Stackfull Software Runbook

Welcome to the team!

Here at Stackfull Software, it is imperative that all employees have properly set up their respective machines. To do this, please follow the steps in the runbook below:

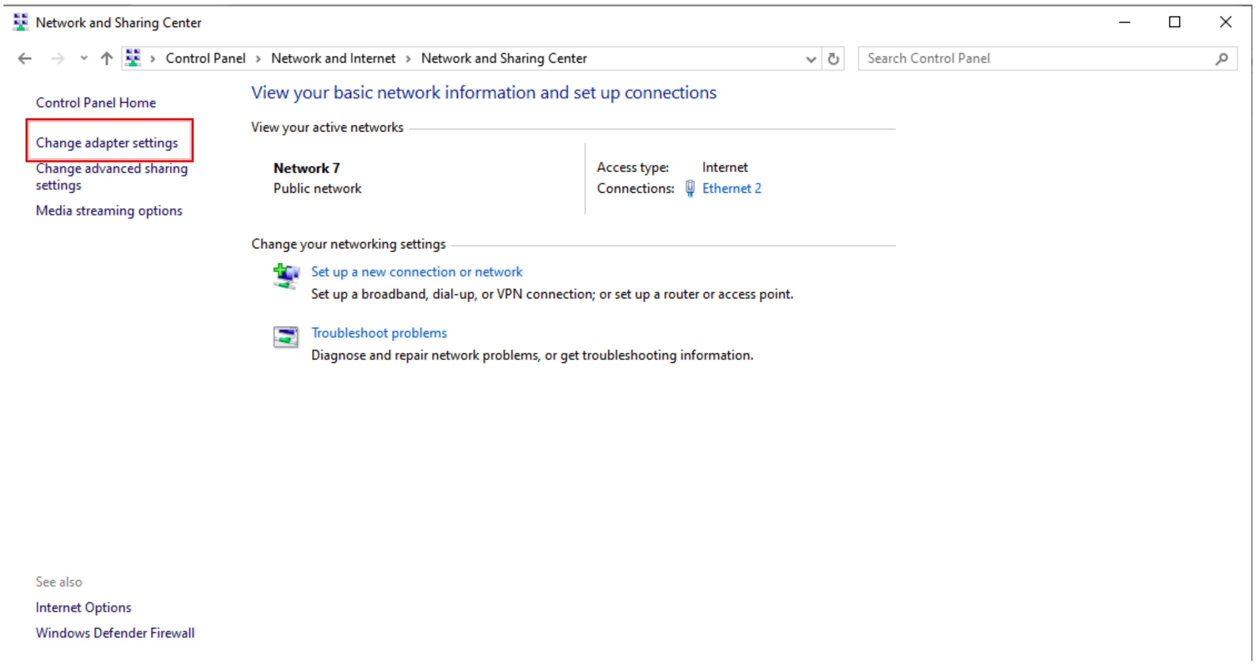
We will be using the following new hire as the example-

Name: John Doe
Role: Sales Associate
Department: Sales

Step 1: Connect to the domain-

The first step is to connect to the domain. This will allow the user's machine to join the Stackfull network. The domain will control the user's security settings and account information while giving them access to the network resources.

In order to join the domain, we must first change our DNS server to the domain controller in the adapter settings. To do this, open up the control panel and click "Network and Internet" and then "Network and Sharing Center." Then on the left hand side, click "Change adapter settings."



Network and Sharing Center

Control Panel › Network and Internet › Network and Sharing Center

Search Control Panel

Control Panel Home
Change adapter settings
Change advanced sharing settings
Media streaming options

View your basic network information and set up connections

View your active networks

Network 7
Public network

Access type: Internet
Connections: Ethernet 2

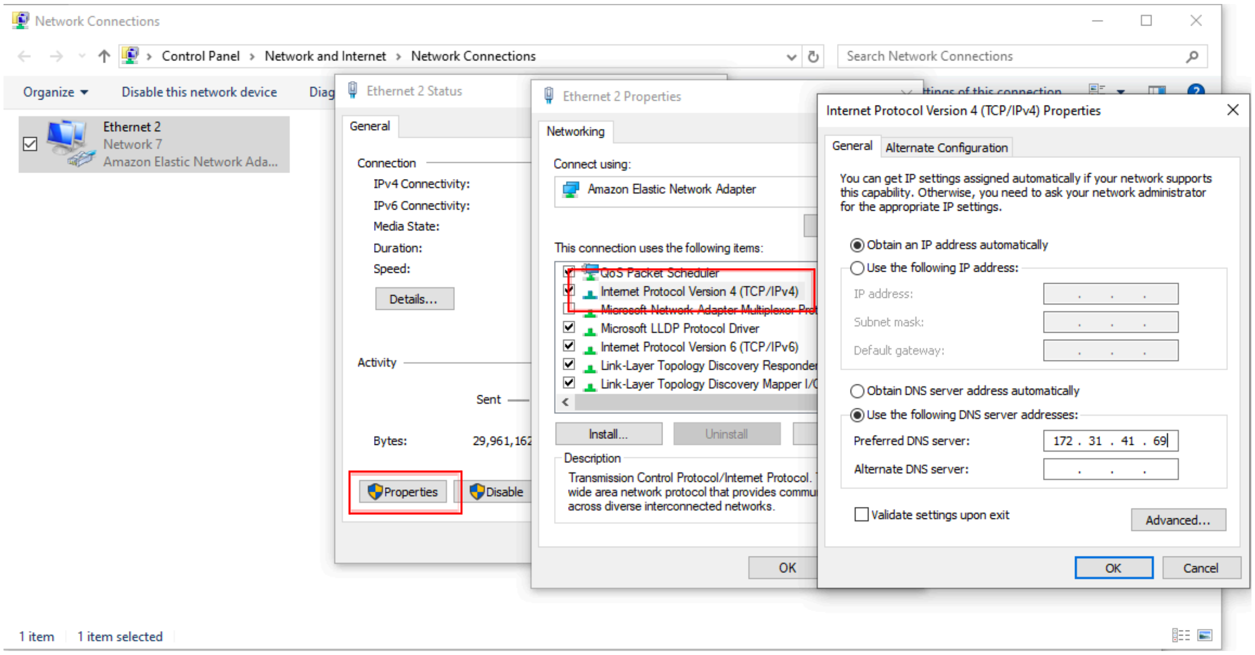
Change your networking settings

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.

See also
Internet Options
Windows Defender Firewall

Then, click “Ethernet 2.” This should open up the Ethernet 2 Status window. Click on “Properties.” This should open up a new window. Scroll down to find “Internet Protocol Version 4” and click on it. In the new window, change the DNS settings to the IP address of the server.



Network Connections
Control Panel > Network and Internet > Network Connections
Search Network Connections
Organize
Disable this network device
Diag
Ethernet 2
Network 7
Amazon Elastic Network Ada...
Ethernet 2 Status
General
Connection
IPv4 Connectivity:
IPv6 Connectivity:
Media State:
Duration:
Speed:
Details...
Activity
Sent
Bytes: 29,961,162
Properties
Disable
Ethernet 2 Properties
Networking
Connect using:
Amazon Elastic Network Adapter
This connection uses the following items:
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
□ Microsoft Network Adapter Multiplexor Prot
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Link-Layer Topology Discovery Responder
☑ Link-Layer Topology Discovery Mapper I/O
Install...
Uninstall
Description
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
IP address:
Subnet mask:
Default gateway:
Advanced...
OK
Cancel
1 item
1 item selected

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

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.

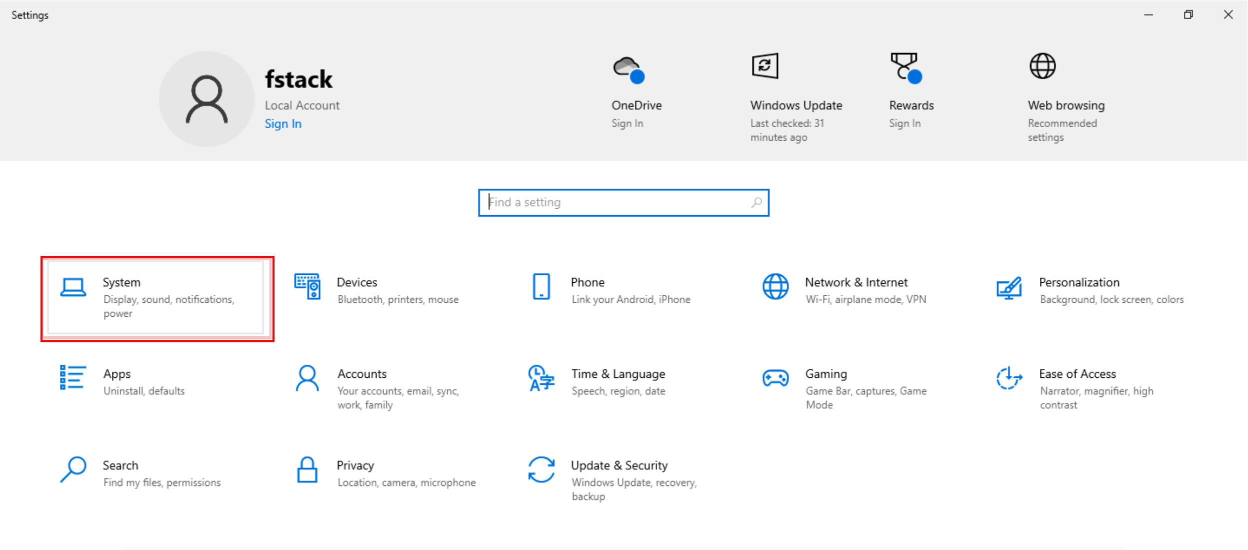
● Obtain an IP address automatically
○ Use the following IP address:

