

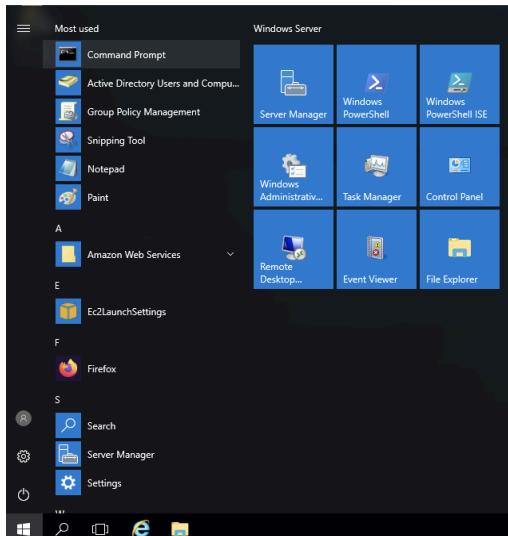
IT Onboarding Runbook

Name: **Vlad Impaler**
Job title: **Recruiter**
Dept: **Human Resources**

Onboarding a new employee requires basic setup of User, Group and Organization as well as establishing a shared drive and permissions and policy for all elements involved.

We need to locate the ip address of the host machine. If not readily accessible in records, we can always run **Cmd or (Command Prompt from Start Menu)> ipconfig** on the host machine in this case “server”.

Server:



Locate the IPv4 address with the command “**ipconfig**” and make note or copy **<ctrl+C>** it to your clipboard.

```
cmd Select Command Prompt
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::f8bf:9cb9%672c:16e1%2
IPv4 Address . . . . . : 172.31.55.202
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . : 172.31.48.1

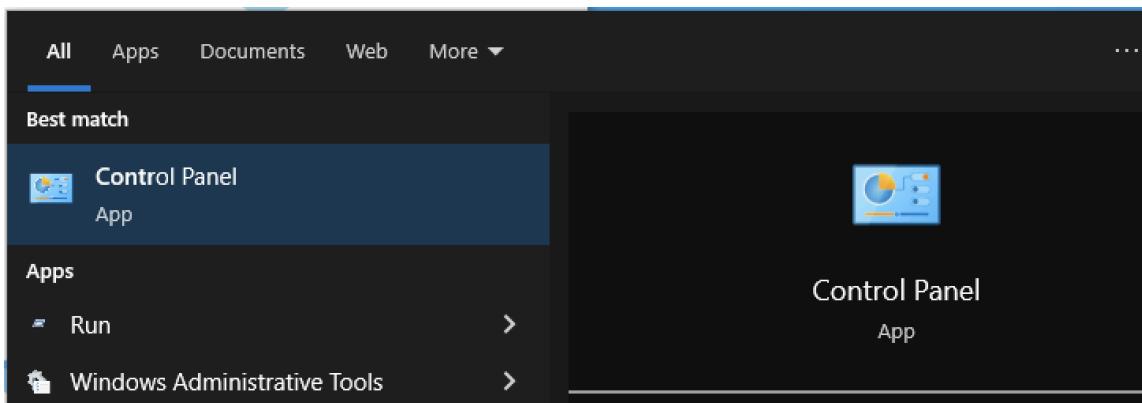
Tunnel adapter Local Area Connection* 3:
```

IT Onboarding Runbook

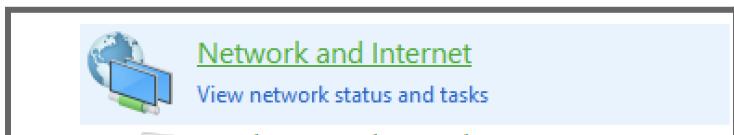
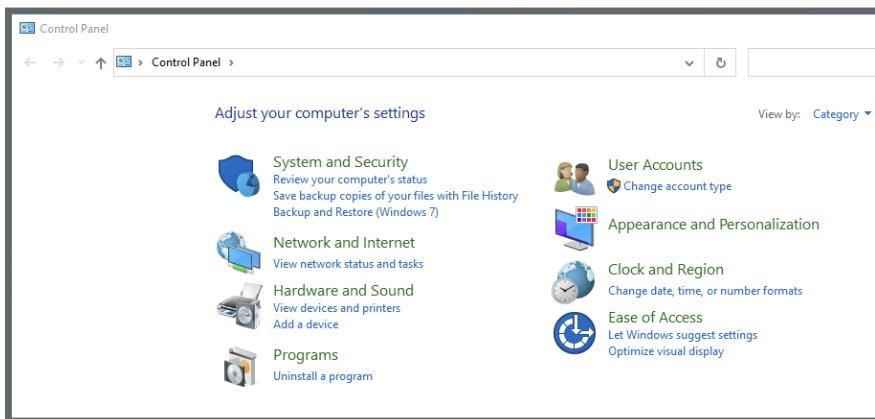
User Machine/Desktop-2:

In the users local machine we need to establish the connectivity to the domain.

The first step will be to point the Desktop-2 at the domain. From the Start menu we need to find the Control Panel.

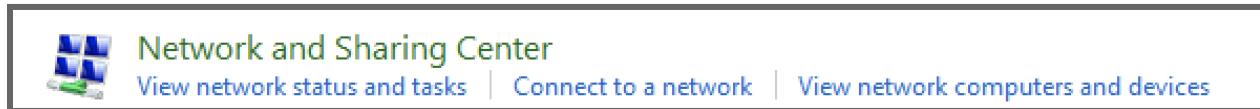


In the Control Panel click on the “**Network and Internet**”

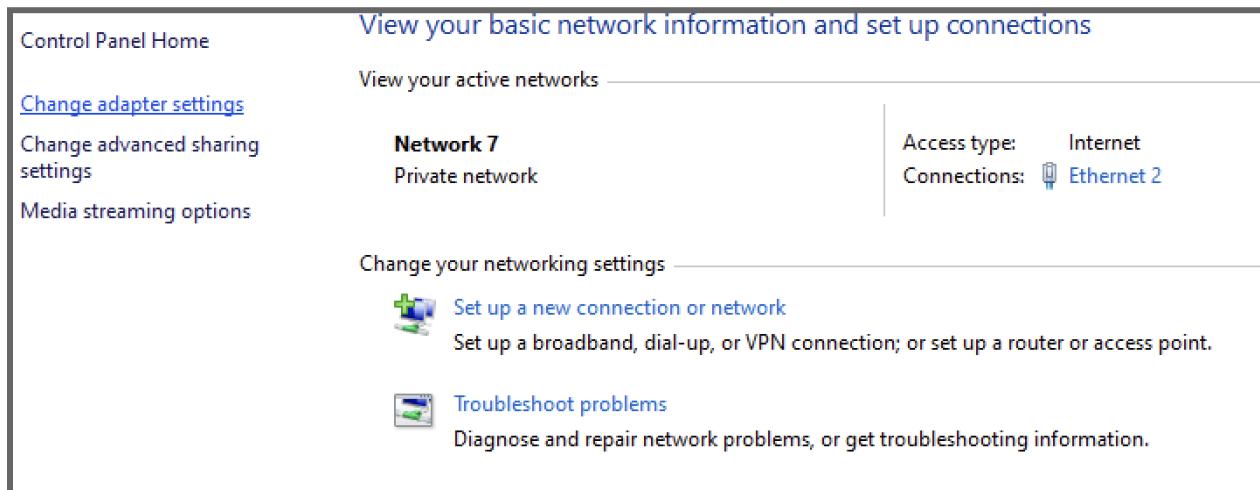


IT Onboarding Runbook

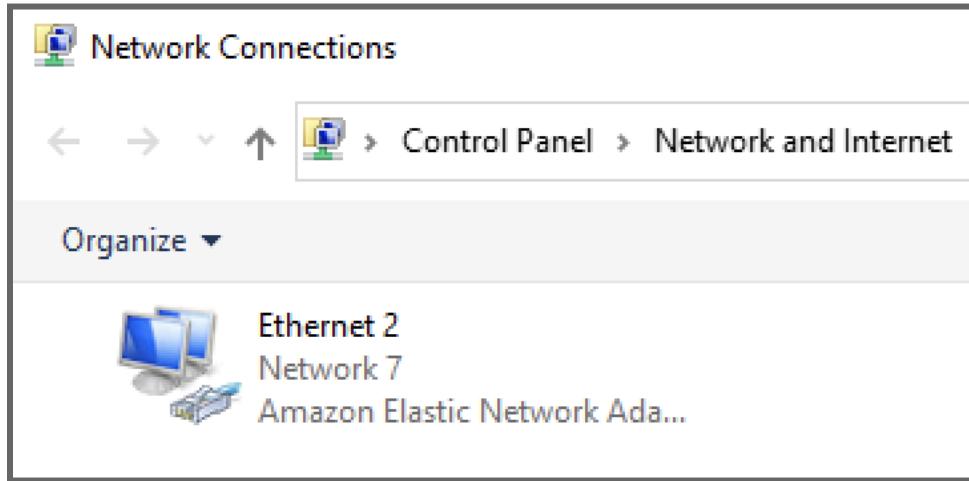
Inside the “Network and Internet” - click on “Network and Sharing Center”



Inside the “Network and Sharing Center” - click on “Change adapter settings”

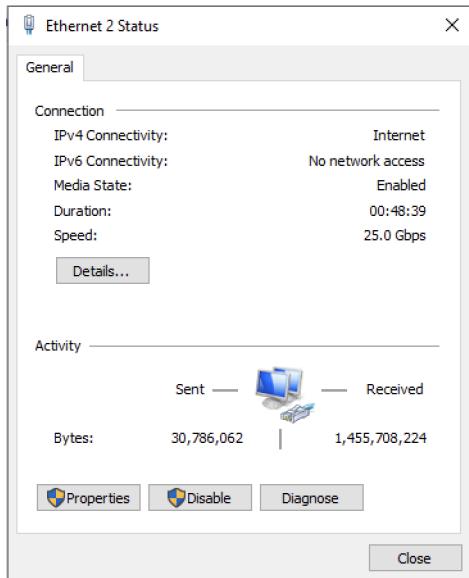


This directs you to “Network Connections” you should see adapter icons. In this case “Ethernet2” right click (rmb) on the icon.

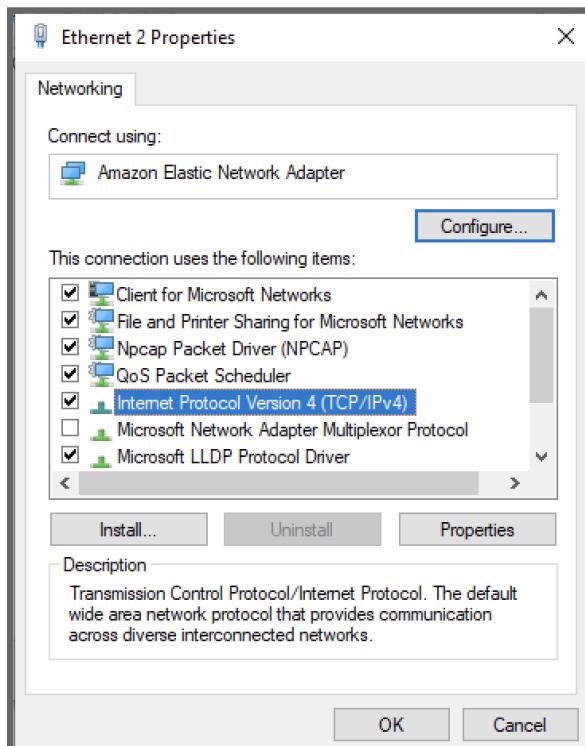


IT Onboarding Runbook

This opens a dialog with information about the Connection. Select the **Properties** button

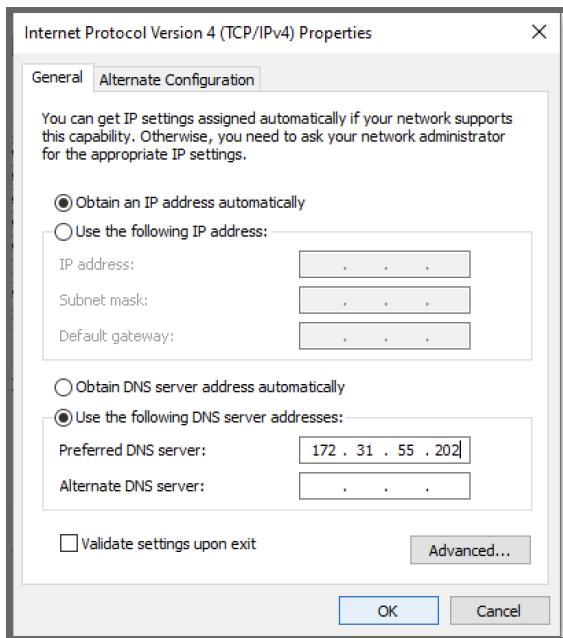


This opens a dialog with the **Ethernet 2 Properties**. Locate the IPv4 selection and click on the Properties button.



IT Onboarding Runbook

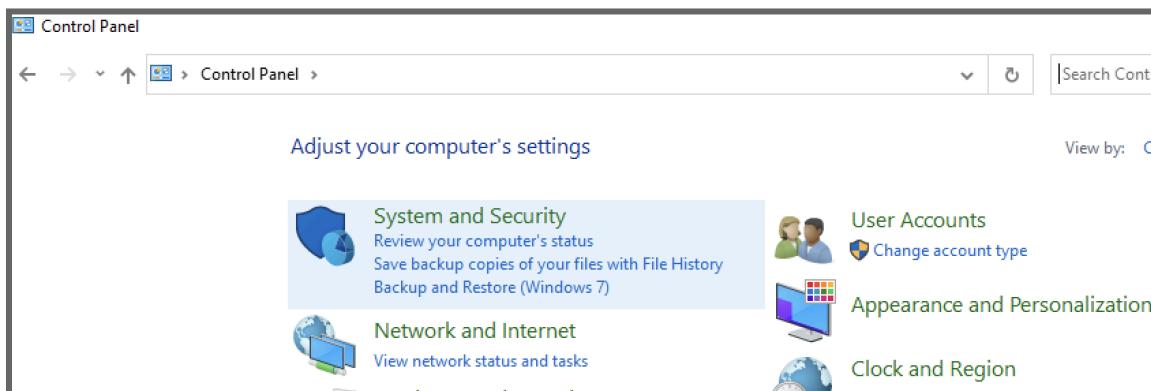
The Internet Protocol Version 4 (TCP/IPv4) Properties are where the IPv4 address we collected from the server gets input. It will necessary to select the “**Use the following DNS server addresses:**” to be able to input the IPv4 address. Click OK.



Close this window and the previously open Ethernet 2 and “Network” windows back to the control panel.

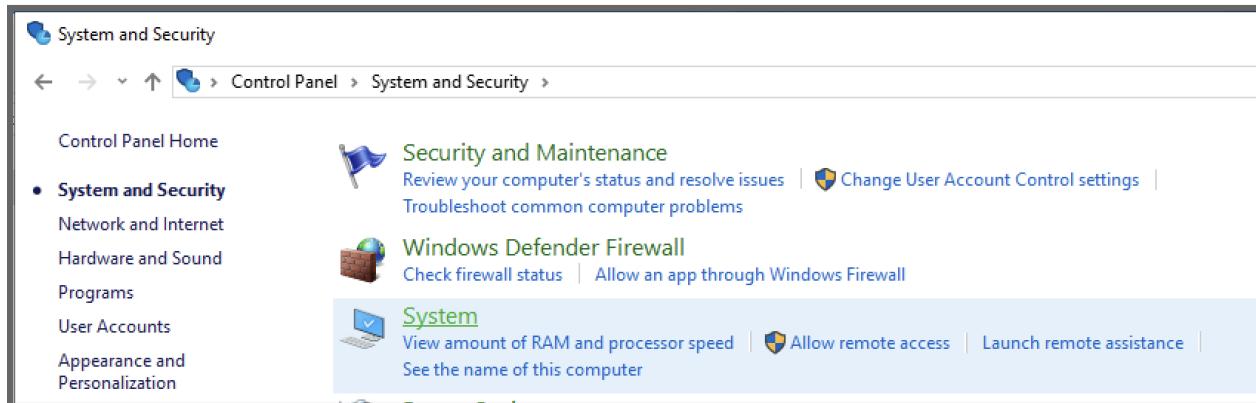
Next we need to establish naming for the domain.

We should see **System and Security** click on the text “**System and Security**”.

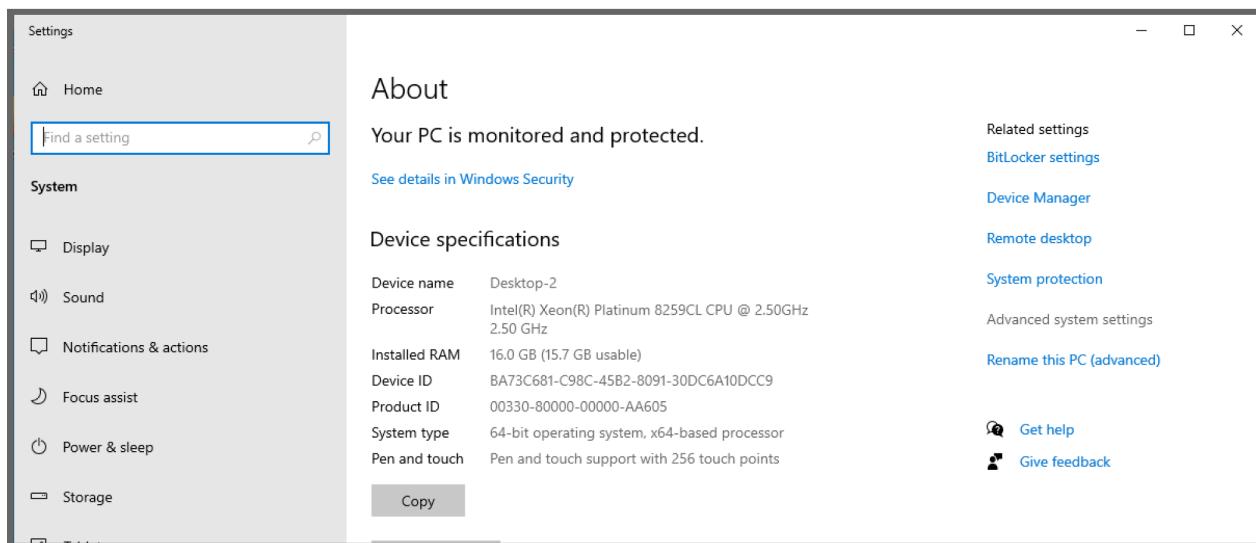


IT Onboarding Runbook

Select the “**System**” text.

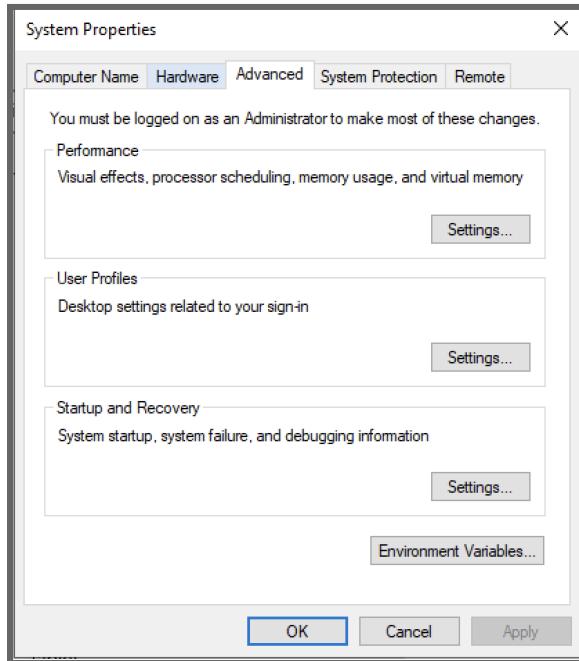


In the in the subsequent “**Settings**” panel we see “Advanced system settings” click on that text.

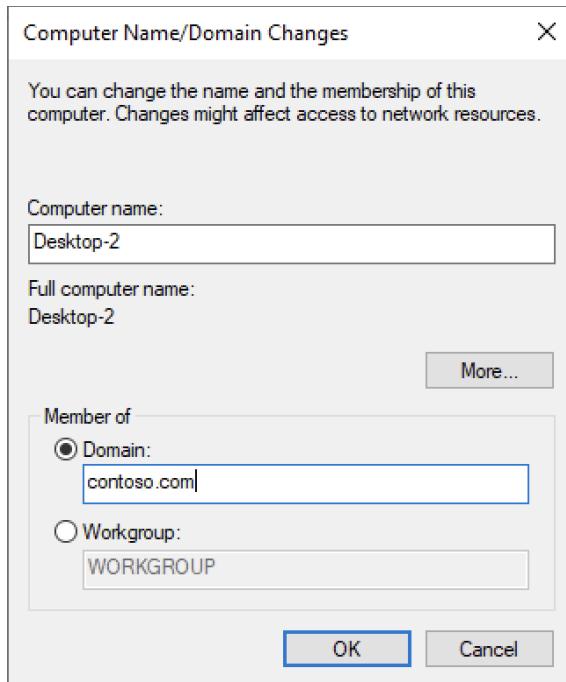


IT Onboarding Runbook

This brings up **System Properties**. Click on the “Computer Name” tab.

