Career Simulation 2

Jason Buehner

March 24, 2023

IT Pre-onboarding Process

New Employee: Johnny Deputy

Non-technical Role: Sales Associate

Department: Sales

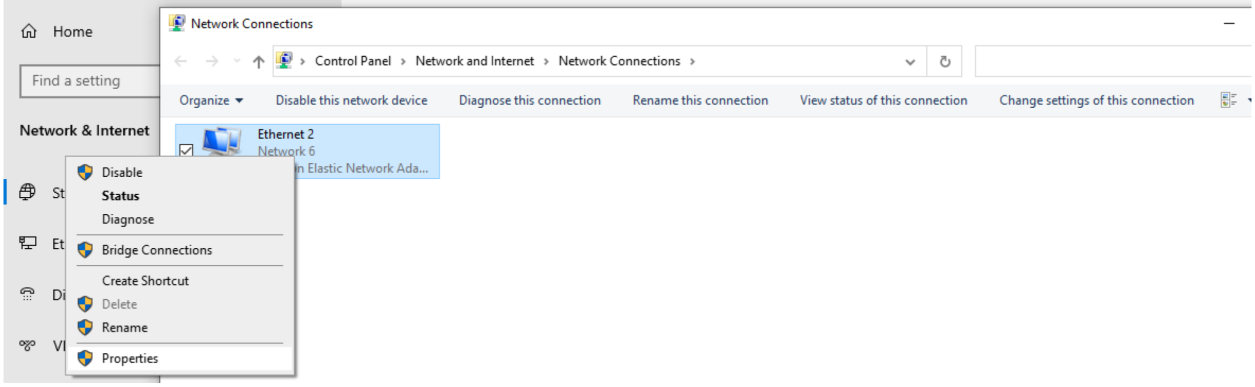
Summary

We've been tasked with creating an onboarding process for our new hires using a runbook. We'll be using Active Directory and PowerShell scripts to automate processes and create an environment to get our new hires ready to be trained as efficiently as possible. This will be a guide to help set everything up and give appropriate privileges to our new users while also ensuring we follow the principle of least privilege. With our knowledge of these systems and programs we'll be sure to create an incredible introduction to our company for our new hires using all these various techniques!

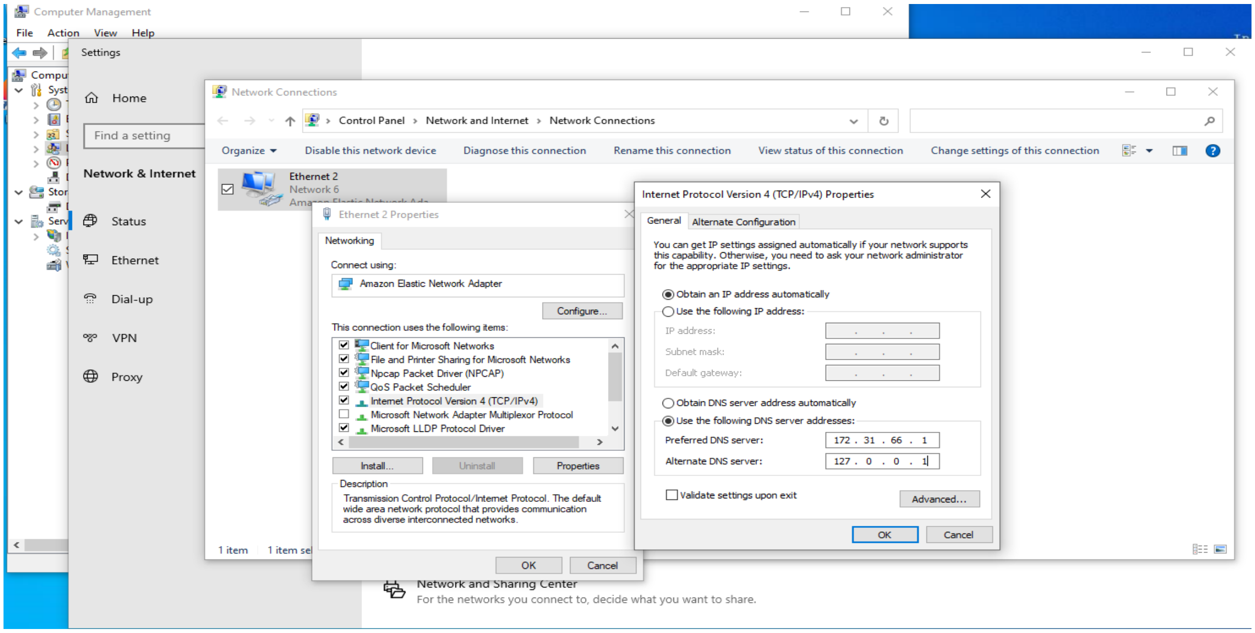
Introduction

We will begin by connecting the client or new user's computer to the domain and then navigate back to the domain controller and use Active Directory and scripting to accomplish all these tasks.

Step 1: To begin we're going to connect the new computer to the domain. To do this, we'll start by heading to the new user's computer. We'll then go to Network Status from the Windows search key. After that, we'll click change adaptor options. This will bring up a window with our Ethernet connection that we will right click, then click properties.



This will bring up the different options for our Ethernet connection, at which point we'll left double click the Internet Protocol Version 4 (TCP/IPv4). This will bring up the General options. Then click to "Use the following DNS server".


Computer Management
File Action View Help
Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy
Network Connections
Control Panel > Network and Internet > Network Connections
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Ethernet 2
Network 6
1 item
Network and Sharing Center
For the networks you connect to, decide what you want to share.

Ethernet 2 Properties

Networking

Connect using:

Amazon Elastic Network Adapter

Configure...