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

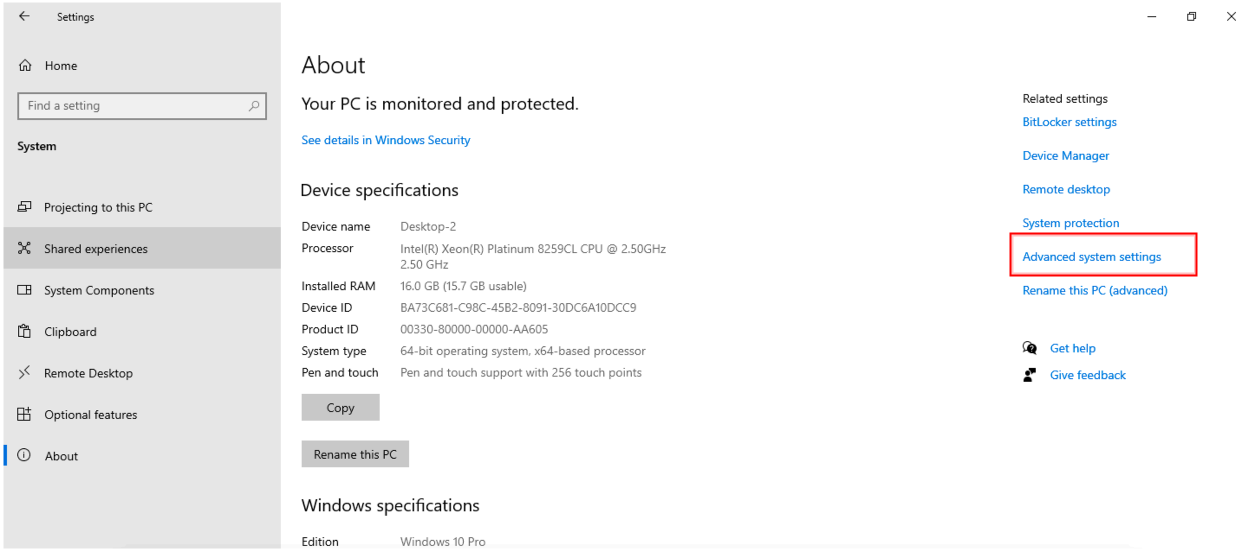
Preferred DNS server: 172 . 31 . 41 . 69
Alternate DNS server: . . .

□ Validate settings upon exit

Then, to join the domain, first open the “settings,” then click into “system,” and then “about.” On the right hand side, click the “advanced system settings” option.



Settings
fstack
Local Account
Sign In
OneDrive
Sign In
Windows Update
Last checked: 31 minutes ago
Rewards
Sign In
Web browsing
Recommended settings
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date
Gaming
Game Bar, captures, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Search
Find my files, permissions
Privacy
Location, camera, microphone
Update & Security
Windows Update, recovery, backup



Settings

Home

Find a setting

System

About

Your PC is monitored and protected.

See details in Windows Security

Device specifications

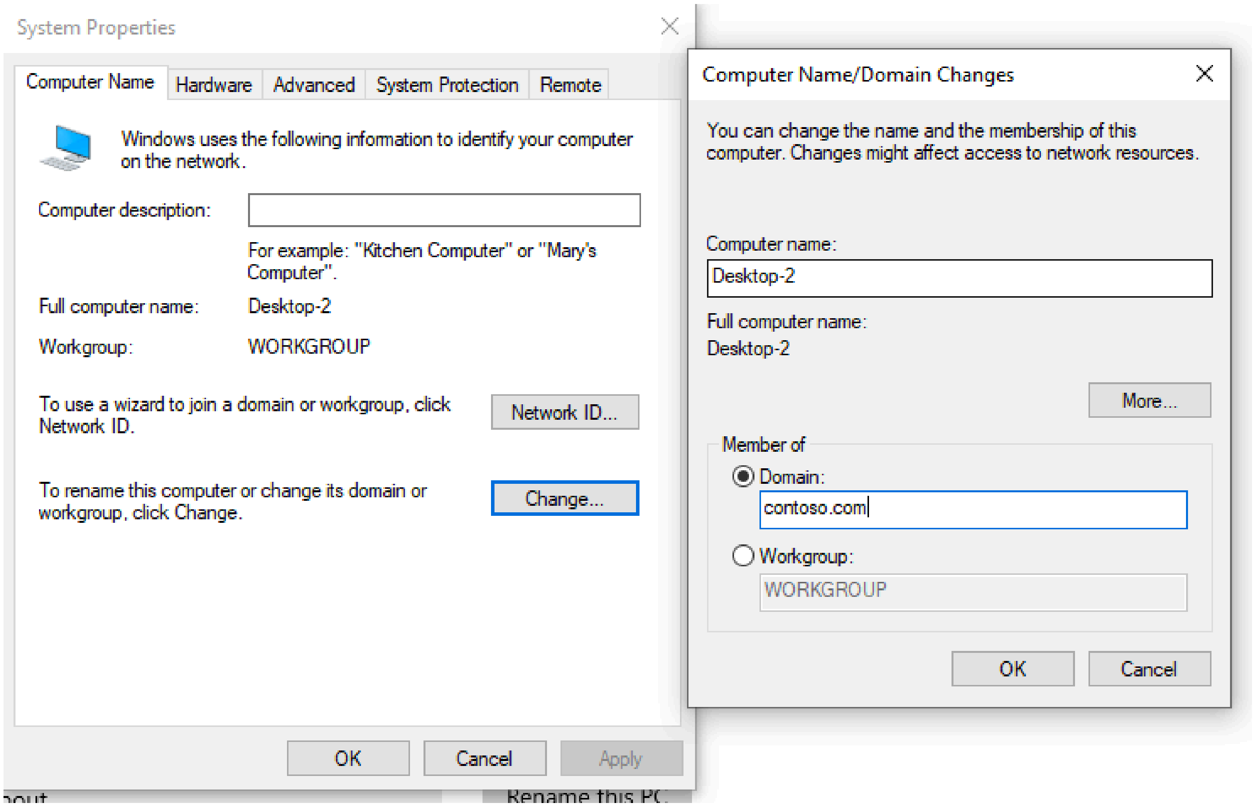
Device name	Desktop-2
Processor	Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz 2.50 GHz
Installed RAM	16.0 GB (15.7 GB usable)
Device ID	BA73C681-C98C-45B2-8091-30DC6A10DCC9
Product ID	00330-80000-00000-AA605
System type	64-bit operating system, x64-based processor
Pen and touch	Pen and touch support with 256 touch points

Windows specifications

Edition	Windows 10 Pro

Related settings

Once the advanced system settings are open, navigate to “computer name” and click “change..” Then, click on “domain” and type in “contoso.com.”



System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: Desktop-2

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

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

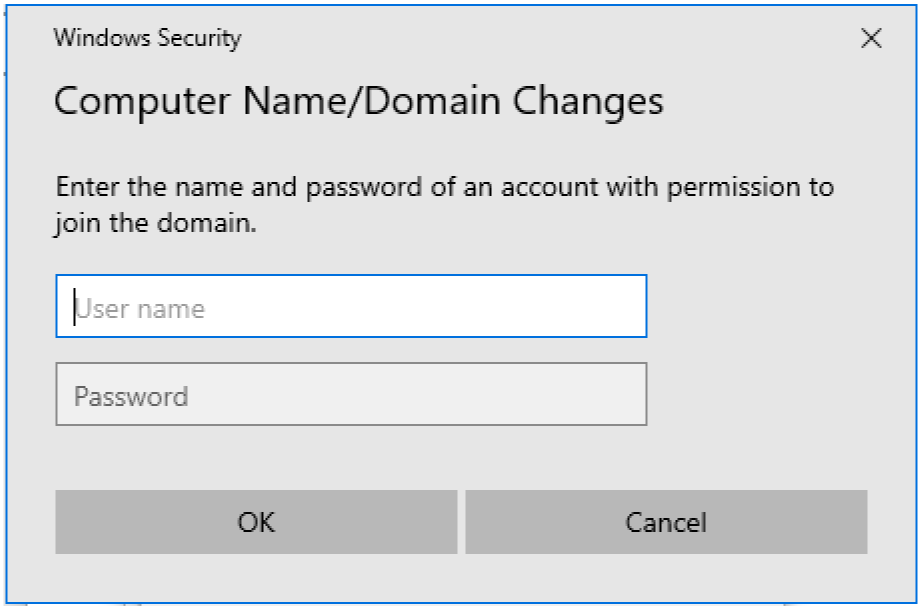
Full computer name:
Desktop-2

Member of

● Domain: contoso.com

○ Workgroup: WORKGROUP

If done properly, you should be prompted to enter user and password credentials in order to join the domain.



