

StackFull Software: New Hire Machine Setup

Confidentiality Notice: *This runbook document is for internal purposes only, contains sensitive personal and company information, and is highly classified. Do not share it with anyone. Breach of this confidentiality policy is grounds for immediate termination and legal fines.*

If you have questions about this policy, or any other questions regarding our information security policies, please reach out to Will Schmidt (SOC Analyst): will@stackfull.com / 314-610-2954

Why Do We Use Runbooks?

An IT runbook is a set of standardized, written procedures that help us formally document our procedures at StackFull Software. They exist as part of our IT Infrastructure Library protocols and touch on everything from routine topics and infrastructure provisioning all the way to emergency operations.

The purpose of this specific runbook is to walk you through the process we take when setting up a new hire's machine. It's important we have everything ready for the new hire before their onboarding begins, so they can arrive on day one and jump right into their new role.

You'll notice that we've also consulted with Will Schmidt, SOC analyst, for all of our runbooks. It's crucial that we both work together to build secure systems, operations, and processes from step zero to minimize our risk appetite and tolerance.

Throughout this runbook, our SOC team has contributed notes on security that you should always be aware of. If you follow this runbook, and reach out with any clarifying questions before implementing changes, you'll help ensure we avoid unnecessary risks and vulnerabilities.

Let's dive in!

Setting Up A New Hire's Machine

New hire and machine details:

- **Name:** John J. Rambo
- **Role:** Account Executive
- **Department:** Sales
- **Machine:** Desktop-2 (virtualized)

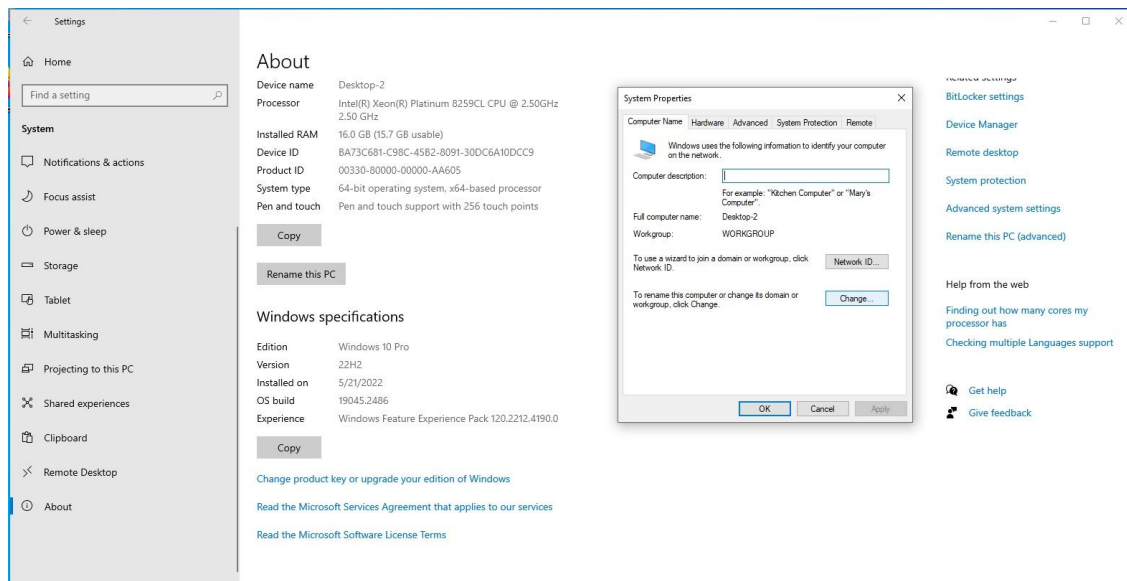
Note from SOC: *These details will change with every new hire. Do your due diligence. Please double, triple, and quadruple check that you have the right information before beginning.*

Step 1: Join the Computer to the Domain

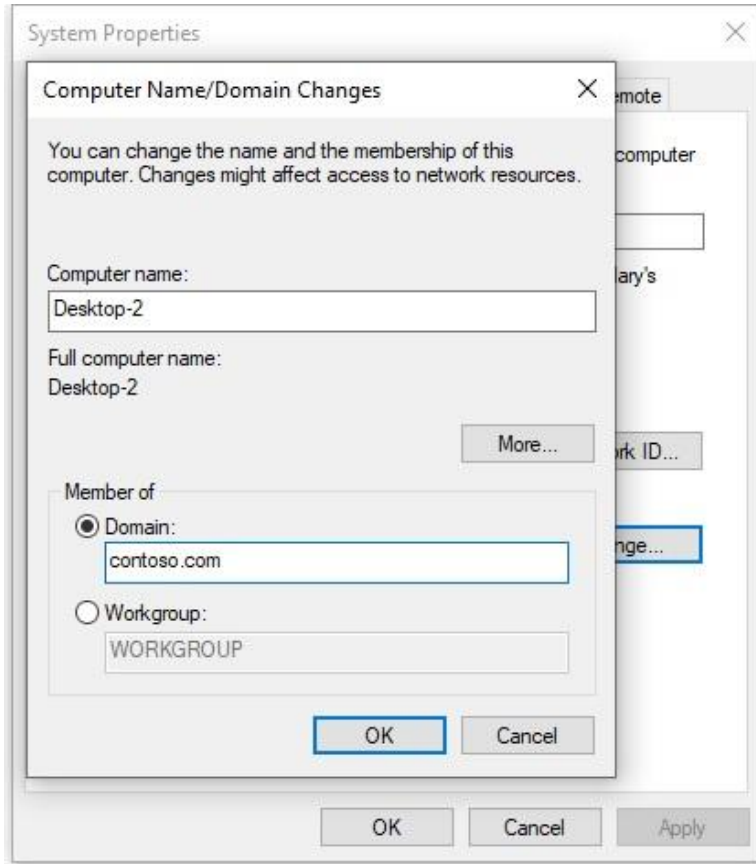
Whenever we have a new machine, we first need to add it to our domain before we create users, groups, or assign permissions. To start, log on to the new machine with your admin credentials.

Open “Settings,” click “System,” and then “About.” In the panel on the right side of the screen, click “Advanced System Settings.”

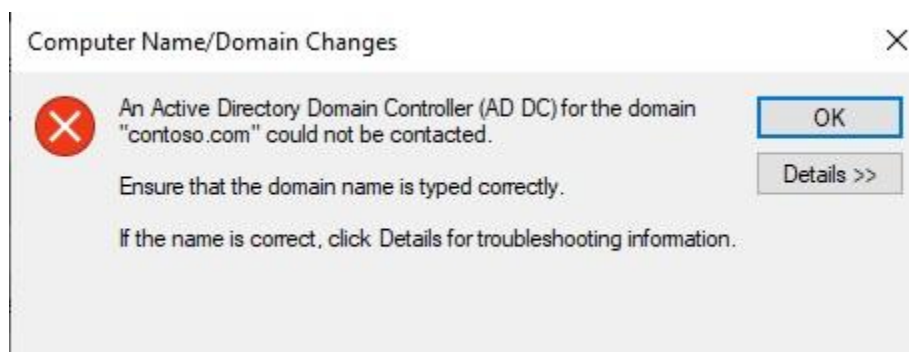
Click on the “Computer Name” tab and then the button “Change.”



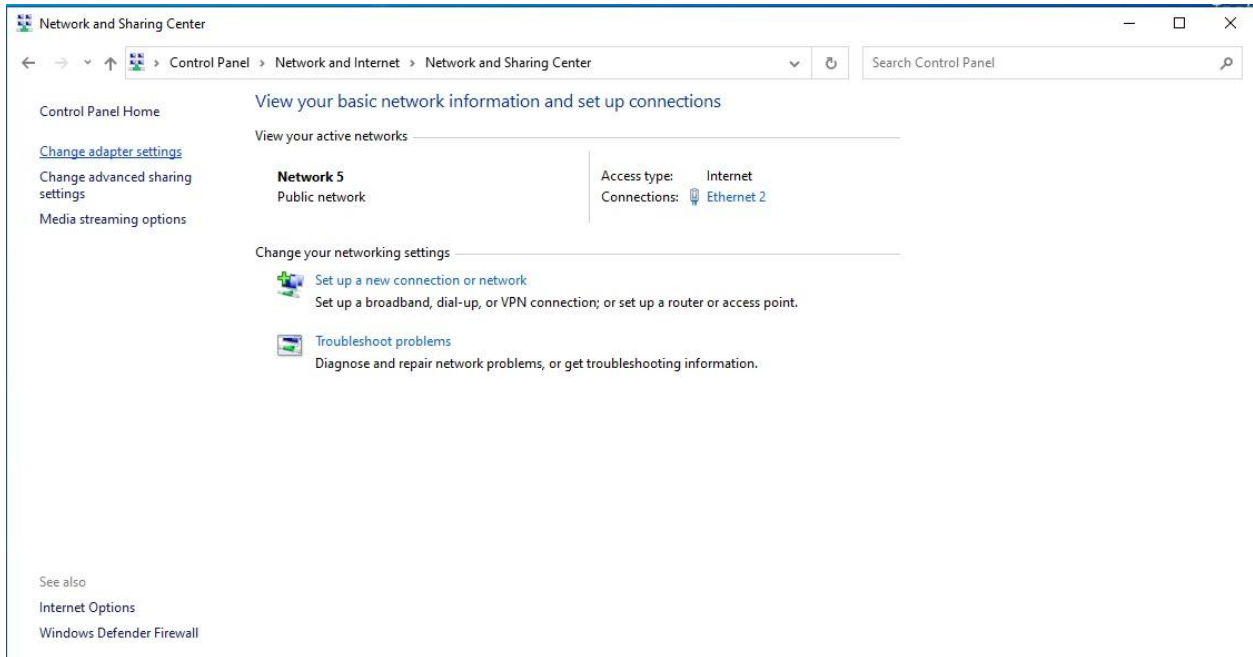
This will open another window where you click “Member of” and then “Domain.” Enter your domain name here, which you’ll receive directly from your manager.



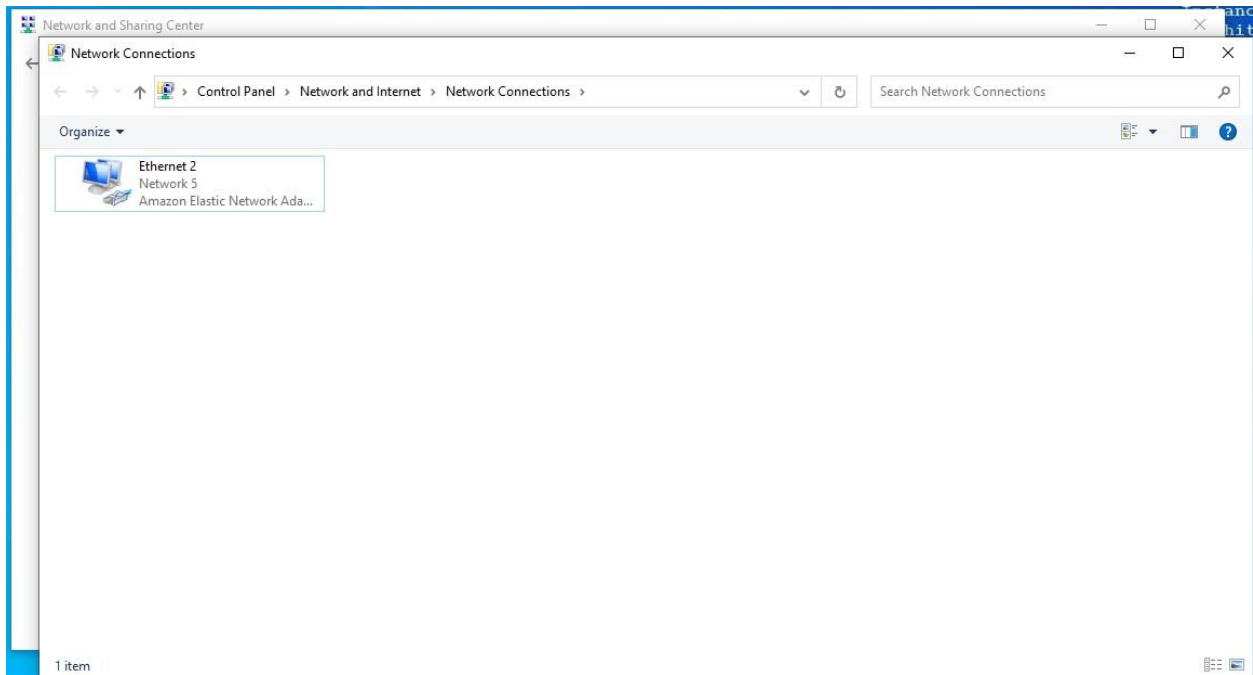
There's a chance this will return an error. If it does, that means we'll have to manually change the IPv4 settings to communicate with our Domain Controller (DC) which acts as the DNS server for our domain. But don't worry, it's not that complicated. If you do get this, please let the IT Manager know so they can investigate further.