This connection uses the following items:

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

Install... Uninstall Properties

Description

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

OK Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 172 . 31 . 66 . 1

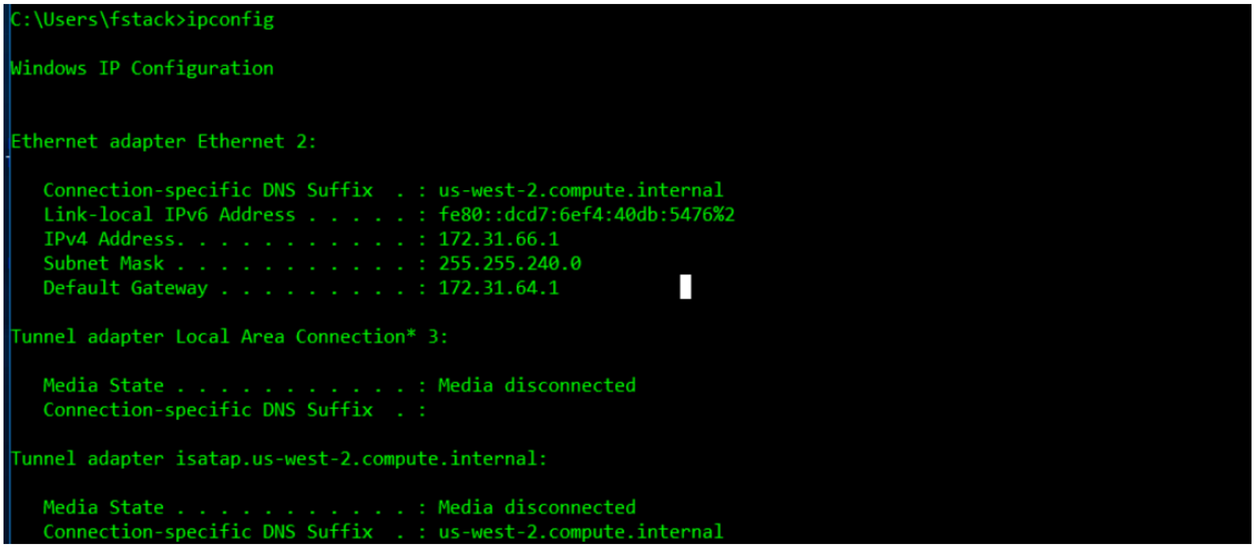
Alternate DNS server: 127 . 0 . 0 . 1

□ Validate settings upon exit

Advanced...

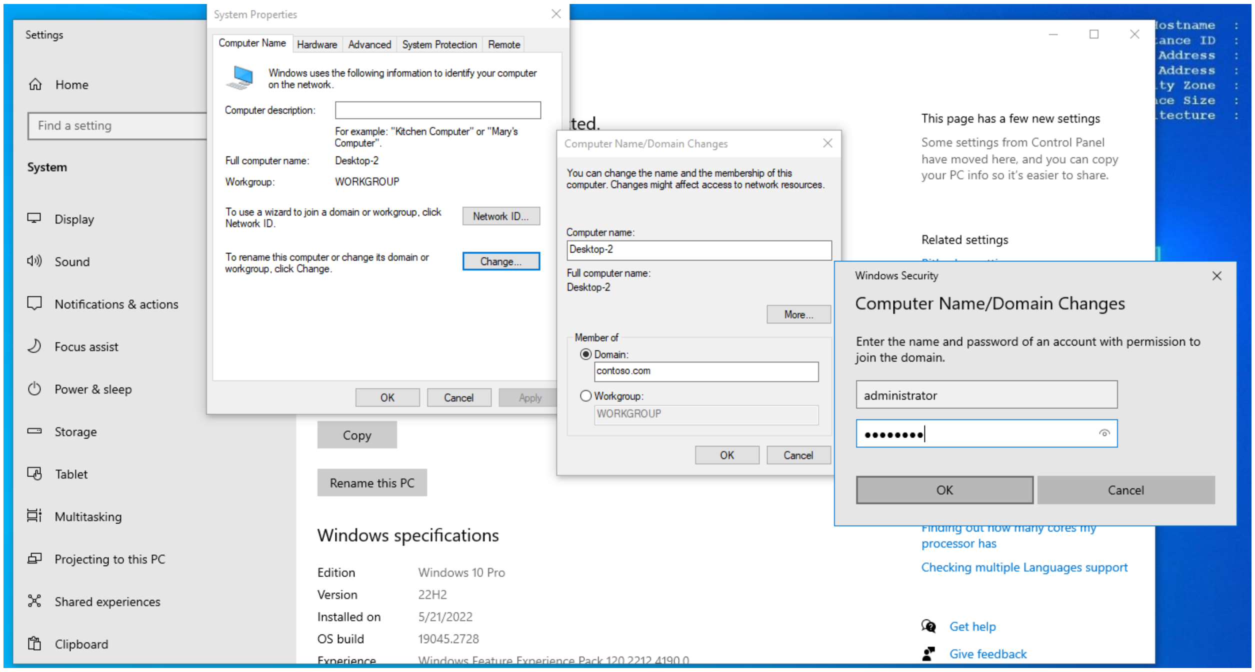
OK Cancel

At this point we'll need to go to the server to pull the IPv4 address from it using the ipconfig command in the command line.



```
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::dcd7:6ef4:40db:5476%2
   IPv4 Address. . . . . . . . . . . : 172.31.66.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.31.64.1

Tunnel adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.us-west-2.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : us-west-2.compute.internal
```

We'll then use that IPv4 address as our DNS server and make it preferred (as of now it is 172.31.66.1, it may change so be sure to check), while also putting the loopback of 127.0.0.1 as the Alternate DNS server. This should connect you to the domain's network. Next we'll set that up by going to Control Panel from the start menu. Click the "System and Security" and then click on "System". In the "System" window, click on "Advanced system settings" on the right hand side. In the "System Properties" window that pops up, click on the "Computer Name" tab and click the "Change" button. In the "Computer Name/Domain Changes" window, select the "Domain" option and enter "contoso.com" as the domain name.



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

Computer Name/Domain Changes

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

administrator

••••••••

This page has a few new settings

Some settings from Control Panel have moved here, and you can copy your PC info so it's easier to share.

