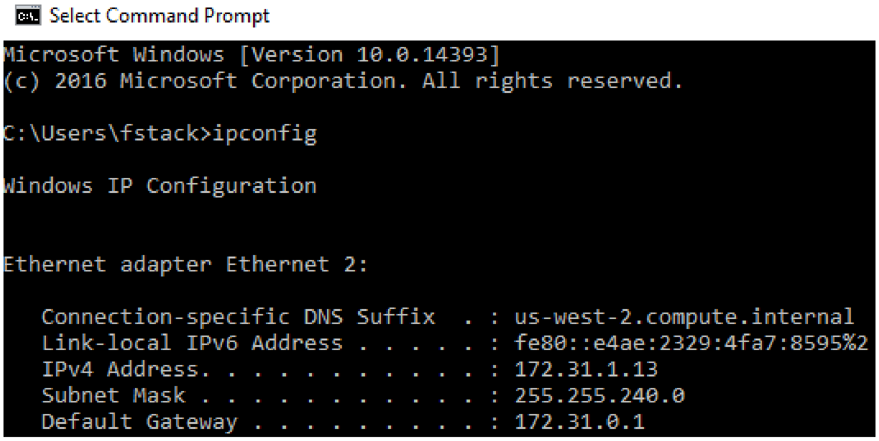


You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

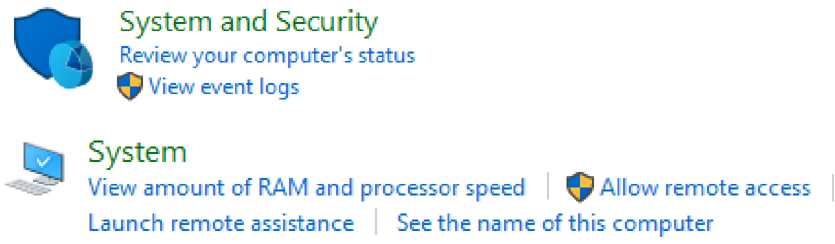
○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: 172 . 31 . 1 . 13
Alternate DNS server: . . .

□ Validate settings upon exit

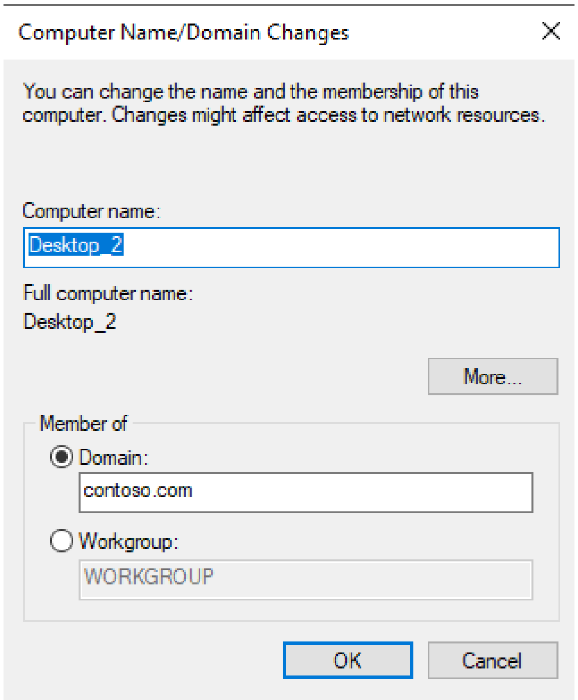


```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\fstack>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : us-west-2.compute.internal
   Link-local IPv6 Address . . . . . : fe80::e4ae:2329:4fa7:8595%2
   IPv4 Address. . . . . . . . . . . : 172.31.1.13
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.31.0.1
```

Now that you’ve changed the IP address, go back to the Control Panel and click into “System and Security” and then “System.”


System and Security
Review your computer's status
View event logs
System
View amount of RAM and processor speed
Allow remote access
Launch remote assistance
See the name of this computer

Within the System, click into “Advanced Settings,” and click “Computer Name Change.” Then change the Computer name to Desktop_2 and below that, change the Domain to contoso.com. Now we are officially signed into the contoso domain.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
Desktop_2

Full computer name:
Desktop_2

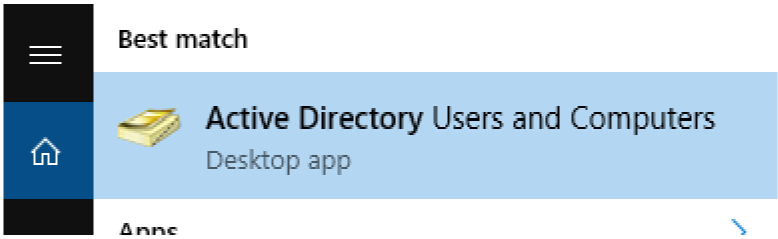
Member of

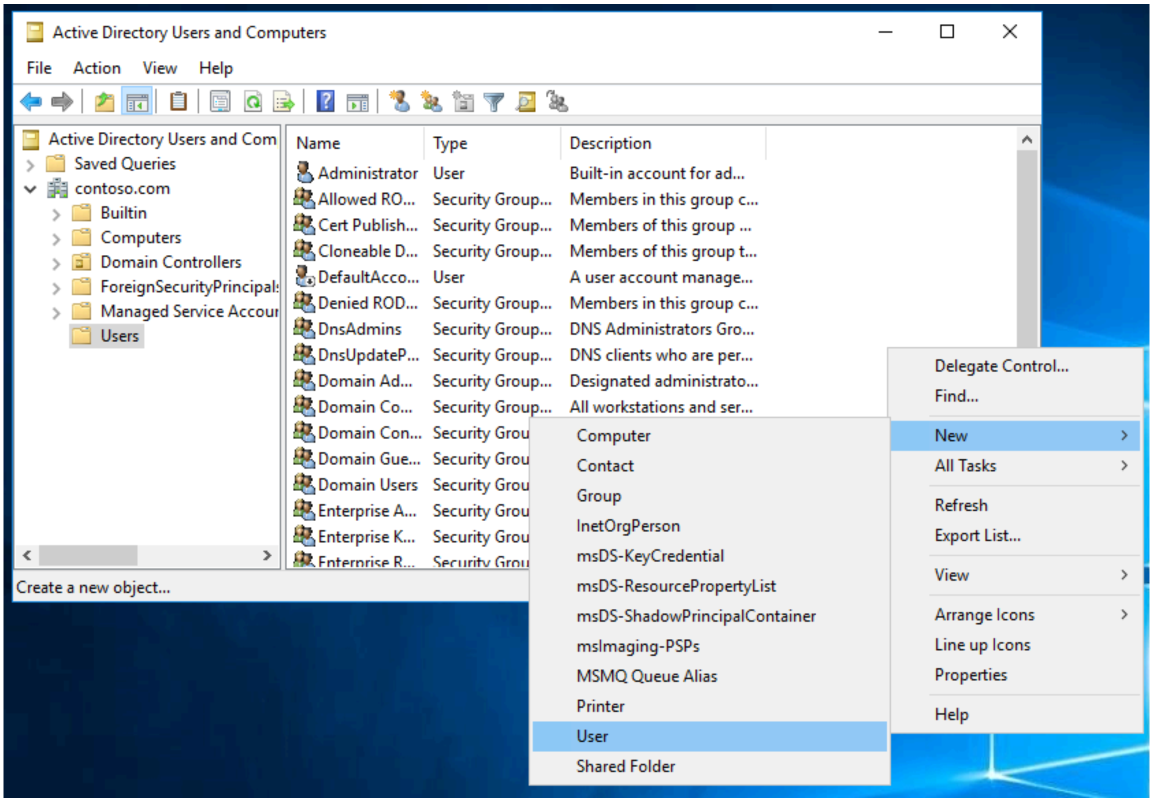
● Domain:
contoso.com

○ Workgroup:
WORKGROUP

2. Create a User

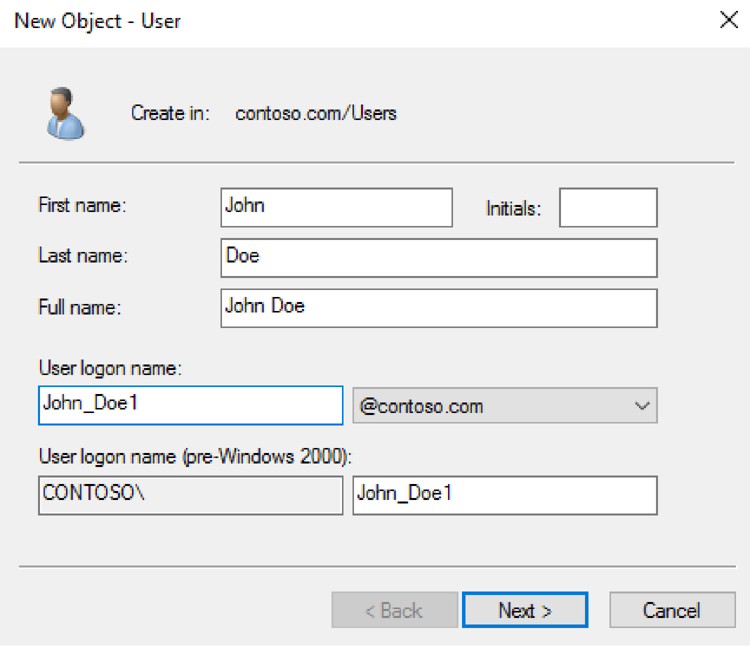
Now that you've changed the computer domain to contoso, switch back to the main server and create a new user for the new hire. Start by clicking the Windows key and search up "Active Directory Users and Computers." Once you're in, click into "Users" and right click the window, hover over "New" and click "User."





Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
DefaultAcco...	User	A user account manage...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Grou	
Domain Gue...	Security Grou	
Domain Users	Security Grou	
Enterprise A...	Security Grou	
Enterprise K...	Security Grou	
Enterprise R...	Security Grou	

This will prompt you to fill in any information regarding the John Doe and create a username, which will be John_Doe1. Once you're done, click next and you'll be prompted to fill out a new password. For this user, you can "Password12345," but it can be changed later on. Click next, and then "Finish" to successfully create the user.