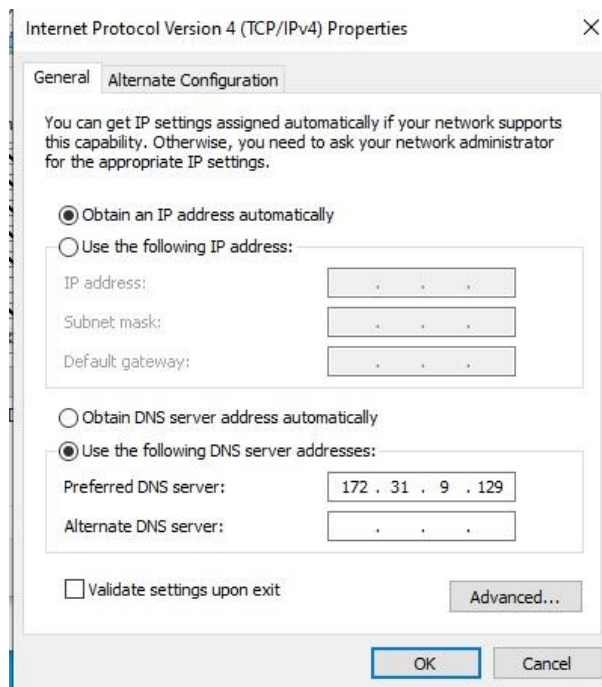
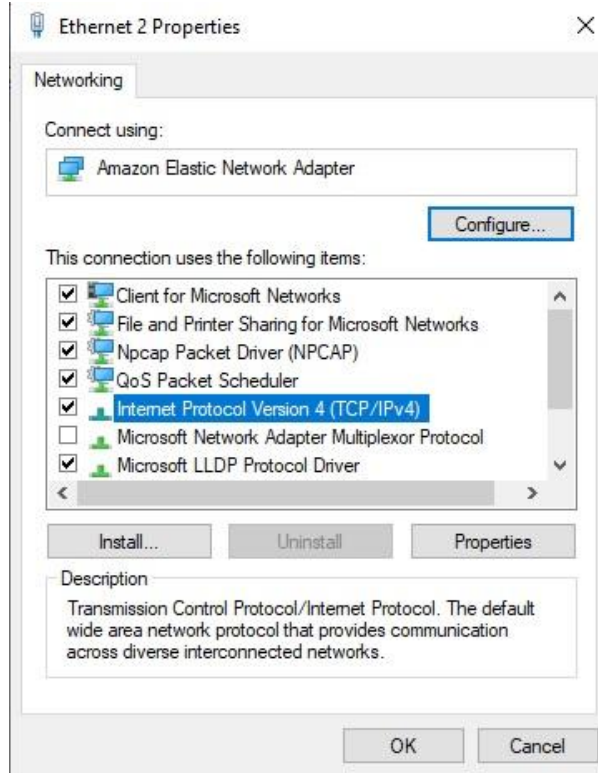
To fix this, go to the Control Panel, click "Network and Internet" and then navigate to the "Network and Sharing Center." Click "Change Adapter Settings" in the left panel.



This opens another window where you'll see your network adapter.




Right click on your adapter and click on "Properties." This opens the properties for the adapter. Find "Internet Protocol Version 4 (TCP/IPv4)" on the list and double click it.



In this new menu, click "Use the following DNS server address." Then, enter the IP address for our DC. Click "OK."

Now, navigate back to “Settings,” “System,” “Advanced System Settings,” and re-enter your domain. It will pull up a dialogue where you can log in with your admin credentials to join the domain.



The image shows a Windows Security dialog box titled "Computer Name/Domain Changes". The dialog box has a close button (X) in the top right corner. Below the title, there is a subtitle "Enter the name and password of an account with permission to join the domain." Below this, there are two input fields: "User name" and "Password". At the bottom of the dialog box, there are two buttons: "OK" and "Cancel".

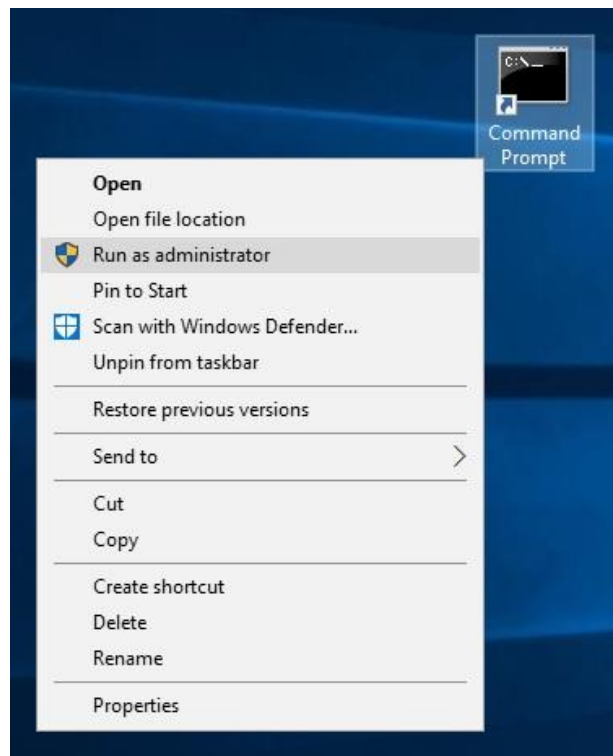
You'll receive a confirmation that welcomes you to the domain. Restart the machine to implement the changes.

Note from SOC: *The domain and the specific IP address for the DC server are sensitive pieces of information. Do not write these down on any kind of paper, and do not leave them in a public place where anyone can find them. Be aware of who is near you when entering this information as well. Consult the IT Manager if you forget the details or need assistance.*

Step 2: Create a Username and Password for the New Hire

Now, it's time to create a username and password for our new hire. To do this, you'll have to switch back to our main server machine.

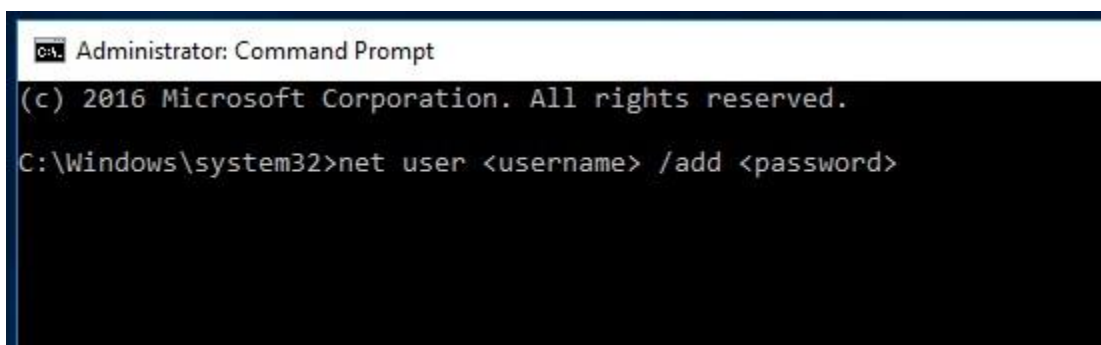
Open the command prompt as an administrator. Right click on the command prompt and click "Run as administrator."



To create a new user, run this command:

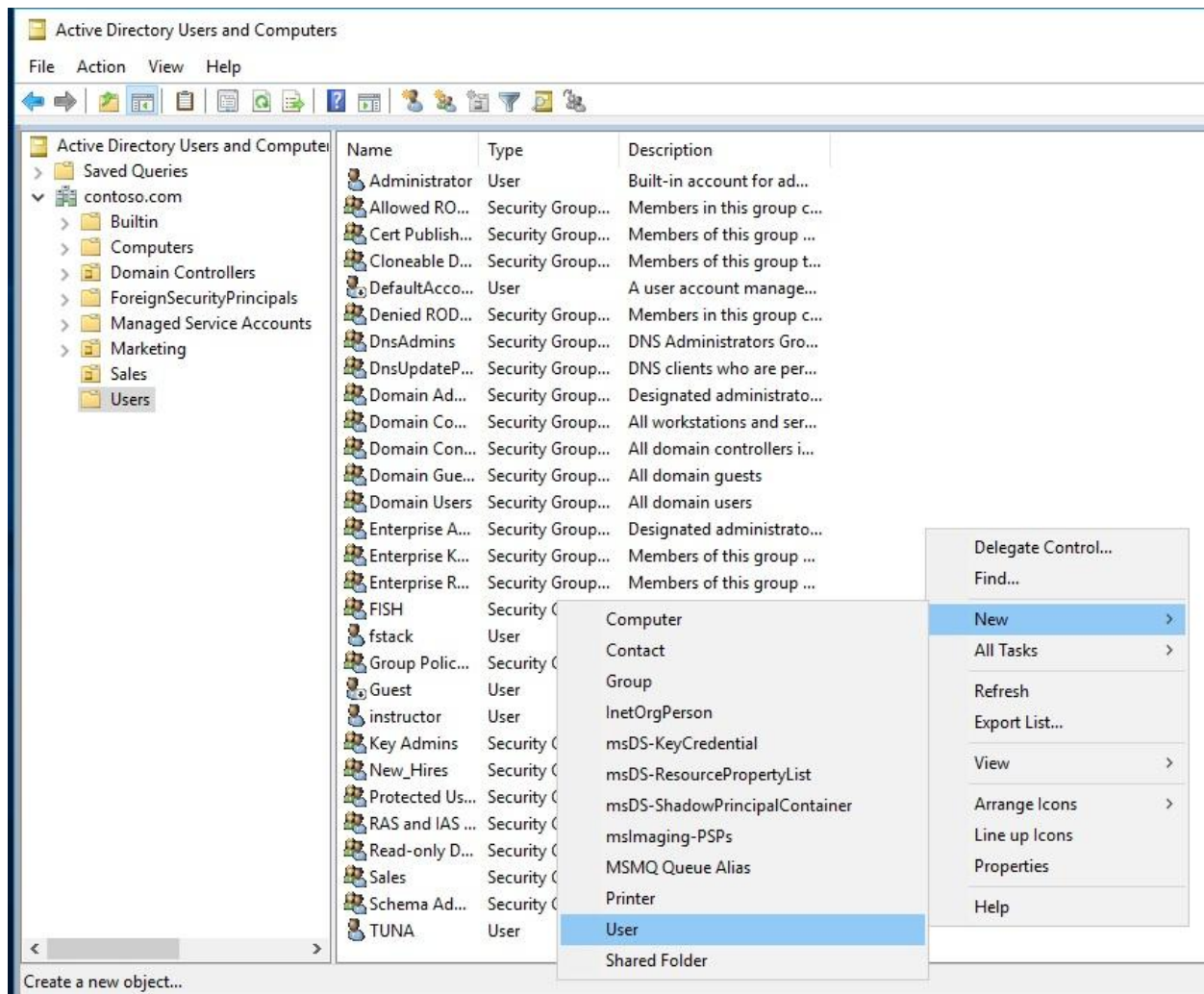
```
net user <username> /add <password>
```

When finished, it will read "The command completed successfully."

A screenshot of a Windows Command Prompt window titled 'Administrator: Command Prompt'. The window has a black background with white text. The text displayed is: '(c) 2016 Microsoft Corporation. All rights reserved.' followed by a new line and the command 'C:\Windows\system32>net user <username> /add <password>'.

Note from SOC: Never use generic passwords like 12345, admin, etc. Never repeat passwords for new users. Everyone gets a unique password, every time. Think about if an attacker was able to get in and found out we assign every new user a password “admin.” Now, they can enter an account before the new hire, lock them out, and access anything in the domain that user is tied to. It’s a major security risk that we want to avoid at all times.

The new user will be prompted to change their password upon logging into their account for the first time. This task can be completed in Active Directory (AD) as well. Open the Active Directory GUI app, enter the “Users” tab, right click, and click “New User.”