Related settings

Windows specifications

Edition Windows 10 Pro

Version 22H2

Installed on 5/21/2022

OS build 19045.2728

Experience Windows Feature Experience Pack 120.2212.4190.0

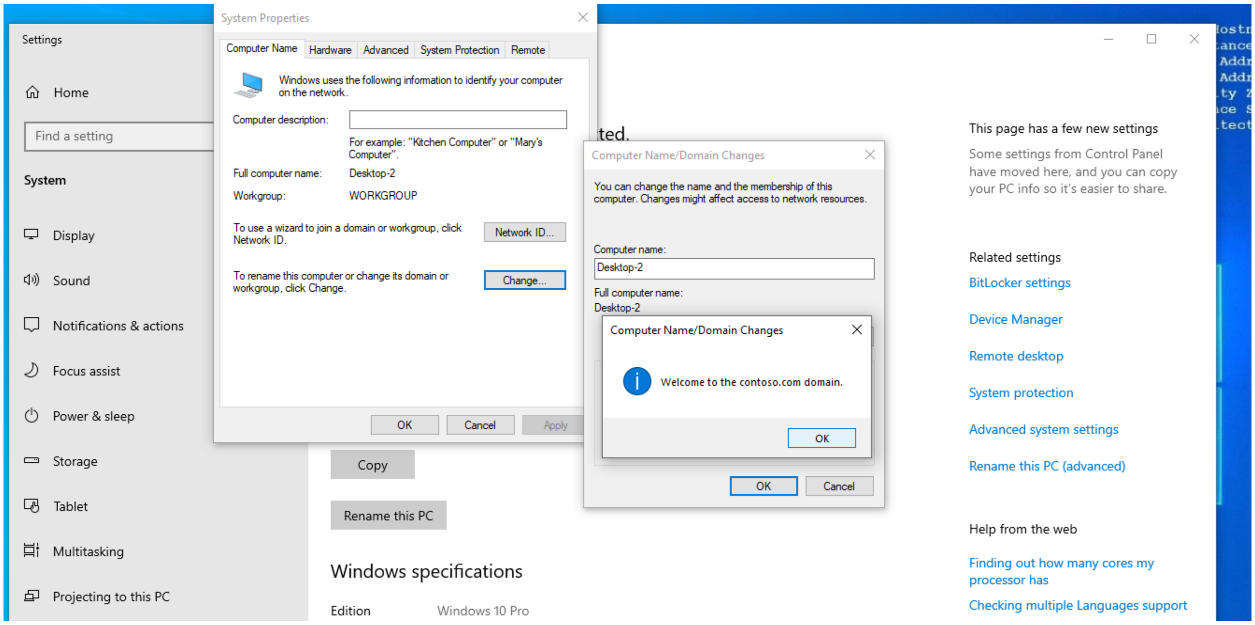
Finding out how many cores my processor has

Checking multiple Languages support

Get help

Give feedback

If all steps have been followed correctly it should give you a prompt, at which time you'll enter the domain username and password to log in. The username is "administrator" and the password is “Pa$$w0rd”. We’ll then have to restart the computer, do so now to apply these changes.



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

Computer Name/Domain Changes

Welcome to the contoso.com domain.

OK

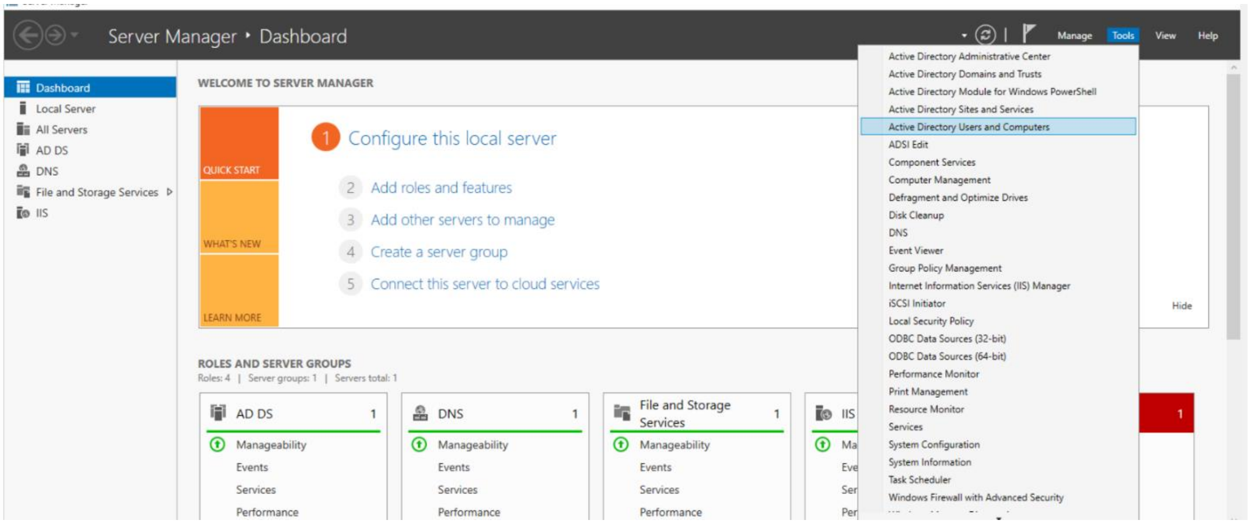
This page has a few new settings

Some settings from Control Panel have moved here, and you can copy your PC info so it's easier to share.