Create in: contoso.com/Users

First name: John

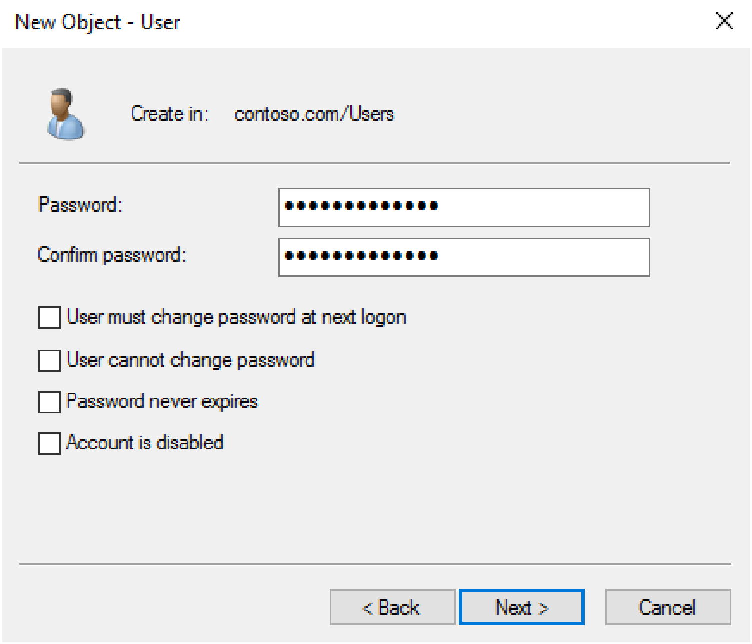
Initials:

Last name: Doe

Full name: John Doe

User logon name: John_Doe1 @contoso.com

User logon name (pre-Windows 2000): CONTOSO\ John_Doe1



New Object - User

Create in: contoso.com/Users

Password: •••••••••••••

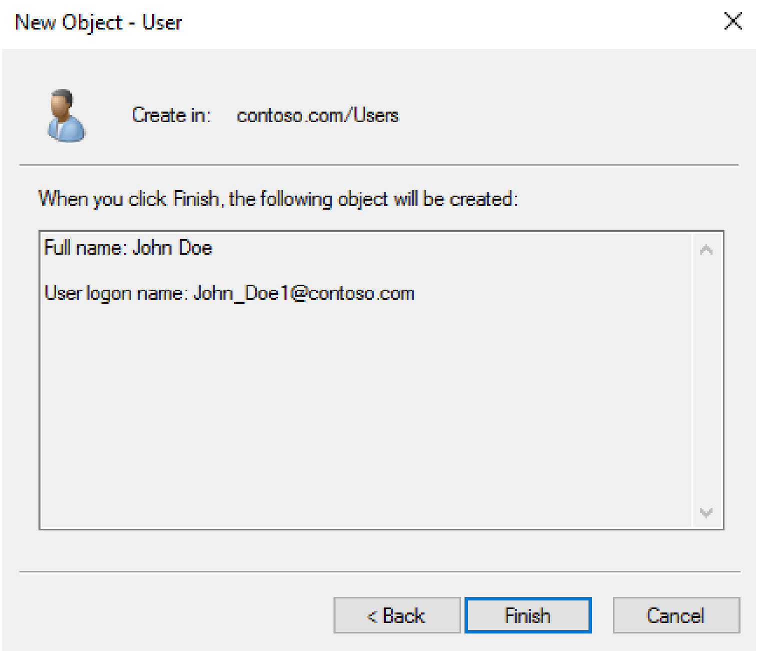
Confirm password: •••••••••••••

□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled



New Object - User

Create in: contoso.com/Users

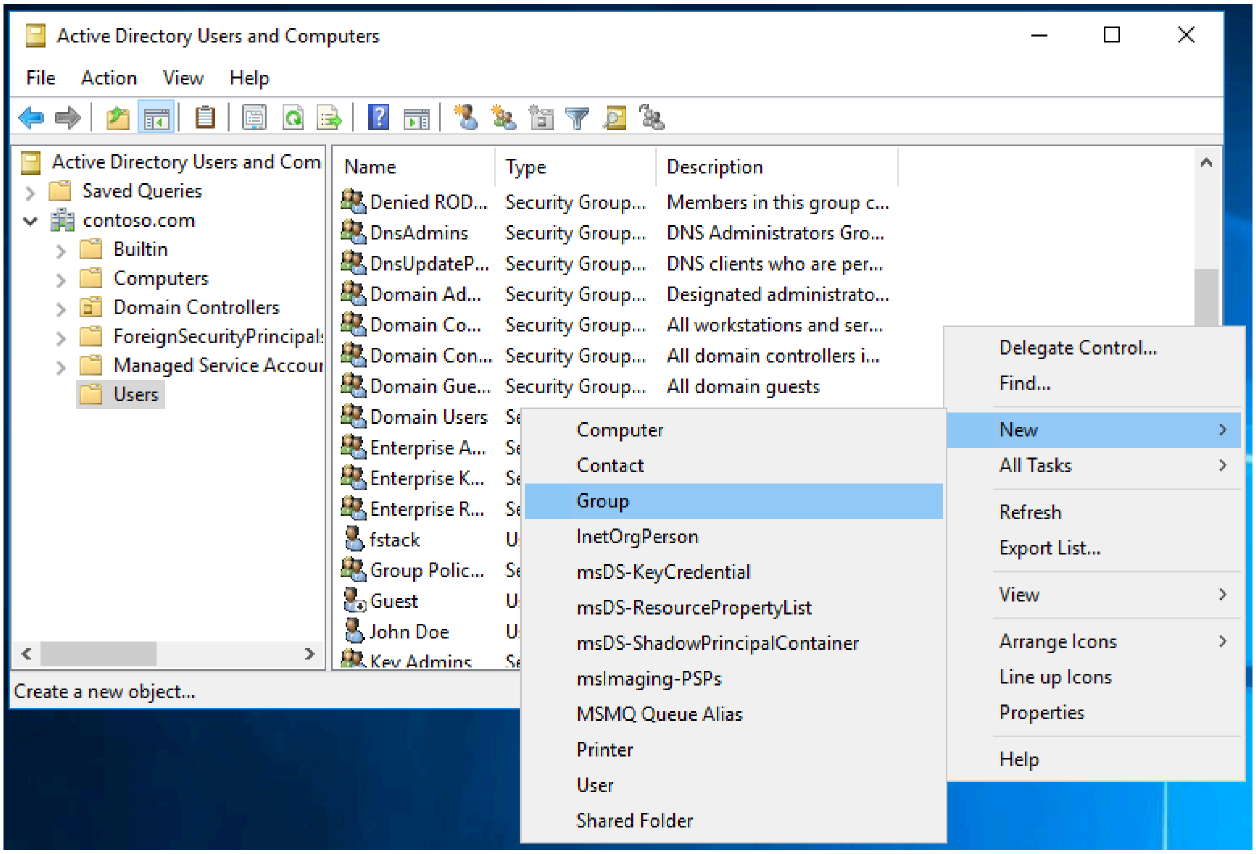
When you click Finish, the following object will be created:

Full name: John Doe

User logon name: John_Doe1@contoso.com

3. Create a Group

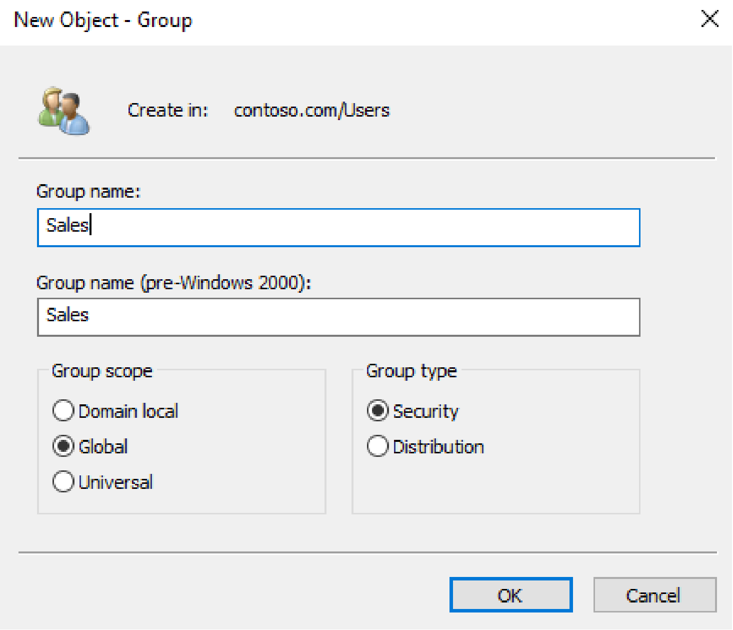
While you’re still in the Active Directory Users and Computers window, click on Users, then right click and hover over New and click on Group.



Name	Type	Description
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Se	
Enterprise A...	Se	
Enterprise K...	Se	
Enterprise R...	Se	
fstack	U	
Group Polic...	Se	
Guest	U	
John Doe	U	
Key Admins	Se	

Create a new object...

This will prompt you to create a new group. Name the group “Sales” then click ok to create the group.