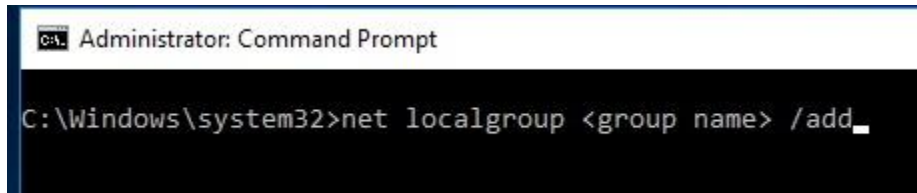


Step 3: Create a Department Group and Place the New Hire In It

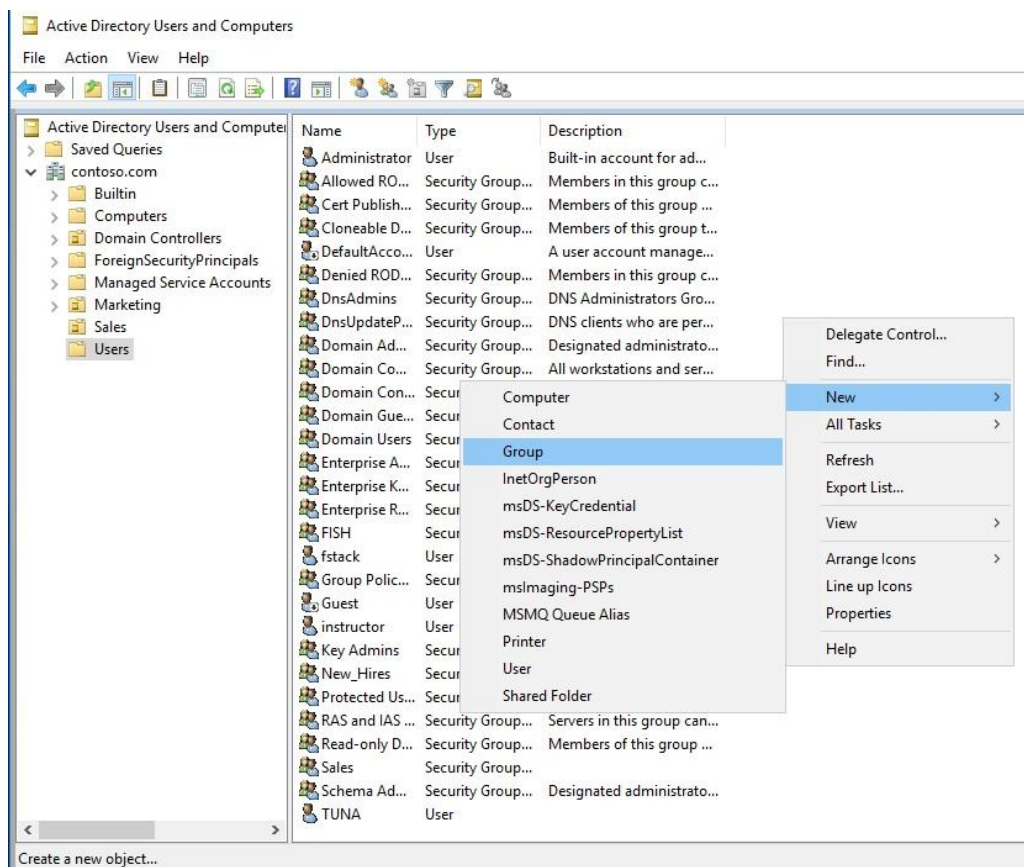
Next, we want to create a new group for this user and add them to it. We can do this either in the administrator command prompt or in Active Directory (AD).

In the command prompt, you would run this code:

```
net localgroup <group name> /add
```



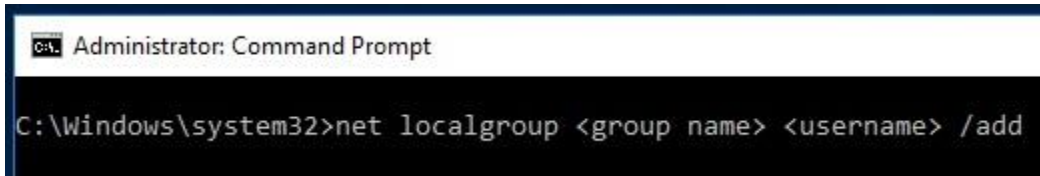
If you want to create it in AD, you would navigate to “Users,” right click, and “Add new group.”



It's worth mentioning that you likely won't need to create new groups though. Typically, all of our groups for departments will already exist. If you find yourself in a unique position to create a new group, it's policy that you clear it with the IT Manager before you take any action.

Since these groups will most likely already exist, in the command line you can easily add new users with the following line:

```
net localgroup <group name> <username> /add
```

A screenshot of a Windows Command Prompt window. The title bar reads "Administrator: Command Prompt". The command prompt shows the command: C:\Windows\system32>net localgroup <group name> <username> /add. The text is displayed in a monospaced font on a dark background.

```
C:\Windows\system32>net localgroup <group name> <username> /add
```

In AD, you right click on a specific user and then “Add to group.” Another important note here: this will only add local groups. We will want to add these users to Organizational Units (OU), but we’ll cover that later in this runbook.

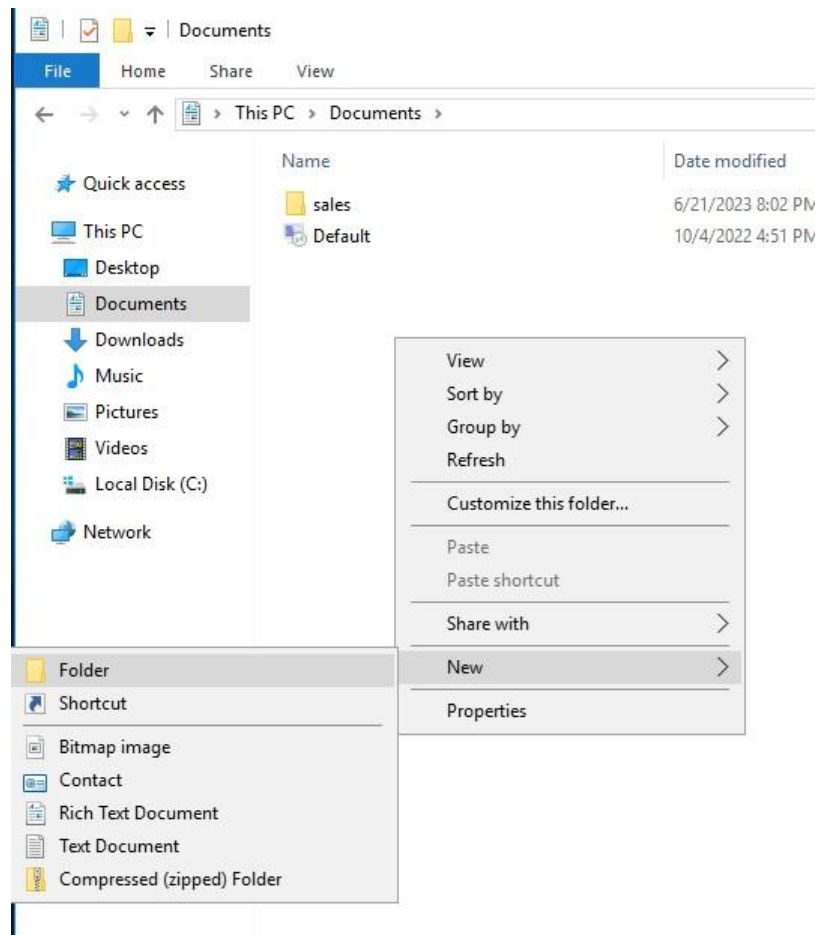
Step 4: Create a Shared Folder on the Server

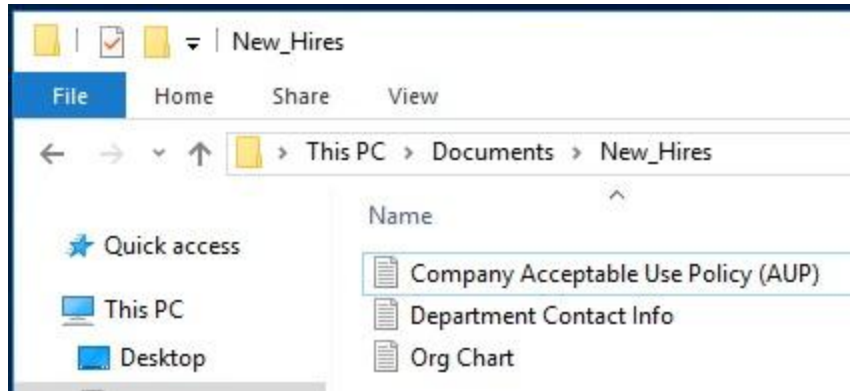
Our next task is to create a shared folder on the server with the department name. Then, we want to share it only with the people who belong to that department with read and write permissions.

We'll want to make sure that every new hire has access to the "New_Hires" shared folder that contains important information they can access from any machine in our domain. For example, it will hold the company Acceptable Use Policy (AUP), organizational charts, and contact information for different departments.

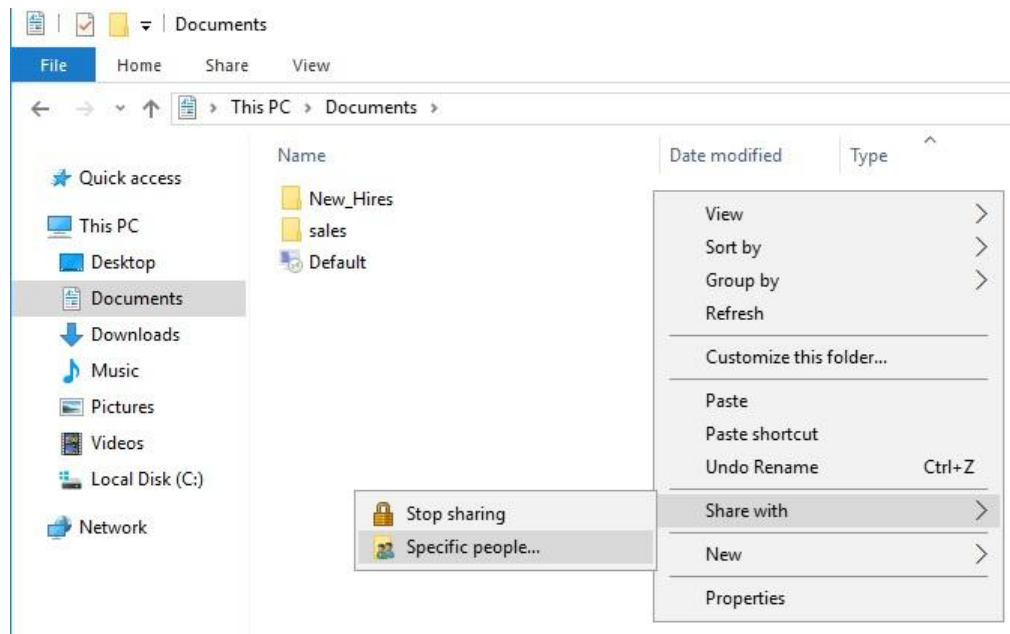
If we ever need to create a new shared folder, here's how we would do it. In this example, we'll be walking you through how we created the "New_Hires" folder.

Create a new folder on the main Domain Controller (DC) machine in the "Documents" directory. After it's created, put all of the files necessary for this group in the folder.

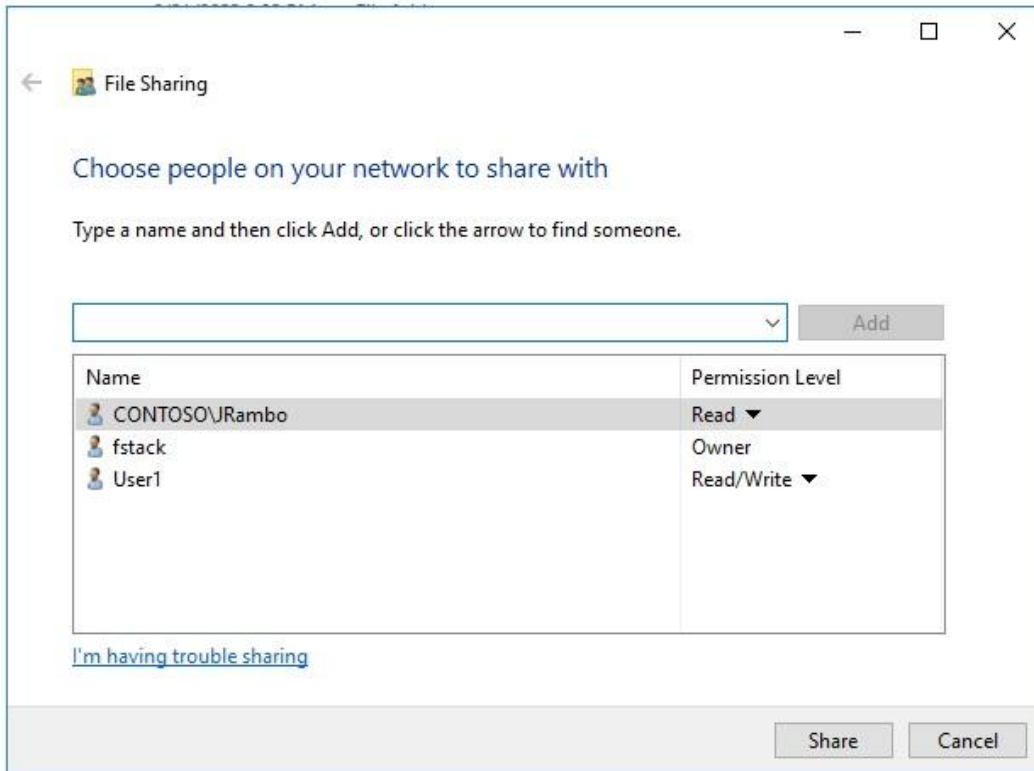




Then, right click the folder and click “Share with.” Select “Specific people.”