Windows Security

Computer Name/Domain Changes

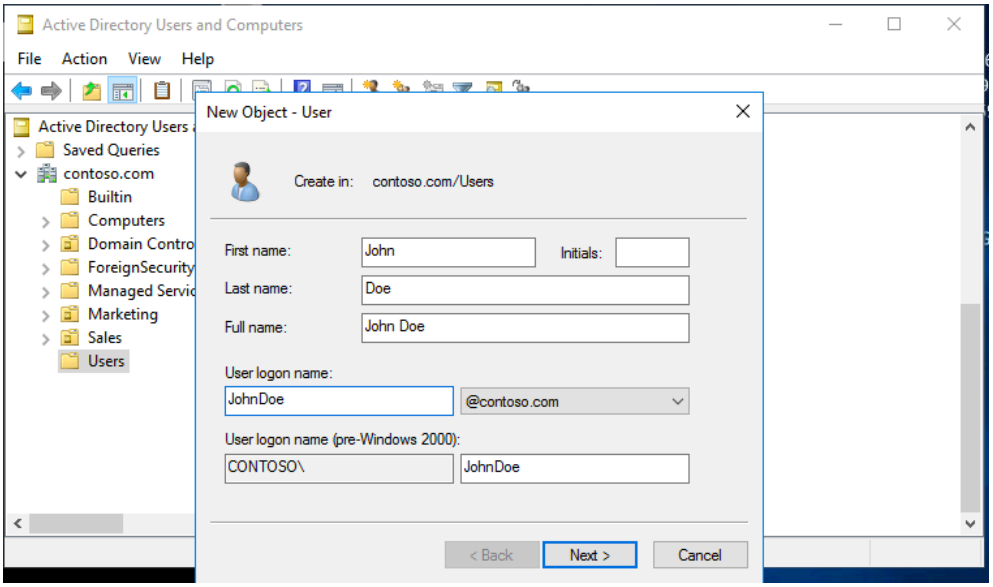
Enter the name and password of an account with permission to join the domain.

Enter the username/password administrator/Pa$$w0rd to join the domain.

Step 2: Create a user and set a password-

Once you've successfully joined the domain, you can now create a username and password for the new hire. Switch onto the server to make the following changes.

Open up the active directory. Then navigate into the "users" folder, right click anywhere, then create a new user. Enter the new user's information and set a temporary password. The new user will be prompted to change their password when they first log in.



Active Directory Users and Computers

New Object - User

Create in: contoso.com/Users

First name: John

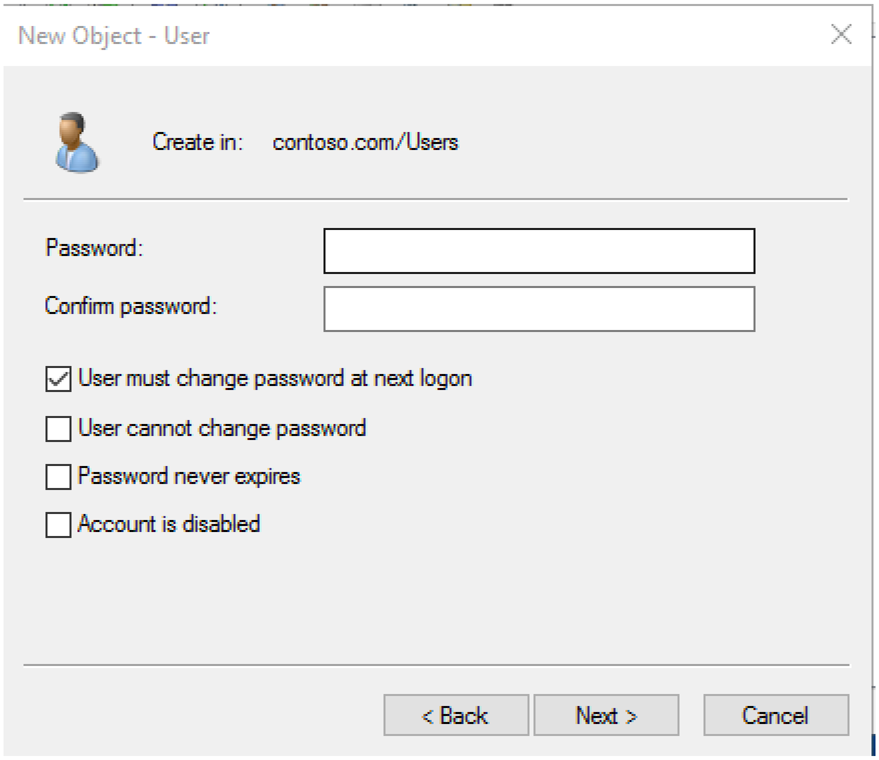
Initials:

Last name: Doe

Full name: John Doe

User logon name: JohnDoe @contoso.com

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



New Object - User

Create in: contoso.com/Users

Password:

Confirm password:

☑ User must change password at next logon

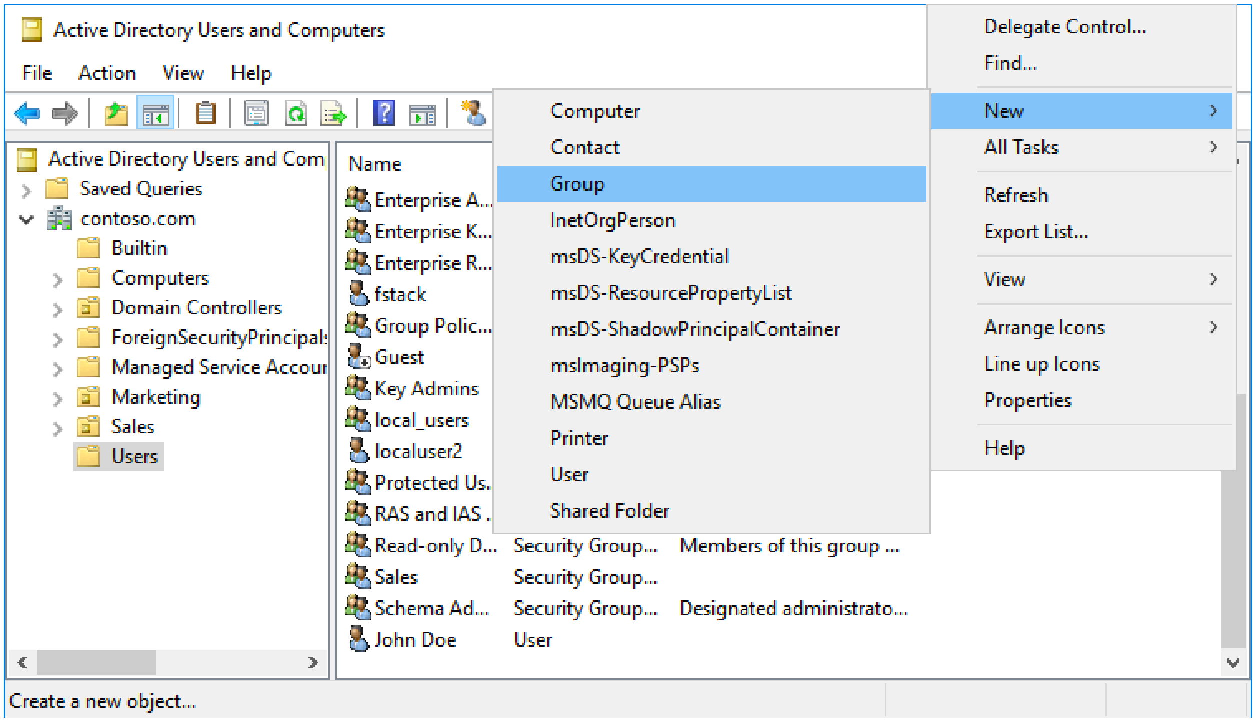
□ User cannot change password

□ Password never expires

□ Account is disabled

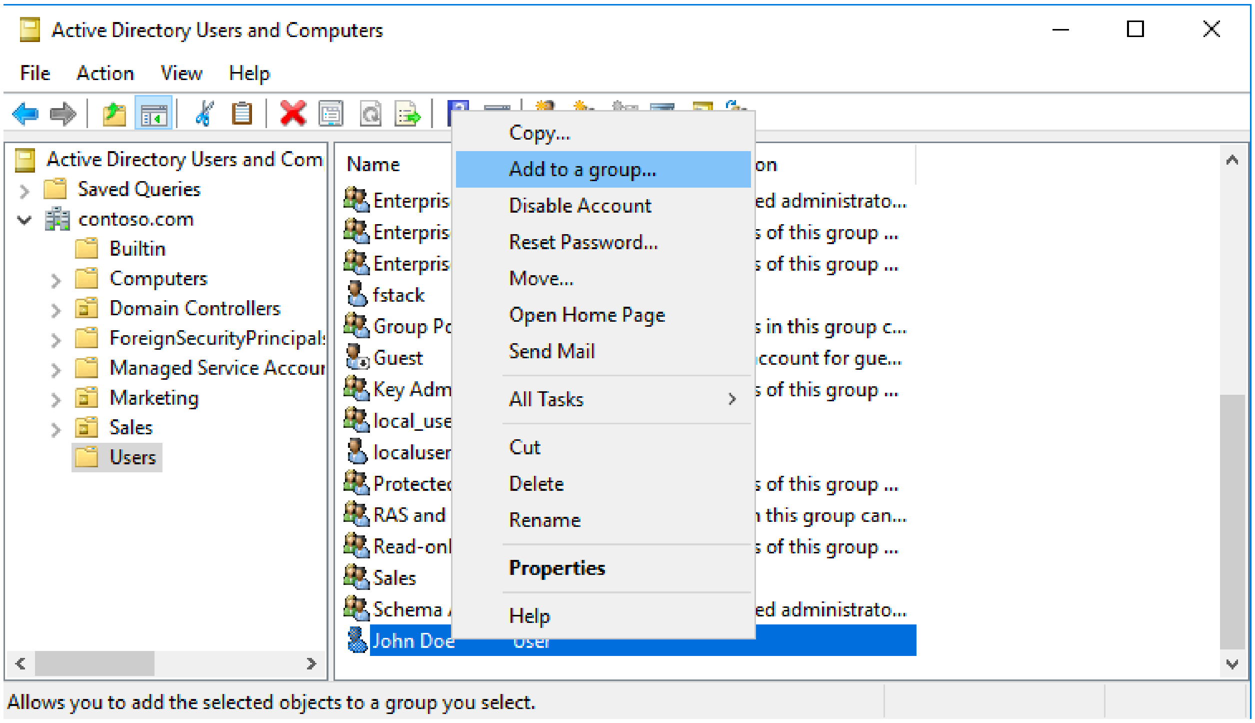
Step 3: Place the user into their respective group-

If the user’s group doesn’t already exist, then we must first create it. To do this, navigate to the “users” folder in the active directory, right click in the folder, and select “new” and then “group.”

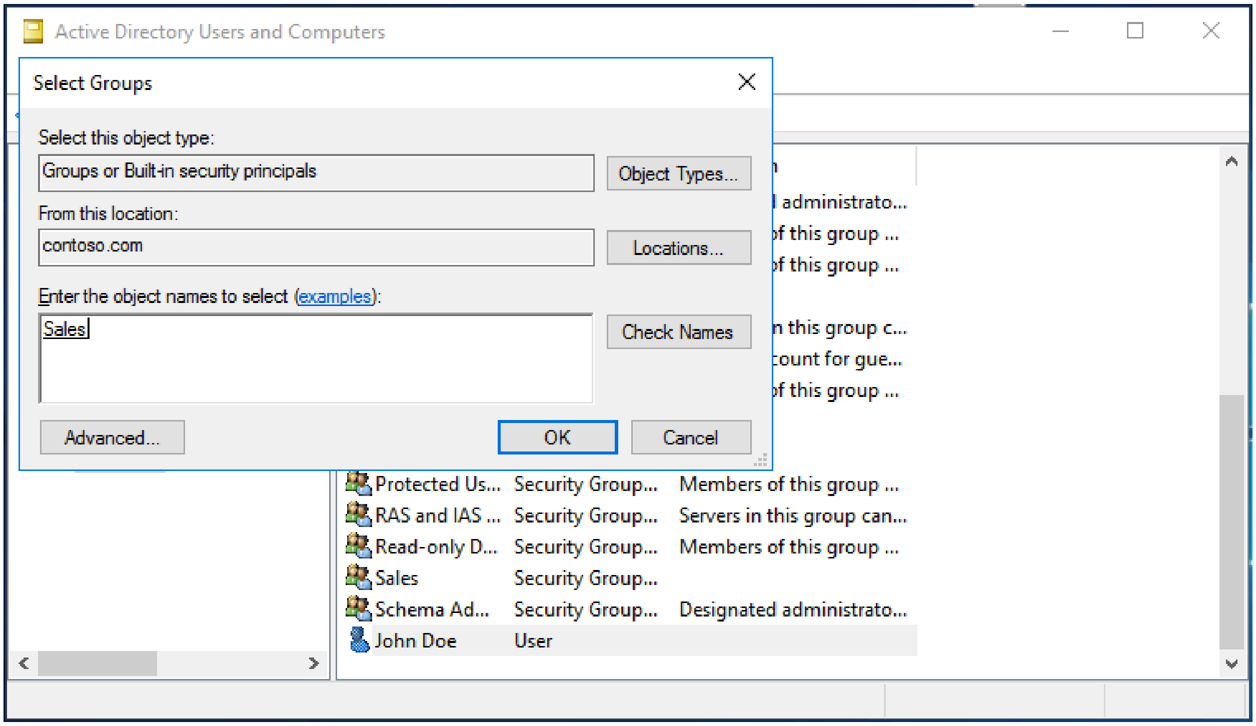


Create a new object...

Create the group by entering the group name and then add the user to the group. To do this, right click the user and click “Add to a group.” Then, simply select the group that the user belongs to and click “OK.”



Allows you to add the selected objects to a group you select.



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

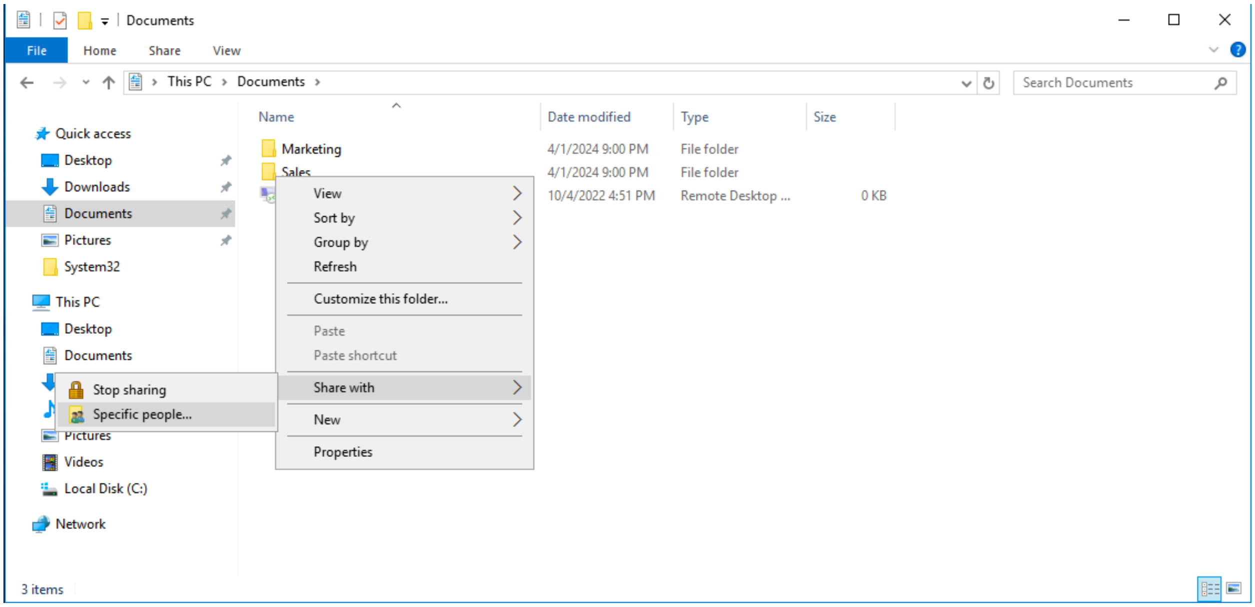
From this location:
contoso.com

Enter the object names to select (examples):
Sales

		l administrato...
		of this group ...
		of this group ...
		n this group c...
		count for gue...
		of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Sales	Security Group...	
Schema Ad...	Security Group...	Designated administrato...
John Doe	User	