Create in: contoso.com/Users

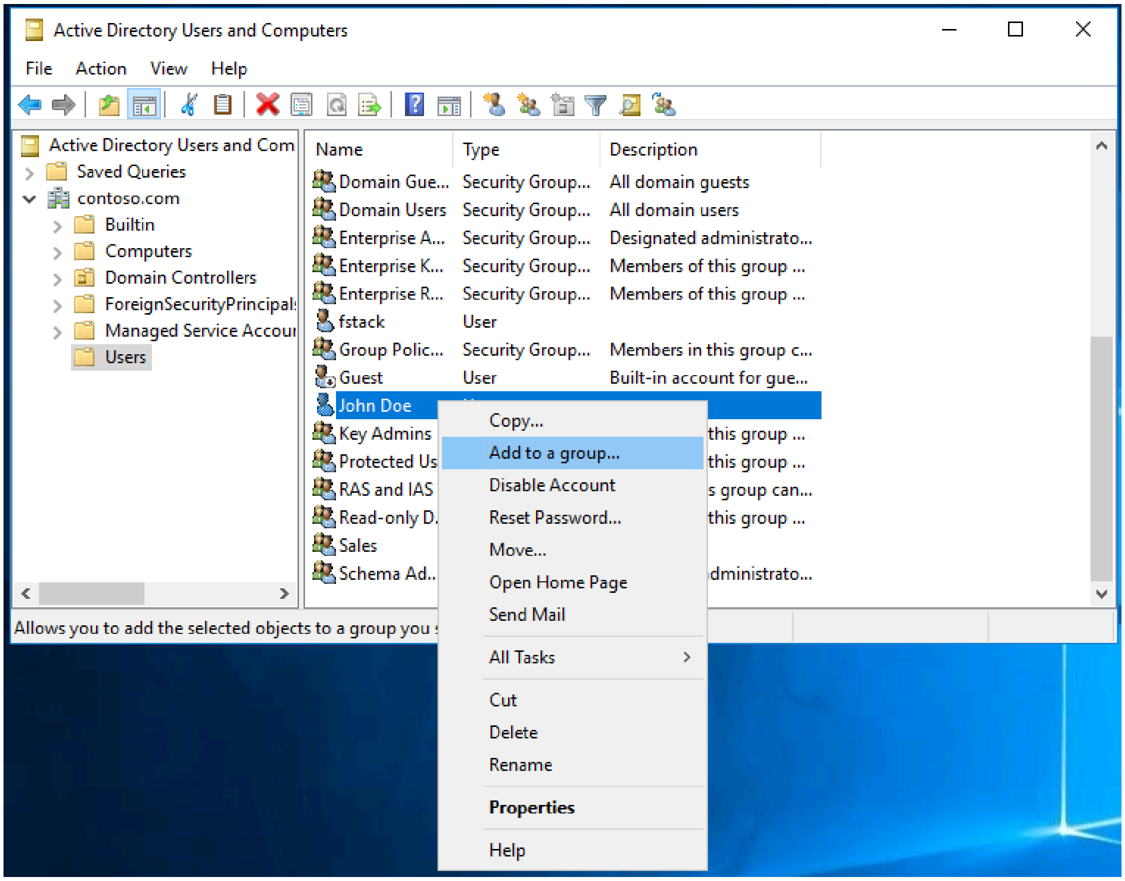
Group name: Sales

Group name (pre-Windows 2000): Sales

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

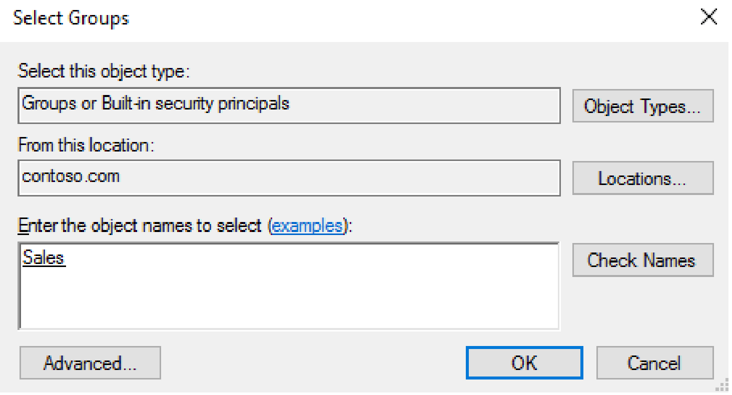
Once you've created the group "Sales," you want to add John Doe to that group so scroll down the Users list until you find the user John Doe and right click the name. You will find the option to "Add to a group." Click that.



Name	Type	Description
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
fstack	User	
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
John Doe		
Key Admins		this group ...
Protected Us		this group ...
RAS and IAS		s group can...
Read-only D.		this group ...
Sales		
Schema Ad..		dministrato...

Allows you to add the selected objects to a group you s

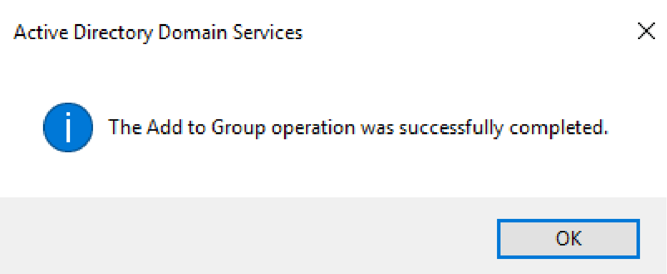
You will be prompted to search for a group, so type the "Sales" into the search box then click ok to confirm. Another window will pop up after to confirm your action.



Select this object type:
Groups or Built-in security principals

From this location:
contoso.com

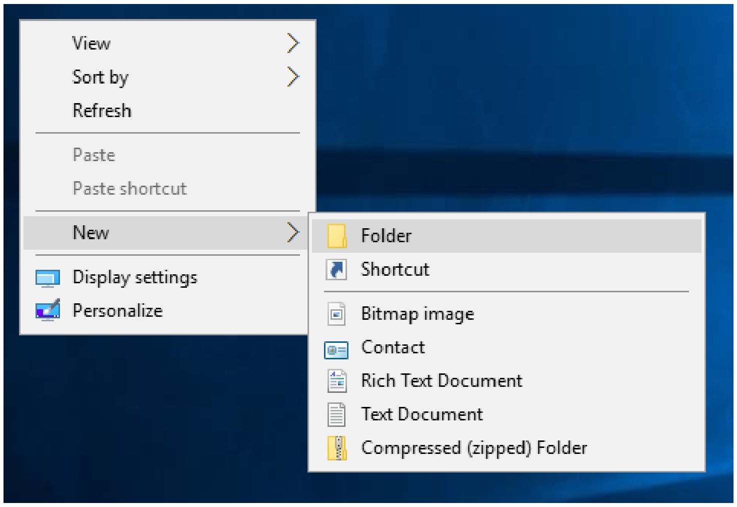
Enter the object names to select (examples):
Sales

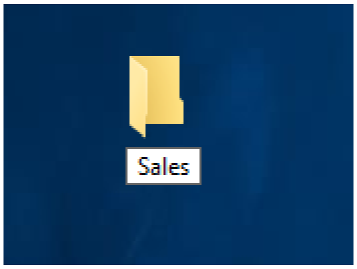

Active Directory Domain Services

The Add to Group operation was successfully completed.

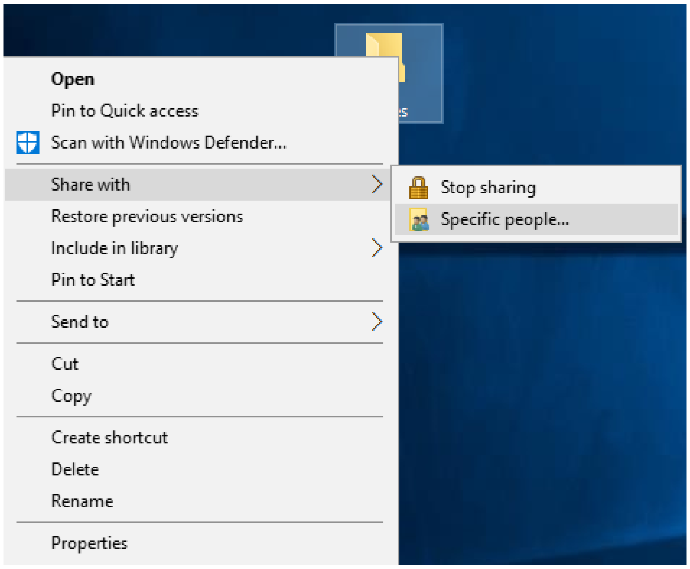
4. Create a shared folder and share

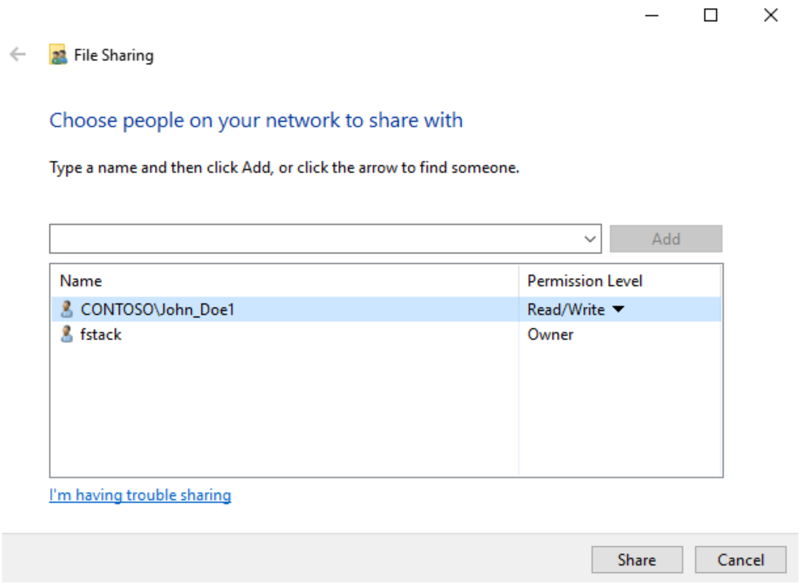
Go to your desktop and right click anywhere and hover over “New,” then click “Folder.” Name the folder “Sales.”





Right click the Sales folder and hover over “Share with” and click “Specific people.” In the window, look up John Doe and add the user to the share list and change the permission from Read to Read/Write.





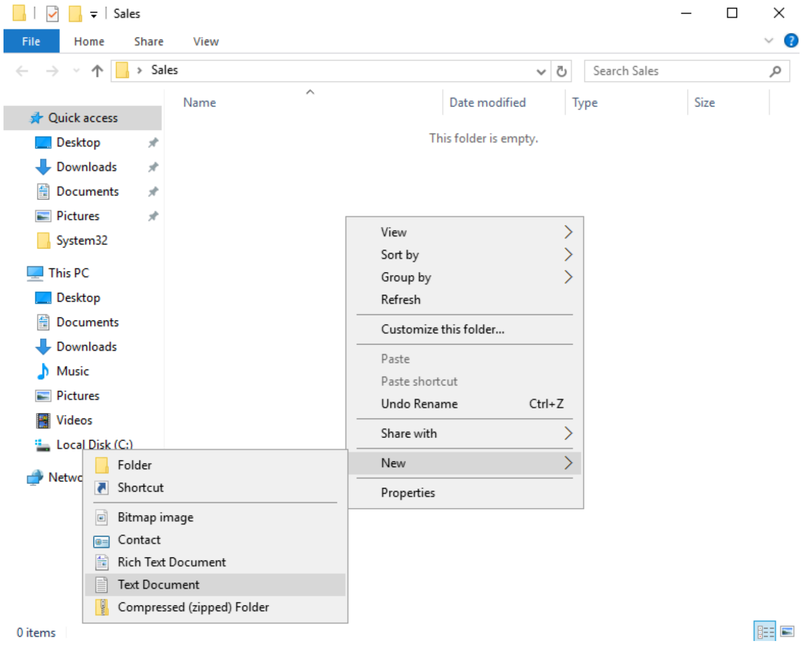
File Sharing

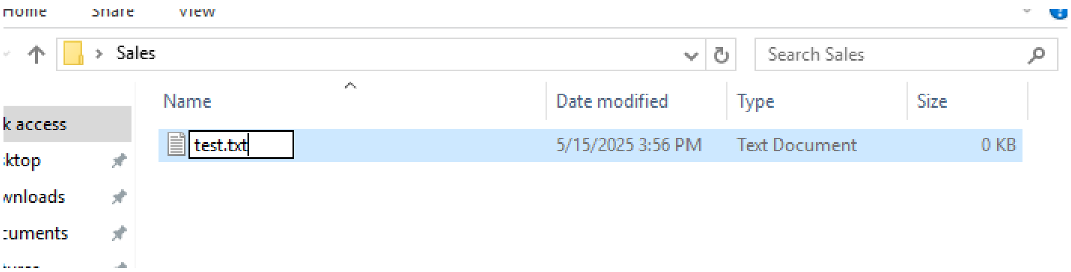
Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
CONTOSO\John_Doe1	Read/Write
fstack	Owner

Go into the folder and create a new text file by right clicking and hovering over "New" and click "Text Document." Name the new file "test.txt."