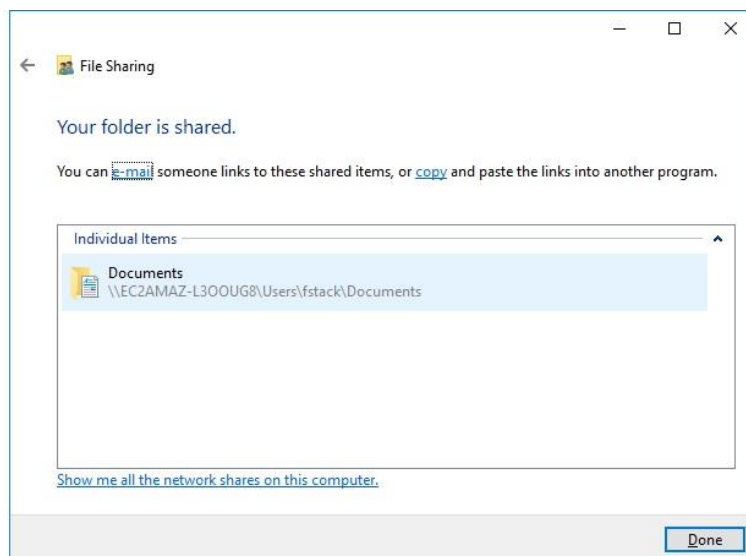


This will open a dialogue that asks who we want to share the folder with. Make sure you input the appropriate user, and add them to the list. Double check they have read and write permissions only.



Note from SOC: Pay very close attention to detail here. Ensure you're typing in the right user or group, and double, triple, quadruple check their permissions are accurate before you click share. This is how we adhere to the Principle of Least Privilege, a core tenant of our security here at StackFull Software. People only get access to things that are absolutely necessary.

Once we've verified all the information for the folder share is correct, we'll click "Share" and it will display the path to the folder on the server. We'll want to share this with the new hires.

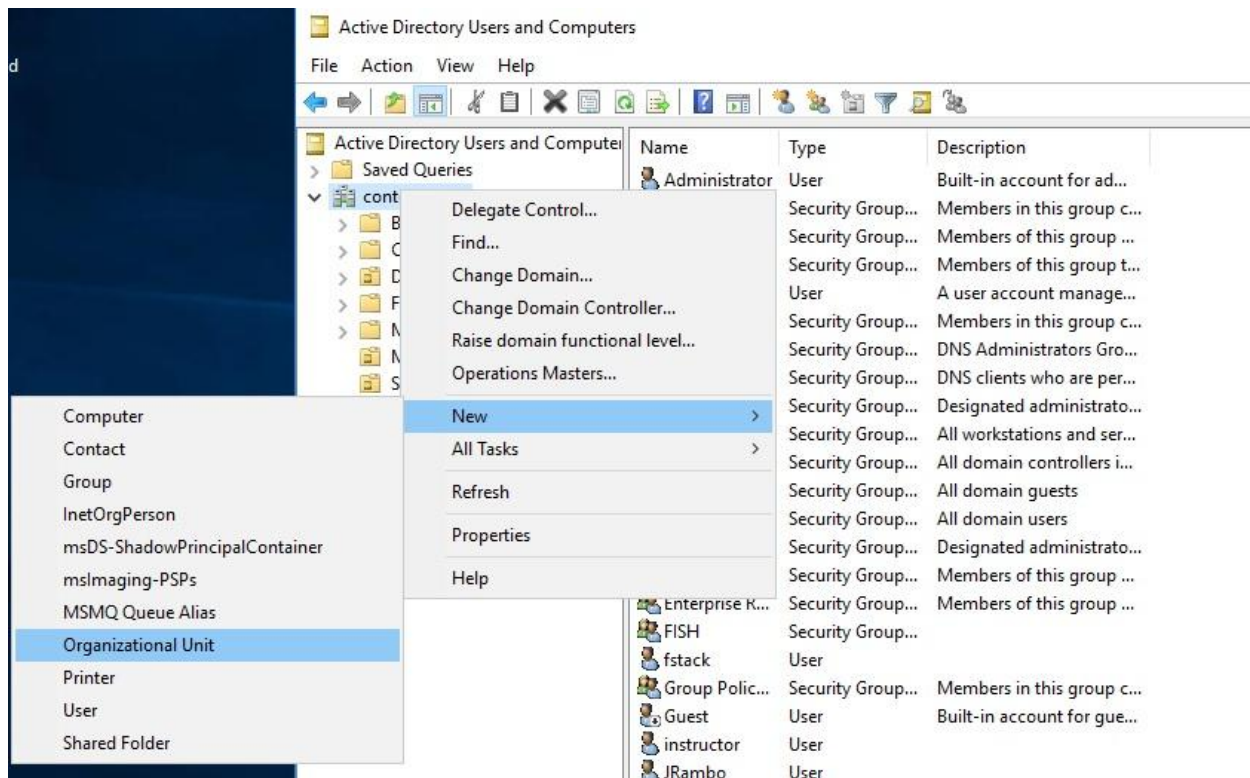


Step 5: Create an Organizational Unit (OU) and Group Policy Object (GPO) for the Department

Now that our user and group is added, it's time to create an Organizational Unit (OU) for the department and add the new hire to it. Then, we want to attach a Group Policy Object (GPO) to that OU. We'll do this all in Active Directory (AD).

Similar to local groups, you likely won't need to create brand new OUs. These will likely already exist. However, if you need to create a new OU first clear it with the IT Manager before taking any action.

In the event you need to create an OU, open the AD app. Then, right click the domain, select "New," and select "Organizational Unit."

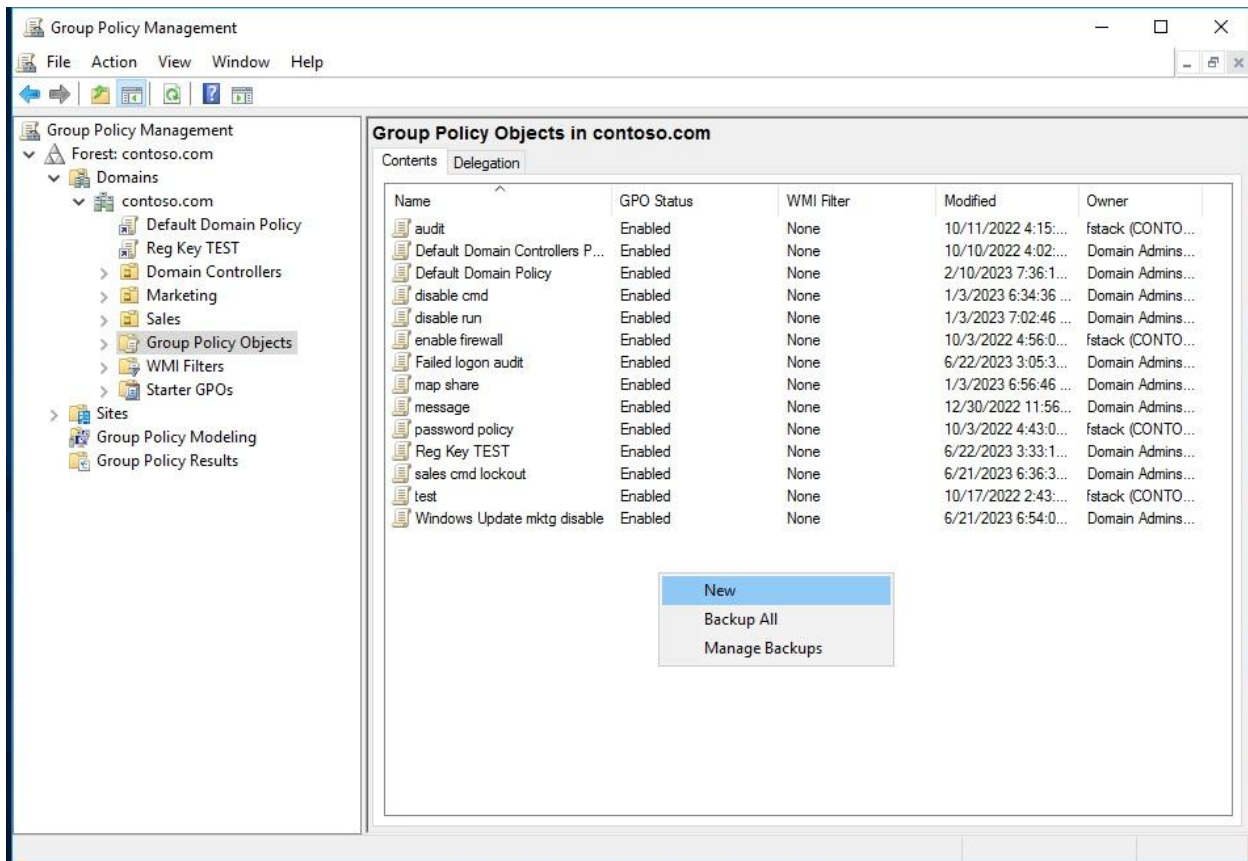


You'll see the OU in the navigation panel on the left. Once it's created, we need to add our user to that OU. We can do this by right clicking on their name, "Add to Group," and then type in the name of the OU. You can also add a new user by simply dragging and dropping them into the proper OU.

Note from SOC: Be extremely careful about what OUs you assign people to. We want to make sure they don't get accidentally added to the wrong OU, which would allow them access to information and data they don't need. Imagine if someone from Sales was accidentally placed in Payroll. They could then see company sensitive financial data.