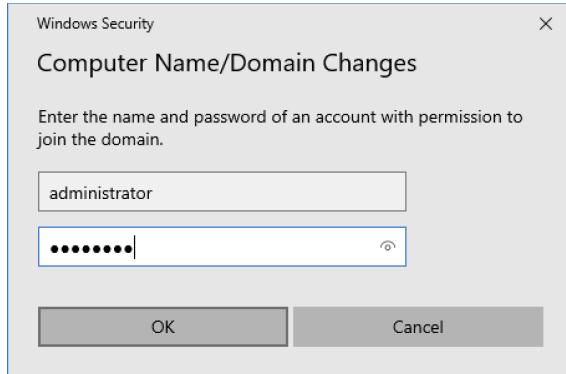


If not already selected changes the “Member of” selection to “Domain”. Enter the domain name in this field. In this case its “contoso.com” Do not change the “Computer name”.

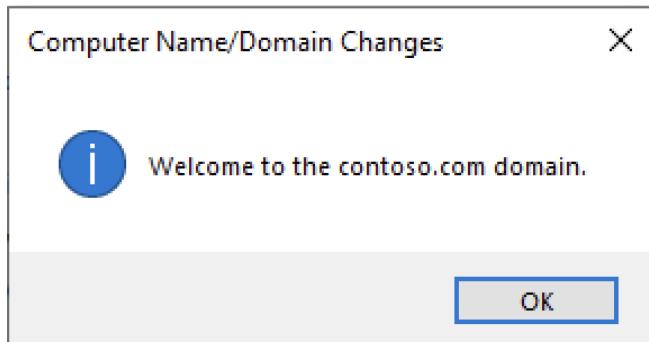


IT Onboarding Runbook

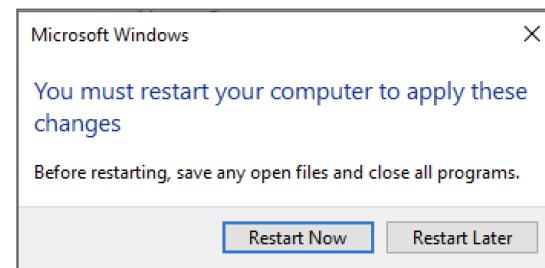
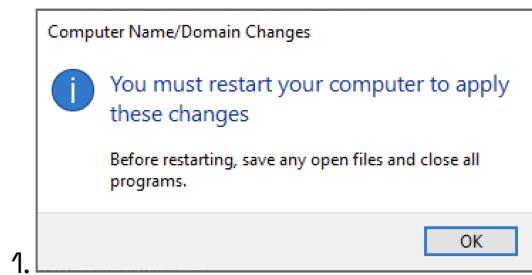
It will call for administrator credentials to join the domain



If the domain is successfully joined you will see this message:



You will then see the (2) following dialogs (respectively) indicating you must restart for the domain setup to initiate



IT Onboarding Runbook

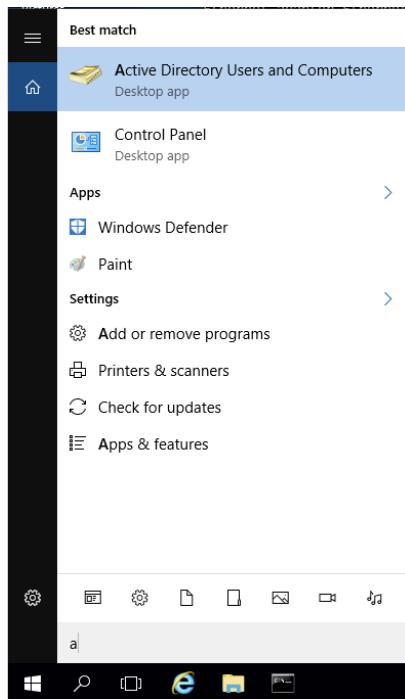
Server:

User/Group/OU Build

Now that we have the local user machine (Desktop-2) setup and connected to the domain we need to build the employee's User, Group and Organizational Unit. We need to initiate structure, setup policy and permissions. The company policy requires limits on usage of the Command line, the Run command and a reminder to not download and install "unauthorized programs".

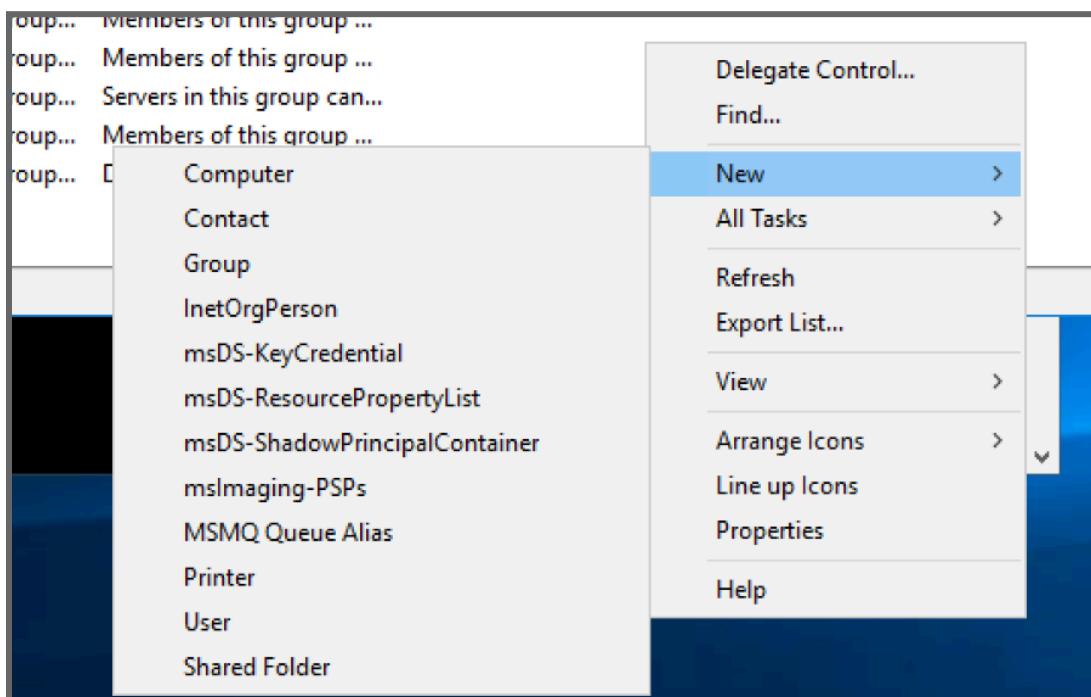
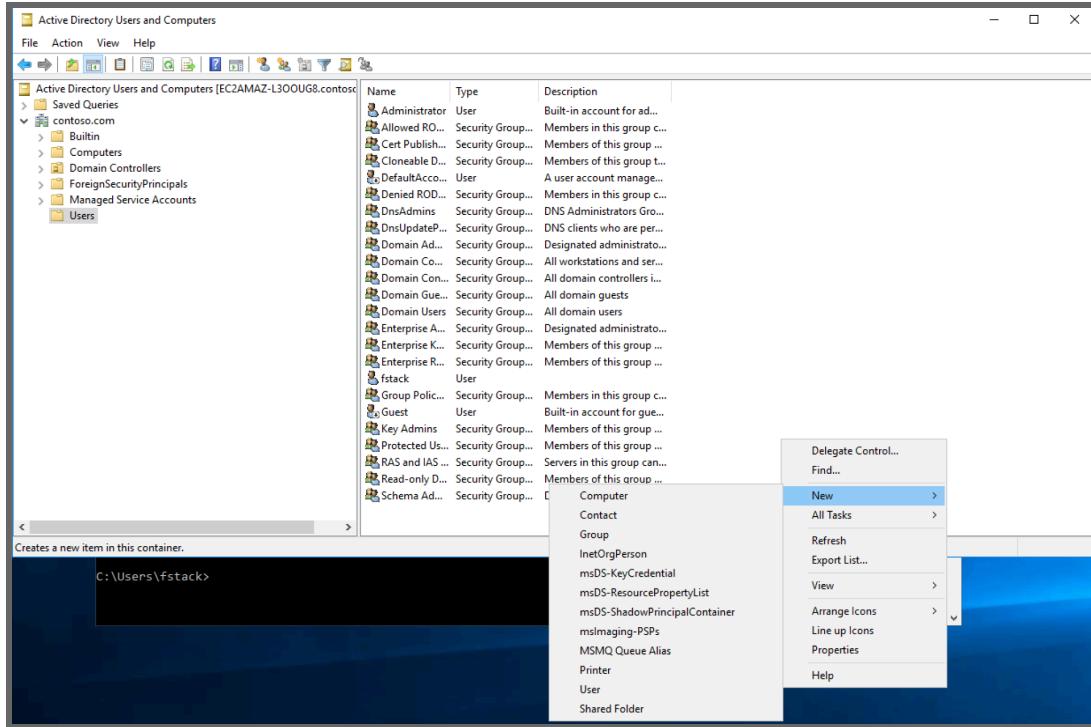
First step is the setup of the User.

From the Start menu locate the "**Active Directory Users and Computers**"(we will call **Active Directory** for sake of efficiency)



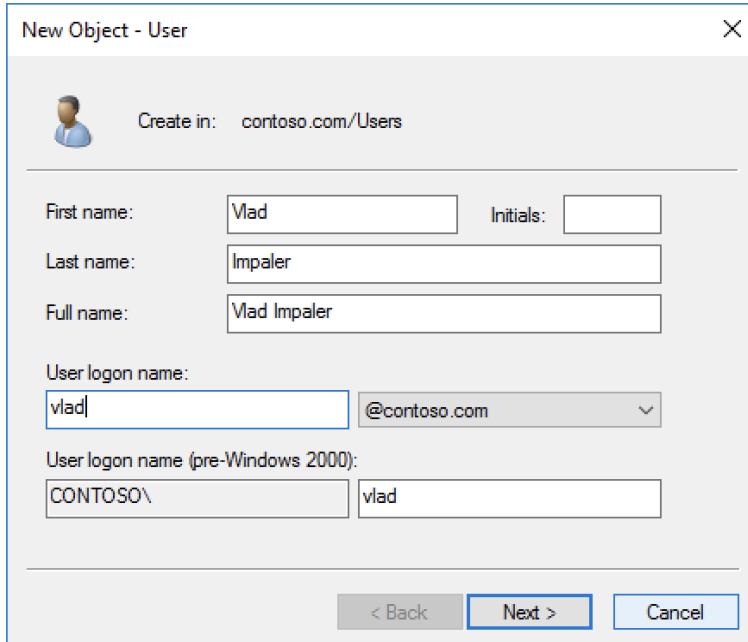
IT Onboarding Runbook

With the “Active Directory” open we select the “Users” directory and right-click within the list of Users > Right-click and select “New”> select “User”

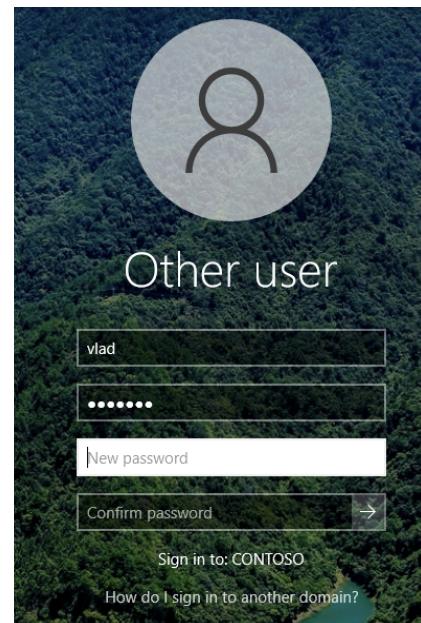
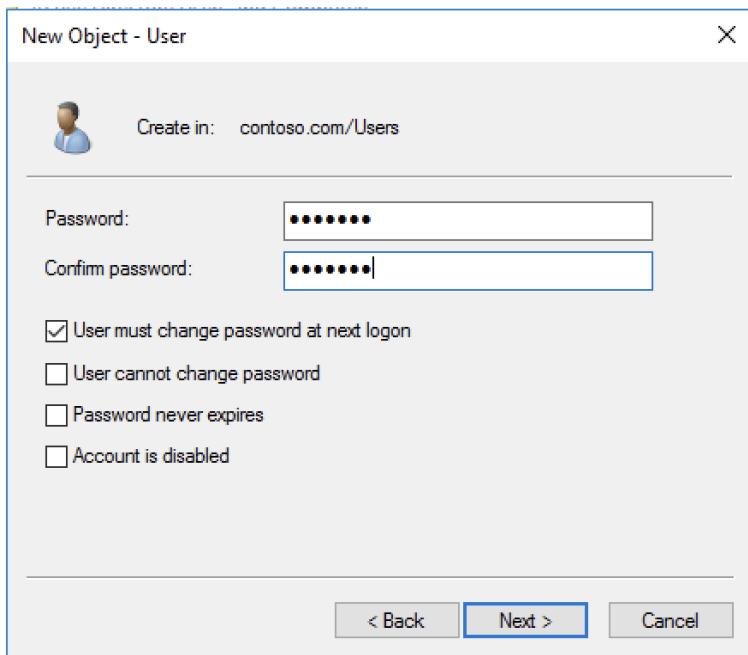


IT Onboarding Runbook

The “**New Object - User**” dialog pops up. Input employees name in respective fields and create a User logon name for the employee. Click **Next** Button.

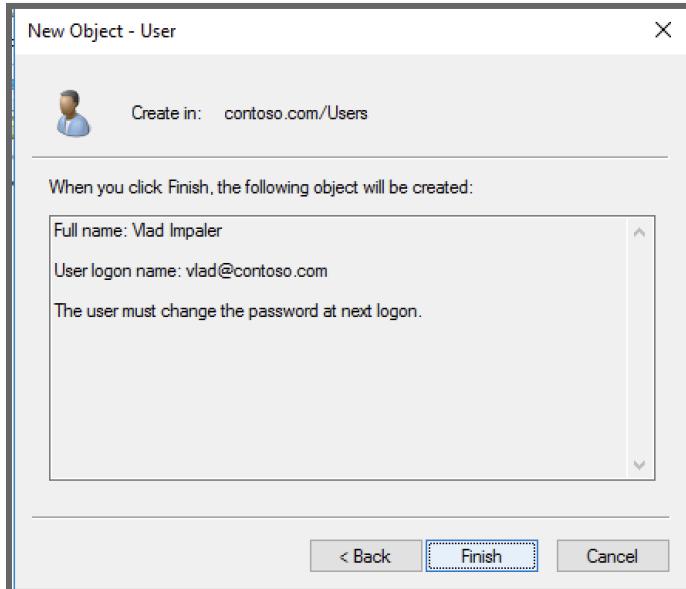


Input the password and confirm. As a security measure the “user” is required to input a new password after their first login. Select the “**User must change password at logon**”. Click **Next** Button.



IT Onboarding Runbook

Confirm information and Click **Finish** Button.



Confirm the user has been updated in the User list.

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers [EC2AMAZ-L30OUG8.contoso.com]

Saved Queries

contoso.com

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipals

Managed Service Accounts

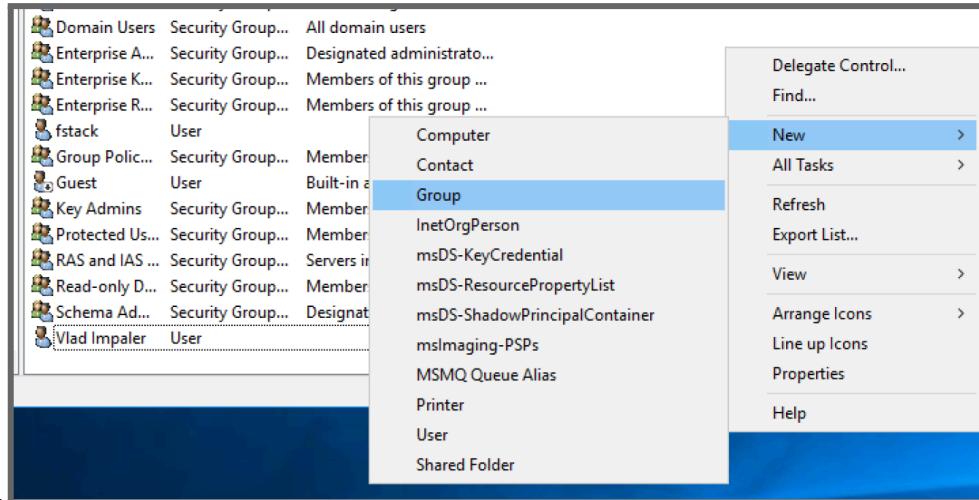
Users

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 Group...	All domain controllers i...
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...
Key Admins	Security Group...	Members 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 ...
Schema Ad...	Security Group...	Designated administrato...
Vlad Impaler	User	

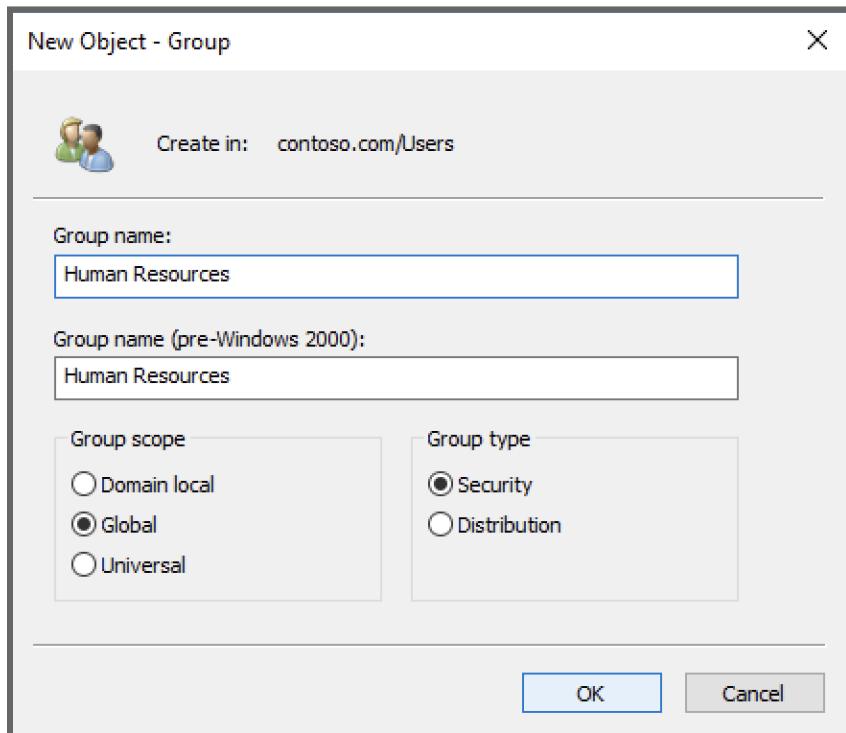
IT Onboarding Runbook

Next we need to create the Department Group in the example we are creating the **Human Resources Group**. We can access this from the same list we accessed for the user as Users and Groups are both listed here.