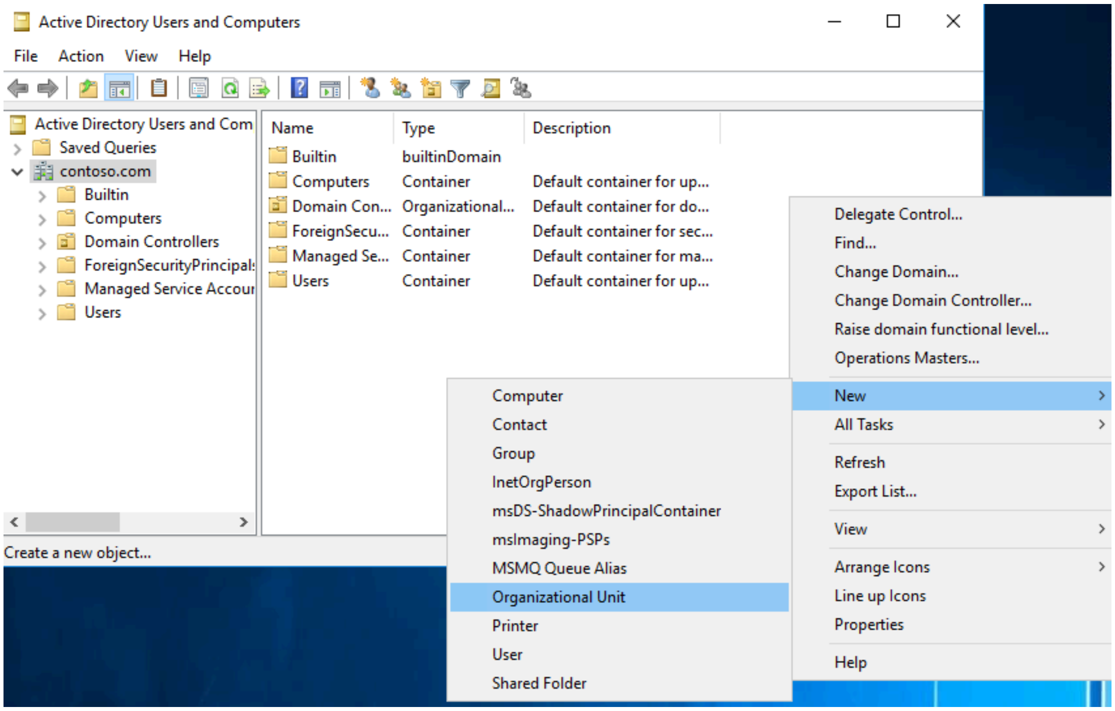




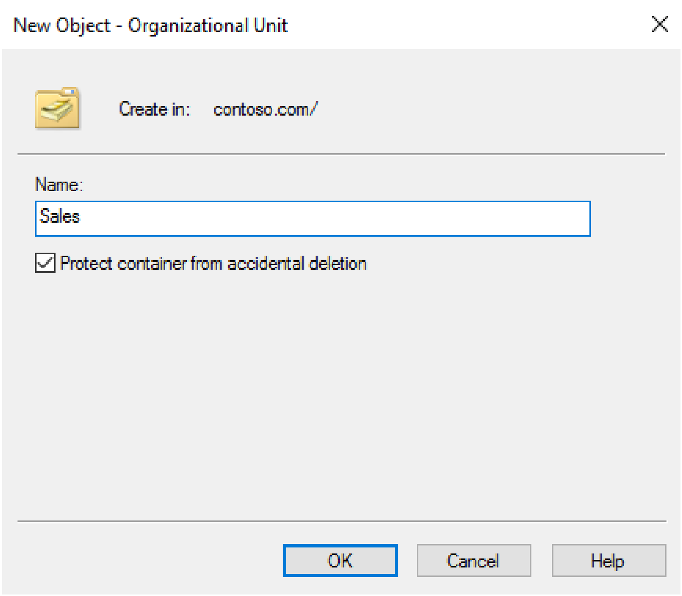
Name	Date modified	Type	Size
test.txt	5/15/2025 3:56 PM	Text Document	0 KB

5. Create an Organization Unit

Search using the windows key to search up and open Active Directory Users and Computers. Within the contoso.com tab, right click and hover “New” and click “Organizational Unit.” Name the new OU “Sales” and click OK to confirm.



Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...

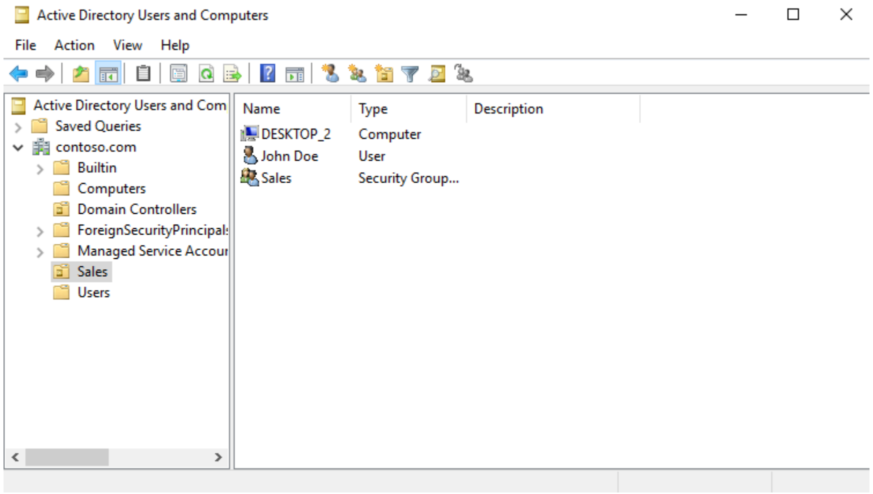


Create in: contoso.com/

Name:
Sales

☑ Protect container from accidental deletion

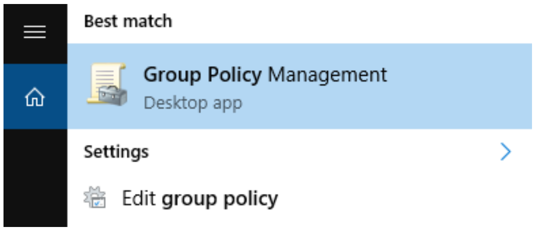
Now drag the Computer, the new User, and the new Group into the OU Sales. It should contain and look like the items below.



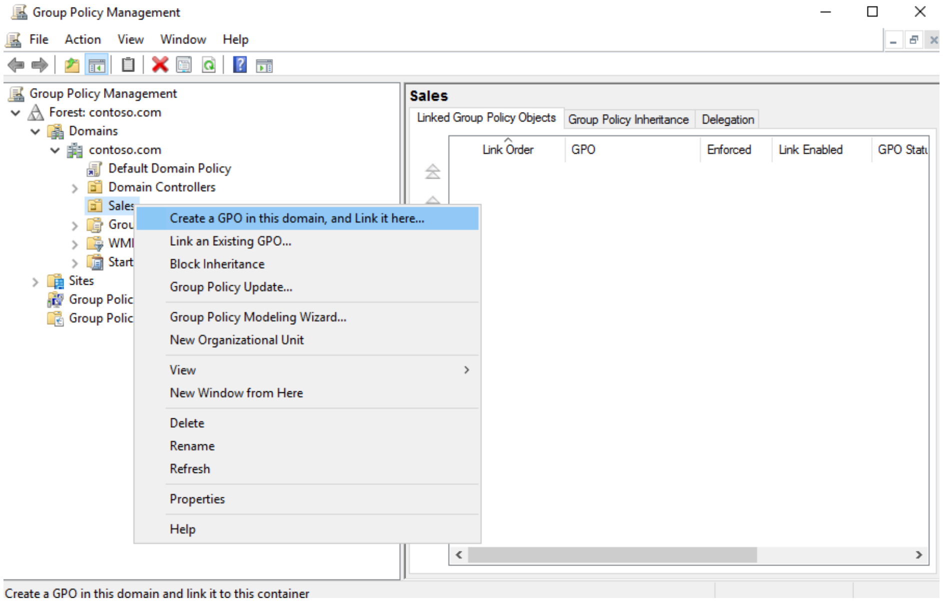
Name	Type	Description
DESKTOP_2	Computer	
John Doe	User	
Sales	Security Group...	

6. Create a Group Policy Unit

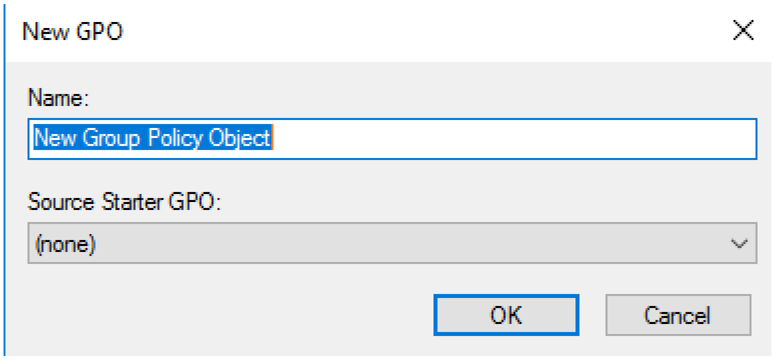
Click the windows key then search "Group Policy Management" and open it.



In that window, on the left side, click on the contoso.com tab, then the Sales OU. Right click it and click on "Create a GPO in this domain, and Link it here." You will be prompted to name the GPO, but I will leave the name as "New Group Policy Object" and click OK to confirm it.