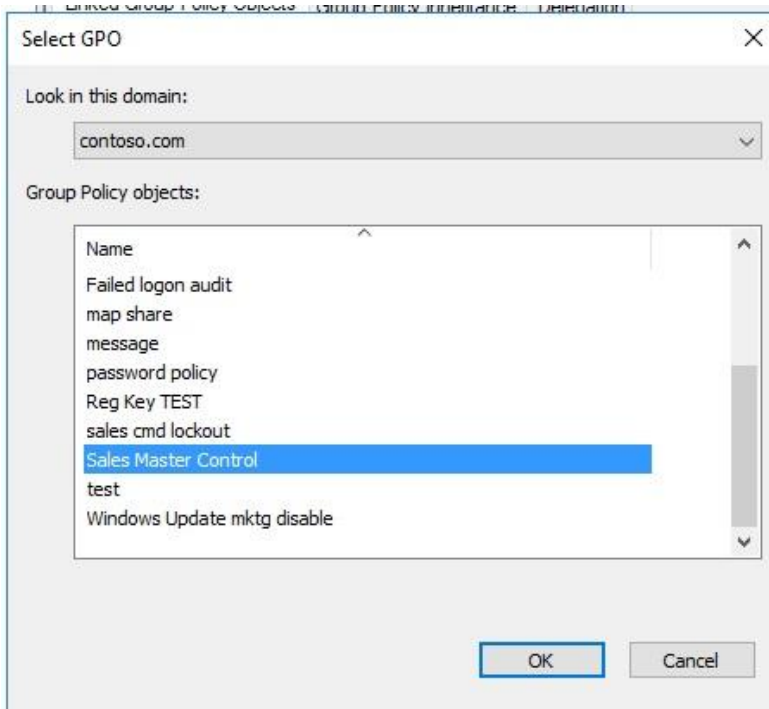
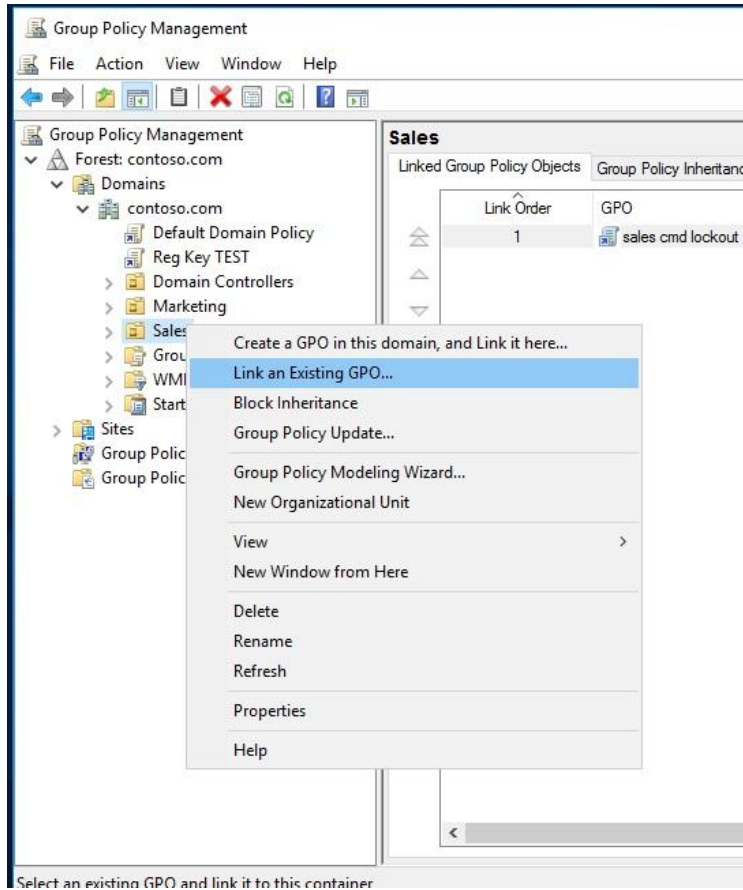
Once they're added to the OU, we want to create a new Group Policy Object (GPO) and attach it to their OU. Everything with Group Policy is done through the Group Policy Management app.

Once you open the Group Policy Management app, right click on "Group Policy Objects." The best practice is to always create new GPOs in this menu and then link them to OUs once they're created. Click "New" and then "Create a GPO."



Title it whatever is most relevant to the policy. For example, if we want to disable the use of the command prompt for Sales, we might title it: "Sales CMD Lockout."

After it's created, we have to link it to the right OU. Right click the OU on the left, click "Link an Existing GPO," and then select the correct GPO you just created.



Sep 6: Edit the Group Policy Object (GPO)

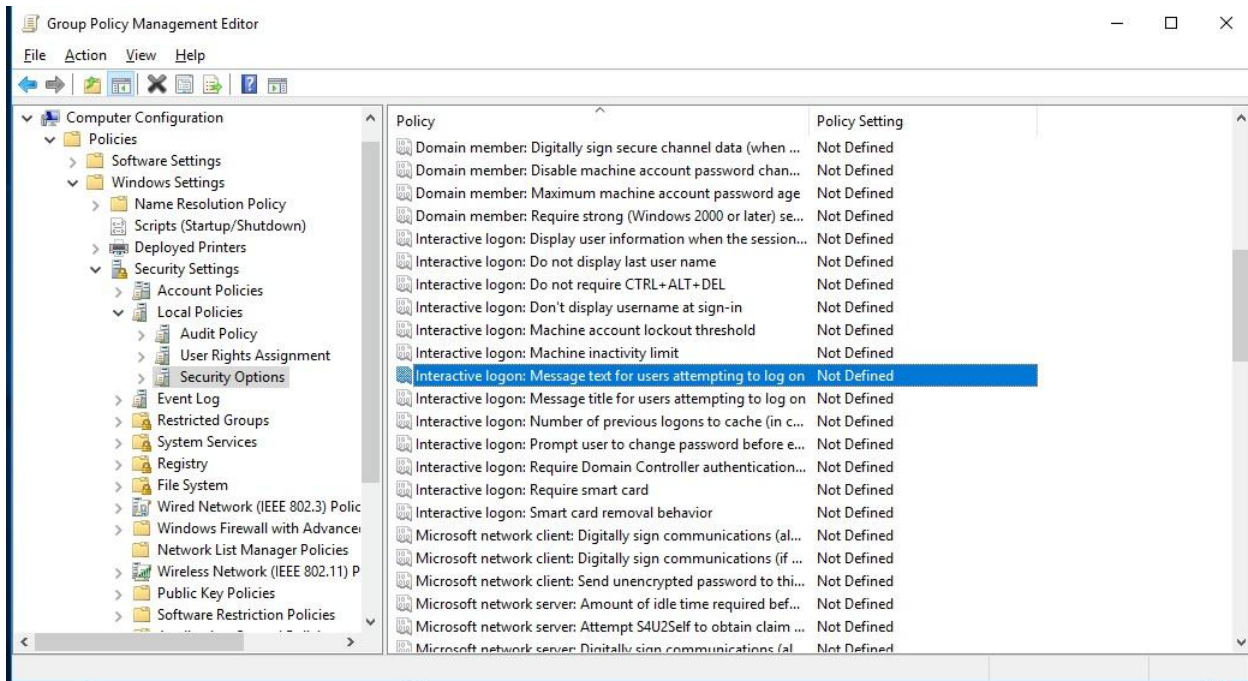
Once the Group Policy Object (GPO) is created and linked, we need to edit the GPO itself. This is done entirely in the Group Policy Management app. In the app, click “Group Policy Objects” on the left, right click your GPO, and click “Edit.”

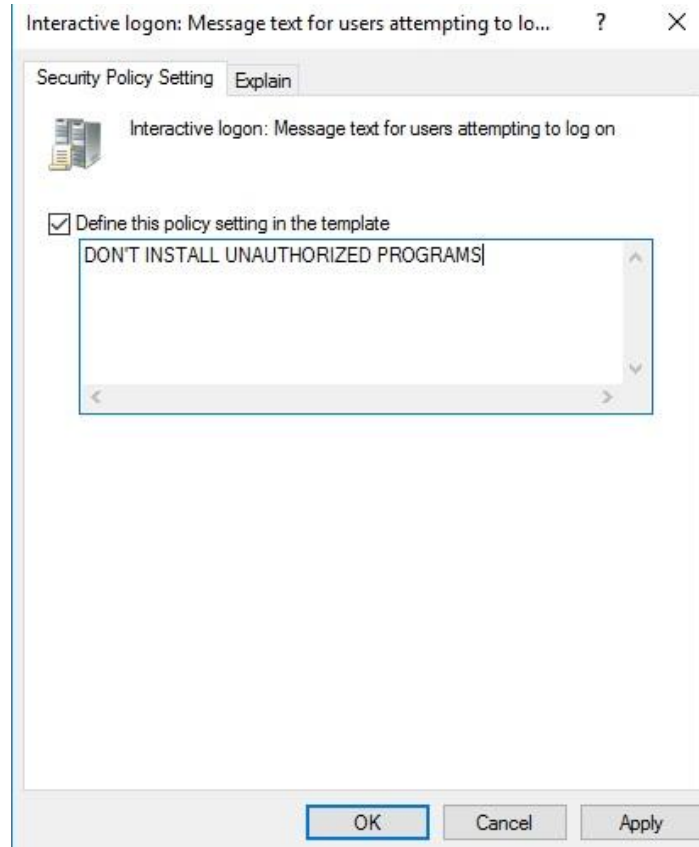
The following four processes are standard for all new hires.

First, we want to have a message pop up whenever a new hire’s computer starts that reads: “DON’T INSTALL UNAUTHORIZED PROGRAMS.” Here is your navigation path to enable this in our GPO:

- Computer configuration
- Policies
- Windows Settings
- Security Settings
- Local Policies
- Security Options

Once here, locate “Interactive logon: Message text for users attempting to log on.” Double click it, define the value, and enter our message.

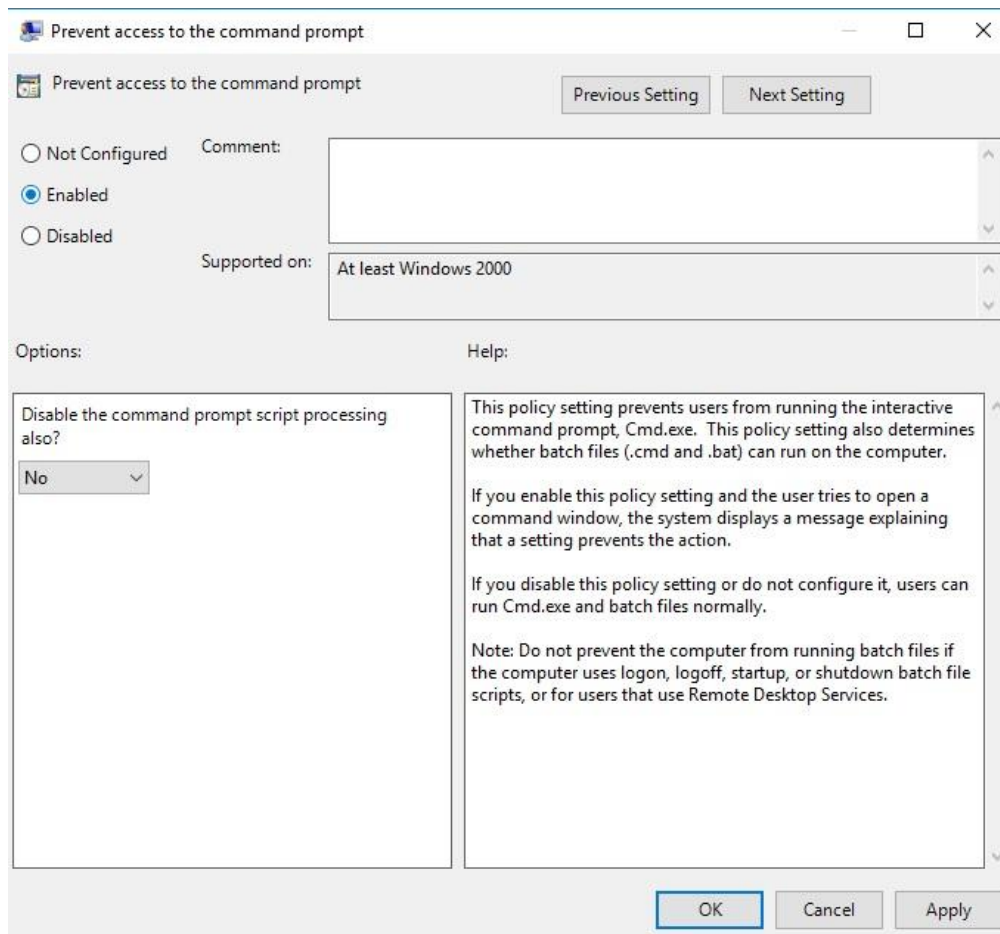
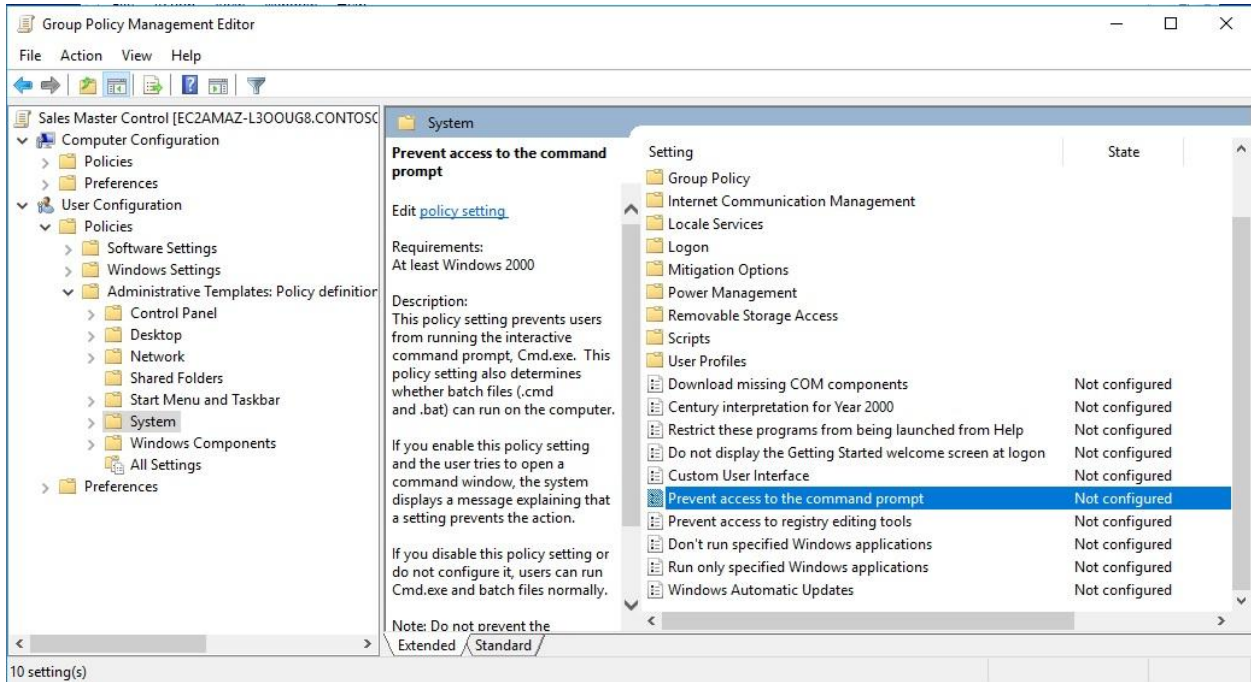