Users > Right-click and select “New”> select “Group”

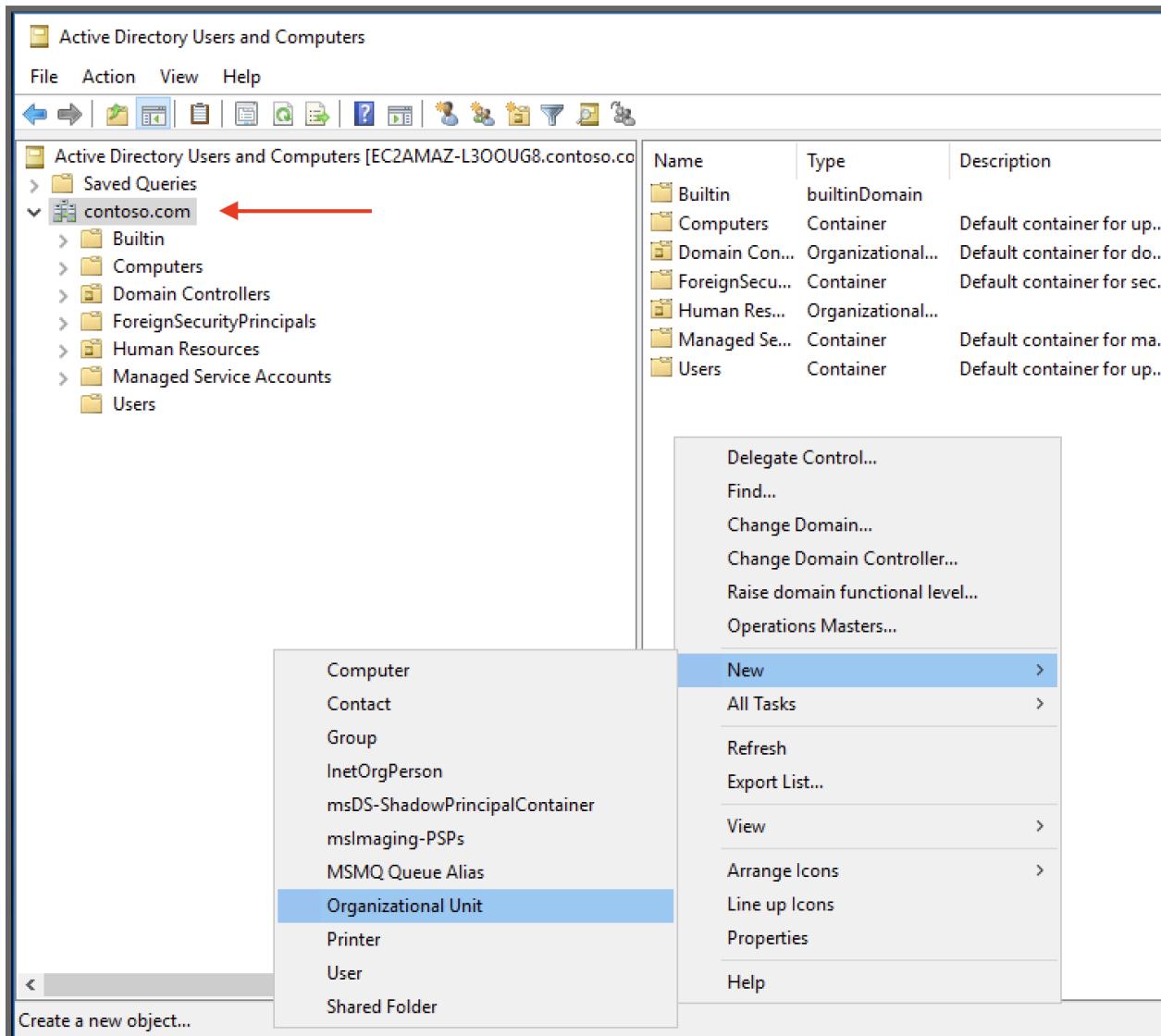


Input the Group name: In the Group scope Select “Global”. Click **OK** button.



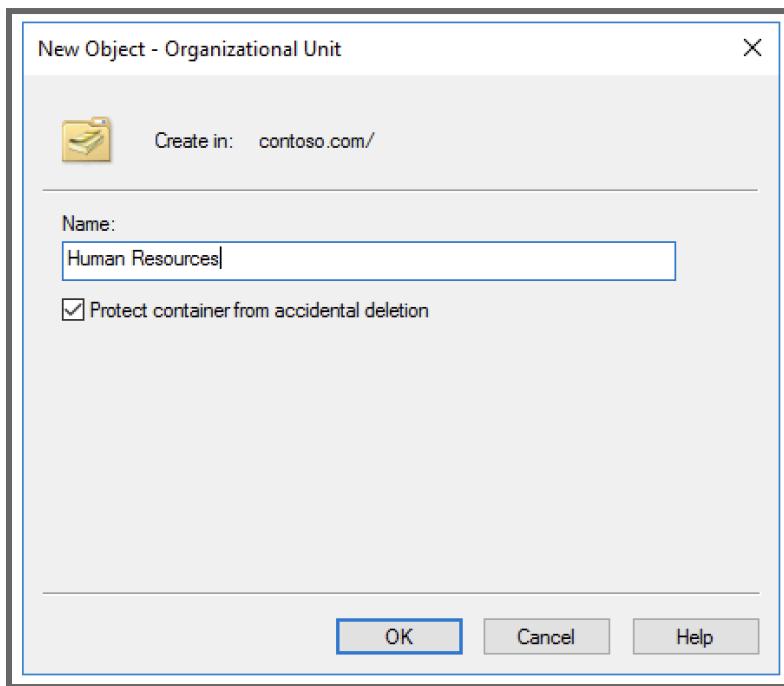
IT Onboarding Runbook

Our next step is to create the **Organizational Unit**. This will be the hub for the employees Group and User profiles. Still in the **Active Directory** we will select the **Domain** (in this case the contoso.com). Right click over the **Domain** > select “**New**” > select **Organizational Unit**.

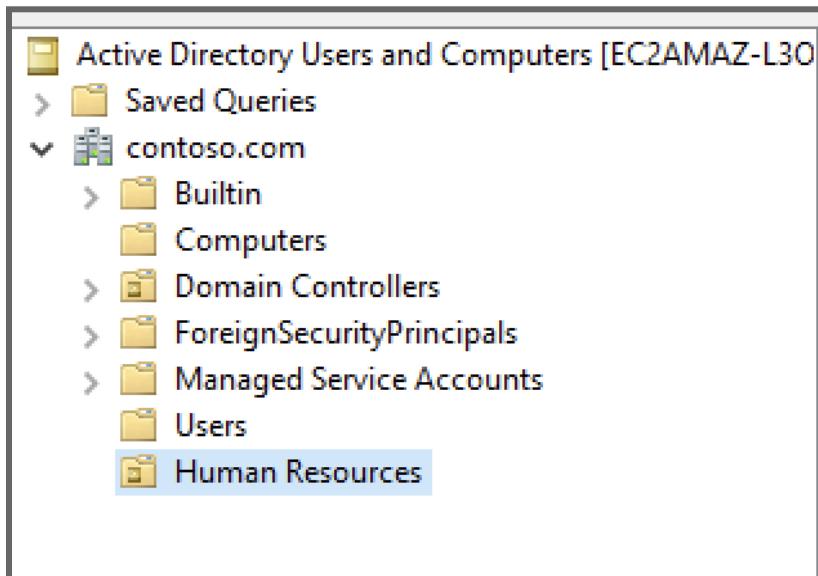


IT Onboarding Runbook

Input the Department's name into the **Organizational Units(OU) Name**(in this case Human Resources). Click **OK**. It defaults with “**Protect container...deletion**” button turned on. Leave that as it is.



The *Department OU* shows up under the domain if done correctly.



IT Onboarding Runbook

In the **Active Directory** still we continue onto the membership assignments for User and Group and OU. Click on the “**Users**” directory to pull up the user/group list.

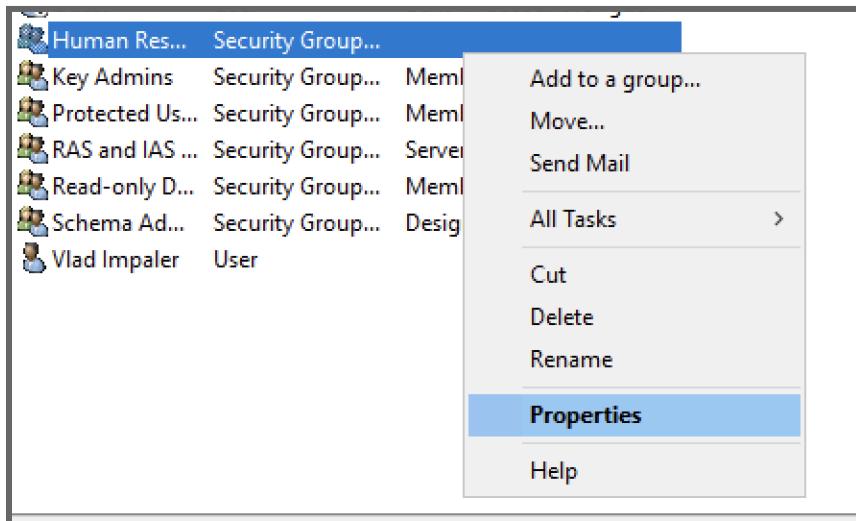
The screenshot shows the Active Directory Users and Computers console window. The left pane displays the navigation tree under 'Active Directory Users and Computers [EC2AMAZ-L3O]'. The 'Users' folder is selected. The right pane lists a table of users and groups, with the 'Human Resources' group highlighted. A context menu is open over the 'Human Resources' entry, showing options like 'Add to a group...', 'Move...', 'Send Mail', 'All Tasks', 'Cut', 'Delete', 'Rename', 'Properties', and 'Help'.

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 Group...	All domain controllers i...
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...
Human Res...	Group	Add to a group... Move... Send Mail All Tasks Cut Delete Rename Properties Help
Key Admini...	User	of this group ...
Protected	User	of this group ...
RAS and I...	User	this group can...
Read-only	User	of this group ...
Schema A...	User	ed administrato...
Vlad Impa...	User	

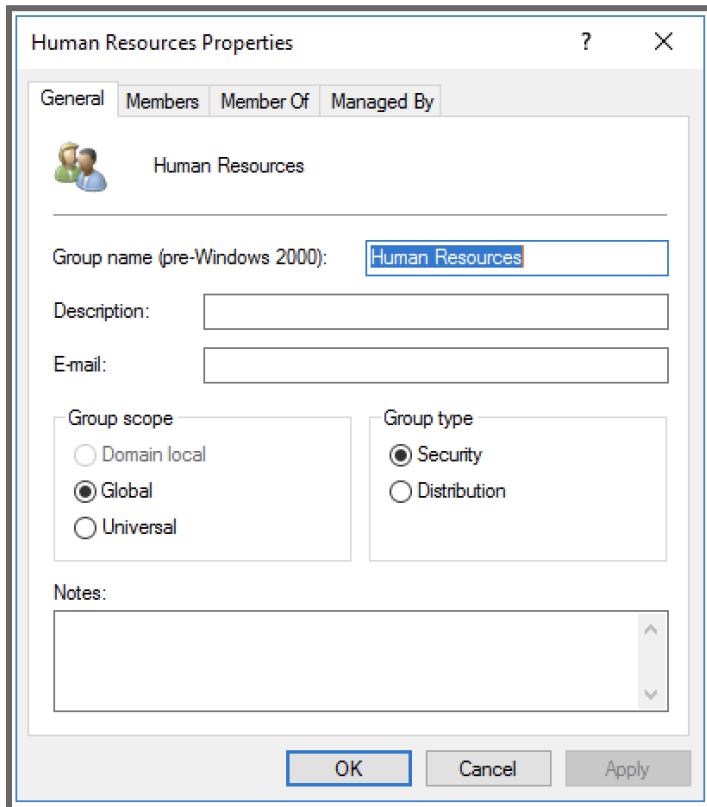
Lets add the employee's **User(Vlad)** to the Department(**Human Resources**) **Group**.

IT Onboarding Runbook

Select the Department Group > right-click > select Properties

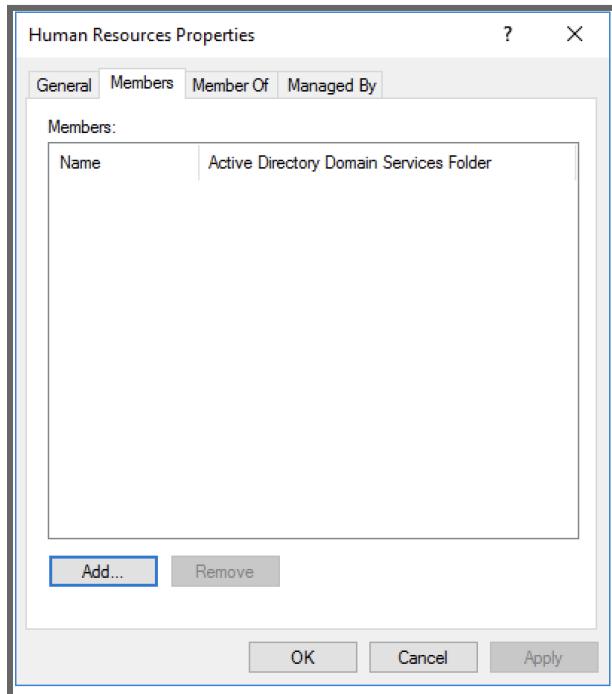


The Group Properties default screen.

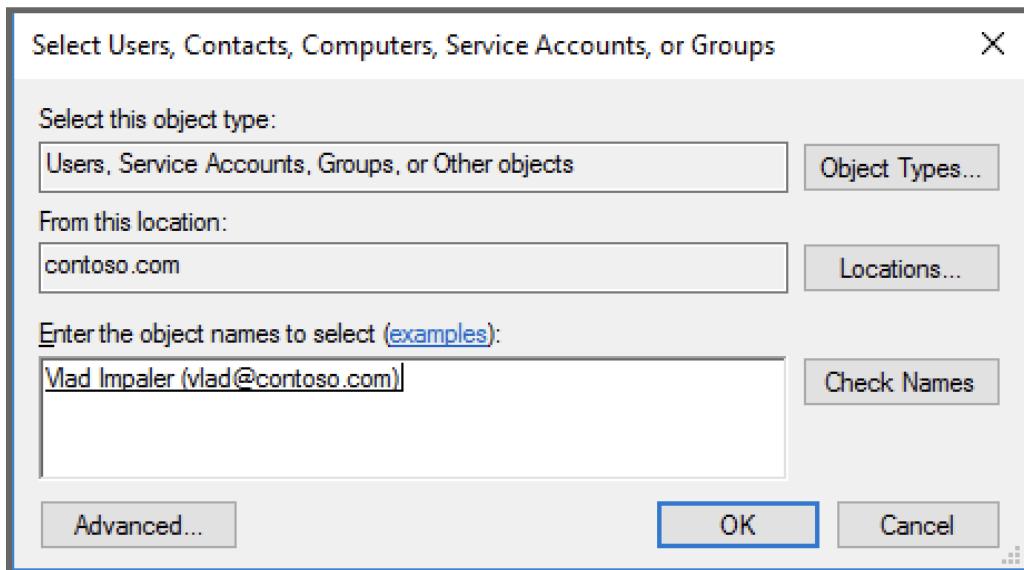


IT Onboarding Runbook

Select the **Members** tab. Click the **Add** button.

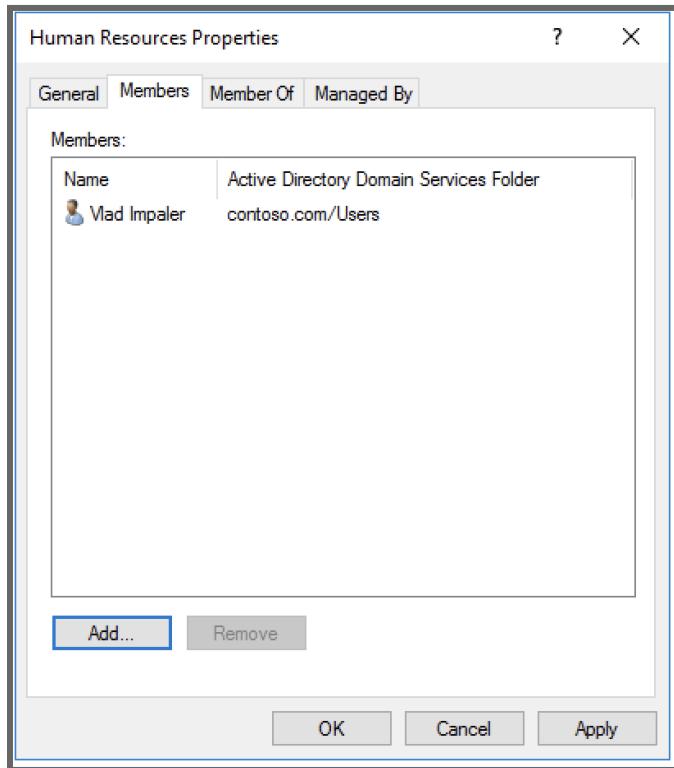


In the “Enter the object names to select” start inputting the user name. Click **Check Names** after a few letters are input to locate the user with matching pattern. Click **OK**.

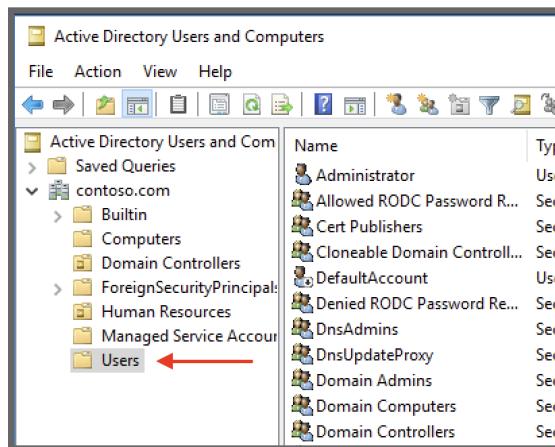


IT Onboarding Runbook

Confirm the Members show the User you just added. Click **OK** to close.

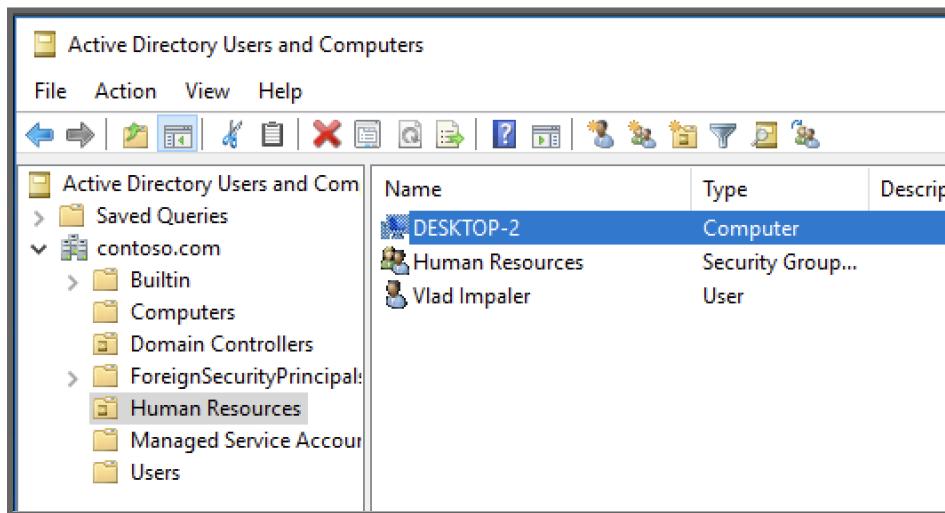


Open the **Active Directory** if its not already open. Adding the *Employee User* (Vlad Impaler) and **Group** (Human Resources) to the Human Resources **OU** is easy as dragging each User and Group into the OU from the “**Users**” directory > list. We may also need to associate the specific computer to the OU.



IT Onboarding Runbook

Open the “**Computers**” directory locate the local machine (this case Desktop 2)
(Roaming accounts will need further application of associations and GPOs. Something we are not concerned with here.)

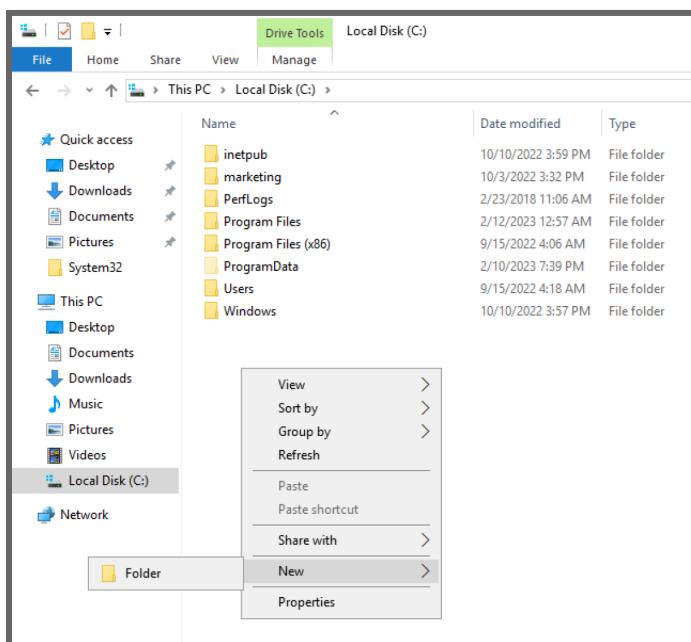


The screenshot shows the 'Active Directory Users and Computers' management console. The left navigation pane shows the tree structure under 'contoso.com': Active Directory Users and Com, Saved Queries, contoso.com (expanded), Builtin, Computers, Domain Controllers, ForeignSecurityPrincipal, Human Resources (selected), Managed Service Account, and Users. The right pane displays a table with three rows:

Name	Type	Description
DESKTOP-2	Computer	
Human Resources	Security Group...	
Vlad Impaler	User	

Share Build -

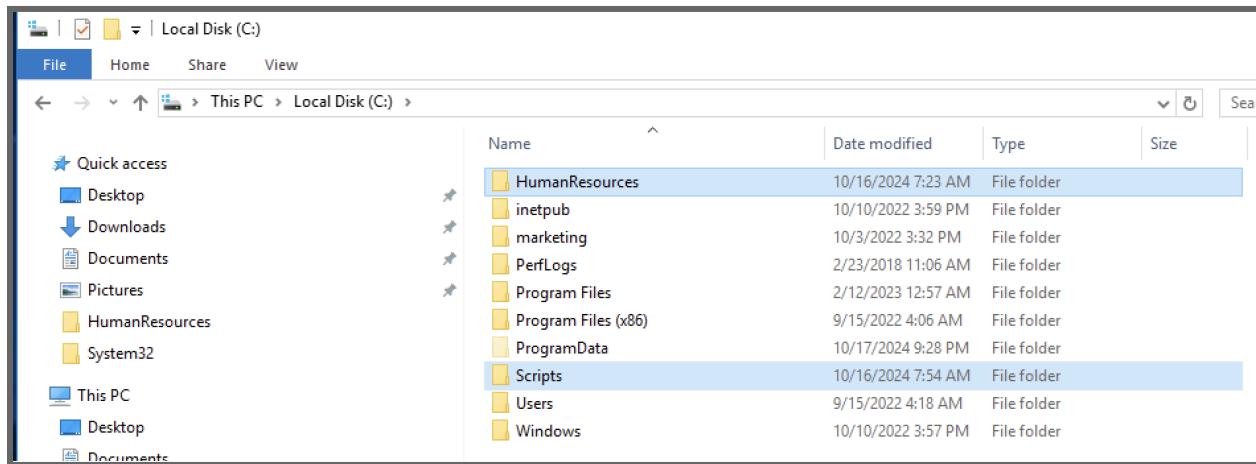
We need to create the “**share**” for the Department. We can build the needed directories with the the “**server**” C:/ Drive. Navigate to the C: Drive in Explorer. In a blank space within the C: Drives create two directories; one for the actual **Department “share”** (**Human Resources**) and one for the **script/s** needed to deploy the share.