Create a GPO in this domain and link it to this container

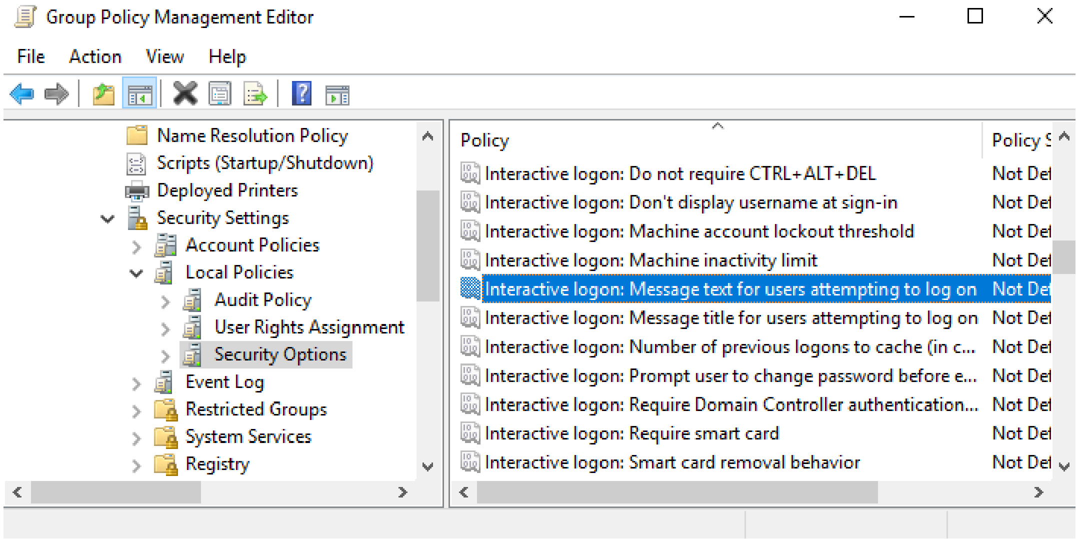


Name: New Group Policy Object

Source Starter GPO: (none)

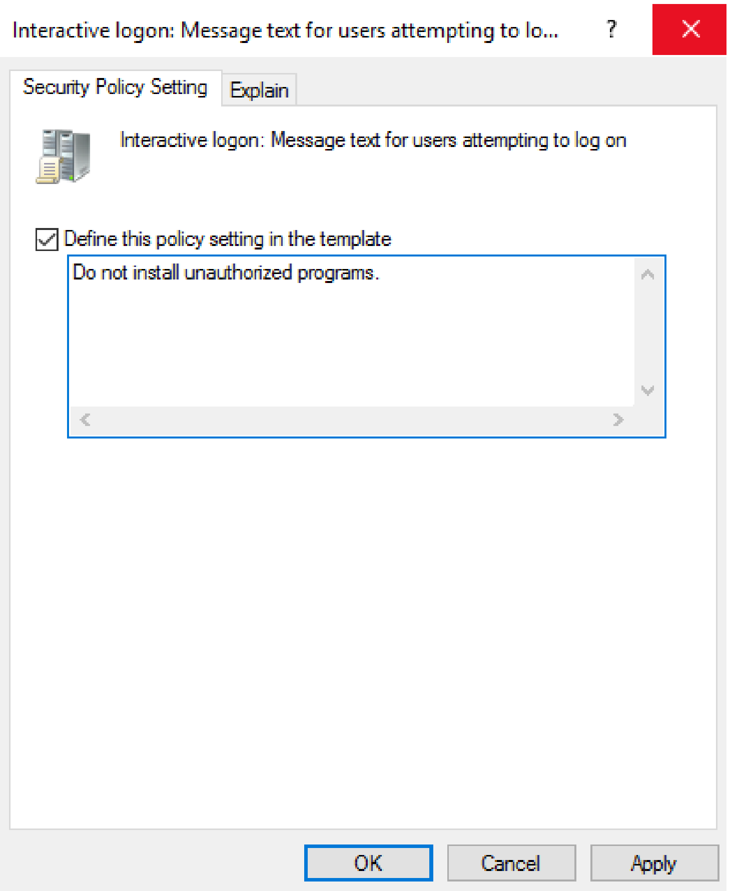
7. **Edit the GPO**

Right click that new GPO and will bring you to a “Group Policy Management Editor” where you will apply multiple rules. The first rule you want to apply is a message that appears whenever the computer starts that says, “Do not install unauthorized programs. In order to get there, you must click on Windows Settings ➡ Security Settings ➡ Local Policies ➡ Security Options, then scroll down the policy list until you see “Interactive logon: Message text for users attempting to log on” and double click it.



Policy	Policy S
Interactive logon: Do not require CTRL+ALT+DEL	Not Def
Interactive logon: Don't display username at sign-in	Not Def
Interactive logon: Machine account lockout threshold	Not Def
Interactive logon: Machine inactivity limit	Not Def
Interactive logon: Message text for users attempting to log on	Not Def
Interactive logon: Message title for users attempting to log on	Not Def
Interactive logon: Number of previous logons to cache (in c...	Not Def
Interactive logon: Prompt user to change password before e...	Not Def
Interactive logon: Require Domain Controller authentication...	Not Def
Interactive logon: Require smart card	Not Def
Interactive logon: Smart card removal behavior	Not Def

You will be prompted to fill in the text box, type in “Do not install unauthorized programs.” and click apply and OK.



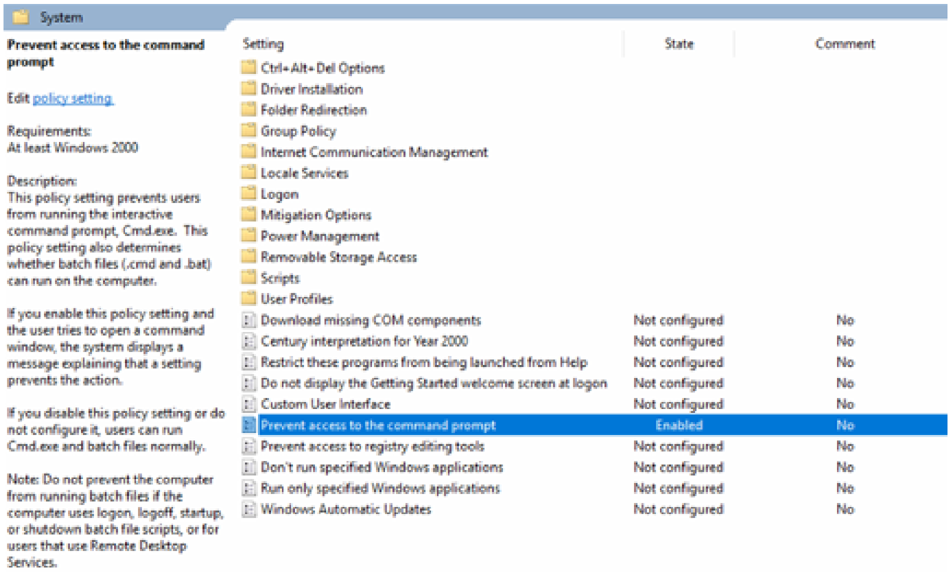
Interactive logon: Message text for users attempting to lo...

Interactive logon: Message text for users attempting to log on

☑ Define this policy setting in the template

Do not install unauthorized programs.

For the next policy, you want to prevent the user's access to CMD. Navigate back to the GPO tabs and click on Administrative Templates: Policy definitions ➡ System, then find the setting titled, "Prevent access to the command prompt," and double click it.



Prevent access to the command prompt

Edit policy setting

Requirements:
At least Windows 2000

Description:
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.

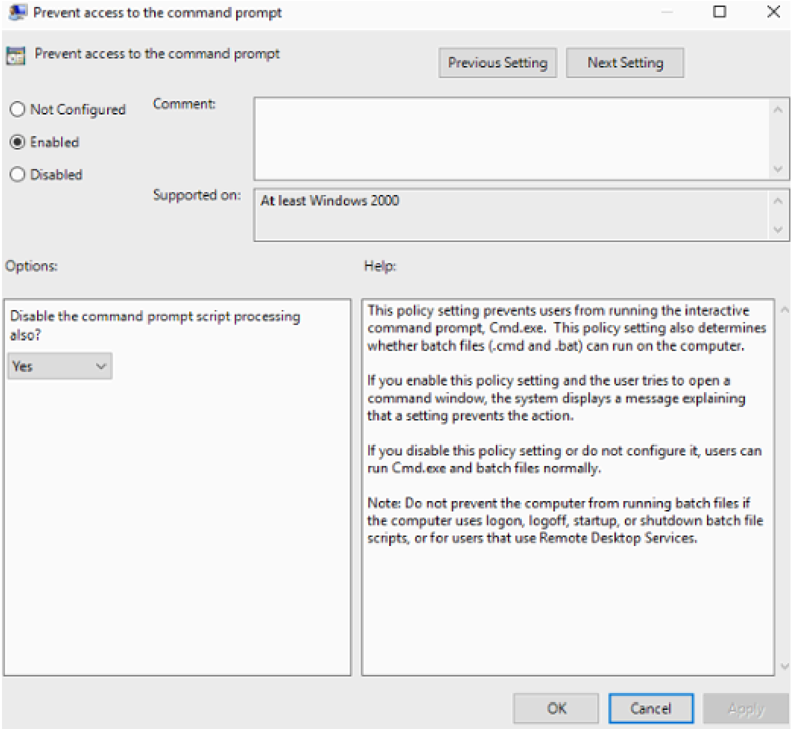
If you enable this policy setting and the user tries to open a command window, the system displays a message explaining that a setting prevents the action.

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.

Setting	State	Comment
Ctrl+Alt+Del Options		
Driver Installation		
Folder Redirection		
Group Policy		
Internet Communication Management		
Locale Services		
Logon		
Mitigation Options		
Power Management		
Removable Storage Access		
Scripts		
User Profiles		
Download missing COM components	Not configured	No
Century interpretation for Year 2000	Not configured	No
Restrict these programs from being launched from Help	Not configured	No
Do not display the Getting Started welcome screen at logon	Not configured	No
Custom User Interface	Not configured	No
Prevent access to the command prompt	Enabled	No
Prevent access to registry editing tools	Not configured	No
Don't run specified Windows applications	Not configured	No
Run only specified Windows applications	Not configured	No
Windows Automatic Updates	Not configured	No

You'll be prompted with another window, where the setting is Disabled. Click enabled then click apply and OK.