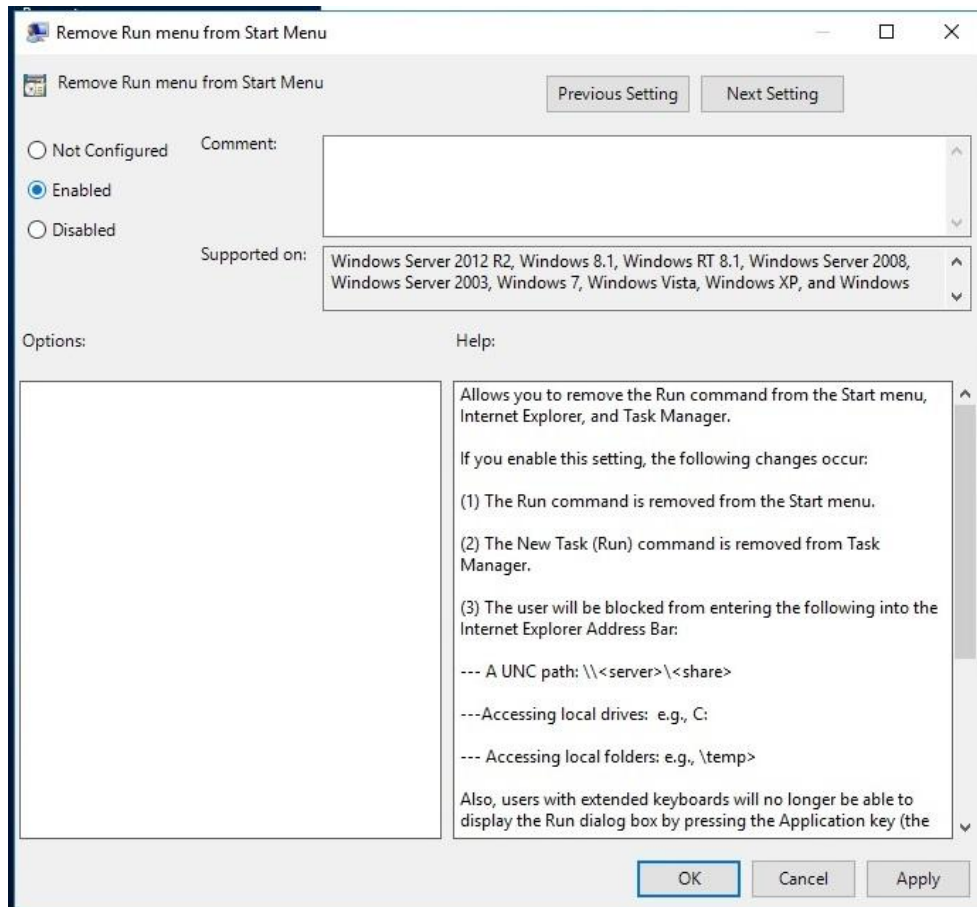
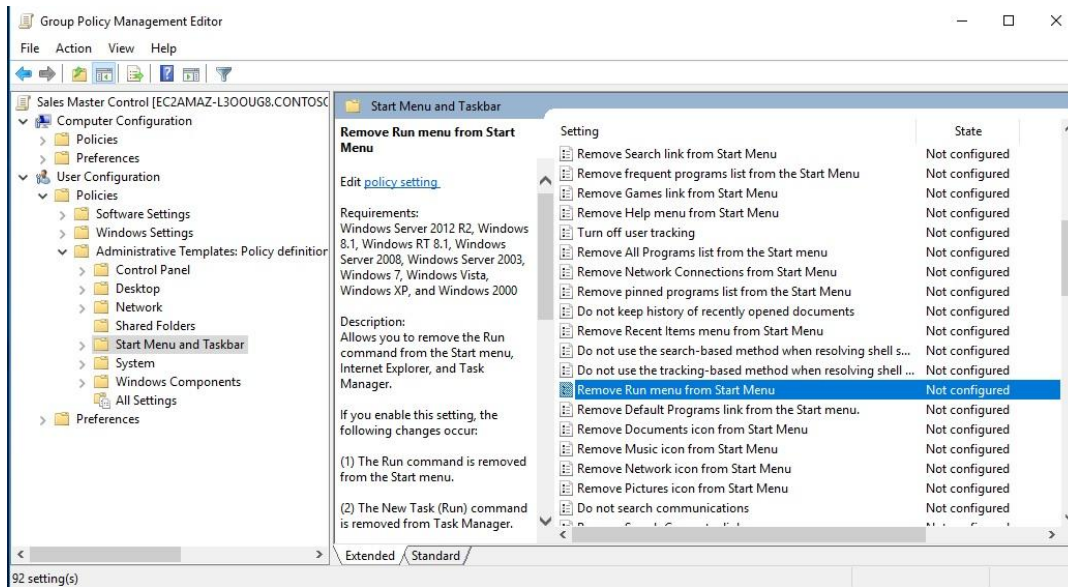
Second, we want to prevent access to the command prompt. Here is your navigation path to enable this in our GPO:

- User configuration
- Policies
- Administrative Templates
- System

Once here, locate “Prevent access to the command prompt.” Double click on it, and enable it.



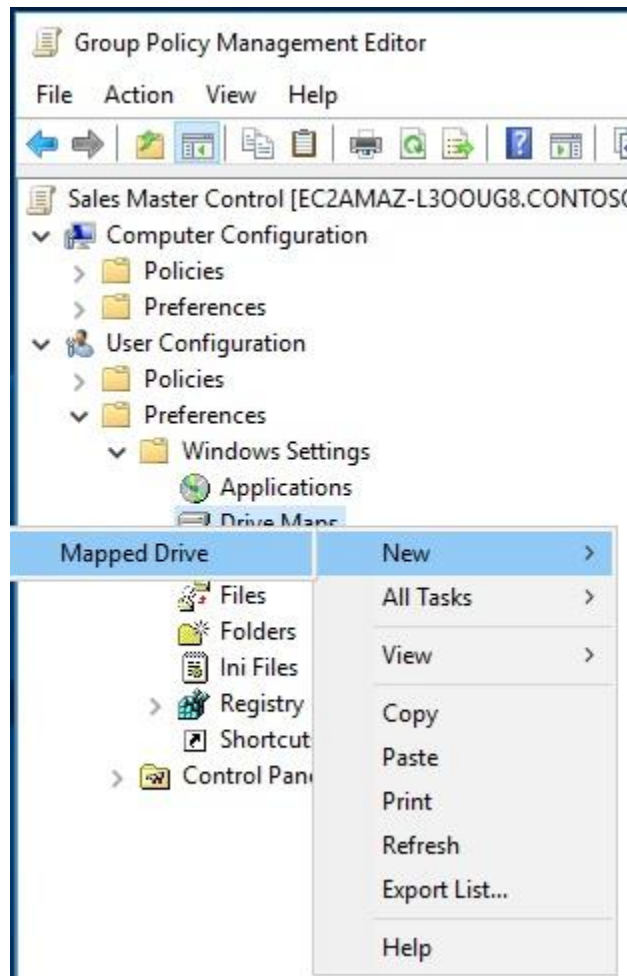
Third, while we're in this same directory, we want to also disable the run command from the start menu. Navigate up one level to the "Start Menu and Taskbar" directory. Once there, locate "Remove run from start menu" and enable it.



Last, we need to map the share we created for the new user. Your navigation path here is:

- User configuration
- Preferences
- Windows Settings
- Drive Maps

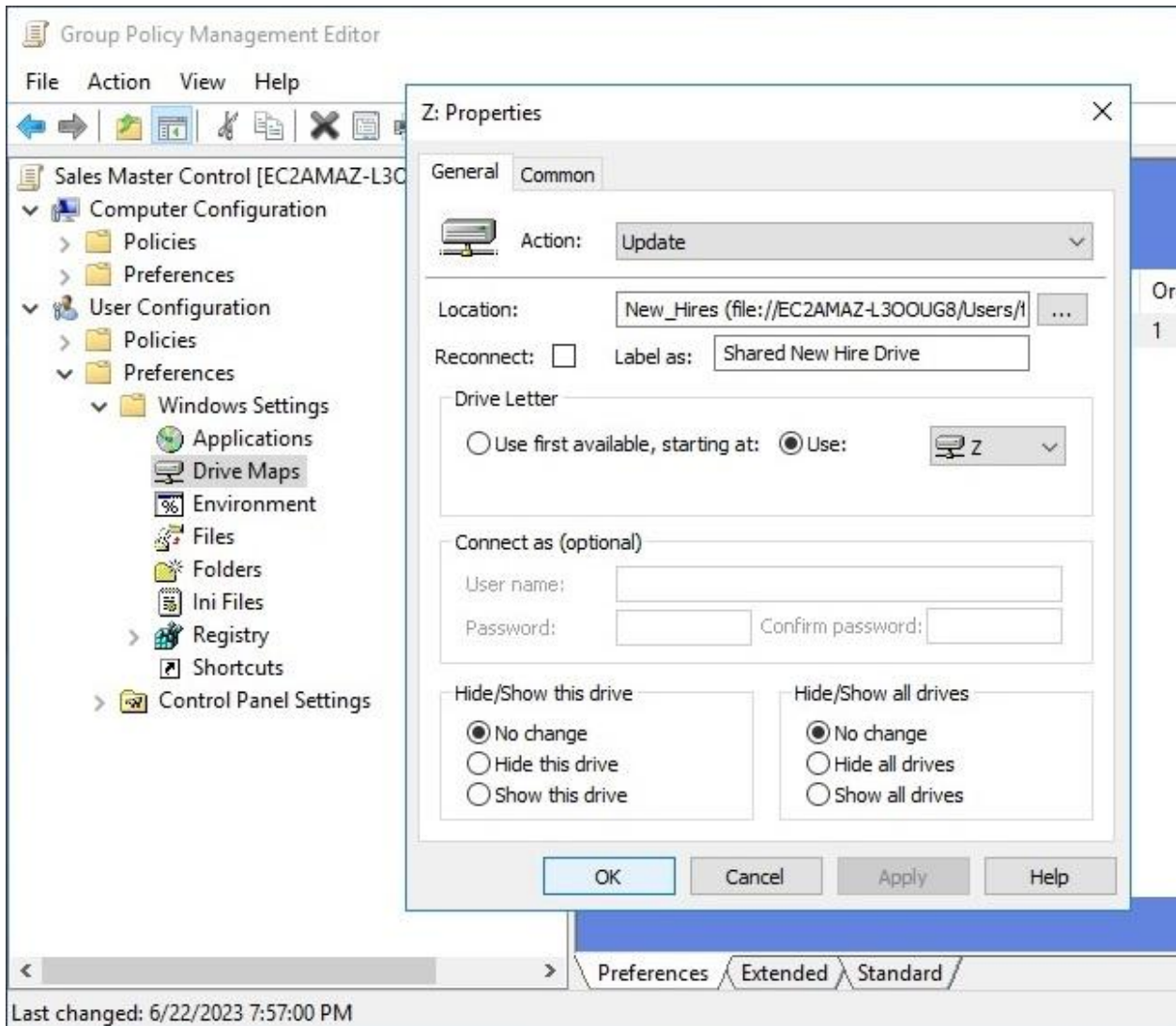
Once here, right click and select “New” and then “Mapped Drive.”