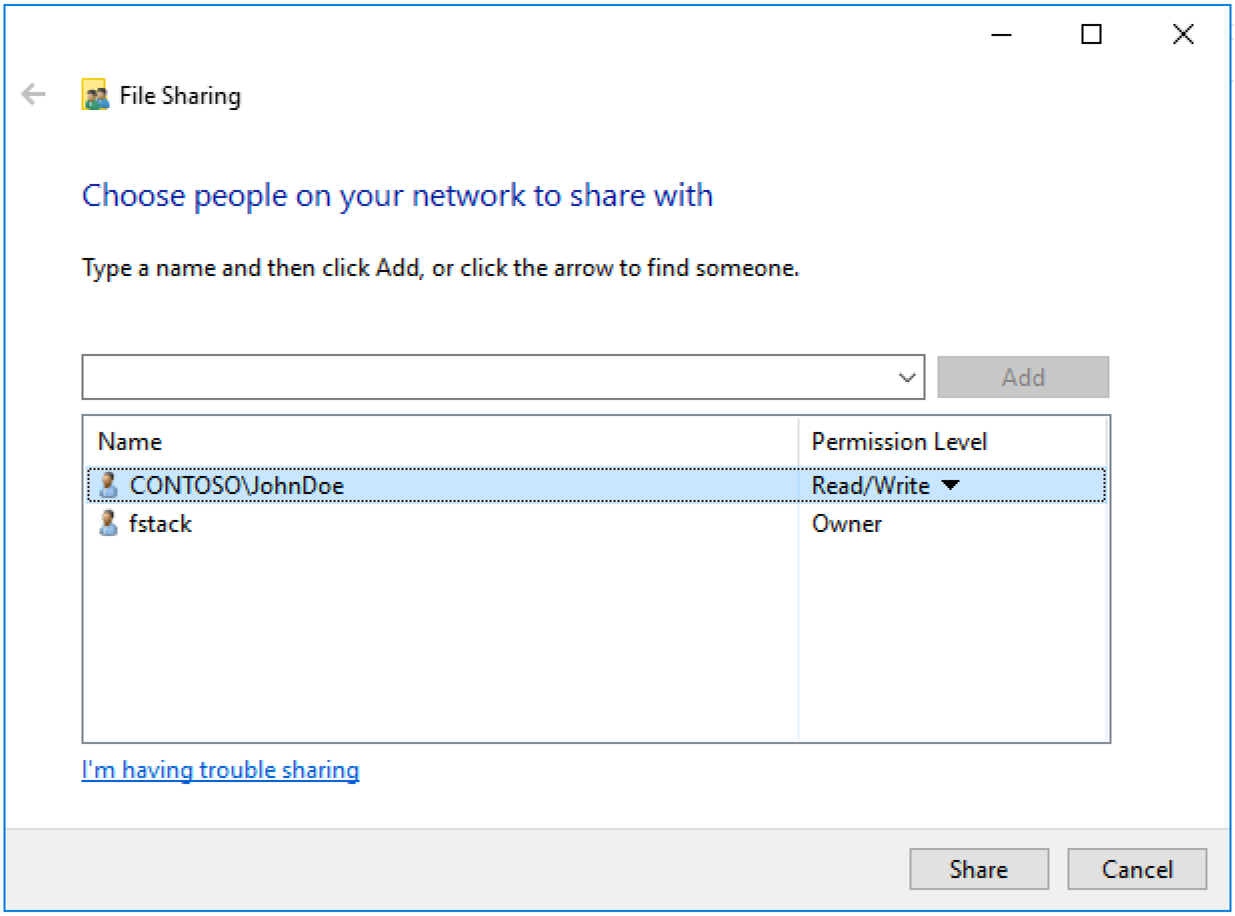
Step 4: Create a shared folder-

To create a shared folder, first open the file explorer and navigate to “Documents.” Right click anywhere and create a new folder. In this case we will be creating a “Sales” folder. Once the folder is created, right click on the folder and click “share with” and then “specific people.”



Name	Date modified	Type	Size
Marketing	4/1/2024 9:00 PM	File folder	
Sales	4/1/2024 9:00 PM	File folder	
	10/4/2022 4:51 PM	Remote Desktop ...	0 KB

Enter the name of the user and set the permissions to read and write.



Choose people on your network to share with

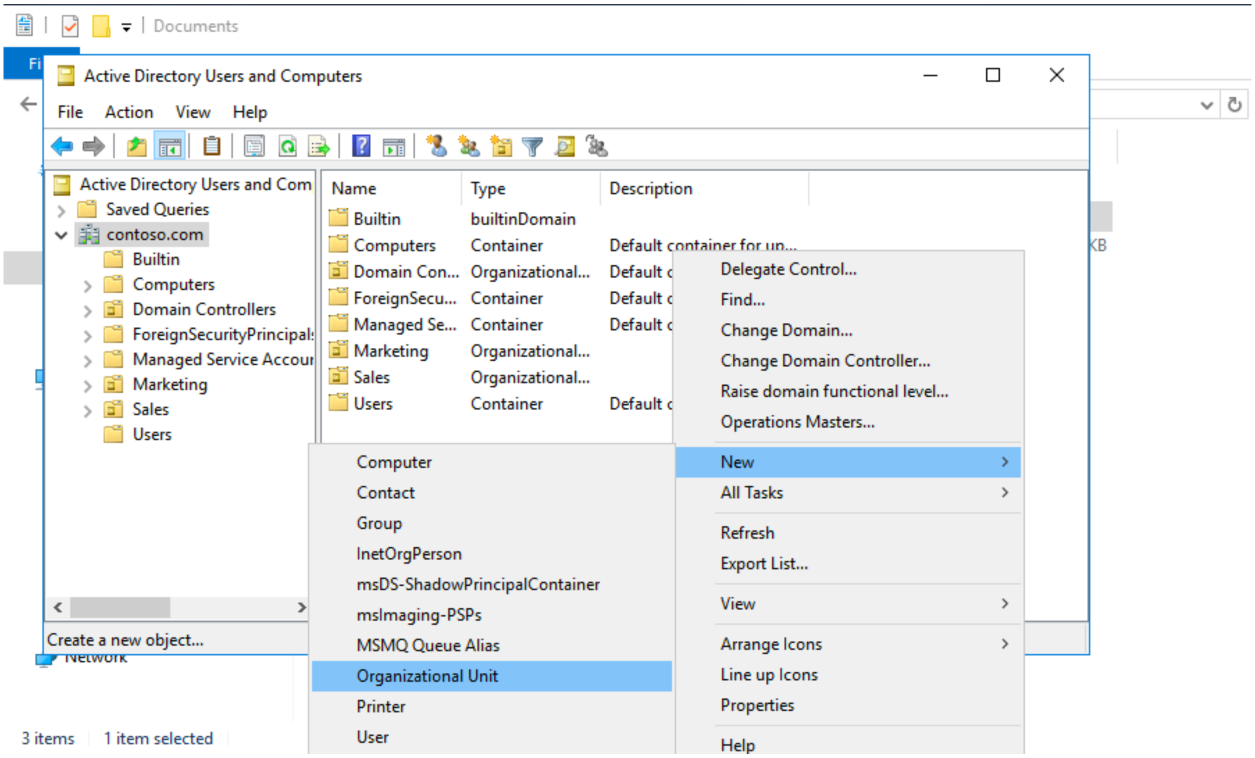
Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
CONTOSO\JohnDoe	Read/Write ▼
fstack	Owner

Click “Share” and the folder should be shared to the user.