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?
Yes

Help:

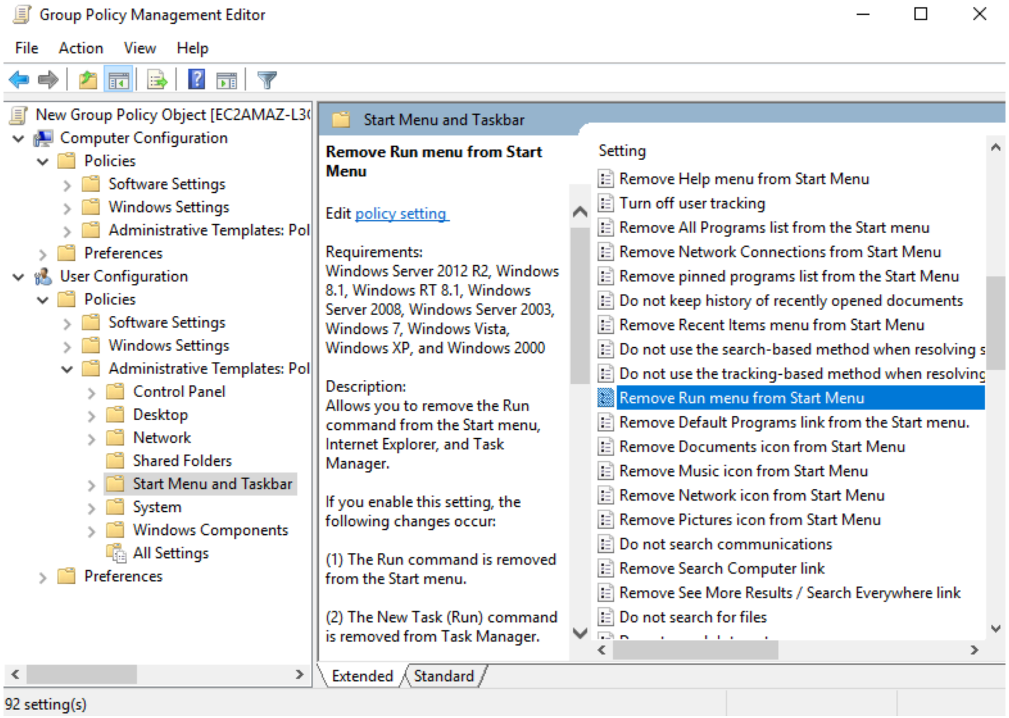
This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.

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.

For the next policy, you want to enable the policy that disables the run command from the start menu. To do that, click User Configuration ➡ Policies ➡ Administrative Templates: Policy definitions ➡ Start Menu and Taskbar, then find the setting "Remove Run menu from Start Menu" and double click it.



New Group Policy Object [EC2AMAZ-L3(
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Pol
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Pol
Control Panel
Desktop
Network
Shared Folders
Start Menu and Taskbar
System
Windows Components
All Settings
Preferences

Start Menu and Taskbar

Remove Run menu from Start Menu

Edit policy setting

Requirements:
Windows Server 2012 R2, Windows 8.1, Windows RT 8.1, Windows Server 2008, Windows Server 2003, Windows 7, Windows Vista, Windows XP, and Windows 2000

Description:
Allows you to remove the Run command from the Start menu, Internet Explorer, and Task Manager.

If you enable this setting, the following changes occur:

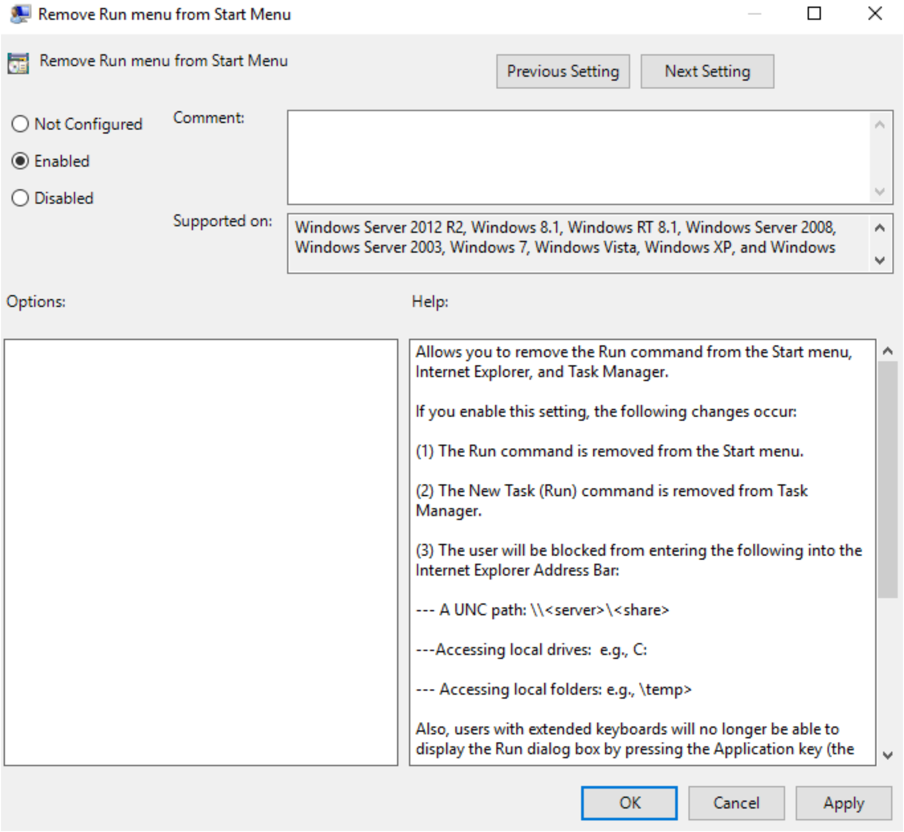
(1) The Run command is removed from the Start menu.

(2) The New Task (Run) command is removed from Task Manager.

Setting
Remove Help menu from Start Menu
Turn off user tracking
Remove All Programs list from the Start menu
Remove Network Connections from Start Menu
Remove pinned programs list from the Start menu
Do not keep history of recently opened documents
Remove Recent Items menu from Start Menu
Do not use the search-based method when resolving s
Do not use the tracking-based method when resolving
Remove Run menu from Start Menu
Remove Default Programs link from the Start menu.
Remove Documents icon from Start Menu
Remove Music icon from Start Menu
Remove Network icon from Start Menu
Remove Pictures icon from Start Menu
Do not search communications
Remove Search Computer link
Remove See More Results / Search Everywhere link
Do not search for files

92 setting(s)

Another window will show up and you will click enabled and then Apply and OK.



Remove Run menu from Start Menu
Remove Run menu from Start Menu
Previous Setting
Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: Windows Server 2012 R2, Windows 8.1, Windows RT 8.1, Windows Server 2008, Windows Server 2003, Windows 7, Windows Vista, Windows XP, and Windows

Options:

Help:

Allows you to remove the Run command from the Start menu, Internet Explorer, and Task Manager.

If you enable this setting, the following changes occur:

(1) The Run command is removed from the Start menu.

(2) The New Task (Run) command is removed from Task Manager.

(3) The user will be blocked from entering the following into the Internet Explorer Address Bar:

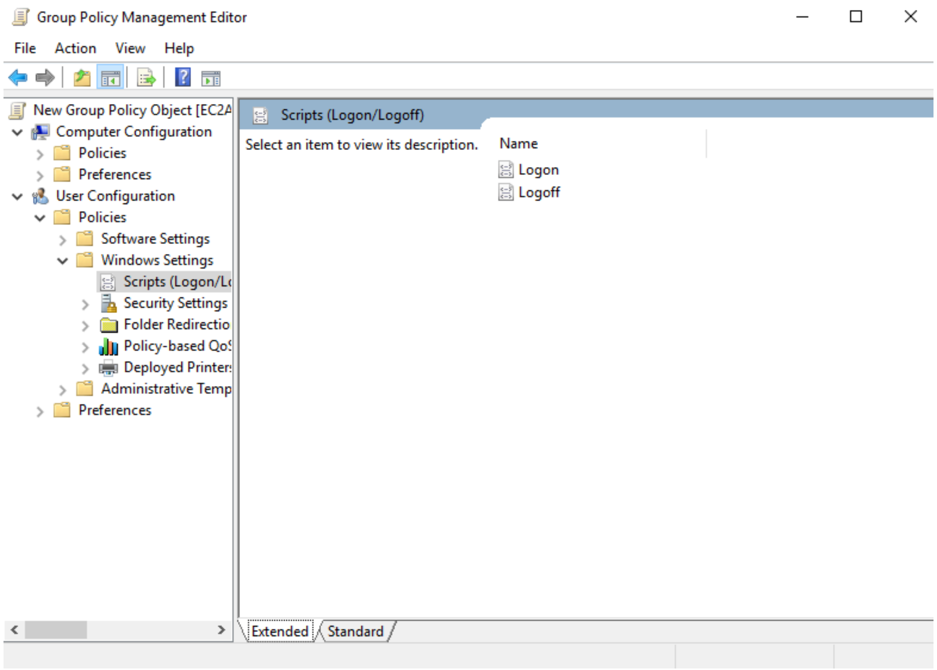
--- A UNC path: \\<server>\<share>

---Accessing local drives: e.g., C:

--- Accessing local folders: e.g., \temp>

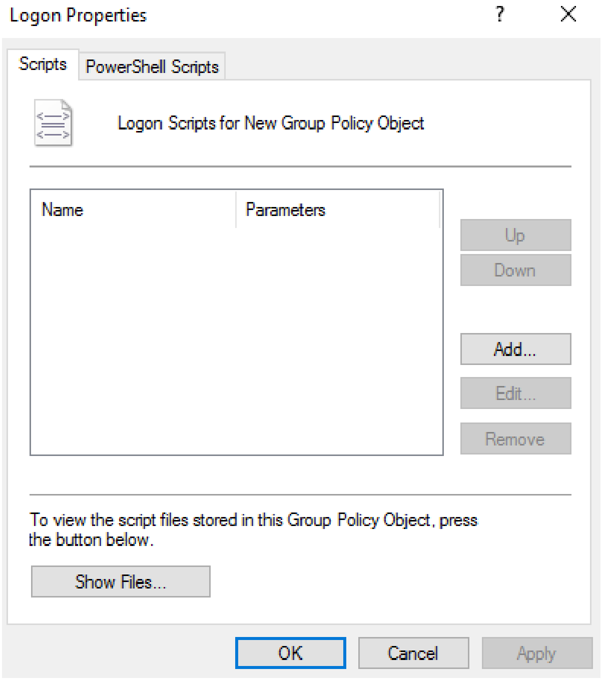
Also, users with extended keyboards will no longer be able to display the Run dialog box by pressing the Application key (the

For the last rule, you want to add a script to the user’s login to map the share you created. To do that, go back to the Group Policy Management Editor and click on User Configuration ➡ Policies ➡ Windows Settings ➡ Scripts (Logon/Logoff) ➡ Logon and double click it.



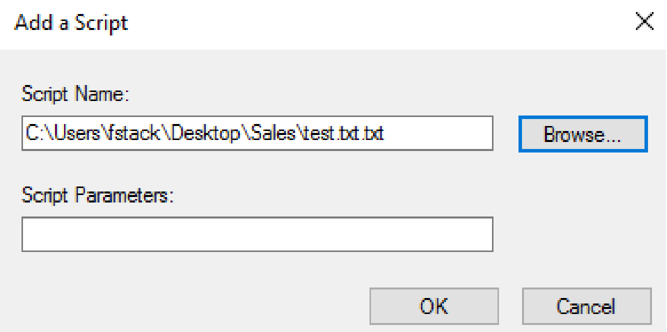
Select an item to view its description.