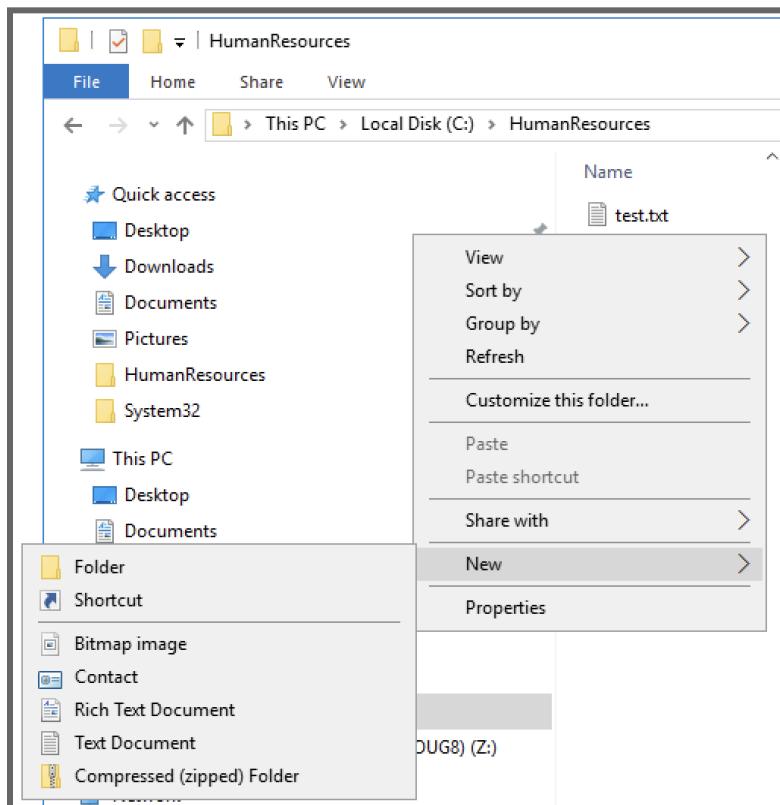
The screenshot shows the Windows File Explorer interface. The left sidebar shows 'This PC > Local Disk (C:)'. The main area lists several folders: inetpub, marketing, PerfLogs, Program Files, Program Files (x86), ProgramData, Users, and Windows. A context menu is open over a blank area at the bottom of the list, showing options: View, Sort by, Group by, Refresh, Paste, Paste shortcut, Share with, New, and Properties. The 'New' option is highlighted.

IT Onboarding Runbook

Right-click >New>Folder and create the Human Resources directory and Scripts.

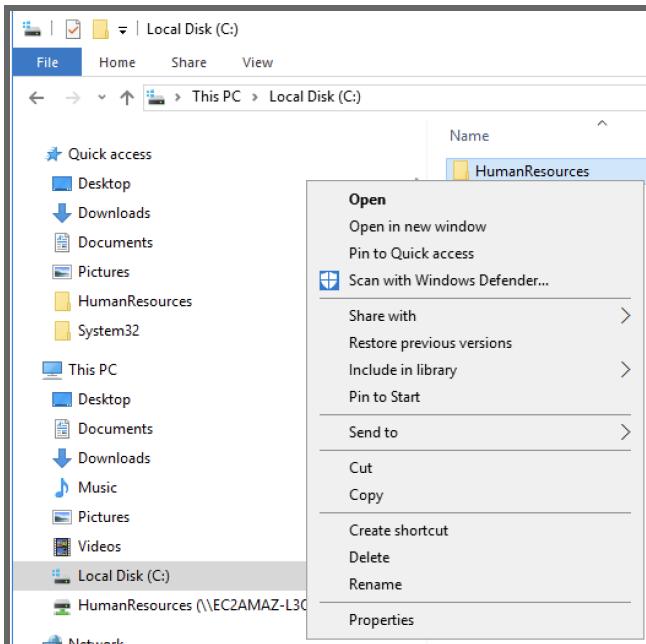


In the Human Resources directory we need to also create a test file for the sake of verification of execution. This can always be deleted later. **Right-click** on the blank space (within the directory list area) > **New > Text Document** named “test”.

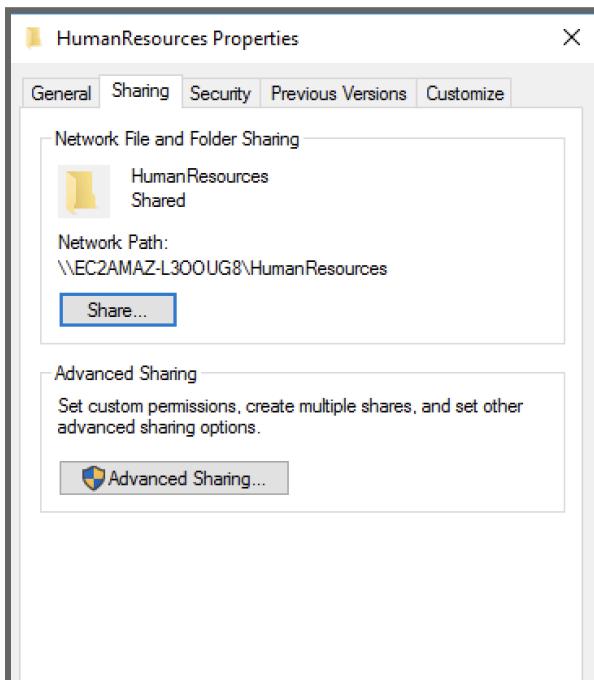


IT Onboarding Runbook

We will also need to verify and or set the sharing to the folder. **Right-click** on the Human Resources directory > **select “Properties”**

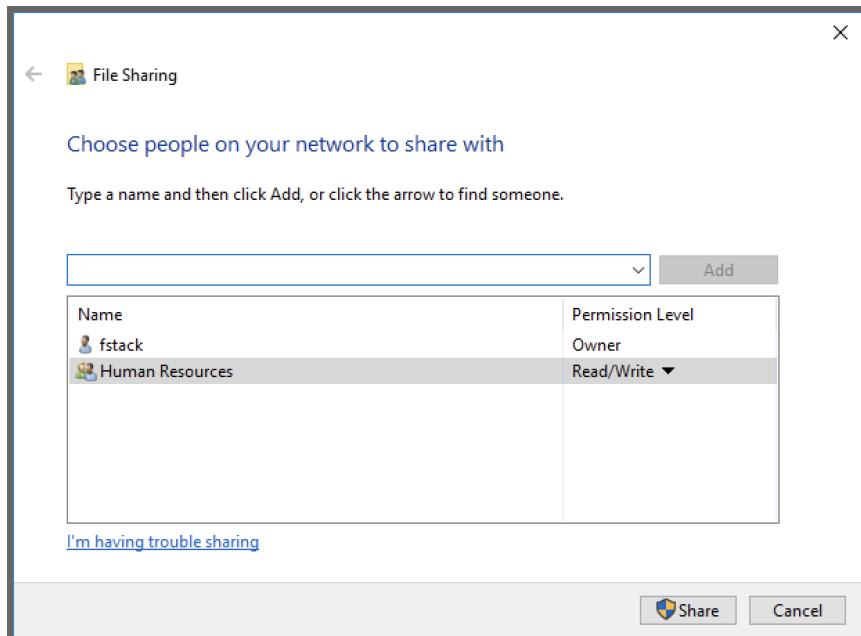


Select the “Sharing” tab. Click on the “Share” button.

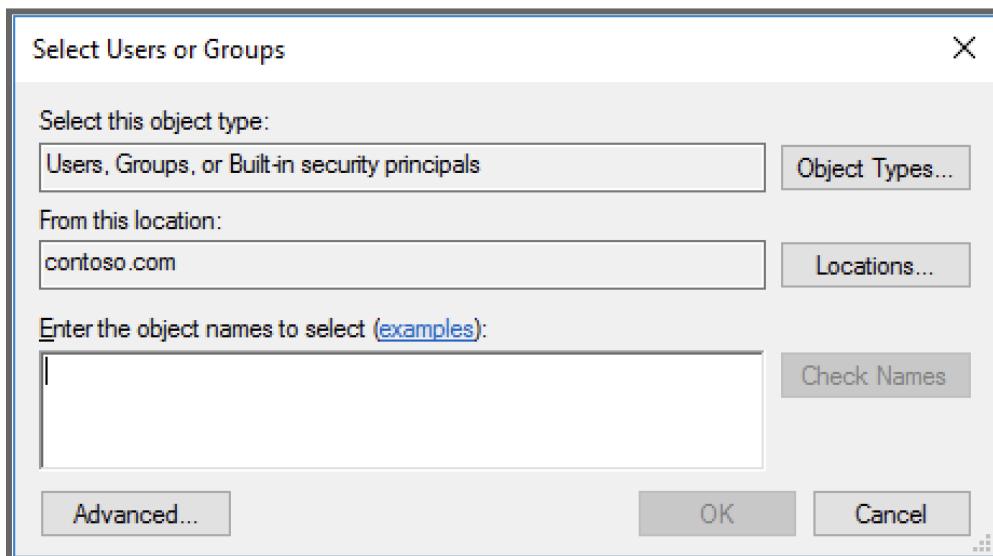


IT Onboarding Runbook

Add the Human Resources group to the list by starting to type the Groups name into the open field. If it doesn't auto fill you can click on the pull down within that same field.

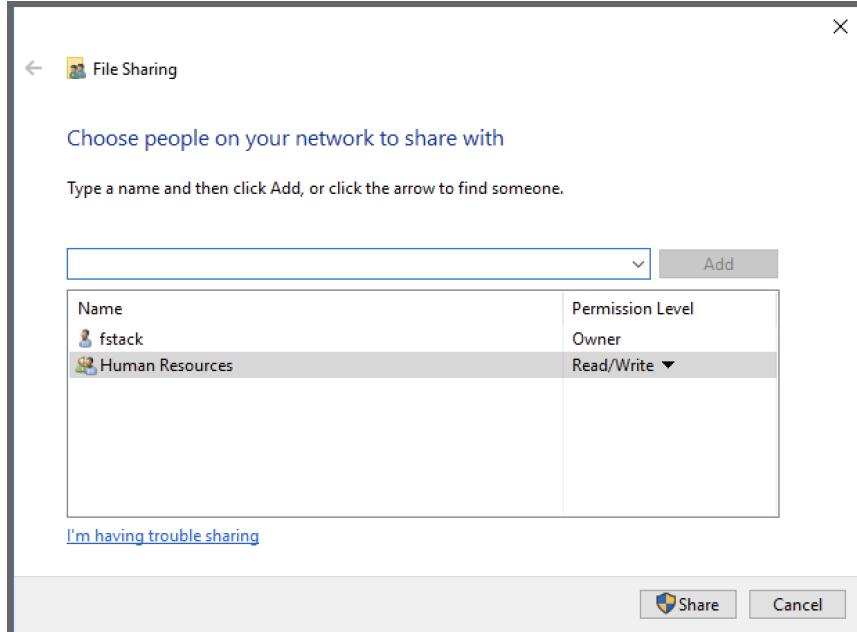


Select Users or Groups pops up. You can start entering the name in the “Enter the object ...” field and the **click on Check Names** > Locate the Group (Human Resources). Click OK.



IT Onboarding Runbook

Back at File Sharing you need to change the “Permissions Level” to **Read/Write** by clicking in that field and scrolling through the pulldown that appears.

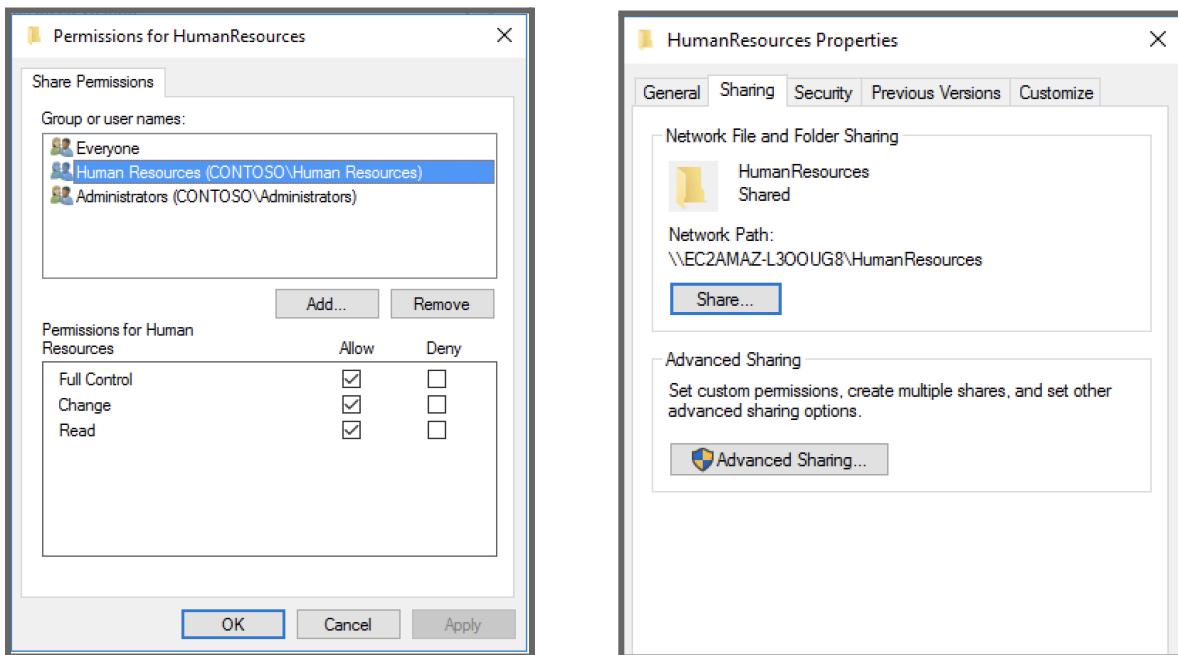


We may need to verify permissions for the “share”. Click on the **“Advanced Sharing”**. Within that >click **“Permissions”**

The screenshot shows two windows side-by-side. The left window is the "HumanResources Properties" dialog under the "Sharing" tab. It shows a "Network File and Folder Sharing" section with a "HumanResources" share listed, and an "Advanced Sharing" section with a "Share..." button. The right window is the "Advanced Sharing" dialog. It has a checked checkbox "Share this folder", a "Settings" section with a "Share name:" dropdown set to "New folder" and "Add" and "Remove" buttons, and a "Limit the number of simultaneous users to:" input field set to "16777". Below these are "Comments:" and "Permissions" tabs. At the bottom are "OK", "Cancel", and "Apply" buttons.

IT Onboarding Runbook

Click on the *Department* (Human Resources) Group and enable required Permissions. In this case **Full Control, Change and Read** are all allowed. Click **OK**. And **OK** Again. Copy the Network Path: **\EC2AMAZ-L300UG8\HumanResources**. (*Note it has been observed that it may make a difference between copying and typing this info into the intended place*)



Now a script will need created to facilitate the “share” (Human Resources) Drive mount on the Users machine. From the Start menu open Notepad.

Map Drive Script

In the Notepad input:

```
@echo off  
net use Z: \EC2AMAZ-L300UG8\HumanResources
```

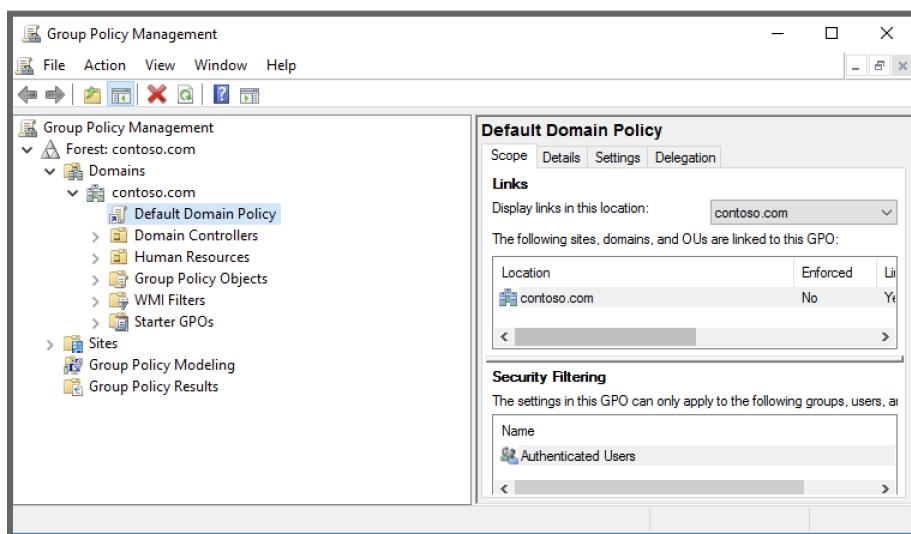
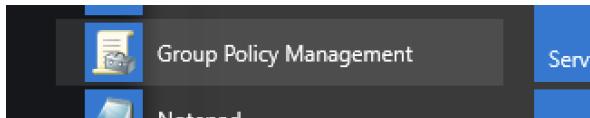
Save the file as a **.bat** file. In this case its called **“mapdrive.bat”** and is saved in the Scripts directory we created when we created the *Department* Human Resources directory.

Repeat the steps we did for the Human Resources directory starting at Page 22 for permissions and sharing configuration but for the Scripts directory.

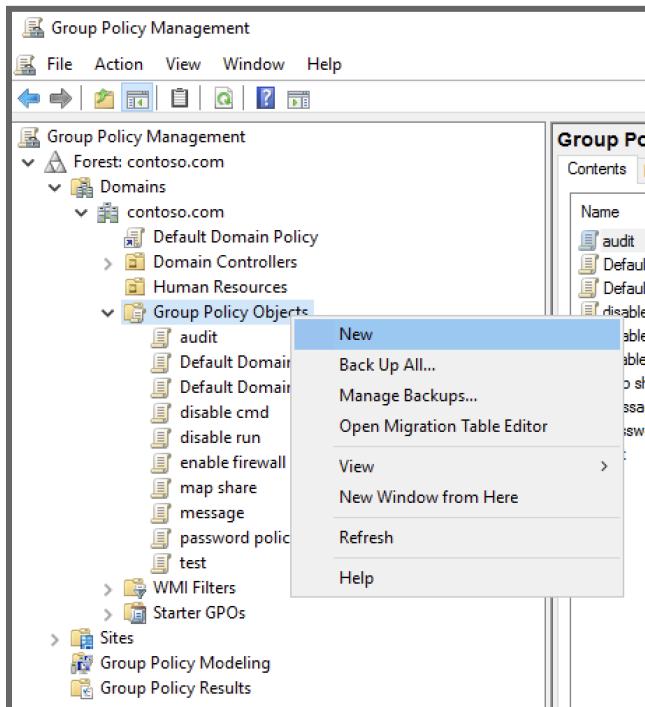
IT Onboarding Runbook

Group Policy Build

Locate Group Policy Management application.