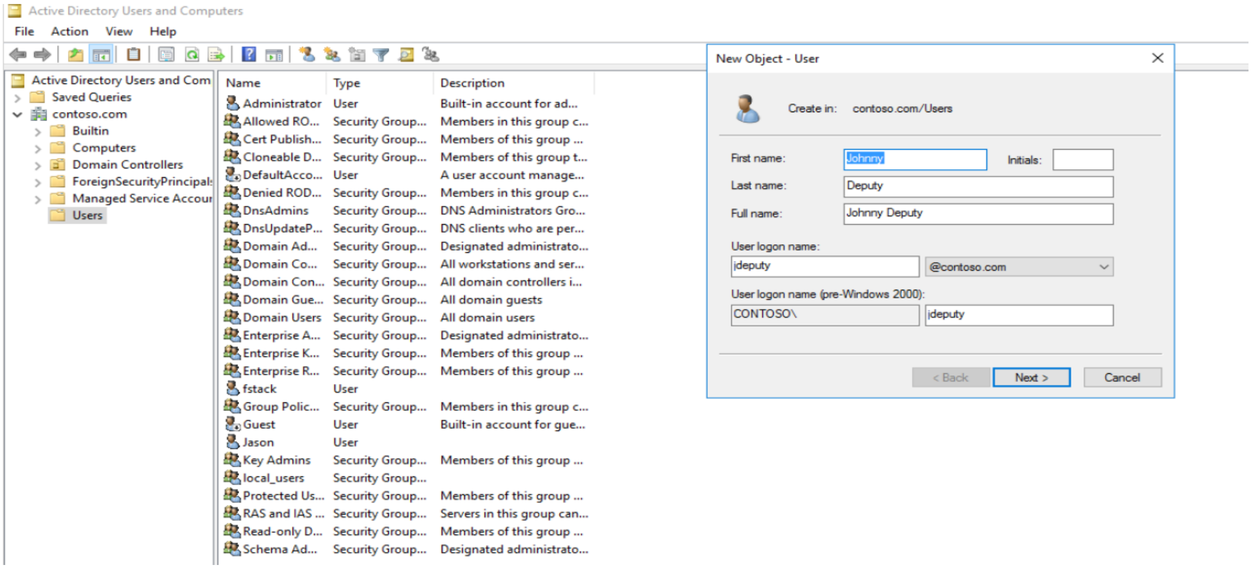
Windows specifications

Edition Windows 10 Pro

Step 2: The next thing we're going to do is switch to the server in order to set up a user account. To do this, open Server Manager in order for us to navigate into Active Directory. Then we'll click under the Tools tab in the top right and select Active Directory Users and Computers.


Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 4 | Server groups: 1 | Servers total: 1
AD DS 1
DNS 1
File and Storage Services 1
IIS
Manageability
Events
Services
Performance
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security

Right click to the right and highlight the new tab, then click User. This will open a New Object User window that we can enter our new credentials for the user with. Enter Johnny's name into the fields and give him a username of "jdeputy". Active directory will then select the rest of the option for setting up credentials, so click next to set up a password for Johnny.



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...
Jason	User	
Key Admins	Security Group...	Members of this group ...
local_users	Security 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...

Create in: contoso.com/Users

First name: Johnny Initials:

Last name: Deputy

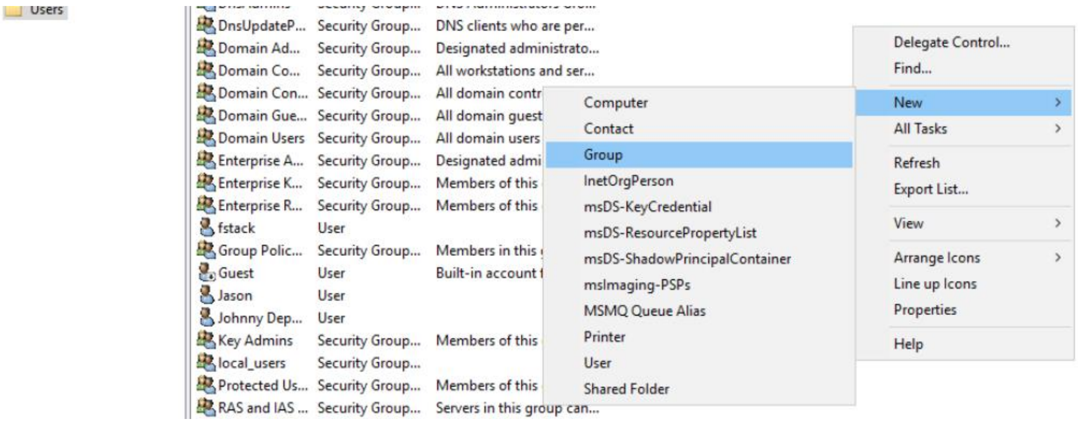
Full name: Johnny Deputy

User logon name: jdeputy @contoso.com

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

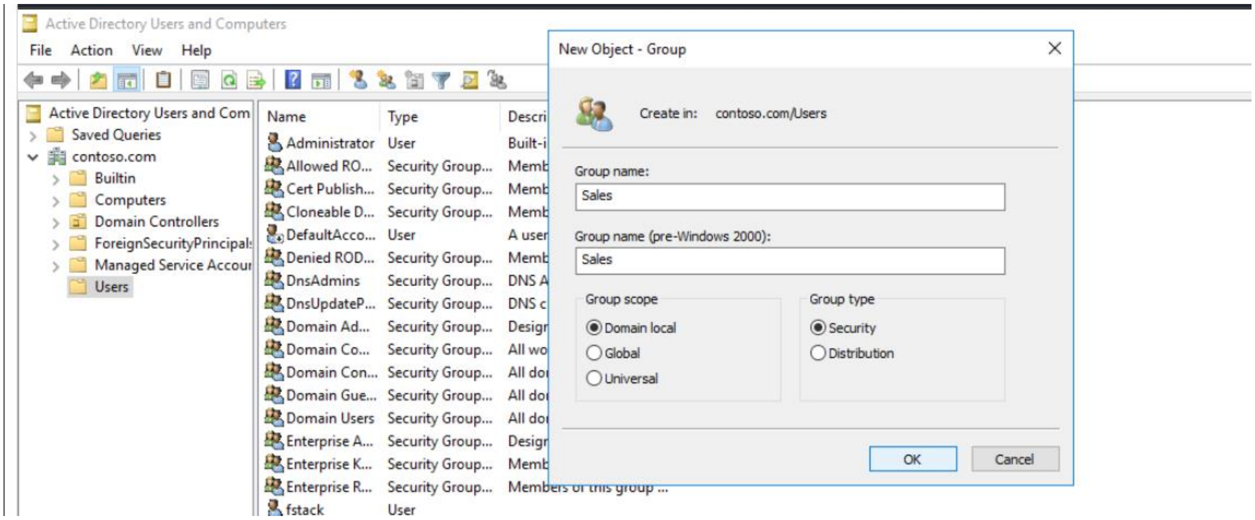
Make the password "academy" and make sure "User must change password at next login" is selected to make sure Johnny sets up a password at his first log in. Click finish on the next window and our new user should be made.

Step 3: Next we'll make a group for the Sales department and put Johnny in it. Since we're already in Active Directory, simply right click again on the left and select new, but this time add a group.



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 contr
Domain Gue...	Security Group...	All domain guest
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated admi
Enterprise K...	Security Group...	Members of this
Enterprise R...	Security Group...	Members of this
fstack	User	
Group Polic...	Security Group...	Members in this
Guest	User	Built-in account f
Jason	User	
Johnny Dep...	User	
Key Admins	Security Group...	Members of this
local_users	Security Group...	
Protected Us...	Security Group...	Members of this
RAS and IAS ...	Security Group...	Servers in this group can...