Step 5: Create an organizational unit-

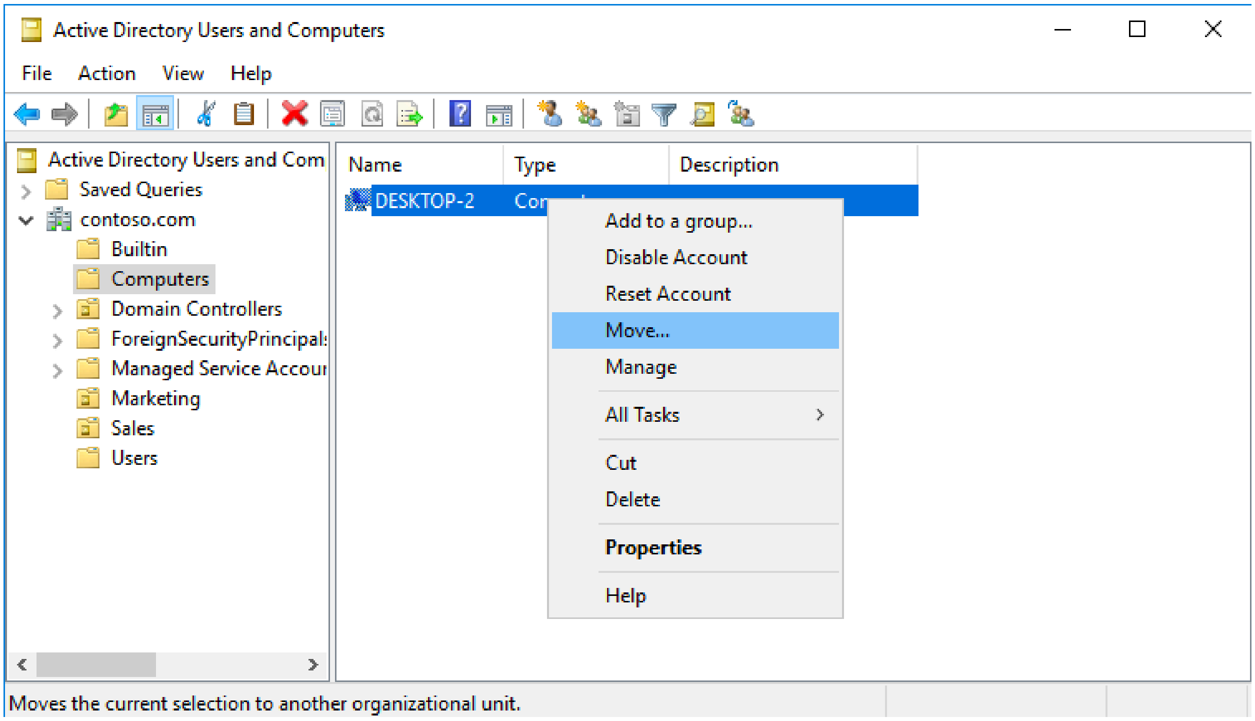
To create an OU, we must go back to the active directory. Navigate to the contoso.com folder, right click anywhere, select “new” and then “organizational unit.” Name the OU “Sales” and then create it.



Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default c
ForeignSecu...	Container	Default c
Managed Se...	Container	Default c
Marketing	Organizational...	
Sales	Organizational...	
Users	Container	Default c

Create a new object...

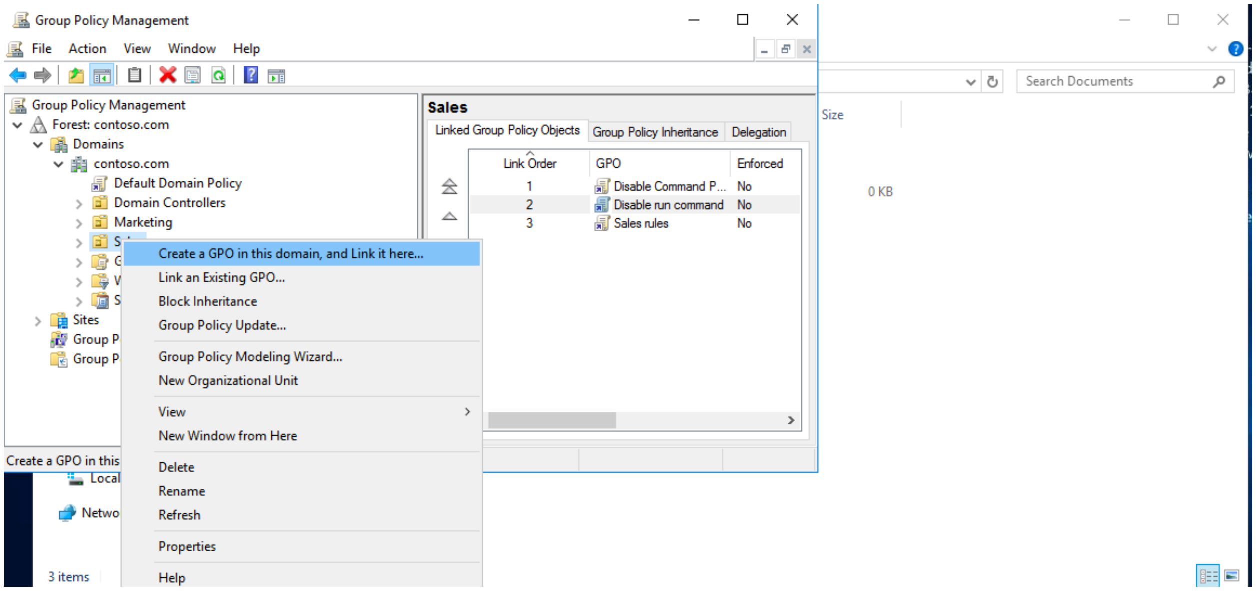
To move the users and computers to the organizational unit, simply find the respective computer/user, right click them, select “move,” and select the destination OU.



Name	Type	Description
DESKTOP-2	Con	

Moves the current selection to another organizational unit.

To create a group policy object and link it to the OU, first open up the Group Policy Management application. Then, right click the respective OU, click “create a GPO in this domain, and link it here” and name the GPO.

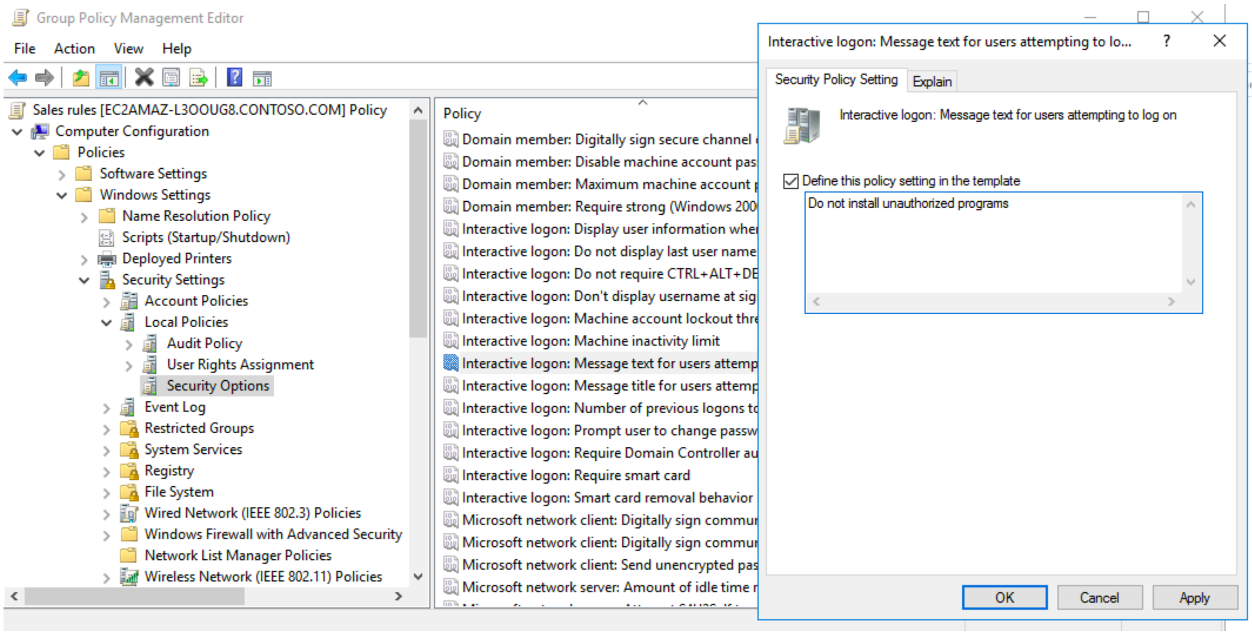


Link Order	GPO	Enforced
1	Disable Command P...	No
2	Disable run command	No
3	Sales rules	No

Step 6: Edit the group policy-

To edit the GPO find the GPO you just created, right click it, and click “edit.” This will open up the group policy management editor window.

The first rule to add to the GPO is to include a message to users upon logging in that says: “do not install unauthorized programs.” To do this, navigate to “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Security Options.” Then, click on “Interactive logon: message text for users attempting to log on. Then, add the desired message and click “OK.”