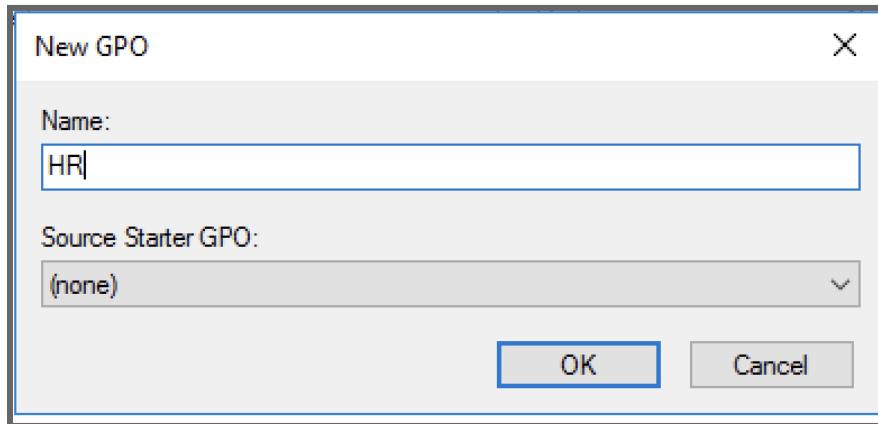


Select Group Policy Objects>right-click>New

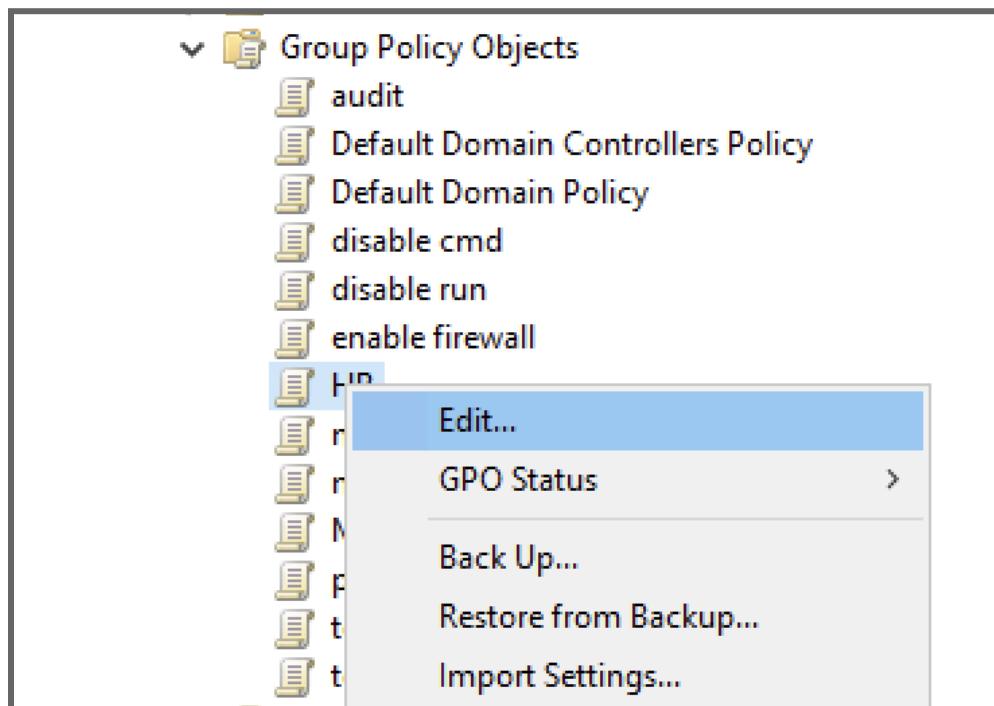


IT Onboarding Runbook

Input the “New Group Policy Object(GPO)” in this case “HR” in the “Name:” field. Click **OK**



Select the GPO we just created and **right-click > Edit**

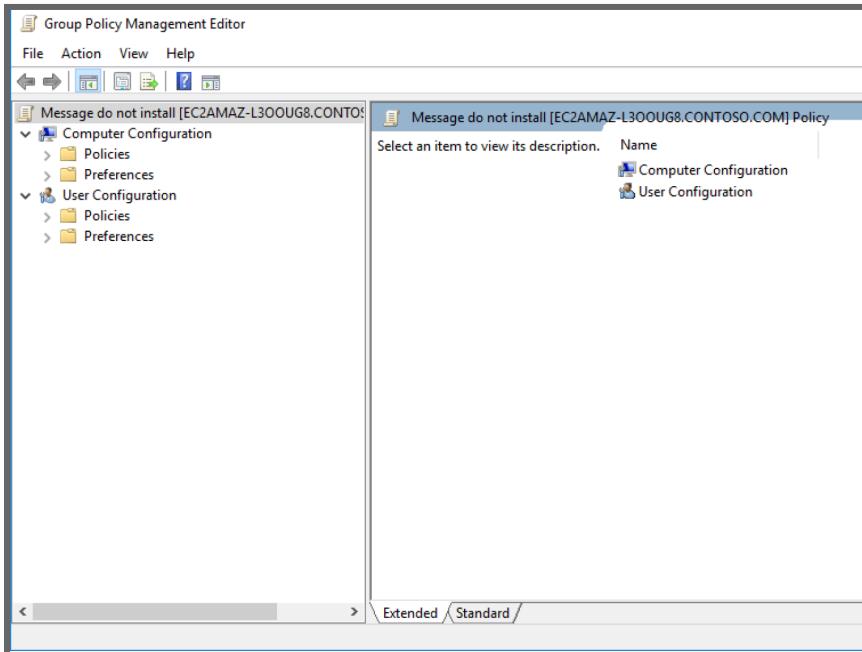


We to need establish the policies for the User and subsequent Groups.

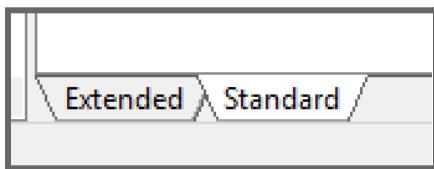
- A message should appear whenever the computer starts (do not install unauthorized programs).
- Prevent the user's access to CMD.
- Add script to the user's login to map the share you created.
- Disable the run command from the start menu.

IT Onboarding Runbook

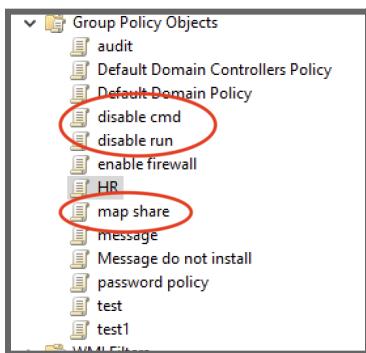
This take us to the “**Group Policy Management Editor**”.



Changing the bottom tab to “Standard” make navigation of the proceeding process cleaner to manage but for sake of clarity “Extended” will be used to see the path process which sit at the top of the list highlighted in blue.



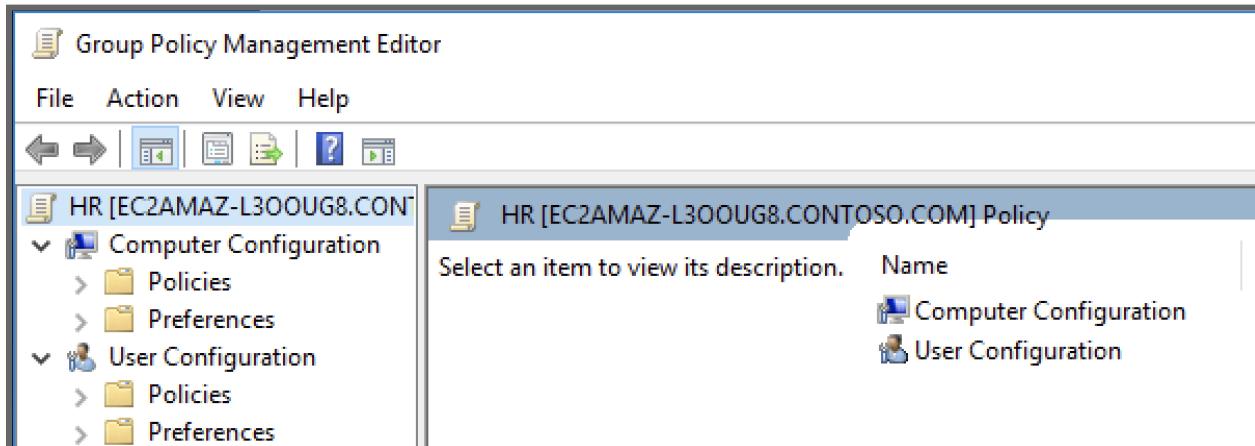
The following processes are staged out for the sake of clarity. However is should be noted that often times “**disable cmd**” and “**disable run**” and “**map share**” are preset in the “Group Policy Objects”.



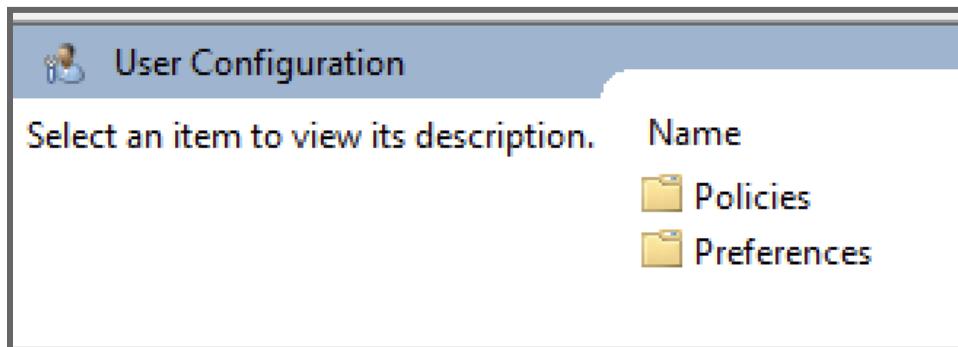
IT Onboarding Runbook

Removing Command Line Access

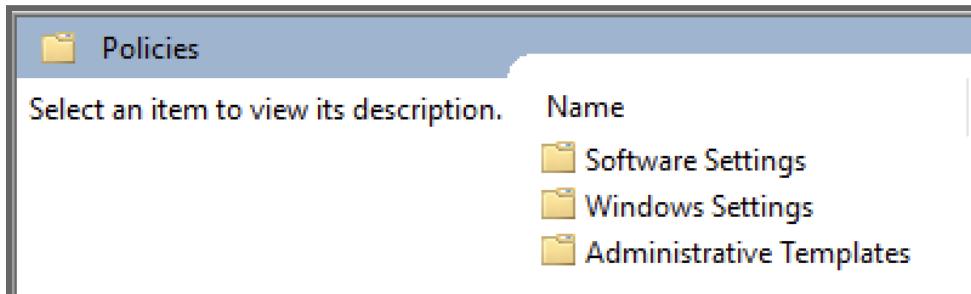
To prevent the users access to “Command line” we need to select the “**User Configuration**”. **Double click** to open to the next stage.



Double click “**Policies**”

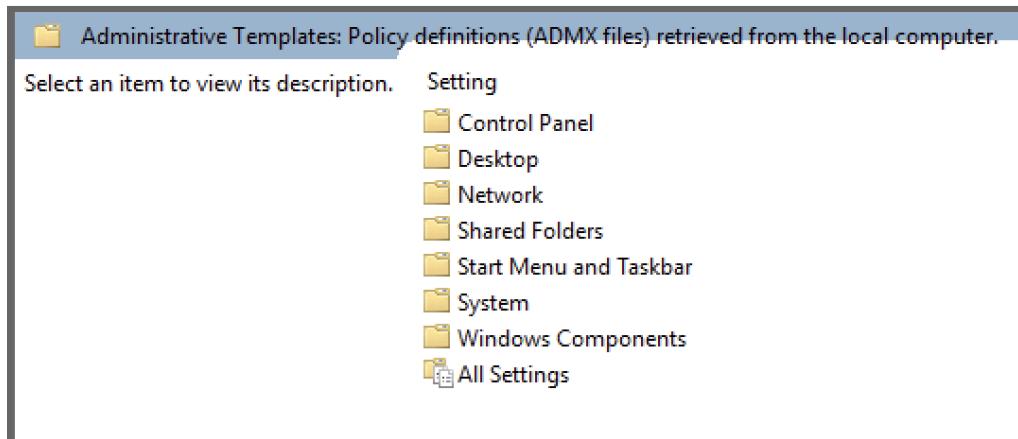


Double click “**Administrative Templates**”

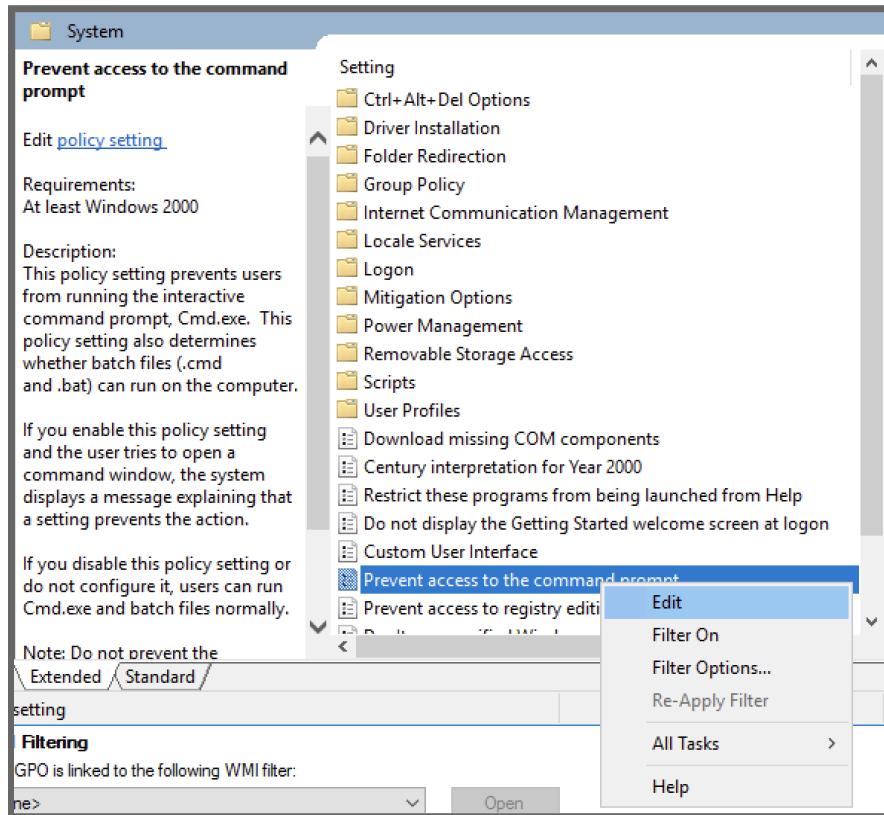


IT Onboarding Runbook

Double click “System”

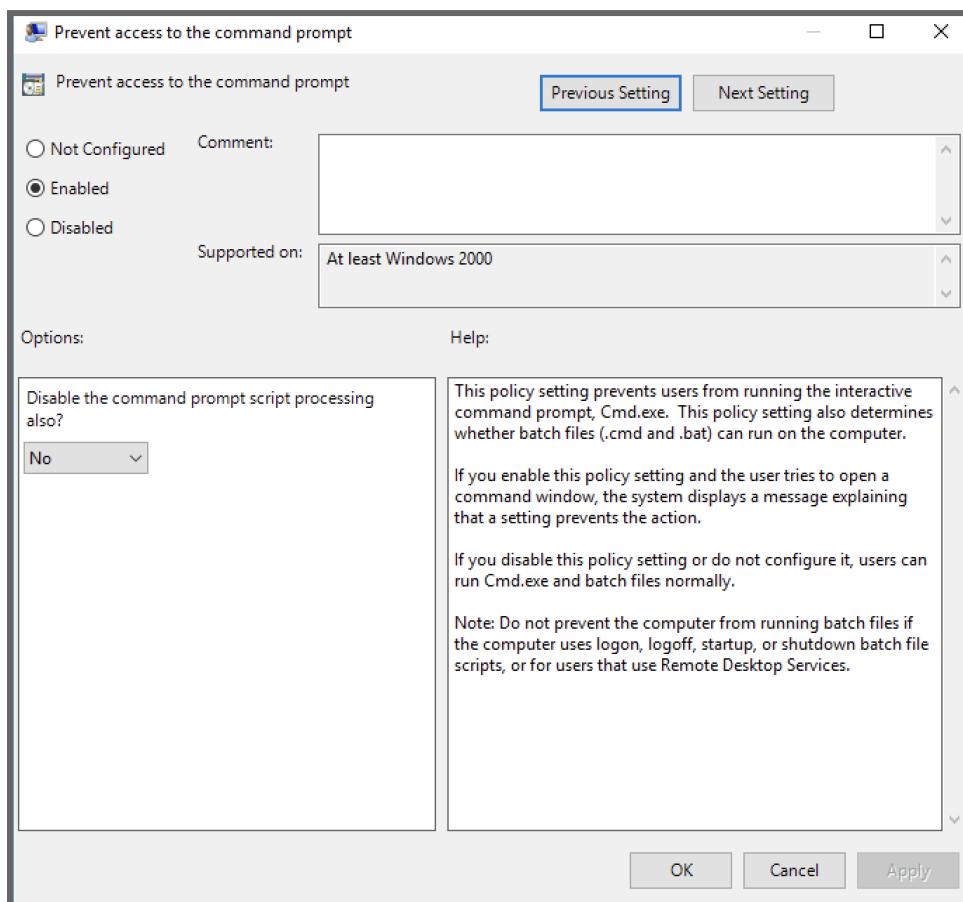


Locate “Prevent access to command prompt”. Right click > Edit

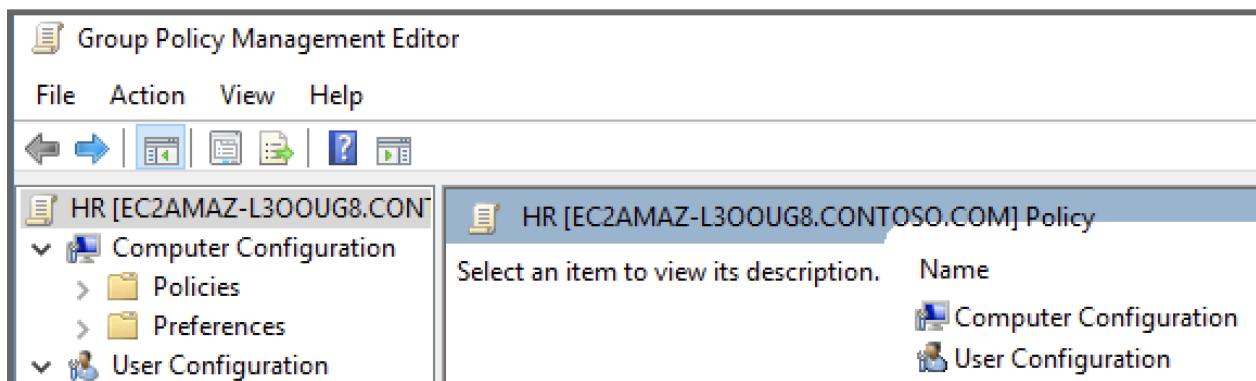


IT Onboarding Runbook

We see a panel with information about the policy under the “Help”, options for disabling the command prompt script processing (which we do not want to do here considering our list of policies of which one sets a command line script to set the “share”). Select the **Enabled** button to ensure the policy functions. **Click OK.**



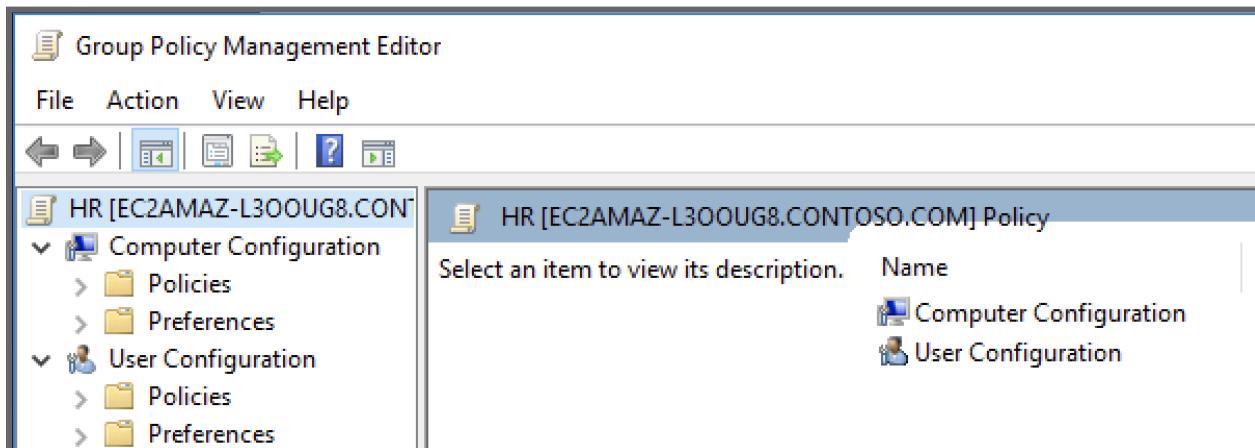
Use the back arrow to get back to the configuration options state.