Make sure to set Sales as the group name, and click ok.



Name	Type	Descri
Administrator	User	Built-i
Allowed RO...	Security Group...	Memb
Cert Publish...	Security Group...	Memb
Cloneable D...	Security Group...	Memb
DefaultAcco...	User	A user
Denied ROD...	Security Group...	Memb
DnsAdmins	Security Group...	DNS A
DnsUpdateP...	Security Group...	DNS c
Domain Ad...	Security Group...	Desigr
Domain Co...	Security Group...	All wo
Domain Con...	Security Group...	All do
Domain Gue...	Security Group...	All do
Domain Users	Security Group...	All do
Enterprise A...	Security Group...	Desigr
Enterprise K...	Security Group...	Memb
Enterprise R...	Security Group...	Members of this group ...
fstack	User	

New Object - Group

Create in: contoso.com/Users

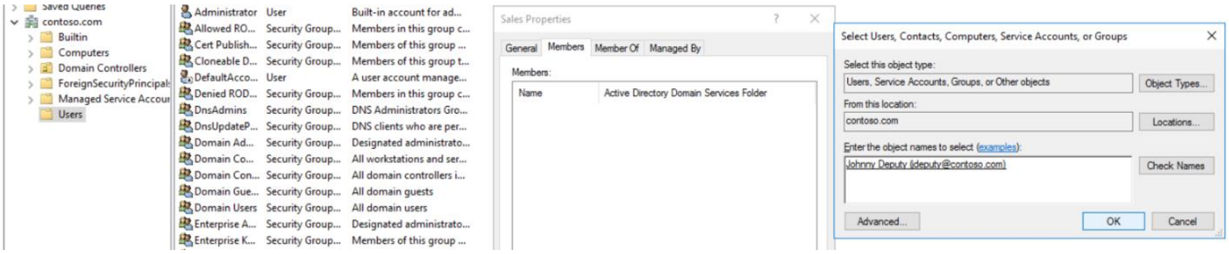
Group name:
Sales

Group name (pre-Windows 2000):
Sales

Group scope
● Domain local
○ Global
○ Universal

Group type
● Security
○ Distribution

This will create our new group, then double click the group to open that, navigate to Members and click add, then type 'jdeputy' in object names and click check names to the right. This will automatically load Johnny's specifics, click ok to add Johnny. Then click apply and ok to get back to the main screen.



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 ...

Sales Properties

Members:

Name	Active Directory Domain Services Folder

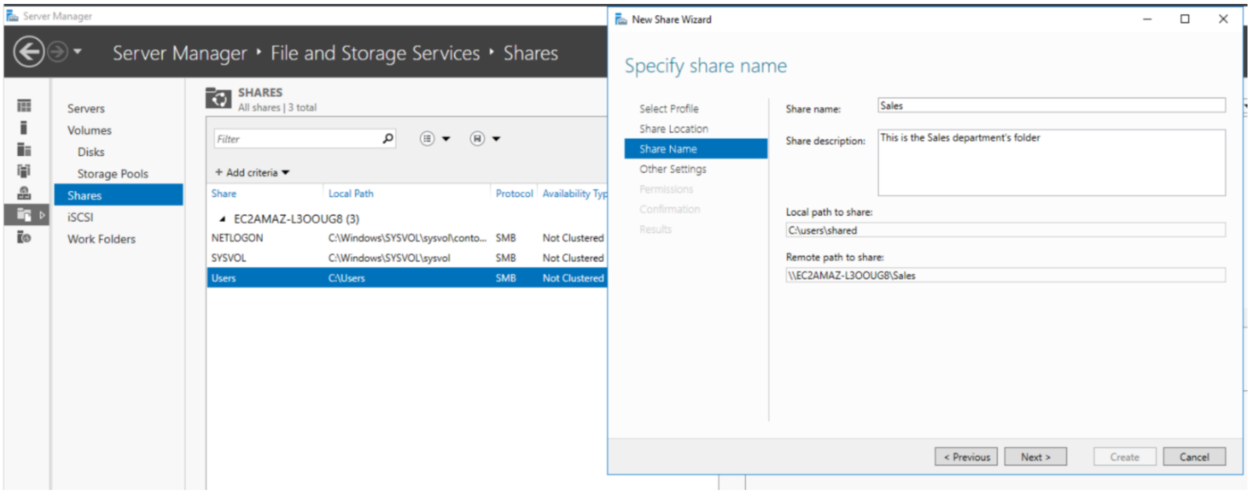
Select Users, Contacts, Computers, Service Accounts, or Groups

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

From this location:
contoso.com

Enter the object names to select (examples):
Johnny Deputy (jdeputy@contoso.com)

Step 4: Next, we're going to create a shared folder on the server with the department's name (sales) and give it read and write permissions. In that folder we'll create a shared text document called test.txt. To begin, go back to Server Manager's primary screen and look to the left. Click Files and Storage Services. Click the Shares tab to the left, and in the Shares window that opens right click and select "New Share…". This will create a shared folder we'll call Sales for the department. First select SMB Share – Quick, Select by volume is selected on the next screen leave it as is, we'll give it the path of "C:\Shares\Sales" in order to keep it organized within the rest of the network (The Wizard that opened will do this automatically if you call the folder Sales in this step), click Enable access based Enumeration on this next tab to make sure only those who have access intentionally can see it, click customize permissions on the next tab and add the Sales group to it, finally click create on the last page.