Policy

- Domain member: Digitally sign secure channel
- Domain member: Disable machine account pas
- Domain member: Maximum machine account
- Domain member: Require strong (Windows 200
- Interactive logon: Display user information whe
- Interactive logon: Do not display last user name
- Interactive logon: Do not require CTRL+ALT+DE
- Interactive logon: Don't display username at sig
- Interactive logon: Machine account lockout thre
- Interactive logon: Machine inactivity limit
- Interactive logon: Message text for users attemp
- Interactive logon: Message title for users attemp
- Interactive logon: Number of previous logons to
- Interactive logon: Prompt user to change passw
- Interactive logon: Require Domain Controller au
- Interactive logon: Require smart card
- Interactive logon: Smart card removal behavior
- Microsoft network client: Digitally sign commu
- Microsoft network client: Digitally sign commu
- Microsoft network client: Send unencrypted pas
- Microsoft network server: Amount of idle time

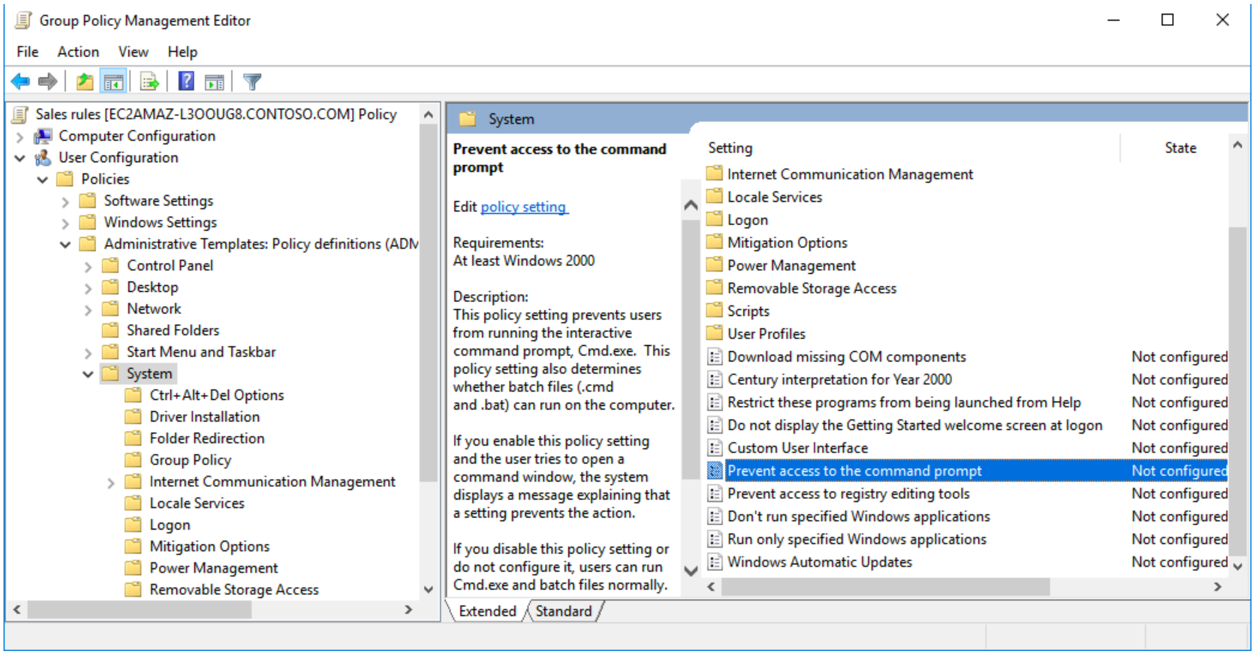
Interactive logon: Message text for users attempting to lo...

Interactive logon: Message text for users attempting to log on

☑ Define this policy setting in the template

Do not install unauthorized programs

The next rule is to disable the user’s access to the command prompt. To do this, navigate to “User Configuration” -> “Policies” -> “Administrative Templates” -> “System.” In the system folder, find the policy “Prevent access to the command prompt.” Double click it and select “enabled,” then click “OK.”



System

Prevent access to the command prompt

Edit policy setting

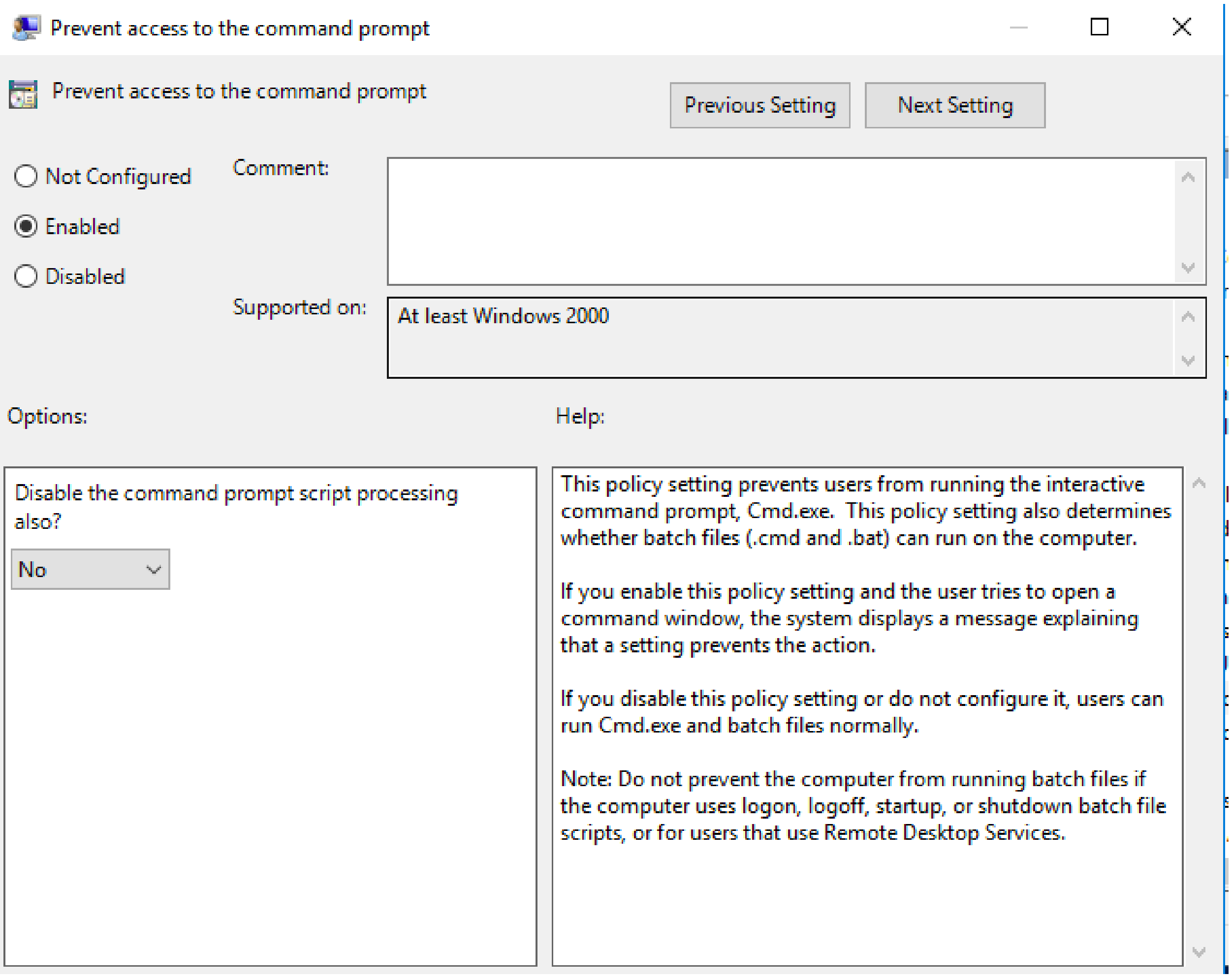
Requirements:
At least Windows 2000

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.

Setting	State
Internet Communication Management	
Locale Services	
Logon	
Mitigation Options	
Power Management	
Removable Storage Access	
Scripts	
User Profiles	
Download missing COM components	Not configured
Century interpretation for Year 2000	Not configured
Restrict these programs from being launched from Help	Not configured
Do not display the Getting Started welcome screen at logon	Not configured
Custom User Interface	Not configured
Prevent access to the command prompt	Not configured
Prevent access to registry editing tools	Not configured
Don't run specified Windows applications	Not configured
Run only specified Windows applications	Not configured
Windows Automatic Updates	Not configured



Prevent access to the command prompt

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?

No

Help:

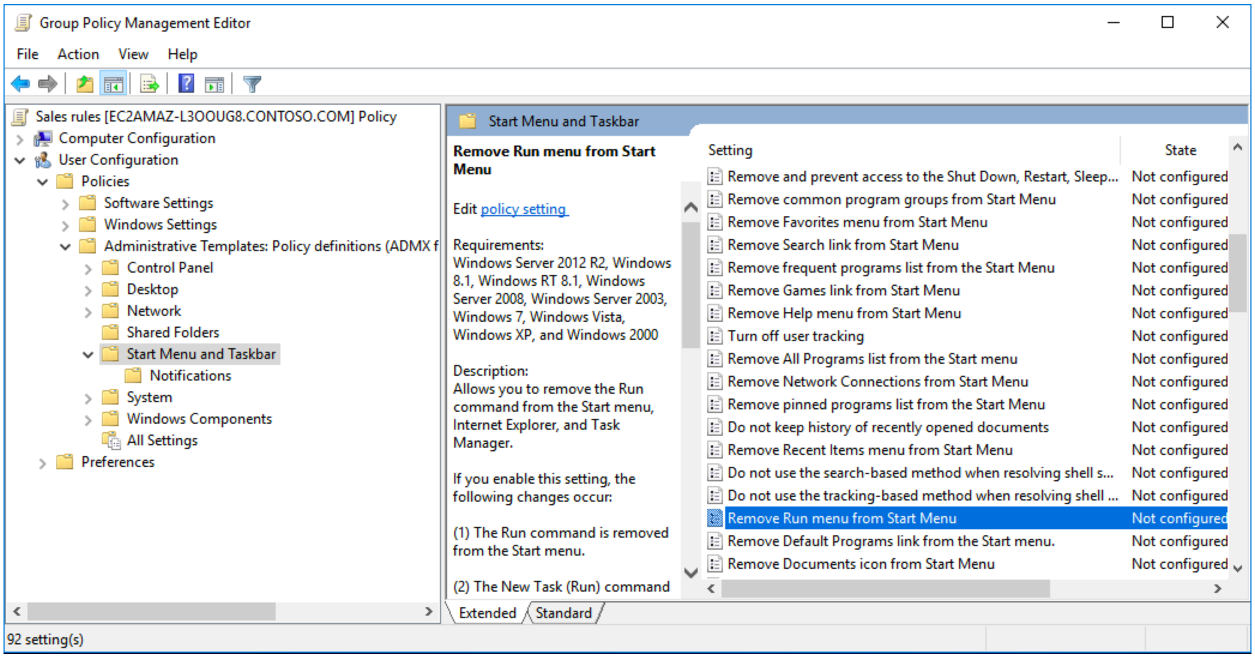
This policy setting prevents users from running the interactive command prompt, Cmd.exe. This policy setting also determines whether batch files (.cmd and .bat) can run on the computer.