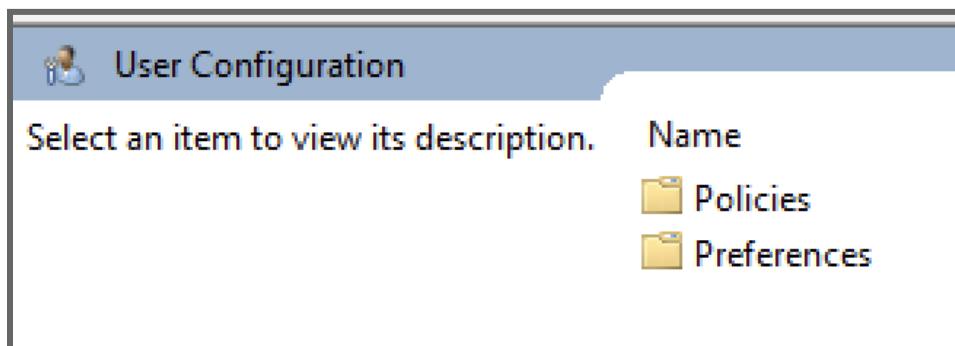
IT Onboarding Runbook

Disable the Run Command

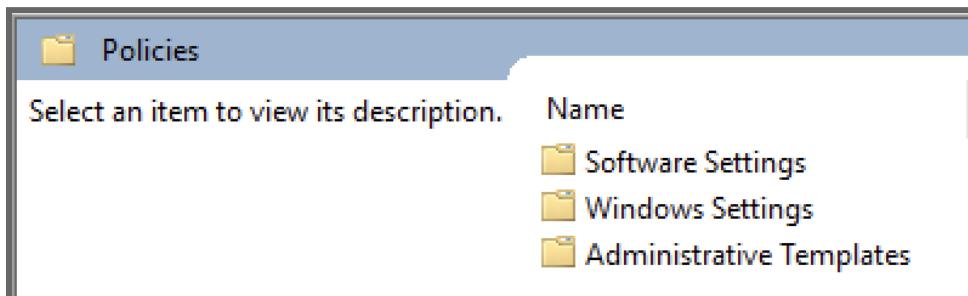
To disable “Run” for the we need to select the “**User Configuration**”. Double click to open to next stage.



Double click “**Policies**”



Double click “**Administrative Templates**”



IT Onboarding Runbook

Locate “Remove Run menu from Start Menu”.

Setting	State	Comment
Add Search Internet link to Start Menu	Not configured	No
Clear history of recently opened documents on exit	Not configured	No
Clear the recent programs list for new users	Not configured	No
Clear tile notifications during log on	Not configured	No
List desktop apps first in the Apps view	Not configured	No
Search just apps from the Apps view	Not configured	No
Add Logoff to the Start Menu	Not configured	No
Force Start to be either full screen size or menu size	Not configured	No
Go to the desktop instead of Start when signing in	Not configured	No
Gray unavailable Windows Installer programs Start Menu sh...	Not configured	No
Turn off personalized menus	Not configured	No
Lock the Taskbar	Not configured	No
Start Layout	Not configured	No
Add “Run in Separate Memory Space” check box to Run dial...	Not configured	No
Turn off notification area cleanup	Not configured	No
Remove Balloon Tips on Start Menu items	Not configured	No
Prevent users from customizing their Start Screen	Not configured	No
Remove and prevent access to the Shut Down, Restart, Sleep...	Not configured	No
Remove common program groups from Start Menu	Not configured	No
Remove Favorites menu from Start Menu	Not configured	No
Remove Search link from Start Menu	Not configured	No
Remove frequent programs list from the Start Menu	Not configured	No
Remove Games link from Start Menu	Not configured	No
Remove Help menu from Start Menu	Not configured	No
Turn off user tracking	Not configured	No
Remove All Programs list from the Start menu	Not configured	No
Remove Network Connections from Start Menu	Not configured	No
Remove pinned programs list from the Start Menu	Not configured	No
Do not keep history of recently opened documents	Not configured	No
Remove Recent Items menu from Start Menu	Not configured	No
Do not use the search-based method when resolving shell s...	Not configured	No
Do not use the tracking-based method when resolving shell ...	Not configured	No
Remove Run menu from Start Menu	Not configured	No
Remove Default Programs link from the Start menu	Not configured	No

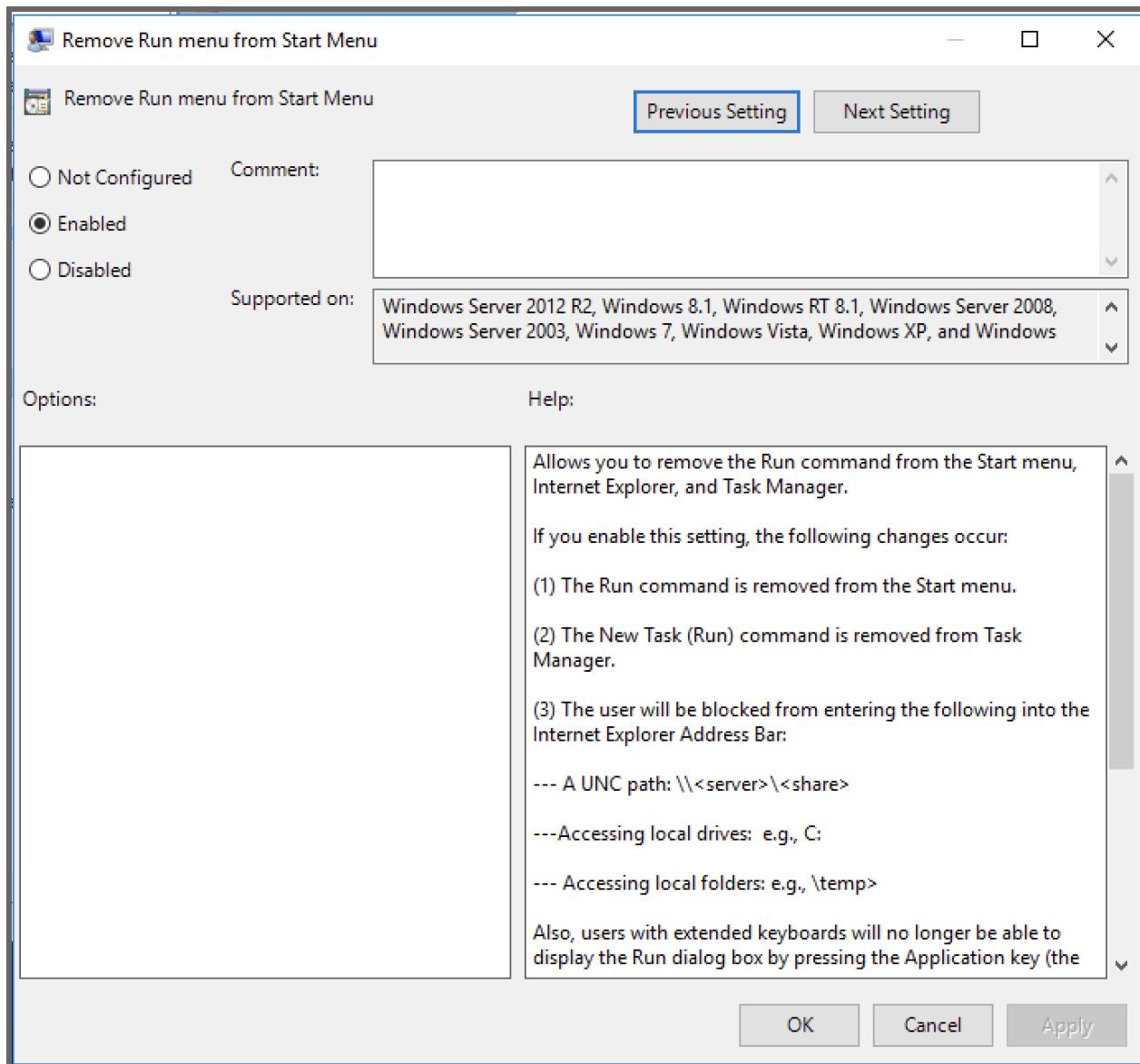
Right-click > Edit

- Do not use the tracking-based method when resolving shell ... Not configured
- Remove Run menu from Start Menu**
- < >

Edit
 Filter On
 Filter Options...
 Re-Apply Filter
 All Tasks >
 Help

IT Onboarding Runbook

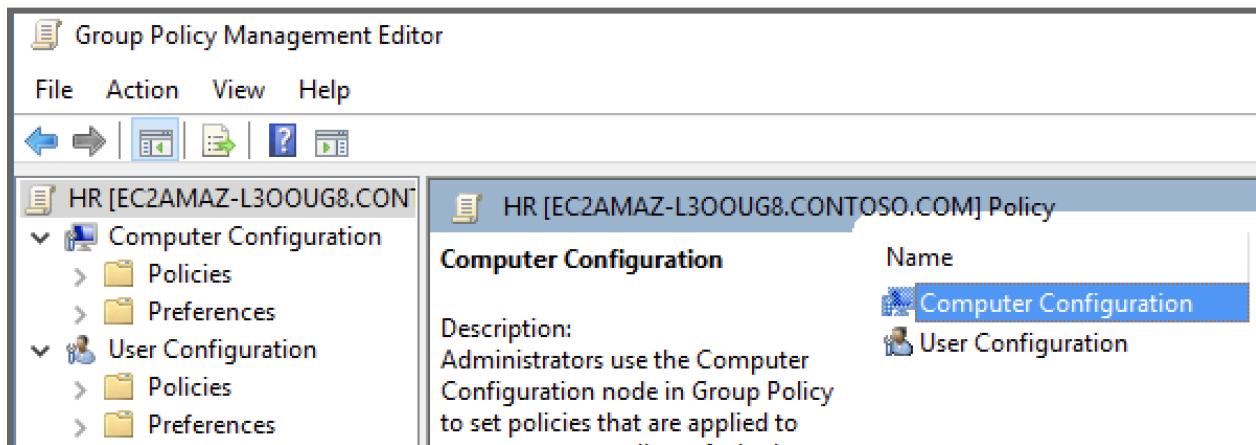
The Remove Run menu Start Menu panel pops up. As before, with the “Command Line disable” verify under the “Help:” that this is the policy needed. **Click on Enabled.** Then **Click OK.**



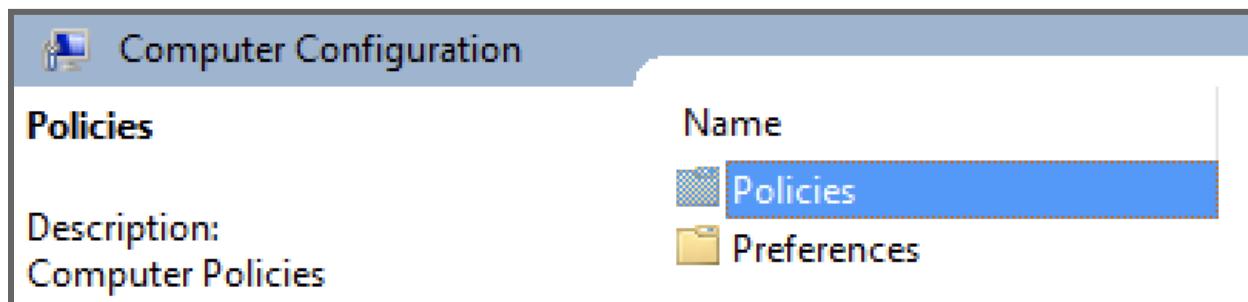
IT Onboarding Runbook

Do Not Install Unauthorized Applications Warning

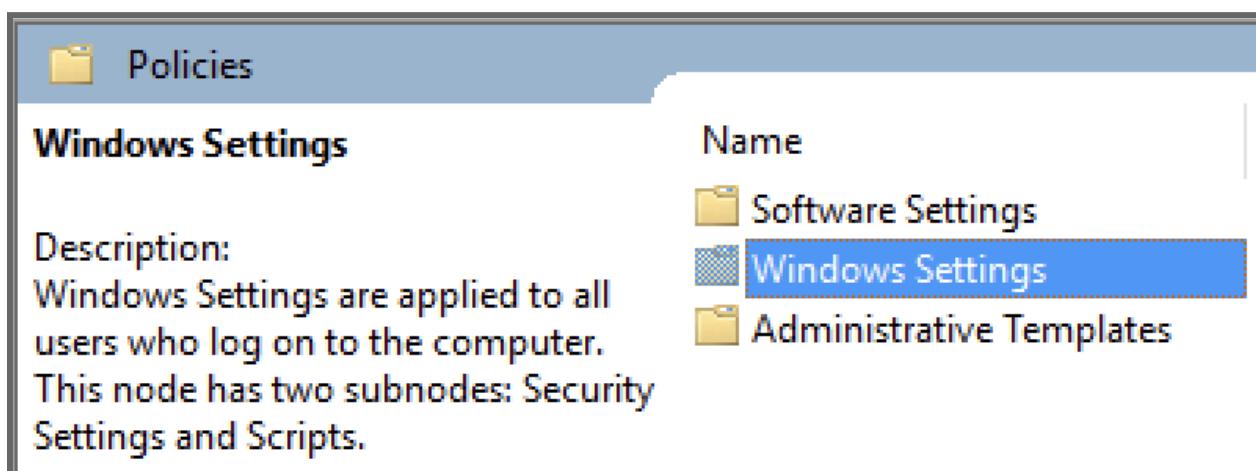
Use the back arrow to get back to the configuration options state. **Double-click "Computer Configuration"** to open to the next stage.



Double Click **"Policies"**.

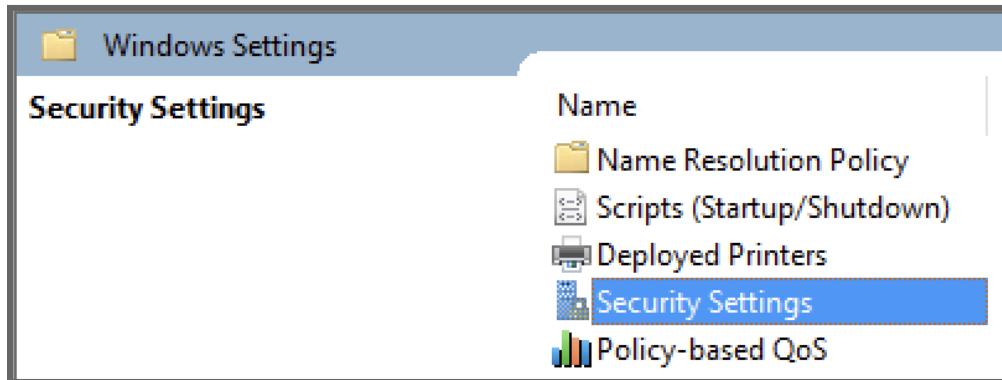


Double Click **"Windows Settings"**.



IT Onboarding Runbook

Double Click “**Security Settings**”.



Double Click “**Local Policies**”.

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Event Log	Event Log
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File system security settings
Wired Network (IEEE 802.3) Policies	Wired Network Policy Administration. Manage ...
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security

Double Click “**Local Policies**”.

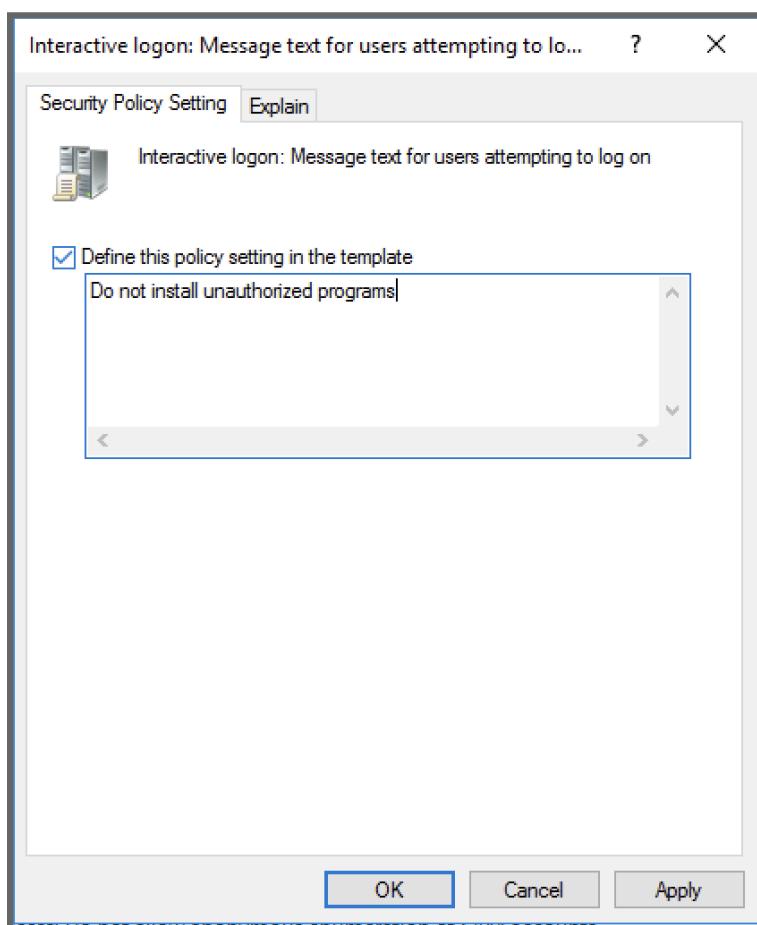
Name	Description
Audit Policy	Audit Policy
User Rights Assignment	User Rights Assignment
Security Options	Security Options

IT Onboarding Runbook

Locate “**Interactive logon: Message text...**” and double Click

Policy	Policy Setting
Domain member: Digitally sign secure channel data (when possible)	Not Defined
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) session key	Not Defined
Interactive logon: Display user information when the session is locked	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	Not Defined
Interactive logon: Prompt user to change password before expiration	Not Defined

Click “**Define this policy setting in the template**” then Type the message “do not install unauthorized programs” into the field. Click **OK**

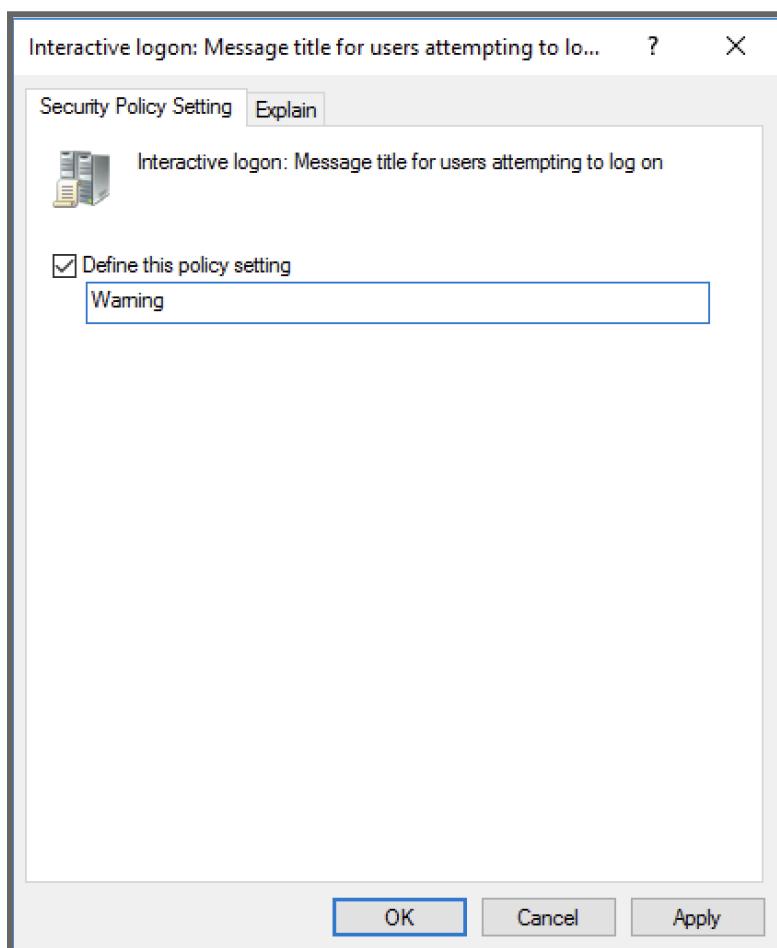


IT Onboarding Runbook

Locate “**Interactive logon: Message title...**” and double click.

Interactive logon: Display user information when the session... Not Defined
Interactive logon: Do not display last user name Not Defined
Interactive logon: Do not require CTRL+ALT+DEL Not Defined
Interactive logon: Don't display username at sign-in Not Defined
Interactive logon: Machine account lockout threshold Not Defined
Interactive logon: Machine inactivity limit Not Defined
Interactive logon: Message text for users attempting to log on do not install unauthorized pro... Not Defined
Interactive logon: Message title for users attempting to log on Not Defined
Interactive logon: Number of previous logons to cache (in c... Not Defined
Interactive logon: Prompt user to change password before e... Not Defined

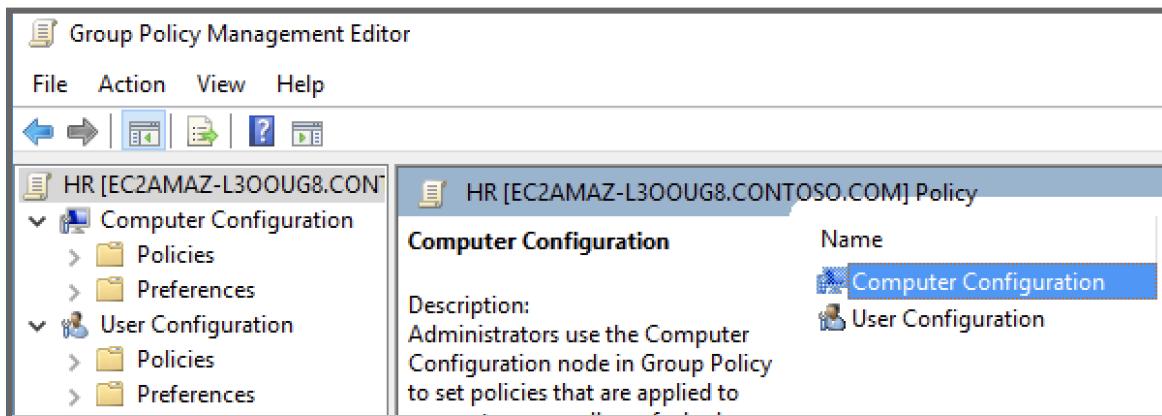
Click “**Define this policy setting in the template**” then Type the message “Warning” into the field. Click **OK**.