In the “General” tab, fill out the following:

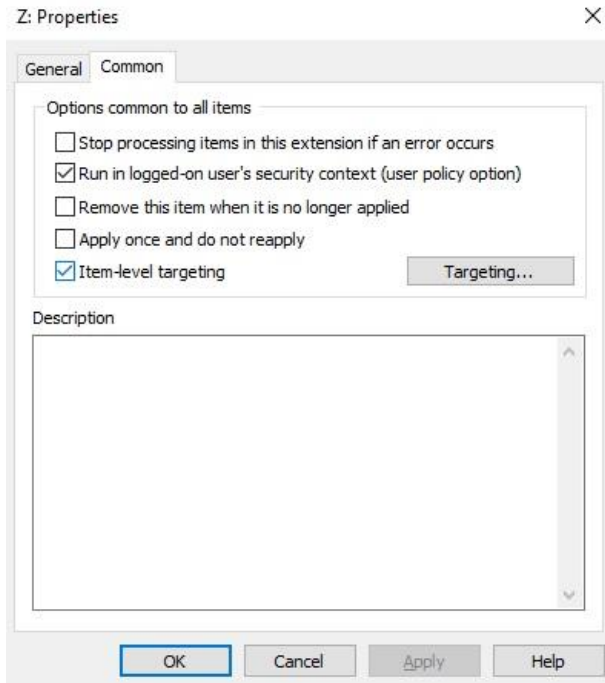
- Action: Update
- Location: Path to shared drive
- Reconnect: Unchecked
 - Makes a network drive permanent (it will be reconnected every time you log in, even if you remove the policy)
- Drive letter: “Use” and then assign a letter to the drive

- Connect as: N/A

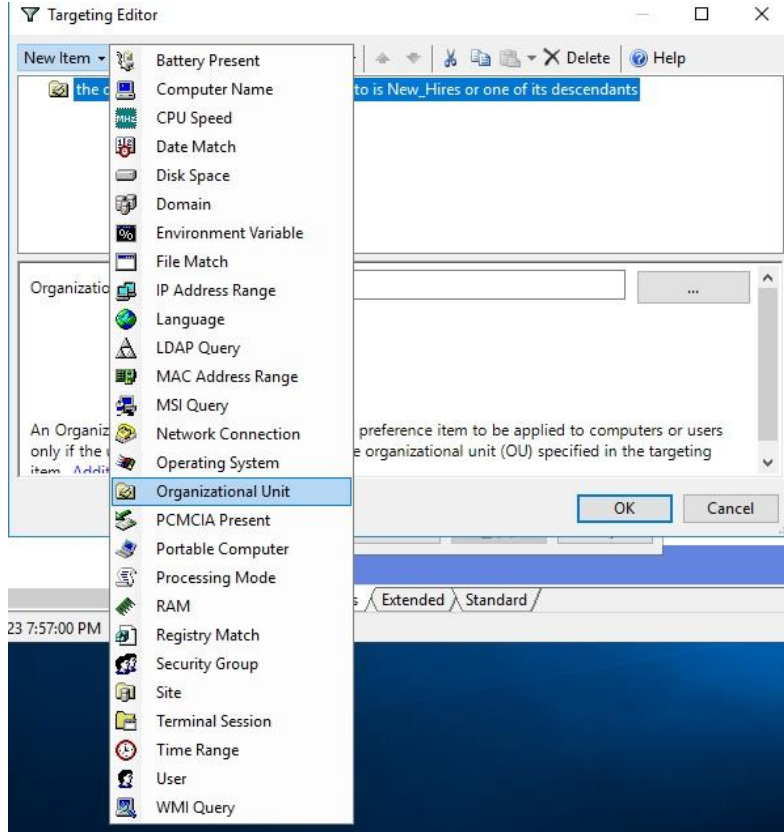


Next, click the “Common” tab and check the following:

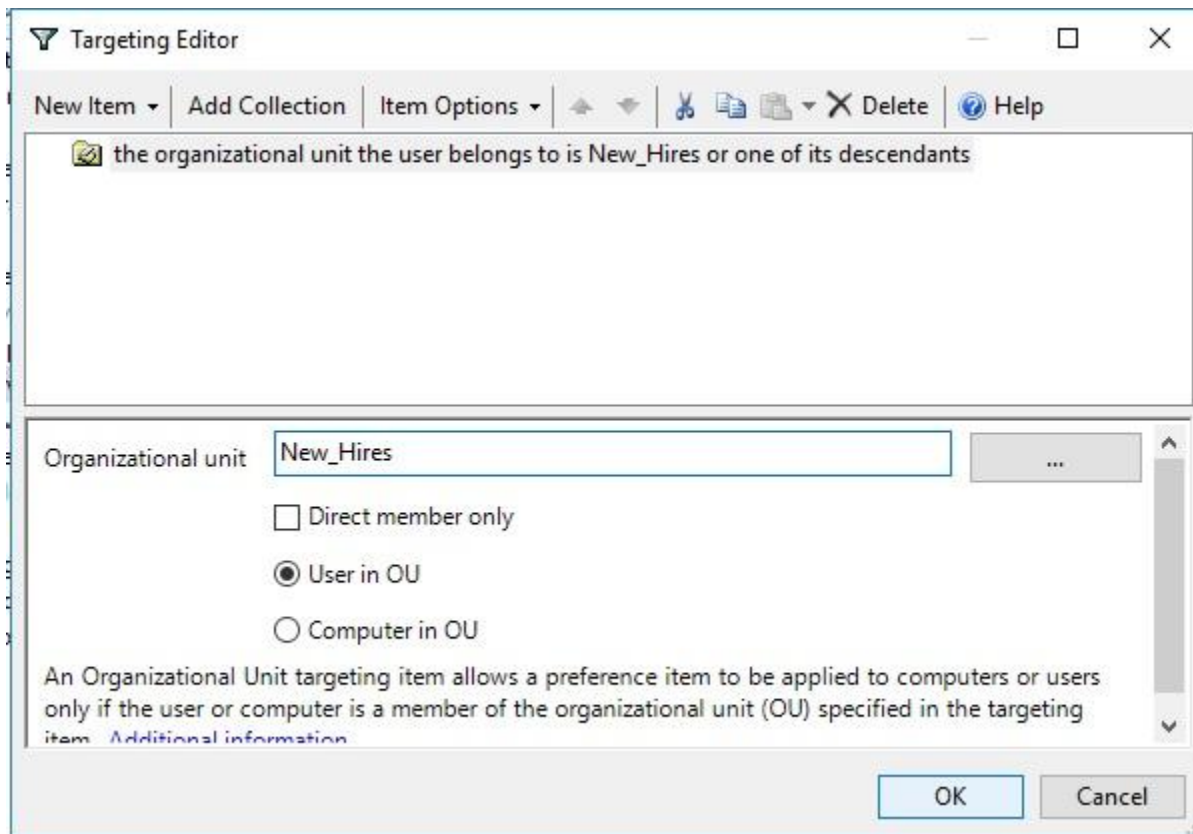
- Check run in logged-on user’s security context
- Item level target
- Click “Targeting”



Then, click “Targeting.” Here, we’ll want to click “New Item” and then select “Organizational Unit.”



Enter the name for the OU.

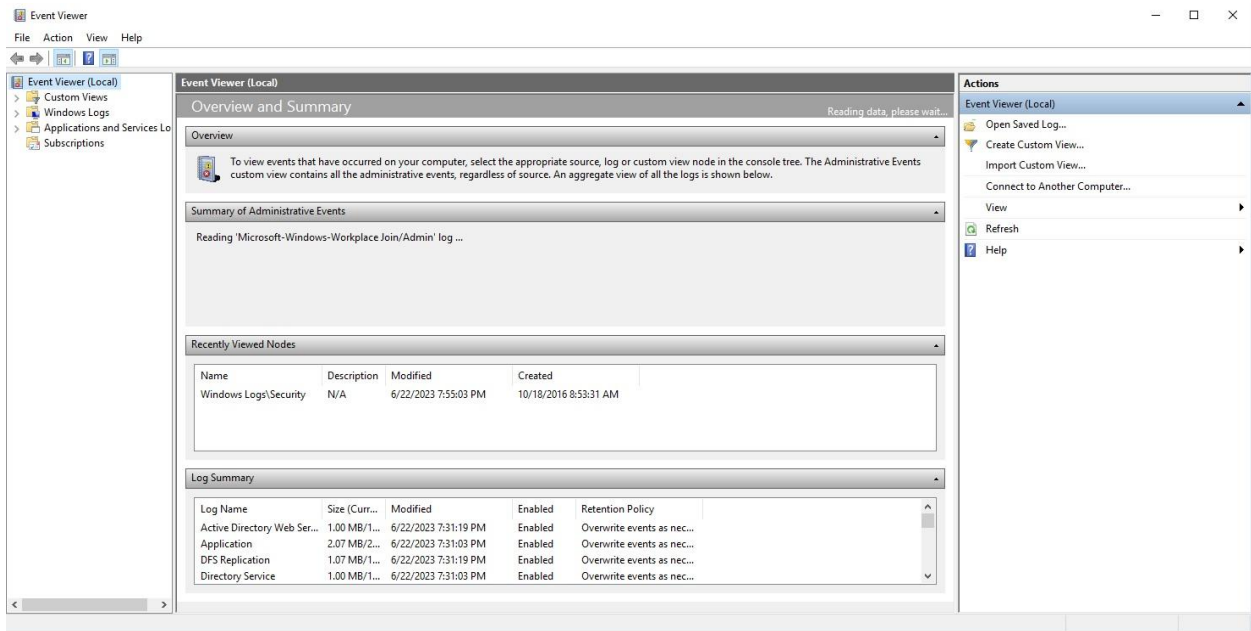


Click “OK” and then you’re finished editing the contents of the GPO. This is already linked to our OU, so these rules will now apply to anyone inside that OU.

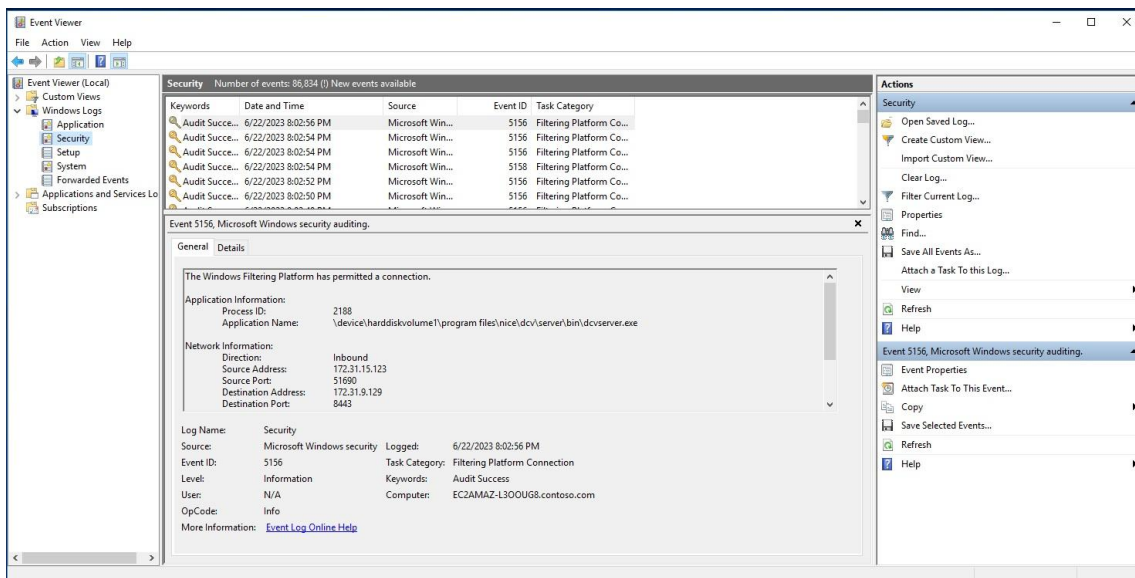
Step 7: Check the Event Viewer for a Successful Login

For this step, we want to check the Security Logs on the Windows Event Viewer to see the last successful login from our user. Essentially, this is a test to see if our new hire is set up well and can log in.

Log in with the new hire credentials. Then, log out. Log back in on the main server account. Open the Windows Event Viewer.



Once in the app, navigate to “Windows logs” and then “Security logs.”



Then, we want to click “Filter Current Log” in the right panel, and look for anything from the last hour. Then, filter to check for eventID 4624, which is a successful log on.