Share	Local Path	Protocol	Availability Typ
EC2AMAZ-L3OOUG8 (3)			
NETLOGON	C:\Windows\SYSVOL\sysvol\conto...	SMB	Not Clustered
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered
Users	C:\Users	SMB	Not Clustered

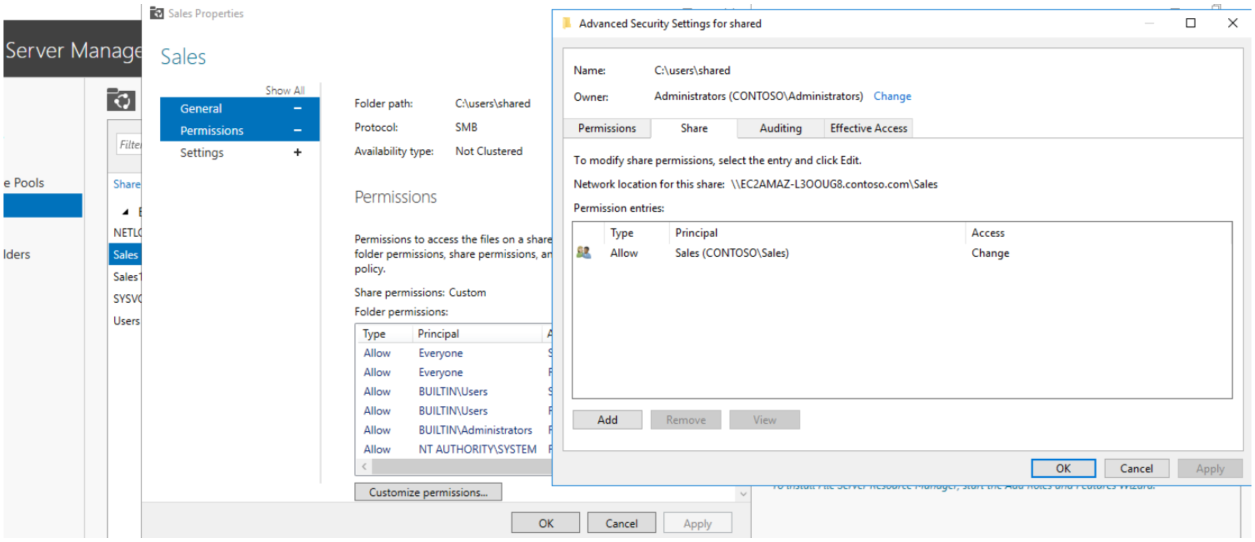
Share name: Sales

Share description: This is the Sales department's folder

Local path to share:
C:\users\shared

Remote path to share:
\\EC2AMAZ-L3OOUG8\Sales

Next, right click our new shared folder so we check Sales is a shared group. We'll select properties from the bottom of the drop down menu then click the permissions tab that comes up in the properties window. Next, scroll to the bottom and click customize permissions then on the window that pops up for Advanced Security Settings click the Share tab. In this tab we can check that our group called Sales is in the shared group for the folder.



Folder path: C:\users\shared
Protocol: SMB
Availability type: Not Clustered

Permissions to access the files on a share folder permissions, share permissions, ar policy.

Share permissions: Custom
Folder permissions:

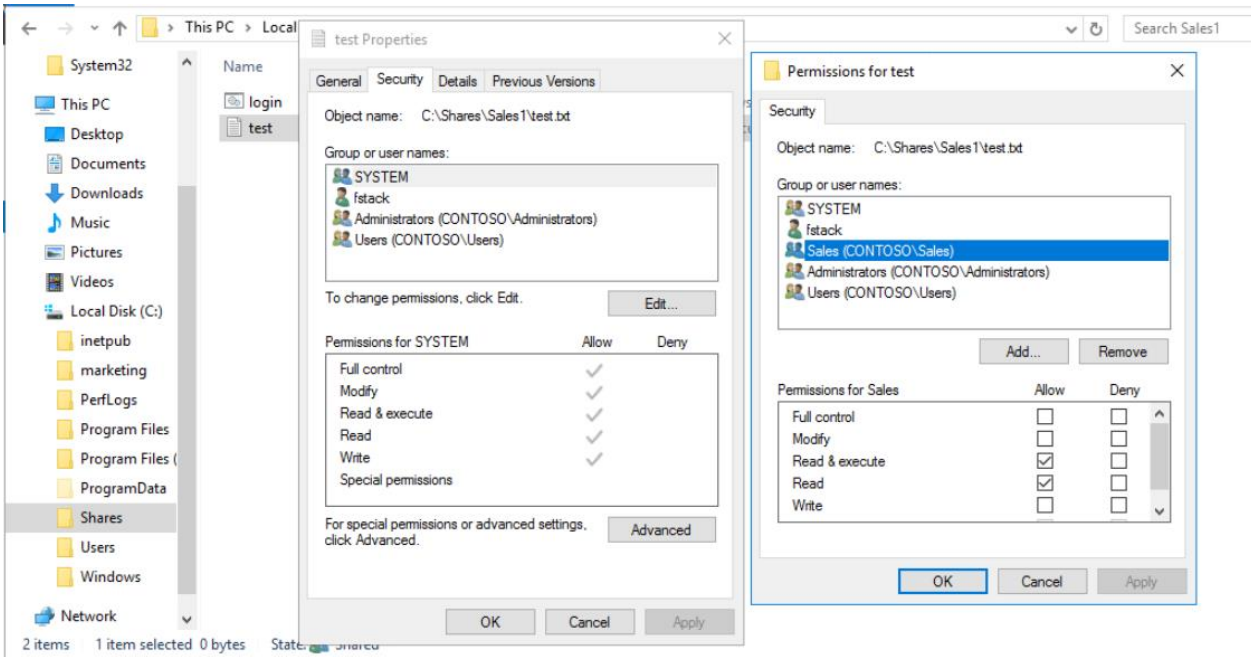
Type	Principal
Allow	Everyone
Allow	Everyone
Allow	BUILTIN\Users
Allow	BUILTIN\Users
Allow	BUILTIN\Administrators
Allow	NT AUTHORITY\SYSTEM

Name: C:\users\shared
Owner: Administrators (CONTOSO\Administrators) Change

To modify share permissions, select the entry and click Edit.
Network location for this share: \\EC2AMAZ-L3OOUG8.contoso.com\Sales
Permission entries:

Type	Principal	Access
Allow	Sales (CONTOSO\Sales)	Change

Finally we can go to add the shared text document called test.txt to this folder. To do so, open Notepad and simply click Save under the drop down in the top left so that we can save and create a blank text file in our shared folder. Be sure to give it correct pathing as C:\users\shared\Sales. Now that we have a file in the folder, right click the file, select Security, the click Edit. In the new window that pops up labeled as “Permissions for test”, click to Add a group or user and enter Sales as the object name then click Check Names. This should select our sales group and add it as a group who has permissions for this text file. Click ok and you should see the Sales group added.