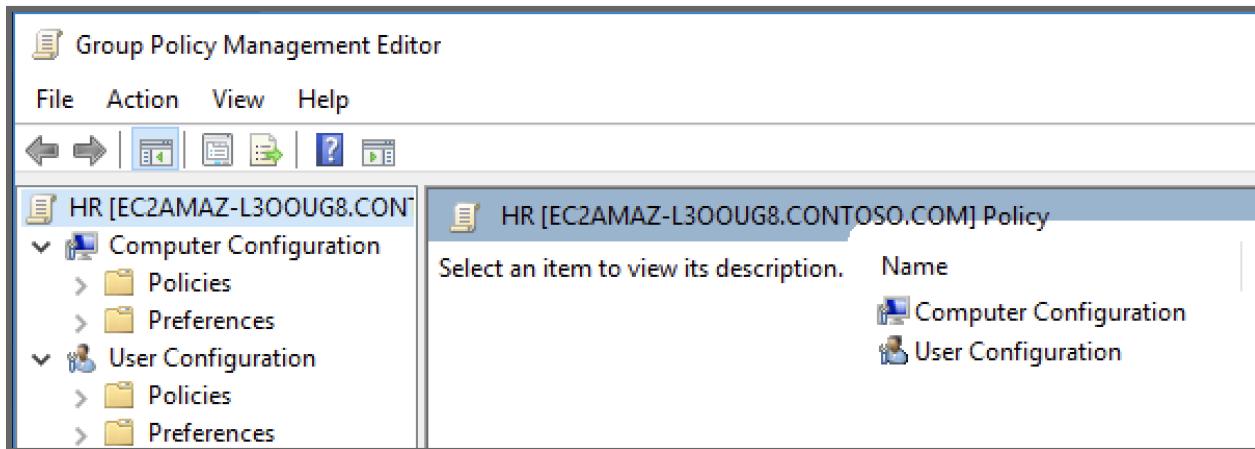
IT Onboarding Runbook

Share Drive Mount Policy

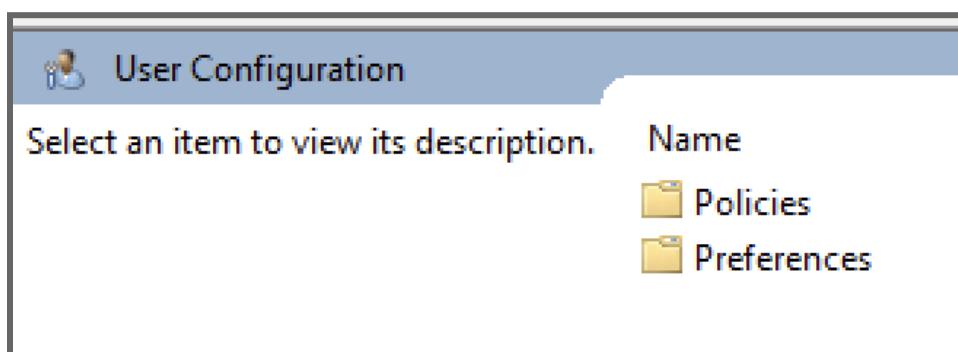
Use the back arrow to get back to the configuration options state. **Double-click “Computer Configuration”** to open to the next stage.



To disable “Run” for the we need to select the “**User Configuration**”. Double click to open to next stage.

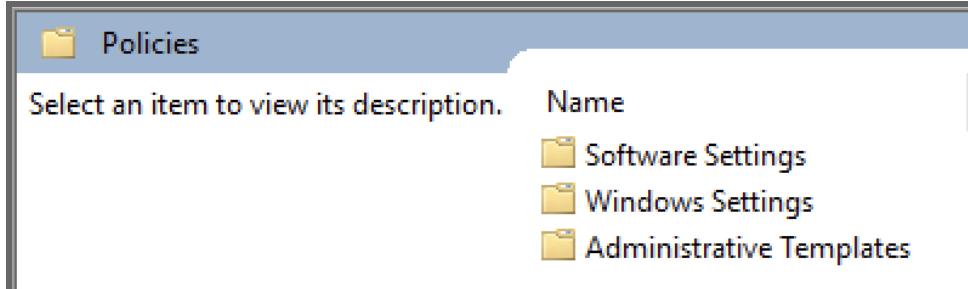


Double click “**Policies**”

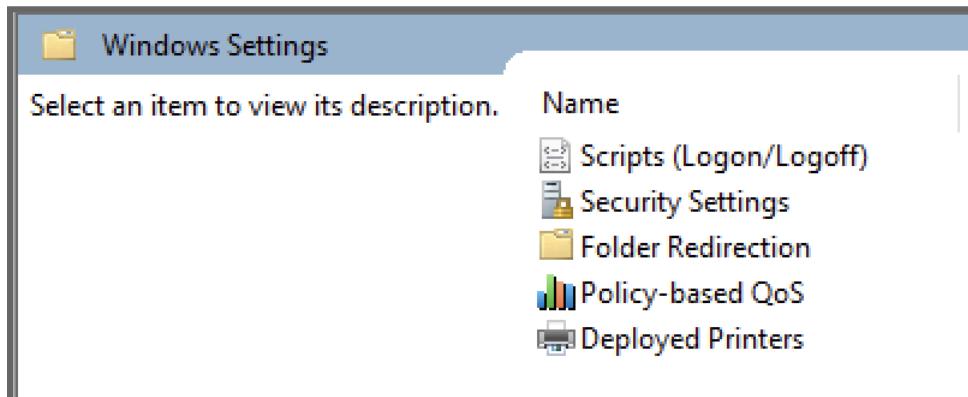


IT Onboarding Runbook

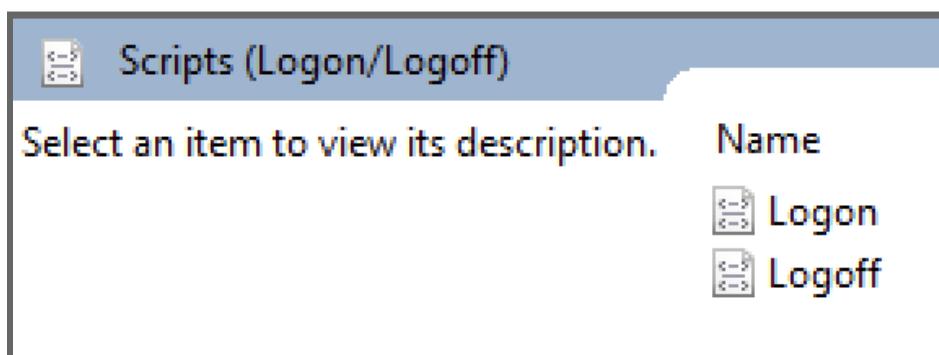
Double click “Windows Settings”



Double click “Scripts Logon/Logoff”

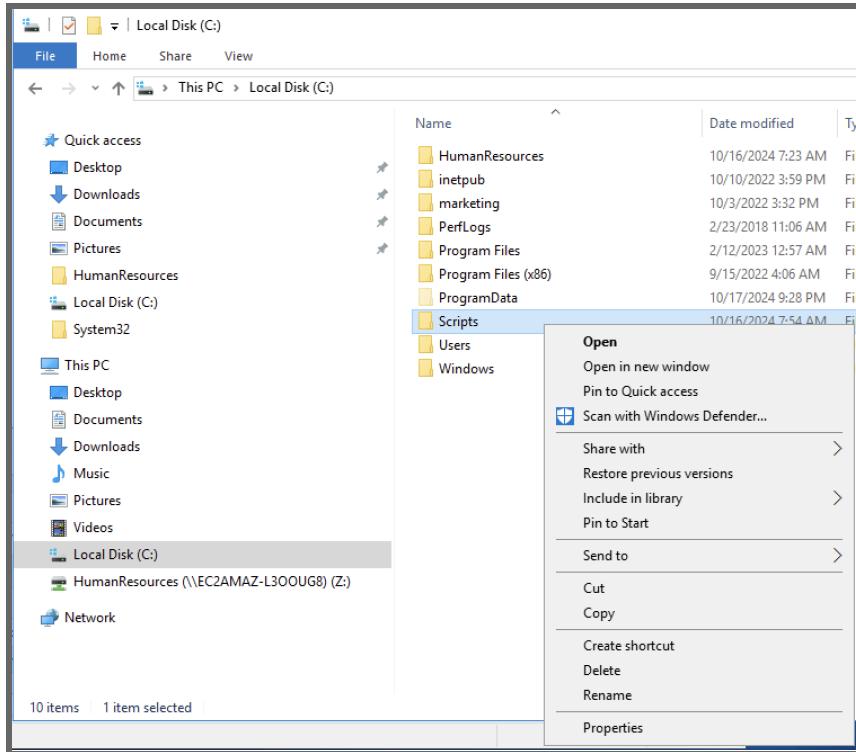


Double click “Logon”



IT Onboarding Runbook

Open Explorer and navigate to the “Local Drive (C:)”. Right-click on the “Scripts” directory. This is where we saved the “mapdrive.bat” script and set the sharing earlier.

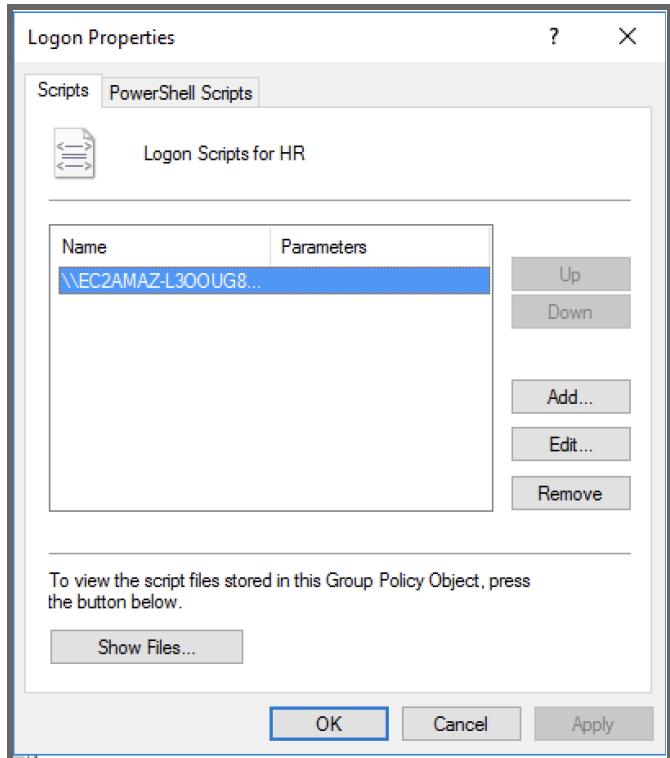


Click on the “Sharing” tab and then Click on the “Share” button. Double check the “Human Resources” Group has Read/Write permission. Copy the “Network Path.”

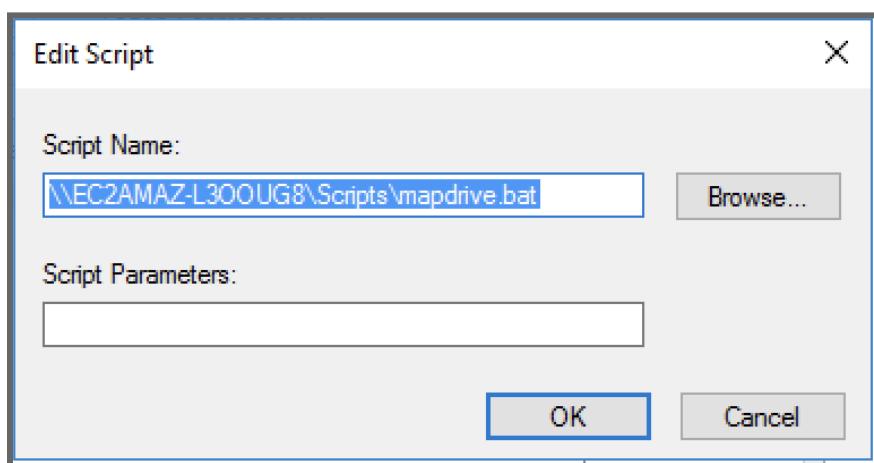
The image contains two side-by-side screenshots. The left screenshot shows the 'Sharing' tab of the 'Scripts Properties' dialog box. It displays a 'Network Path' of '\\EC2AMAZ-L300UG8\Scripts' and a 'Share...' button. The right screenshot shows the 'File Sharing' dialog box, which lists 'fstack' and 'Human Resources' under 'Name' with 'Permission Level' set to 'Owner' and 'Read/Write'. Both dialogs have a 'Cancel' and 'OK' button at the bottom.

IT Onboarding Runbook

In the Logon Properties check the Name/Parameters list. It is likely it is not linked to the “share” drive (or Human Resources). Click on **Edit**.



In the “Edit Script” paste the copied path from the Scripts directory. You will also need to append the script name itself. In this case **\\EC2AMAZ-L300UG8\Scripts\mapdrive.bat**. Click **OK**. And **OK** again in the “Logon Properties”.

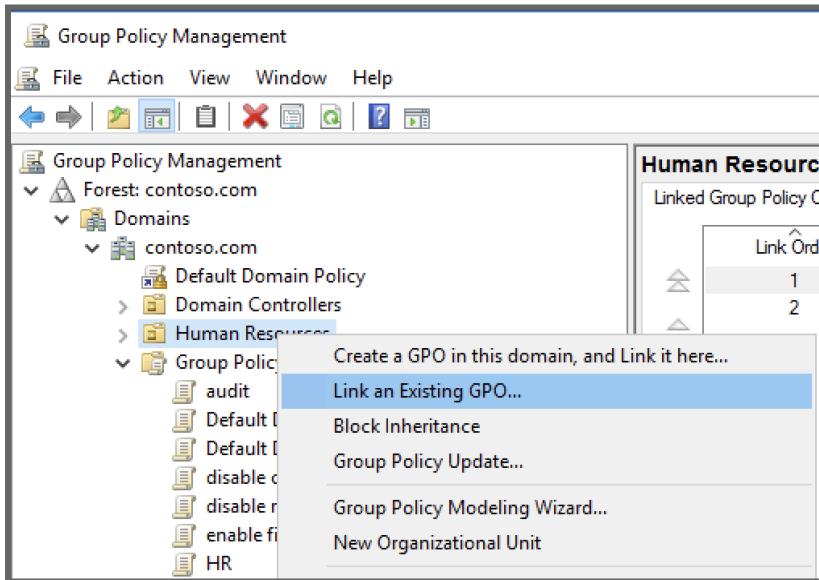


Close the Group Policy Management Editor.

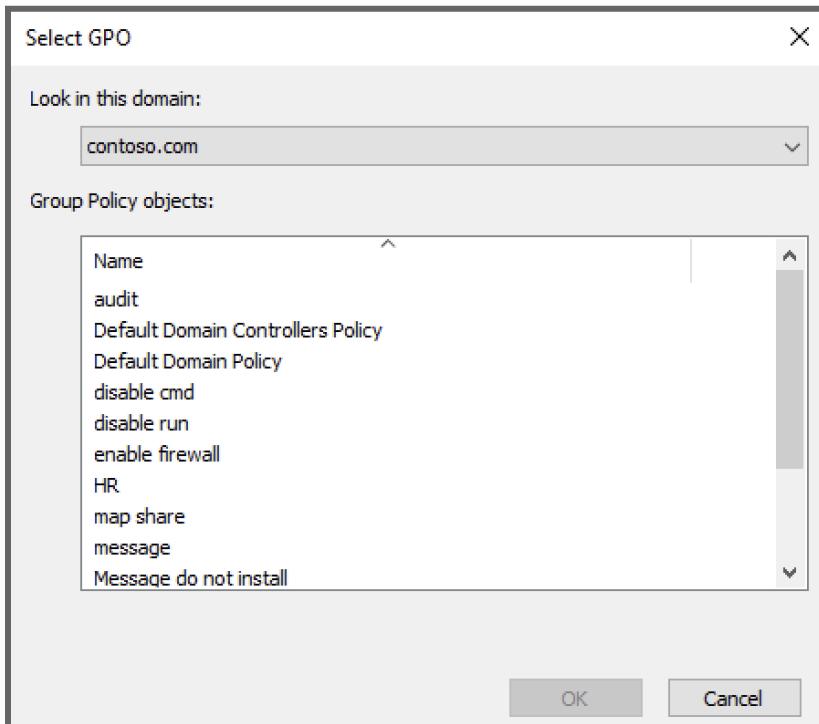
IT Onboarding Runbook

Linking GPO to Organizational Unit

In the Group Policy Management select the **OU** (in this case “**Human Resources**”). Right click > **Link an Existing GPO**.

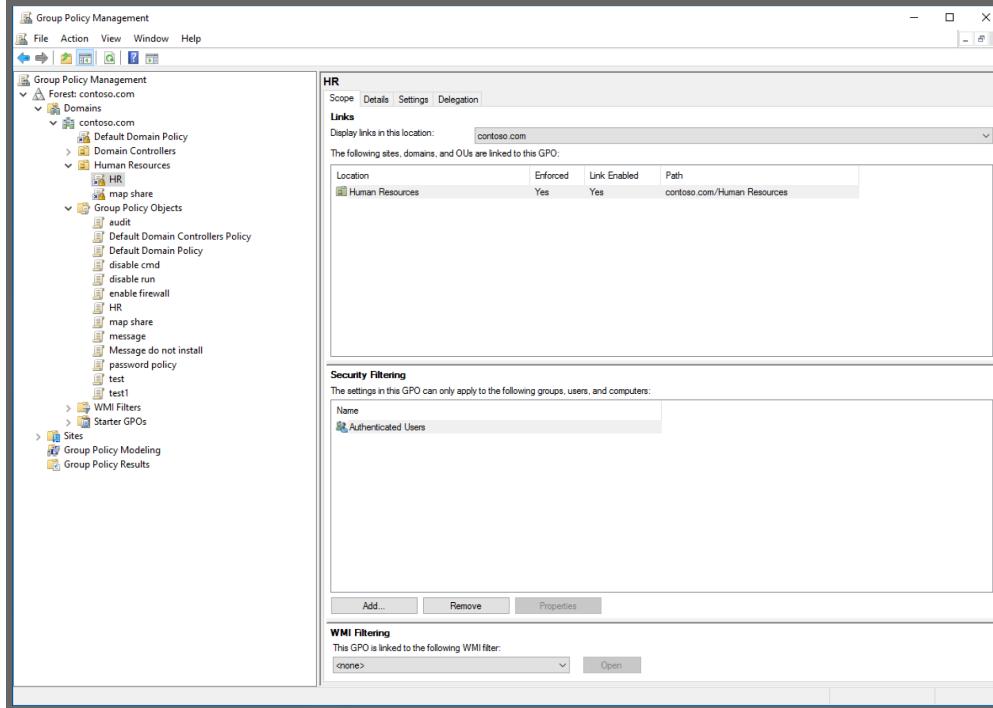


In the “Select GPO” panel under the “Group Policy objects:” select the (respective Group Policy object) **“HR”**. Click **OK**.



IT Onboarding Runbook

Select the now linked GPO “HR”. Doing so reveals Scope, Details, Settings and Delegation. For now we are only really concerned with Scope and Settings.

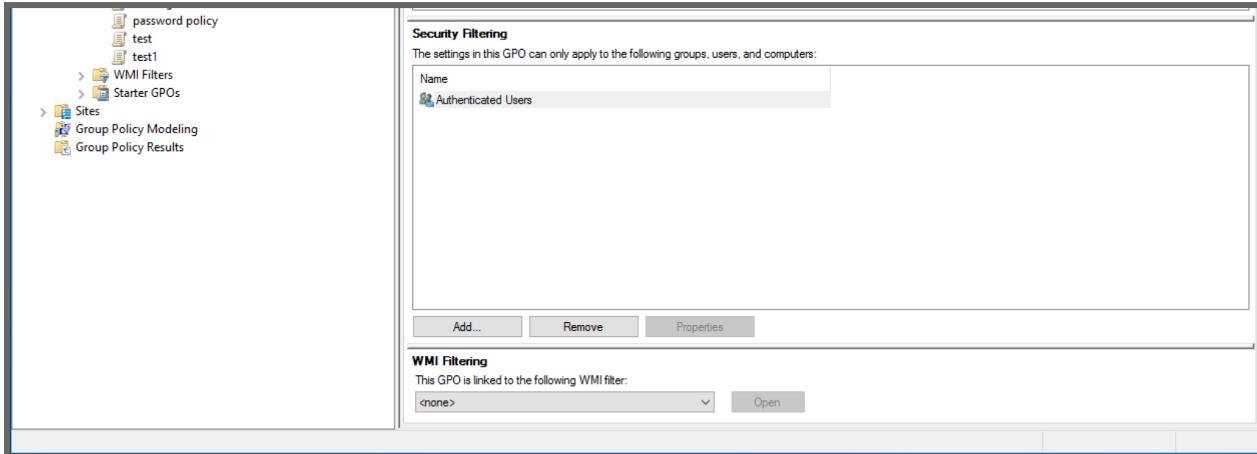


The Scope **Links** block indicates we are Enforcing and Link Enabled. If this were not true we could **right click** on each column value and enable the respective values needed.