Filter Current Log

Filter XML

Logged: Last hour

Event level: Critical Warning Verbose
 Error Information

By log By source

Event logs: Security

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>

Clear

OK Cancel

Step 8: Use PowerShell to Check Latest Program Installations

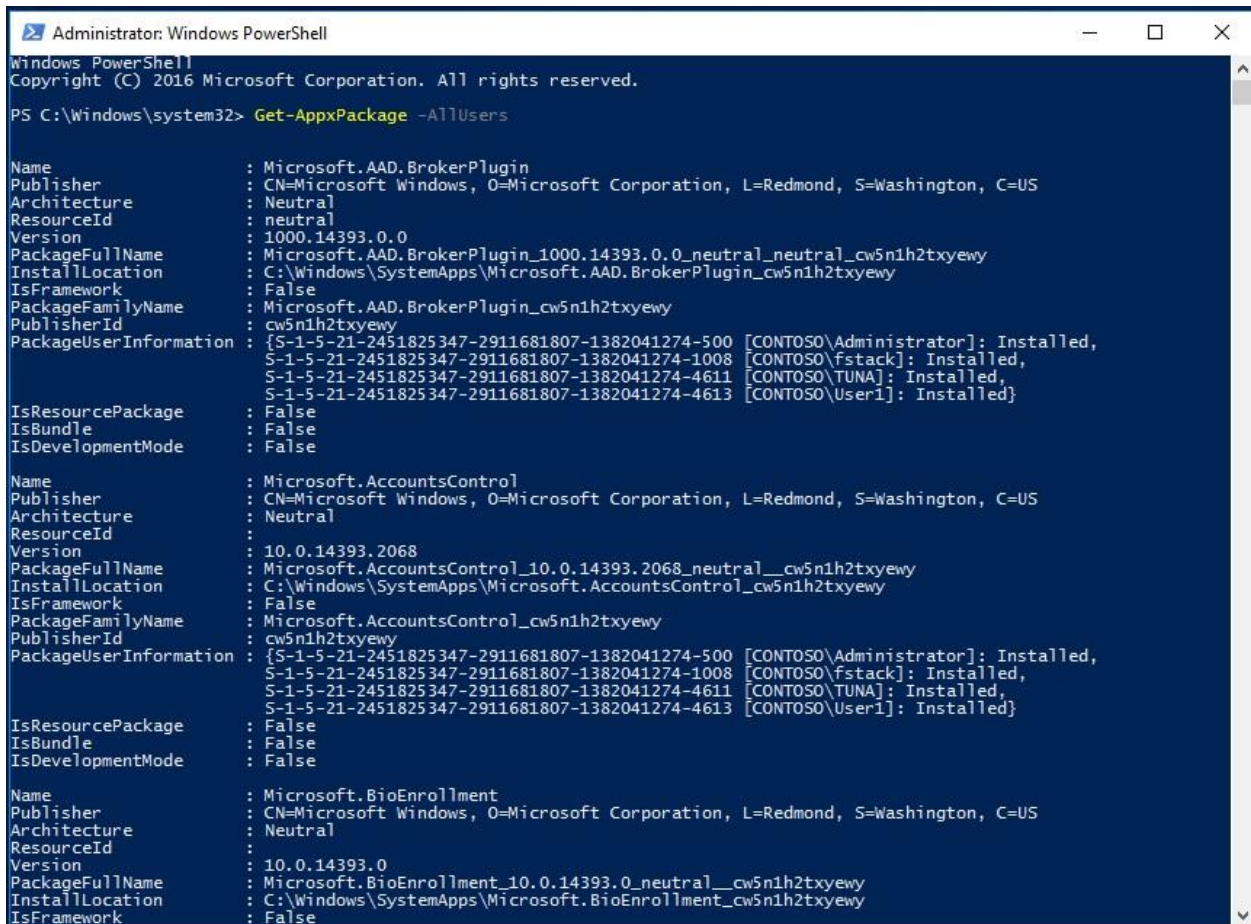
Now, we want to check to verify the latest programs installed on the computer. We'll want to run PowerShell as an admin to start.

Once we're in PowerShell, we'll use this line of code:

```
Get-AppxPackage -AllUsers
```

We could also specify to see our newest user and any programs they've installed with this line of code:

```
Get-AppxPackage -User <username>
```



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

PS C:\Windows\system32> Get-AppxPackage -AllUsers

Name                : Microsoft.AAD.BrokerPlugin
Publisher           : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Architecture       : Neutral
ResourceId          : neutral
Version            : 1000.14393.0.0
PackageFullName    : Microsoft.AAD.BrokerPlugin_1000.14393.0.0_neutral_neutral_cw5n1h2txyewy
InstallLocation    : C:\Windows\SystemApps\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy
IsFramework       : False
PackageFamilyName  : Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy
PublisherId        : cw5n1h2txyewy
PackageUserInformation : {S-1-5-21-2451825347-2911681807-1382041274-500 [CONTOSO\Administrator]: Installed,
S-1-5-21-2451825347-2911681807-1382041274-1008 [CONTOSO\fstack]: Installed,
S-1-5-21-2451825347-2911681807-1382041274-4611 [CONTOSO\TUNA]: Installed,
S-1-5-21-2451825347-2911681807-1382041274-4613 [CONTOSO\User1]: Installed}
IsResourcePackage  : False
IsBundle           : False
IsDevelopmentMode  : False

Name                : Microsoft.AccountsControl
Publisher           : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Architecture       : Neutral
ResourceId          :
Version            : 10.0.14393.2068
PackageFullName    : Microsoft.AccountsControl_10.0.14393.2068_neutral__cw5n1h2txyewy
InstallLocation    : C:\Windows\SystemApps\Microsoft.AccountsControl_cw5n1h2txyewy
IsFramework       : False
PackageFamilyName  : Microsoft.AccountsControl_cw5n1h2txyewy
PublisherId        : cw5n1h2txyewy
PackageUserInformation : {S-1-5-21-2451825347-2911681807-1382041274-500 [CONTOSO\Administrator]: Installed,
S-1-5-21-2451825347-2911681807-1382041274-1008 [CONTOSO\fstack]: Installed,
S-1-5-21-2451825347-2911681807-1382041274-4611 [CONTOSO\TUNA]: Installed,
S-1-5-21-2451825347-2911681807-1382041274-4613 [CONTOSO\User1]: Installed}
IsResourcePackage  : False
IsBundle           : False
IsDevelopmentMode  : False

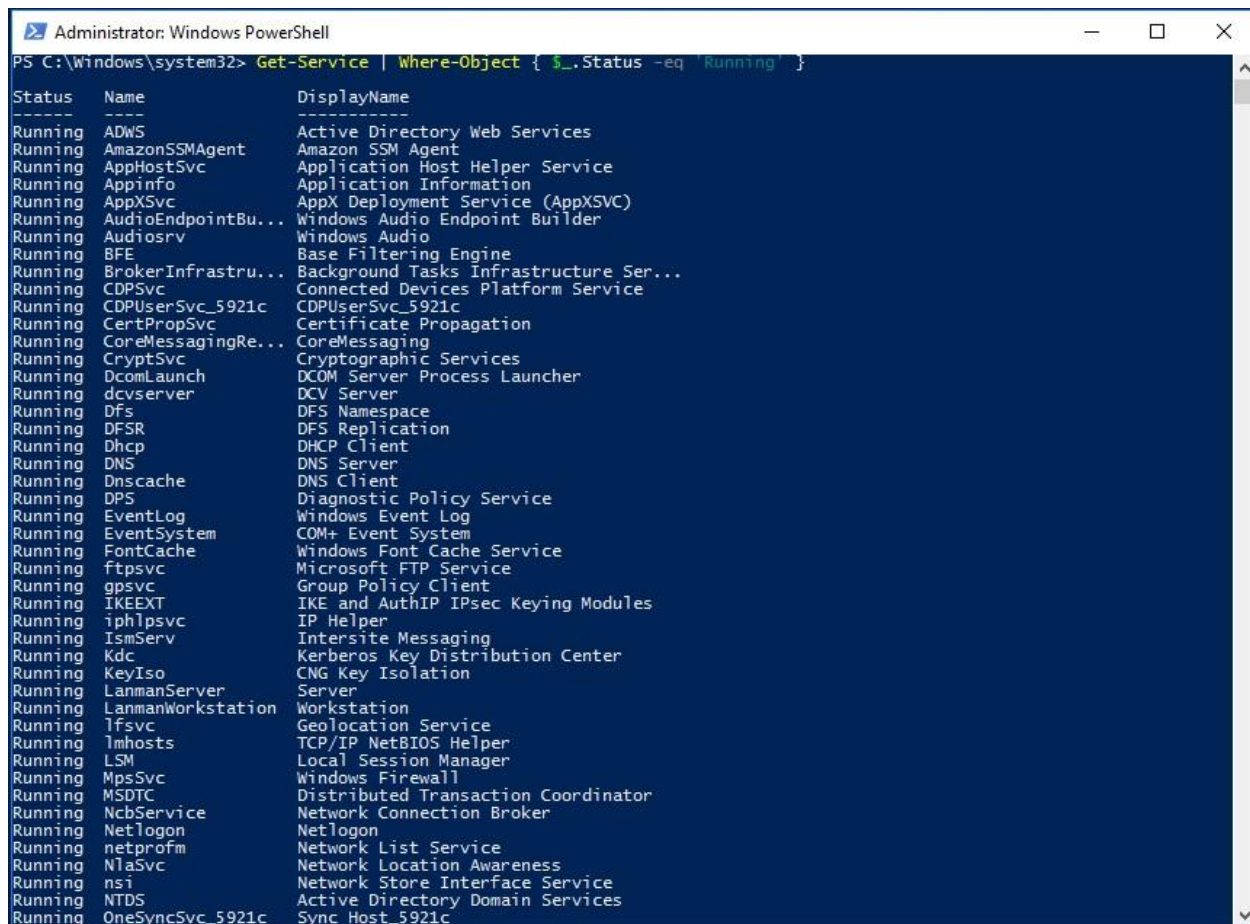
Name                : Microsoft.BioEnrollment
Publisher           : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Architecture       : Neutral
ResourceId          :
Version            : 10.0.14393.0
PackageFullName    : Microsoft.BioEnrollment_10.0.14393.0_neutral__cw5n1h2txyewy
InstallLocation    : C:\Windows\SystemApps\Microsoft.BioEnrollment_cw5n1h2txyewy
IsFramework       : False
```

Step 9: Write a PowerShell Script That Maps All Running Services and Outputs Them Into a File

The last piece of our new hire machine setup is to write a script in PowerShell that returns a list of all currently running services and redirects the output into a file named `running_services.txt`.

We'll run PowerShell as an admin, and then type this line of code:

```
Get-Service | Where-Object [ $_.Status -eq 'Running' ] }
```



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt shows the command `Get-Service | Where-Object { $_.Status -eq 'Running' }` being executed. The output is a list of services with columns for Status, Name, and DisplayName. The status for all listed services is "Running".

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	AppXSvc	AppX Deployment Service (AppXSvc)
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_5921c	CDPUserSvc_5921c
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	iphlpvc	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	netprofm	Network List Service
Running	NlaSvc	Network Location Awareness
Running	nsi	Network Store Interface Service
Running	NTDS	Active Directory Domain Services
Running	OneSyncSvc_5921c	Sync Host_5921c

Run that line, and make sure you're returning it with no errors. It should display a list of all running services. Once you confirm that it works, re-enter the code into PowerShell. But we're also going to put an `Out-File` command here now as well:

```
Get-Service | Where-Object [ $_.Status -eq 'Running' ]" | Out-File  
-filepath "C:\users\fstack\desktop\running_services.txt"
```

Open the file to verify your command worked, and we're finally finished.

running_services - Notepad

File Edit Format View Help

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	CDUserSvc_5921c	CDUserSvc_5921c
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	iphlpvc	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

Closing Thoughts

If you have any questions about the processes outlined in this runbook, please reach out to the IT Manager directly before taking action. The last thing we want is for you to accidentally create, delete, add permissions, etc for anyone in our system.

That is to say, we love getting questions from our employees! It means you're thinking critically and are prioritizing the wellbeing of StackFull Software.

Similarly, if you have any questions or concerns about the security best practices here, or you want further explanation on any of them, please don't hesitate to reach out to our SOC Team. They're great and will be more than happy to talk your ear off about all things security. Seriously...they don't ever stop talking about it. But we love them.

Last, if you have any input for how we can improve the quality of our runbooks we're all ears. Schedule time to present new ideas or processes and we'll see if we can implement them in future iterations of our runbooks.

Welcome to StackFull Software!