Object name: C:\Shares\Sales1\test.txt

Group or user names:
SYSTEM
fstack
Administrators (CONTOSO\Administrators)
Users (CONTOSO\Users)

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

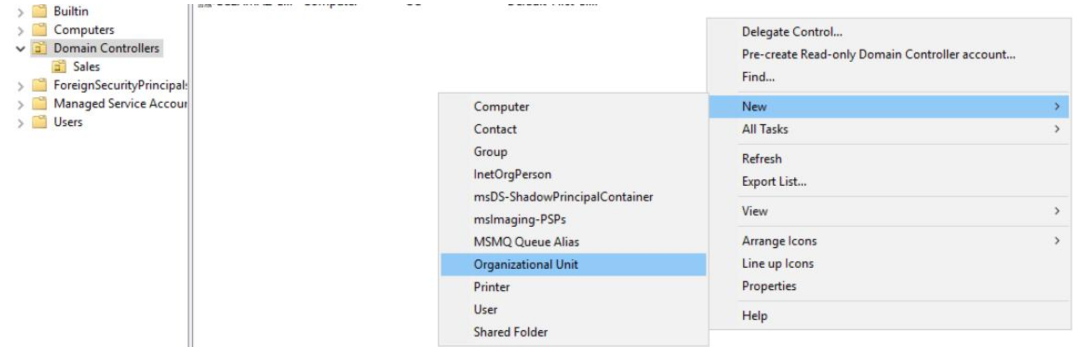
For special permissions or advanced settings, click Advanced.

Object name: C:\Shares\Sales1\test.txt

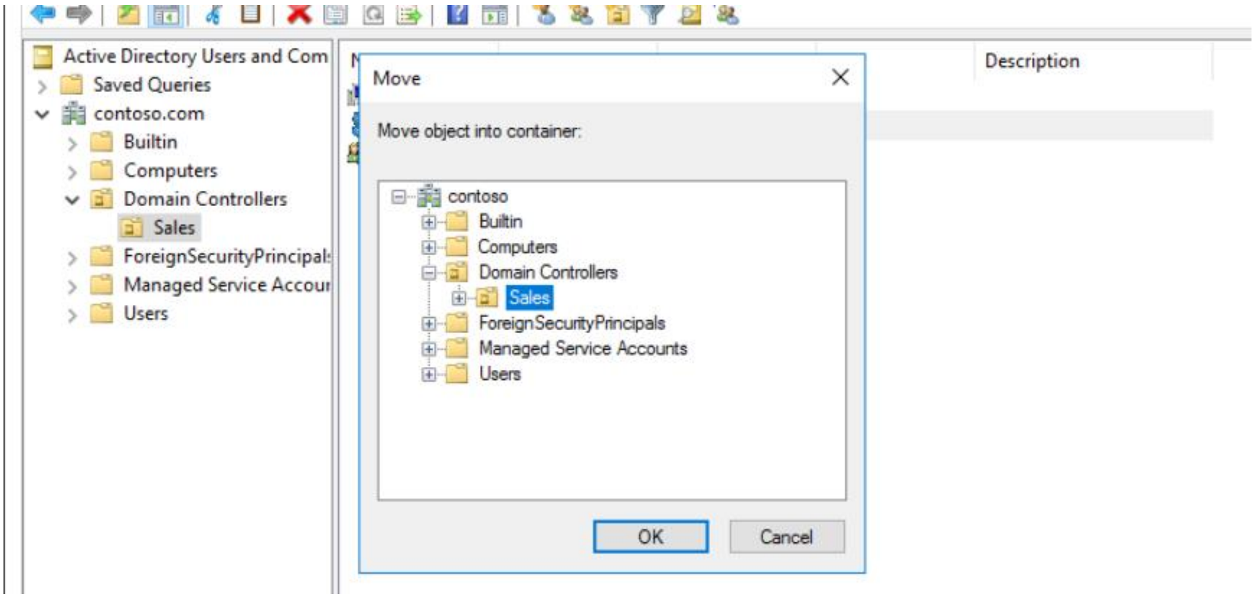
Group or user names:
SYSTEM
fstack
Sales (CONTOSO\Sales)
Administrators (CONTOSO\Administrators)
Users (CONTOSO\Users)

Permissions for Sales	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	☑	□
Read	☑	□
Write	□	□

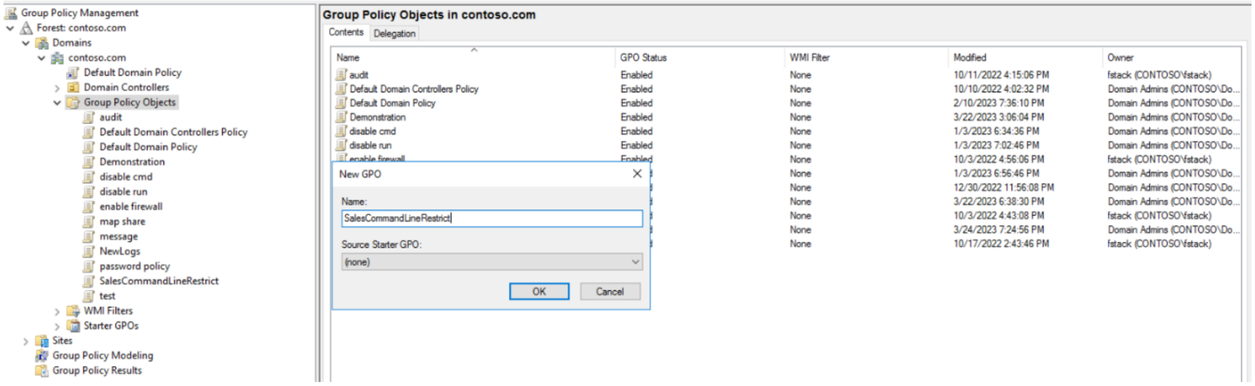
Step 5: Next we’re going to create and Organizational Unit with the name of Sales and place the new user jdeputy, the Sales group, and the computer into the OU. Finally we’ll attach a GPO to said OU limiting certain permissions. To begin navigate back to Server Manager and click the Tools on the top right, then navigate back to Users and Computers again. Make sure to select the Domain Controller on the left since we’ll be making an OU. Within the window to the right click and select New then Organizational Unit. Call the OU Sales after the department.