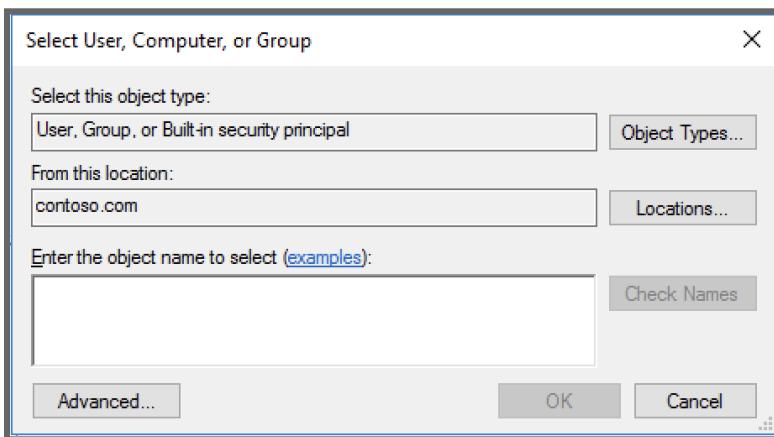
Location	Enforced	Link Enabled	Path
Human Resources	Yes	Yes	contoso.com/Human Resources

IT Onboarding Runbook

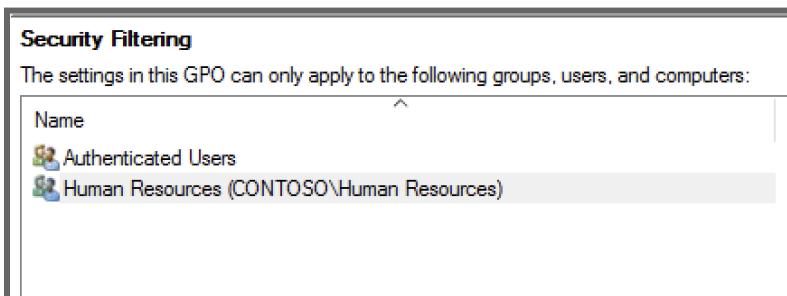
The **Security Filtering** indicates what users are cleared for application. Authenticated Users is a blanketed application. In most cases we would need the User Group added to ensure policy applies only to those in the Group. Here we are going to cover all bases.



Click on **Add**



The “Human Resources” group has been applied.



IT Onboarding Runbook

Select the “**Settings**” tab. Click on Show all in the upper right corner above the yellow bar. Note Links values they should match the “**Links**” tab.

The screenshot shows the properties of the 'HR' Group Policy Object (GPO) in the Windows Group Policy Management console. The 'General' tab is selected, displaying basic information such as the domain (contoso.com), owner (CONTOSO\Domain Admins), and creation date (10/16/2024 8:24:46 PM). The 'Links' tab shows a single link to 'Human Resources' with 'Yes' enforced. The 'Security Filtering' tab lists groups ('CONTOSO\Human Resources', 'NT AUTHORITY\Authenticated Users') that can apply settings. The 'Delegation' tab shows permissions for various users and groups, with 'Edit settings, delete, modify security' allowed for most.

Name	Allowed Permissions	Inherited
CONTOSO\Domain Admins	Edit settings, delete, modify security	No
CONTOSO\Enterprise Admins	Edit settings, delete, modify security	No
CONTOSO\Human Resources	Read (from Security Filtering)	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

IT Onboarding Runbook

If we scroll down we can see the policy and their Configurations at a glance. This is the check down to make sure they are enabled, their associations and the specifics of the policies.

Computer Configuration (Enabled)		
Policies		
Windows Settings		
Security Settings		
Local Policies/Security Options		
Interactive Logon		
Policy	Setting	
Interactive logon: Message text for users attempting to log on	do not install unauthorized programs	hide
Interactive logon: Message title for users attempting to log on	"Warning"	hide
User Configuration (Enabled)		
Policies		
Windows Settings		
Scripts		
Logon		
For this GPO, Script order: Not configured		
Name	Parameters	
\EC2AMAZ-L300UG8\Scripts\mapdrive.bat		hide
Administrative Templates		
Policy definitions (ADMX files) retrieved from the local computer.		
Start Menu and Taskbar		
Policy	Setting	Comment
Remove Run menu from Start Menu	Enabled	hide
System		
Policy	Setting	Comment
Prevent access to the command prompt	Enabled	hide
Disable the command prompt script processing also?	No	

IT Onboarding Runbook

To ensure the GPO are pushed we run **gpupdate /force**

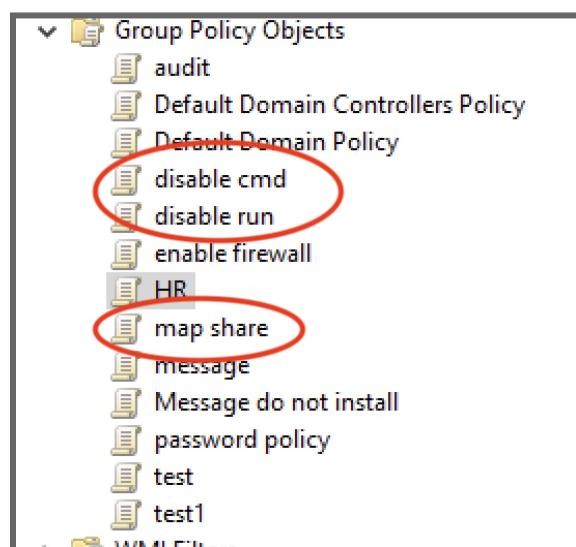
```
Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\fstack>gpupdate /force
Updating policy...

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

C:\Users\fstack>
```

***** Reminder the preceding processes are staged out for the sake of clarity. However it should be noted that often times “**disable cmd**” and “**disable run**” and “**map share**” are preset in the “Group Policy Objects”. We would still need to follow the workpaths for each respectively as we did manually. But the shortcuts are already pointed where we need them.*****



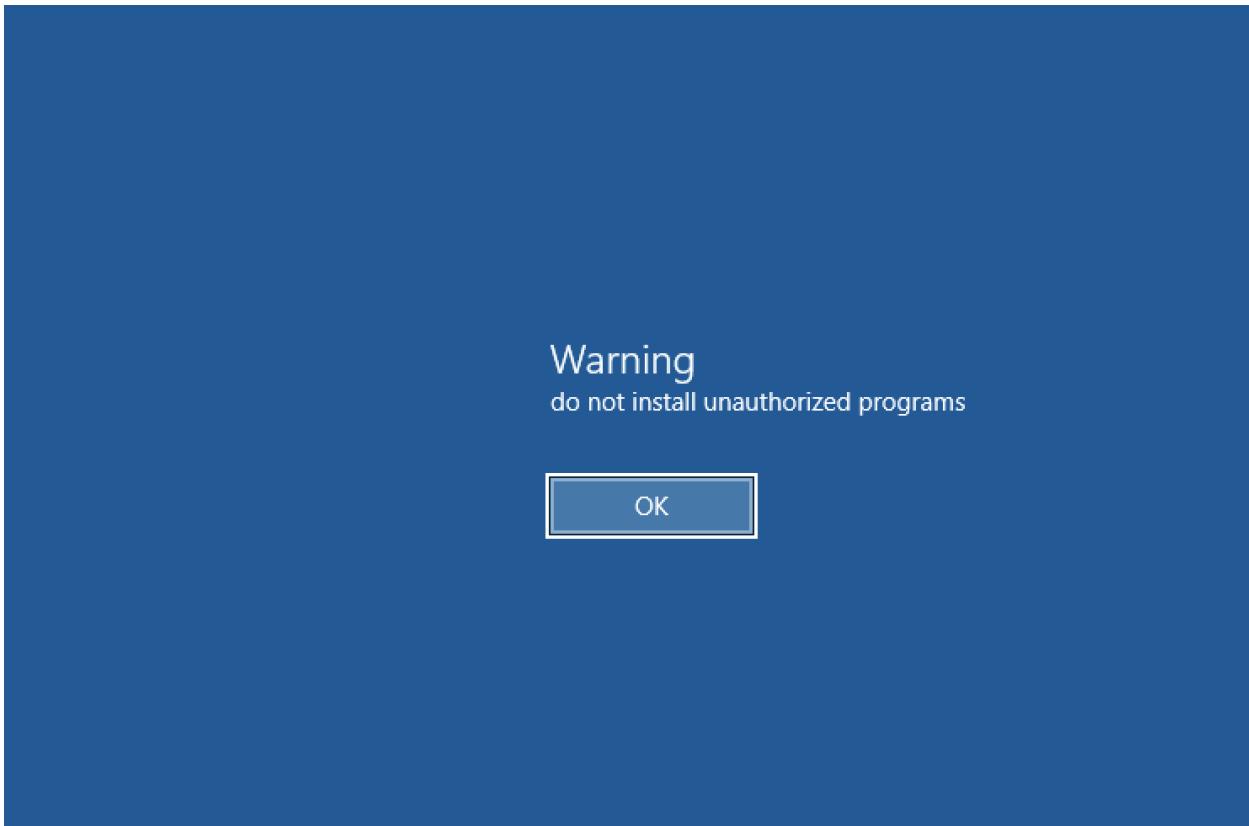
IT Onboarding Runbook

Verification

We need to verify the client machine is responding as we expect.

The machine in this case is the **Desktop-2**

Start up the Desktop-2 machine. This is the first indicator things are working as they should in regard to the “**Warning**” messaging.



IT Onboarding Runbook

Sign in to with the user (**Vlad**) As we had it set to change password we need to do that.

Password: 12345678 (for sake of assignment)

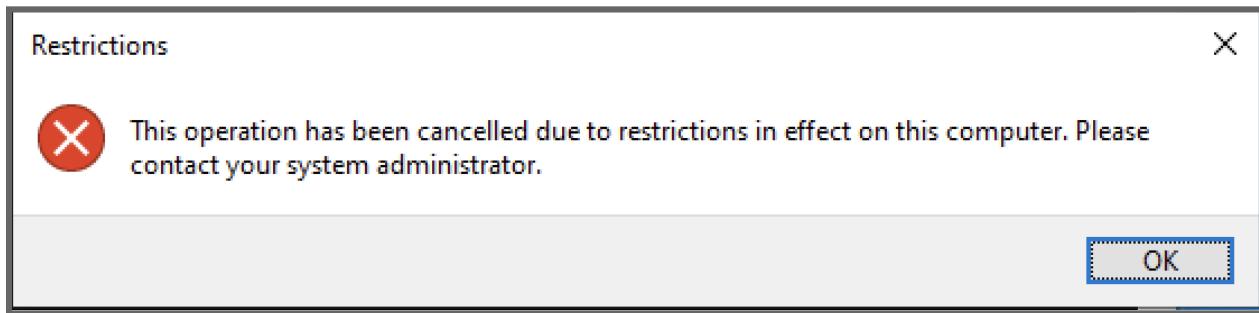
Try using the CMD/Command Prompt. The following message indicates our “**Disable the Command Prompt**” policy if working as expected.

```
Windows PowerShell
Microsoft Windows [Version 10.0.19045.5011]
(c) Microsoft Corporation. All rights reserved.

The command prompt has been disabled by your administrator.

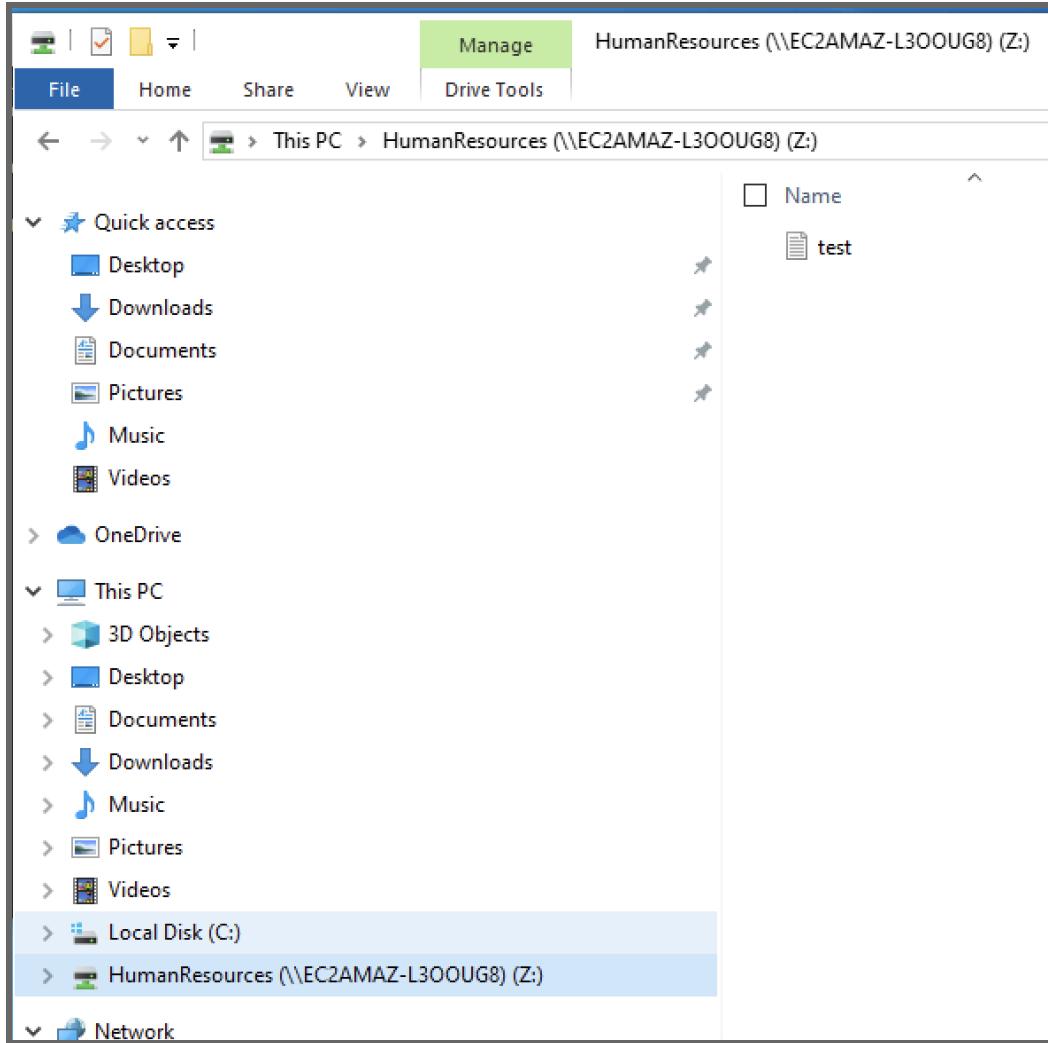
Press any key to continue . . .
```

Try using the Run menu. This message indicates our policy is doing as expected.



IT Onboarding Runbook

Lastly we need to verify the Share. Open up the Explorer to verify the **HumanResources(\EC2AMAZ-L300UG8) Z: Drive** - is available

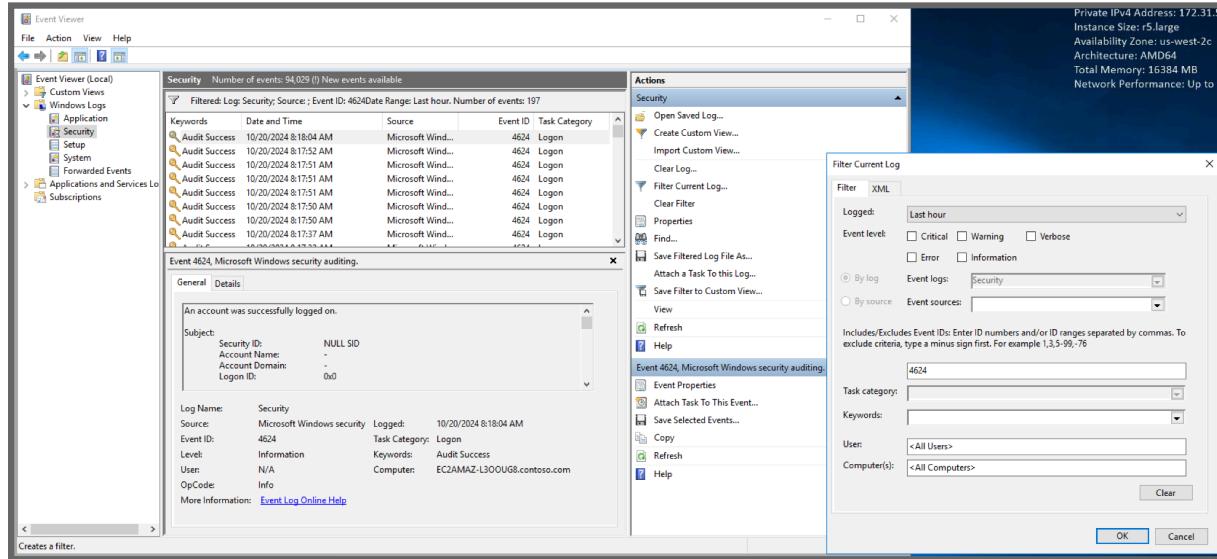


IT Onboarding Runbook

EVENTS VIEWER CHECK

LOGON to
Administrator Pa\$\$wOrd

EVENTS VIEWER



Event “4624”

The left side of the image shows the 'Filter Current Log' dialog box. It has tabs for 'Filter' and 'XML'. Under 'Filter', the 'Logged' dropdown is set to 'Last hour'. The 'Event level' section has checkboxes for 'Critical', 'Warning', 'Verbose', 'Error', and 'Information', with 'Information' checked. The 'By log' section has a dropdown set to 'Security'. The 'By source' section has a dropdown set to 'Event logs'. Below these are fields for 'Task category', 'Keywords', 'User', and 'Computer(s)'. The 'Task category' field contains '4624'. The 'OK' button is at the bottom right of the dialog.

The right side of the image shows the Event Viewer details pane for 'Event 4624, Microsoft Windows security auditing'. It displays the event properties: Log Name: Security; Source: Microsoft Windows security; Event ID: 4624; Task Category: Logon; Level: Information; User: N/A; Computer: EC2AMAZ-L300UG8.contoso.com. The event details state: 'An account was successfully logged on.' with subject information: Security ID: NULL SID, Account Name: -, Account Domain: -, Logon ID: 0x0.

User logged on at 10/20/2024 8:18:04 AM based on Machines time. Which by indications is coming from China. Within that region.

IT Onboarding Runbook

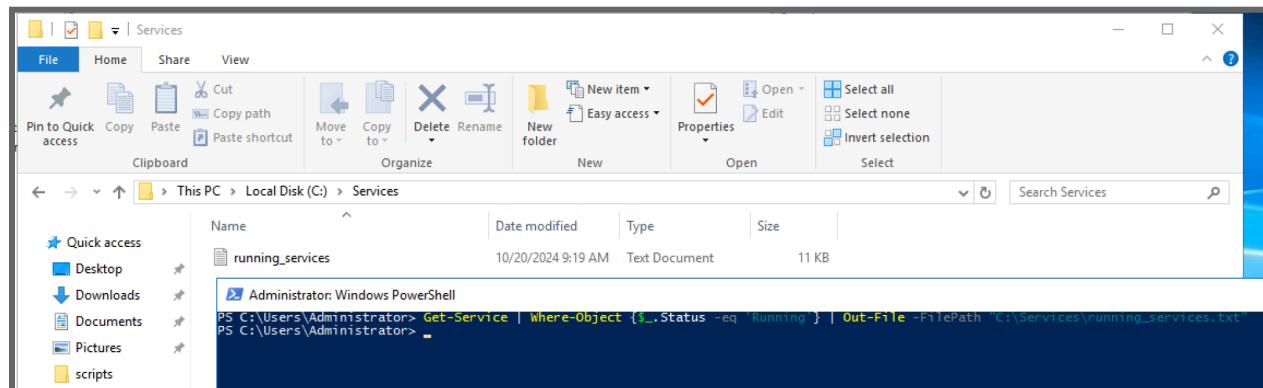
POWERSHELL LATEST PROGRAM

```
PS C:\Users\Administrator> Get-WmiObject -Class Win32_Product | Sort-Object -Property InstallDate -Descending | Select-Object -First 1

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

IdentifyingNumber : {5A6DED90-DBEF-47F5-AAAB-915E6447CA58}

Name : Amazon SSM Agent
Vendor : Amazon Web Services
Version : 3.2.582.0
Caption : Amazon SSM Agent



```
Get-Service | Where-Object {$_.Status -eq 'Running'} | Out-File -FilePath  
"C:\Services\running_services.txt"
```