A “Logon Properties” window will open, click “Add” and you’ll be prompted to add a file. Add the test.txt file that was saved in the Sales folder.



Logon Scripts for New Group Policy Object

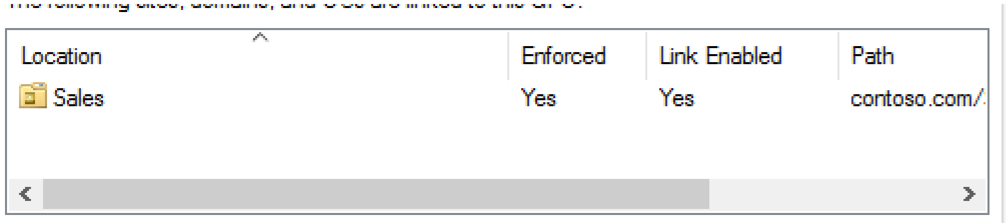
To view the script files stored in this Group Policy Object, press the button below.



Script Name: C:\Users\fstack\Desktop\Sales\test.txt.txt

Script Parameters:

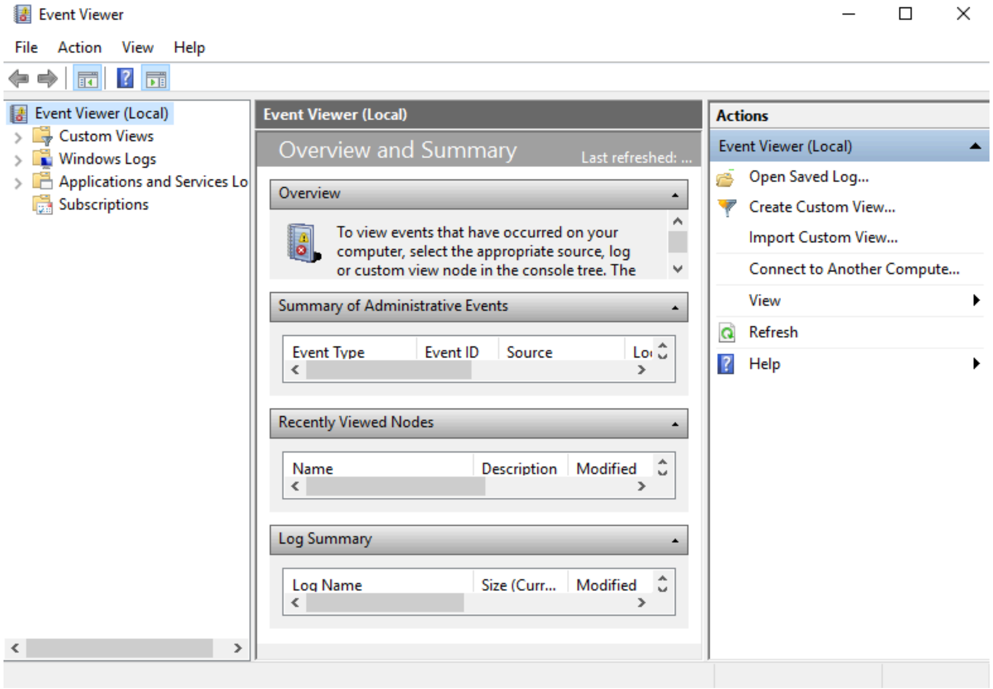
Once you’re done, go back to the Group Policy Management window and make sure that the GPO you just made is enforced.



Location	Enforced	Link Enabled	Path
Sales	Yes	Yes	contoso.com/

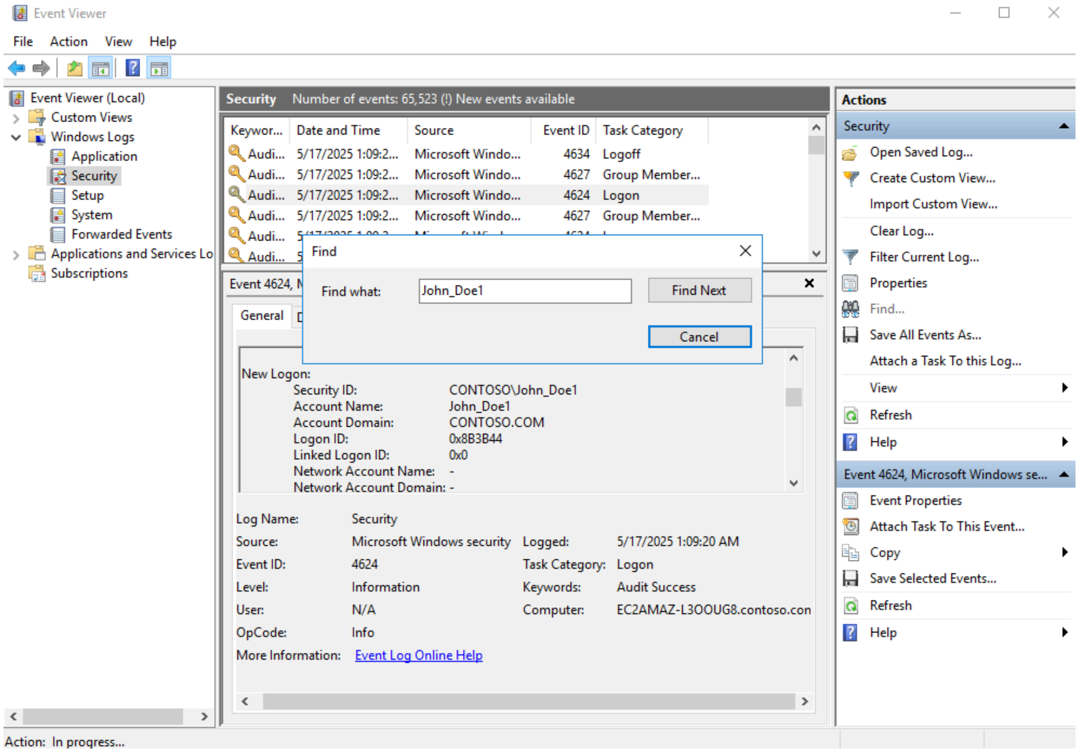
8. Event Viewer Logs

Using the “Event Viewer,” we want to write down the last successful login from the user. Click the Windows key and search for “Event Viewer” and open it. You will have a window that looks like this:



To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The

Click on “Windows Logs” and then “Security.” On the top left of the window, click on “Action” and then “Find.” You will be prompted to input a search keyword; input “John_Doe1” and click enter. You can see that the last successful login was 5/17/2025 1:09:20 AM.



Security Number of events: 65,523 (!) New events available

Keywor...	Date and Time	Source	Event ID	Task Category
Audi...	5/17/2025 1:09:2...	Microsoft Windo...	4634	Logoff
Audi...	5/17/2025 1:09:2...	Microsoft Windo...	4627	Group Member...
Audi...	5/17/2025 1:09:2...	Microsoft Windo...	4624	Logon
Audi...	5/17/2025 1:09:2...	Microsoft Windo...	4627	Group Member...

Find

Find what: John_Doe1

Event 4624, M

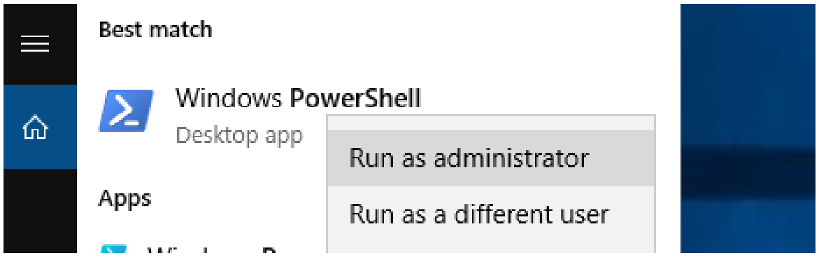
```
New Logon:
        Security ID:            CONTOSO\John_Doe1
        Account Name:           John_Doe1
        Account Domain:         CONTOSO.COM
        Logon ID:               0x8B3B44
        Linked Logon ID:        0x0
        Network Account Name:   -
        Network Account Domain: -
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          5/17/2025 1:09:20 AM
Event ID:          4624                         Task Category:   Logon
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        EC2AMAZ-L3OOUG8.contoso.con
OpCode:            Info
More Information:  Event Log Online Help
```

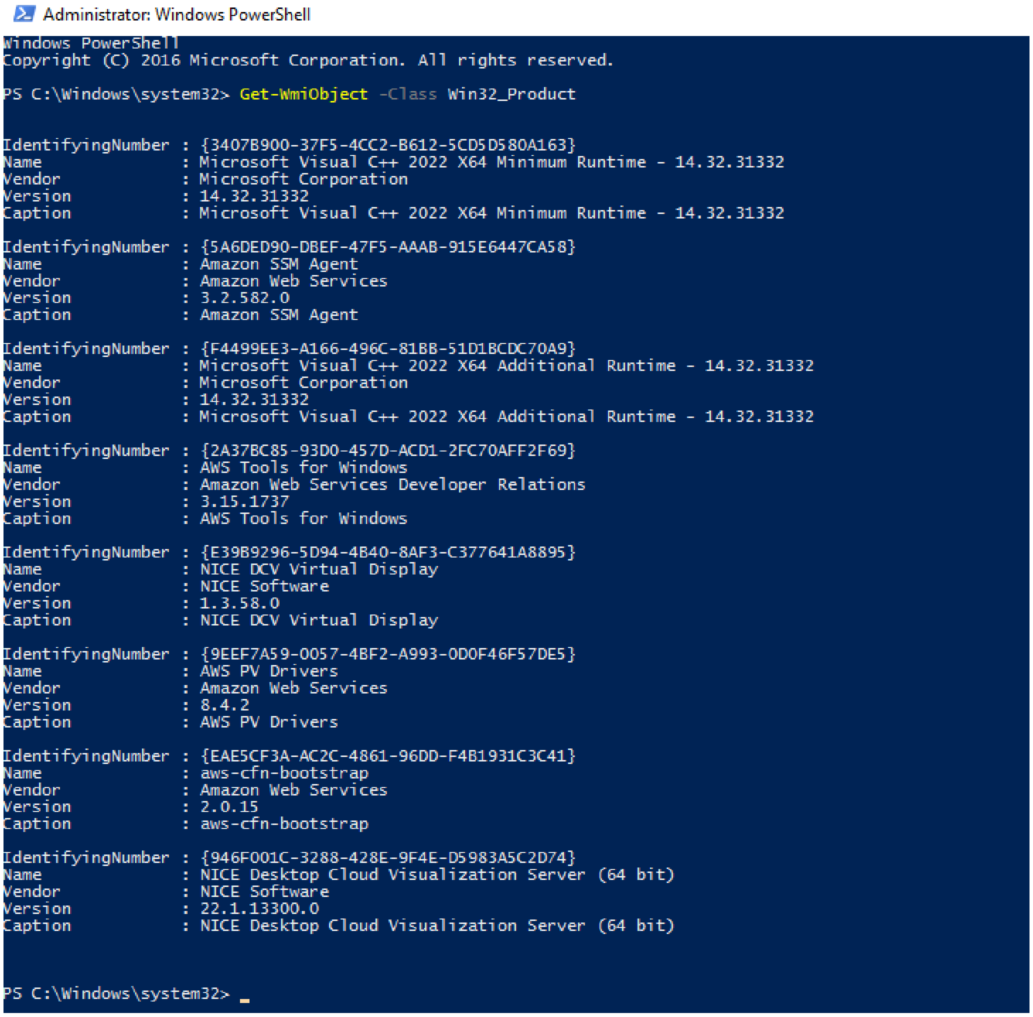
Action: In progress...