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.

Finally, we want to disable the run command from the start menu. To do this, navigate to “User Configuration” -> “Policies” -> “Administrative Templates” -> “Start Menu and Taskbar.” Scroll down until you find “Remove run menu from start menu.” Double click it and select “Enabled,” then click “OK”



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:

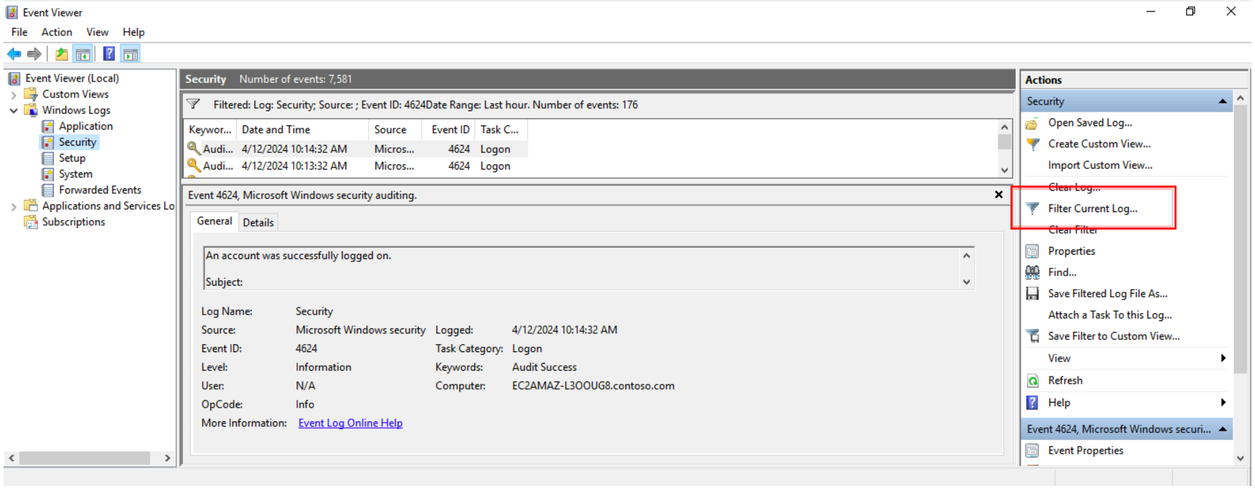
(1) The Run command is removed from the Start menu.

(2) The New Task (Run) command

Setting	State
Remove and prevent access to the Shut Down, Restart, Sleep...	Not configured
Remove common program groups from Start Menu	Not configured
Remove Favorites menu from Start Menu	Not configured
Remove Search link from Start Menu	Not configured
Remove frequent programs list from the Start Menu	Not configured
Remove Games link from Start Menu	Not configured
Remove Help menu from Start Menu	Not configured
Turn off user tracking	Not configured
Remove All Programs list from the Start menu	Not configured
Remove Network Connections from Start Menu	Not configured
Remove pinned programs list from the Start Menu	Not configured
Do not keep history of recently opened documents	Not configured
Remove Recent Items menu from Start Menu	Not configured
Do not use the search-based method when resolving shell s...	Not configured
Do not use the tracking-based method when resolving shell ...	Not configured
Remove Run menu from Start Menu	Not configured
Remove Default Programs link from the Start menu.	Not configured
Remove Documents icon from Start Menu	Not configured

Step 7: Check the event viewer for the last successful login-

To check the last successful login, open the Event Viewer application. In the Event Viewer, navigate to “Windows Logs,” then “Security.” To check for logins, we can filter this log. On the right hand side, click “Filter Current Log.” You can then change the time frame to the past hour and change the event id to 4624, which is a successful login.



Security Number of events: 7,581

Filtered: Log: Security; Source: ; Event ID: 4624Date Range: Last hour. Number of events: 176

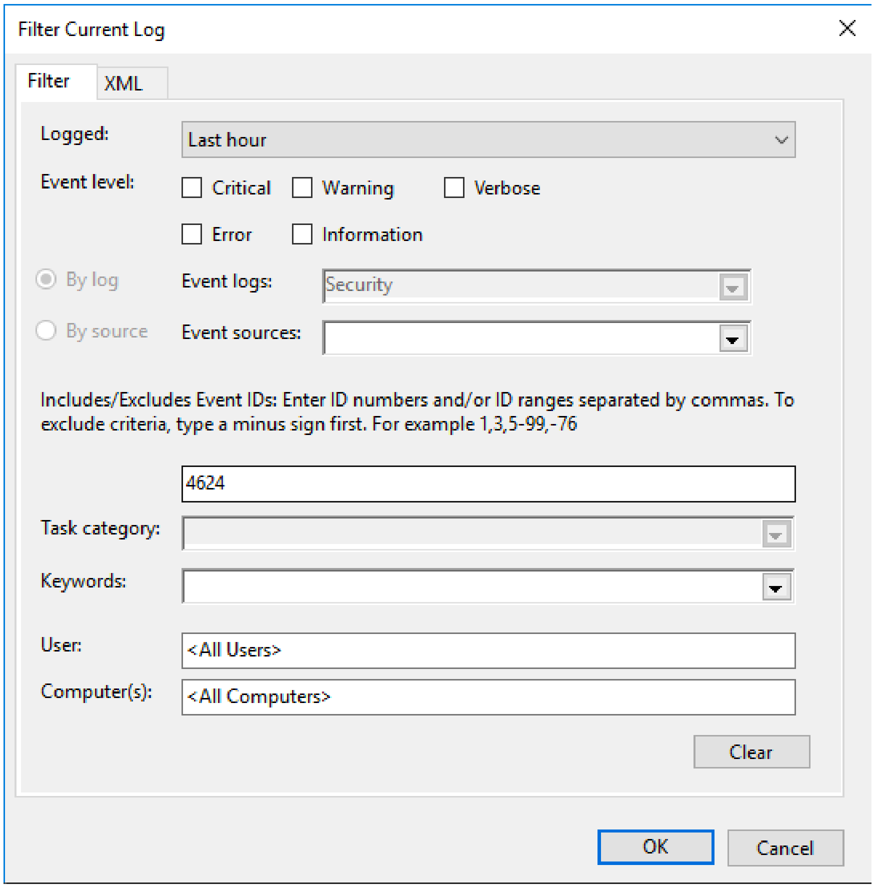
Keywor...	Date and Time	Source	Event ID	Task C...
Audi...	4/12/2024 10:14:32 AM	Micros...	4624	Logon
Audi...	4/12/2024 10:13:32 AM	Micros...	4624	Logon

Event 4624, Microsoft Windows security auditing.

An account was successfully logged on.

Subject:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	4/12/2024 10:14:32 AM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	EC2AMAZ-L3OOUG8.contoso.com
OpCode:	Info		
More Information:	Event Log Online Help		



Logged: Last hour

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: Security

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4624

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Step 8: Use Powershell to check the latest installed program-

To check the latest installed programs, we must first open up Powershell. When we are in Powershell, type the command `Get-AppxPackage` to see a list of all installed Microsoft app packages. To check the latest installed programs for our specific user, open Powershell as administrator and run the command `Get-AppxPackage -user JohnDoe`

Step 9: Write a Powershell script that lists all running services-

To list all running services, open Powershell and run the following command:

```
Get-Service | where-object { $_.Status -eq 'running' }
```

Next, we just need to redirect the output to a file. To do this, we will add the following changes to the previous command:

```
Get-Service | where-object { $_.Status -eq 'running' } | Out-File
-FilePath C:users\fstack\desktop\services.txt
```