9. Powershell Installed Programs

Click the Windows key and search up “Powershell,” and before you open it, right click and open Powershell as administrator.



In Powershell, you want to check what the latest programs installed on the computer are. To do that, type in, “Get-WmiObject -Class Win32_Product” and click enter. You get a similar result like the picture below.

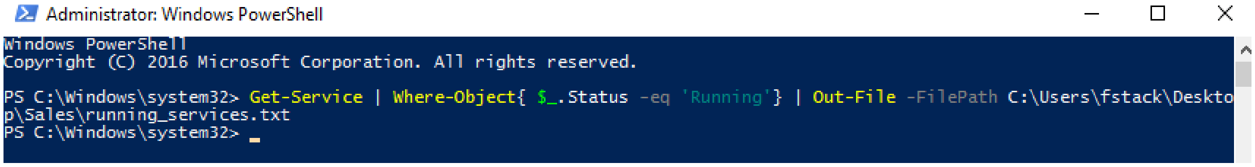


Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Get-WmiObject -Class Win32_Product


IdentifyingNumber : {3407B900-37F5-4CC2-B612-5CD5D580A163}
Name              : Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31332
Vendor            : Microsoft Corporation
Version           : 14.32.31332
Caption           : Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31332

IdentifyingNumber : {5A6DED90-DBEF-47F5-AAAB-915E6447CA58}
Name              : Amazon SSM Agent
Vendor            : Amazon Web Services
Version           : 3.2.582.0
Caption           : Amazon SSM Agent

IdentifyingNumber : {F4499EE3-A166-496C-81BB-51D1BCDC70A9}
Name              : Microsoft Visual C++ 2022 X64 Additional Runtime - 14.32.31332
Vendor            : Microsoft Corporation
Version           : 14.32.31332
Caption           : Microsoft Visual C++ 2022 X64 Additional Runtime - 14.32.31332

IdentifyingNumber : {2A37BC85-93D0-457D-ACD1-2FC70AFF2F69}
Name              : AWS Tools for Windows
Vendor            : Amazon Web Services Developer Relations
Version           : 3.15.1737
Caption           : AWS Tools for Windows

IdentifyingNumber : {E39B9296-5D94-4B40-8AF3-C377641A8895}
Name              : NICE DCV Virtual Display
Vendor            : NICE Software
Version           : 1.3.58.0
Caption           : NICE DCV Virtual Display

IdentifyingNumber : {9EEF7A59-0057-4BF2-A993-0D0F46F57DE5}
Name              : AWS PV Drivers
Vendor            : Amazon Web Services
Version           : 8.4.2
Caption           : AWS PV Drivers

IdentifyingNumber : {EAE5CF3A-AC2C-4861-96DD-F4B1931C3C41}
Name              : aws-cfn-bootstrap
Vendor            : Amazon Web Services
Version           : 2.0.15
Caption           : aws-cfn-bootstrap

IdentifyingNumber : {946F001C-3288-428E-9F4E-D5983A5C2D74}
Name              : NICE Desktop Cloud Visualization Server (64 bit)
Vendor            : NICE Software
Version           : 22.1.13300.0
Caption           : NICE Desktop Cloud Visualization Server (64 bit)



PS C:\Windows\system32> _
```

10. Powershell Running Services List Script

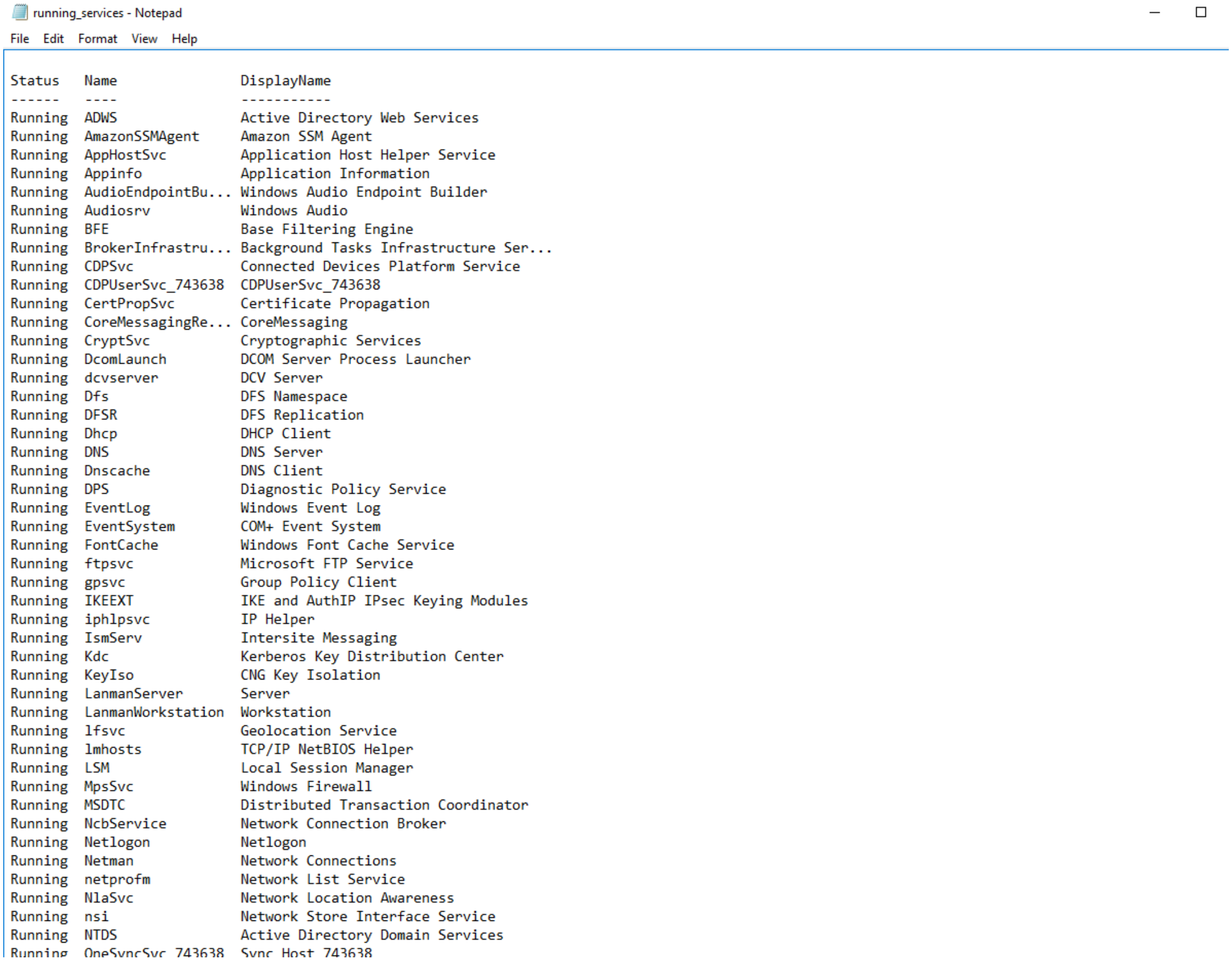
You will retrieve a list of all the running services on the computer and put it into a new file named “running_services.txt.” With Powershell still open, you can type in the command, “Get-Service | Where-Object{ $_.Status -eq ‘Running’} | Out-File -FilePath C:\Users\fstack\Desktop\Sales\running_services.txt”.



Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Get-Service | Where-Object{ $_.Status -eq 'Running'} | Out-File -FilePath C:\Users\fstack\Deskto
p\Sales\running_services.txt
PS C:\Windows\system32> _
```

Now when you open the new “running_services” file in the Sales folder, it will look something like this:



```
Status   Name               DisplayName
------   ----               -----------
Running  ADWS               Active Directory Web Services
Running  AmazonSSMAgent     Amazon SSM Agent
Running  AppHostSvc         Application Host Helper Service
Running  Appinfo            Application Information
Running  AudioEndpointBu... Windows Audio Endpoint Builder
Running  Audiosrv           Windows Audio
Running  BFE                Base Filtering Engine
Running  BrokerInfrastru... Background Tasks Infrastructure Ser...
Running  CDPSvc             Connected Devices Platform Service
Running  CDPUserSvc_743638  CDPUserSvc_743638
Running  CertPropSvc        Certificate Propagation
Running  CoreMessagingRe... CoreMessaging
Running  CryptSvc           Cryptographic Services
Running  DcomLaunch         DCOM Server Process Launcher
Running  dcvserver          DCV Server
Running  Dfs                DFS Namespace
Running  DFSR               DFS Replication
Running  Dhcp               DHCP Client
Running  DNS                DNS Server
Running  Dnscache           DNS Client
Running  DPS                Diagnostic Policy Service
Running  EventLog           Windows Event Log
Running  EventSystem        COM+ Event System
Running  FontCache          Windows Font Cache Service
Running  ftpsvc             Microsoft FTP Service
Running  gpsvc              Group Policy Client
Running  IKEEXT             IKE and AuthIP IPsec Keying Modules
Running  iphlpsvc           IP Helper
Running  IsmServ            Intersite Messaging
Running  Kdc                Kerberos Key Distribution Center
Running  KeyIso             CNG Key Isolation
Running  LanmanServer       Server
Running  LanmanWorkstation  Workstation
Running  lfsvc              Geolocation Service
Running  lmhosts            TCP/IP NetBIOS Helper
Running  LSM                Local Session Manager
Running  MpsSvc             Windows Firewall
Running  MSDTC              Distributed Transaction Coordinator
Running  NcbService         Network Connection Broker
Running  Netlogon           Netlogon
Running  Netman             Network Connections
Running  netprofm           Network List Service
Running  NlaSvc             Network Location Awareness
Running  nsi                Network Store Interface Service
Running  NTDS               Active Directory Domain Services
Running  OneSyncSvc_743638  Sync Host_743638
```