Now we’re going to add the User, Group, and Computer to this new OU. Navigate to where they are within your Active Directory which should be under the Users folder to the left and right click the user Johnny Deputy then click move. Under contoso.com then Domain Controllers, select the new Sales OU we created to move Johnny there. Follow these steps for the group “Sales” and also the computer being added. Remember the computer being added will be in the Computers folder to the left so be sure to look there for it.



Next we’ll create a GPO to attach to the new OU so that we can set it up. Navigate back to the main screen for Windows Server and select Tools again but this time navigate to the Group Policy Management category. This should take you straight to the Group Policy Object folder to the left at which time you’ll right click below the lowest GPO and select New. We’ll name our new GPO “SalesCommandLineRestrict” since we’ll be restricting command line for them.



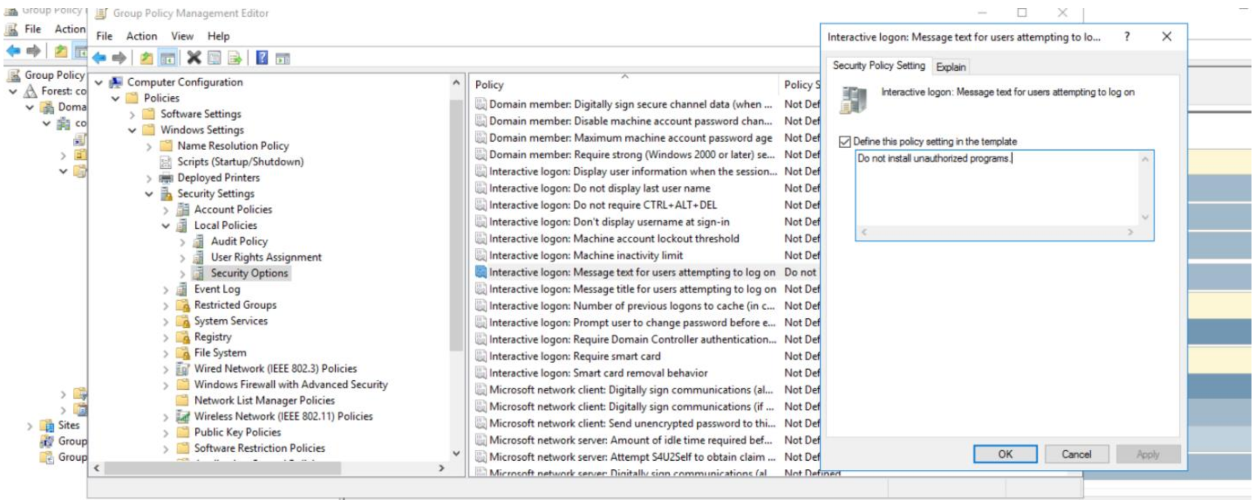
Group Policy Objects in contoso.com

Name	GPO Status	WMI Filter	Modified	Owner
audit	Enabled	None	10/11/2022 4:15:06 PM	fstack (CONTOSO\fstack)
Default Domain Controllers Policy	Enabled	None	10/10/2022 4:02:32 PM	Domain Admins (CONTOSO\Do...
Default Domain Policy	Enabled	None	2/10/2023 7:36:10 PM	Domain Admins (CONTOSO\Do...
Demonstration	Enabled	None	3/22/2023 3:06:04 PM	Domain Admins (CONTOSO\Do...
disable cmd	Enabled	None	1/3/2023 6:34:36 PM	Domain Admins (CONTOSO\Do...
disable run	Enabled	None	1/3/2023 7:02:46 PM	Domain Admins (CONTOSO\Do...
enable firewall	Enabled	None	10/3/2022 4:56:06 PM	fstack (CONTOSO\fstack)
		None	1/3/2023 6:56:46 PM	Domain Admins (CONTOSO\Do...
		None	12/30/2022 11:56:08 PM	Domain Admins (CONTOSO\Do...
		None	3/22/2023 6:38:30 PM	Domain Admins (CONTOSO\Do...
		None	10/3/2022 4:43:08 PM	fstack (CONTOSO\fstack)
		None	3/24/2023 7:24:56 PM	Domain Admins (CONTOSO\Do...
		None	10/17/2022 2:43:46 PM	fstack (CONTOSO\fstack)

Name: SalesCommandLineRestrict

Source Starter GPO: (none)

Step 6: Next we'll edit our GPO to set up restrictions. We will be making a message appear on login to warn of install unauthorized programs, preventing CMD line access, adding a script to map our shared folder, and disabling the run command from the start menu. To begin we will Right-click on the new GPO and select "Edit" to open the Group Policy Editor. Navigate to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options. Locate the "Interactive logon: Message text for users attempting to log on" setting and double-click on it. Enter the message text you want to display every time the computer starts (e.g. "Do not install unauthorized programs") in the text box. Click "OK" to save the message text. Close the Group Policy Editor and link the GPO to the appropriate OU by right-clicking on the OU and selecting "Link an existing GPO." Select the GPO you just created and click "OK."



Policy	Policy S
Domain member: Digitally sign secure channel data (when ...	Not Def
Domain member: Disable machine account password chan...	Not Def
Domain member: Maximum machine account password age	Not Def
Domain member: Require strong (Windows 2000 or later) se...	Not Def
Interactive logon: Display user information when the session...	Not Def
Interactive logon: Do not display last user name	Not Def
Interactive logon: Do not require CTRL+ALT+DEL	Not Def
Interactive logon: Don't display username at sign-in	Not Def
Interactive logon: Machine account lockout threshold	Not Def
Interactive logon: Machine inactivity limit	Not Def
Interactive logon: Message text for users attempting to log on	Do not
Interactive logon: Message title for users attempting to log on	Not Def
Interactive logon: Number of previous logons to cache (in c...	Not Def
Interactive logon: Prompt user to change password before e...	Not Def
Interactive logon: Require Domain Controller authentication...	Not Def
Interactive logon: Require smart card	Not Def
Interactive logon: Smart card removal behavior	Not Def
Microsoft network client: Digitally sign communications (al...	Not Def
Microsoft network client: Digitally sign communications (if ...	Not Def
Microsoft network client: Send unencrypted password to thi...	Not Def
Microsoft network server: Amount of idle time required bef...	Not Def
Microsoft network server: Attempt S4U2Self to obtain claim ...	Not Def
Microsoft network server: Digitally sign communications (al...	Not Defined

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

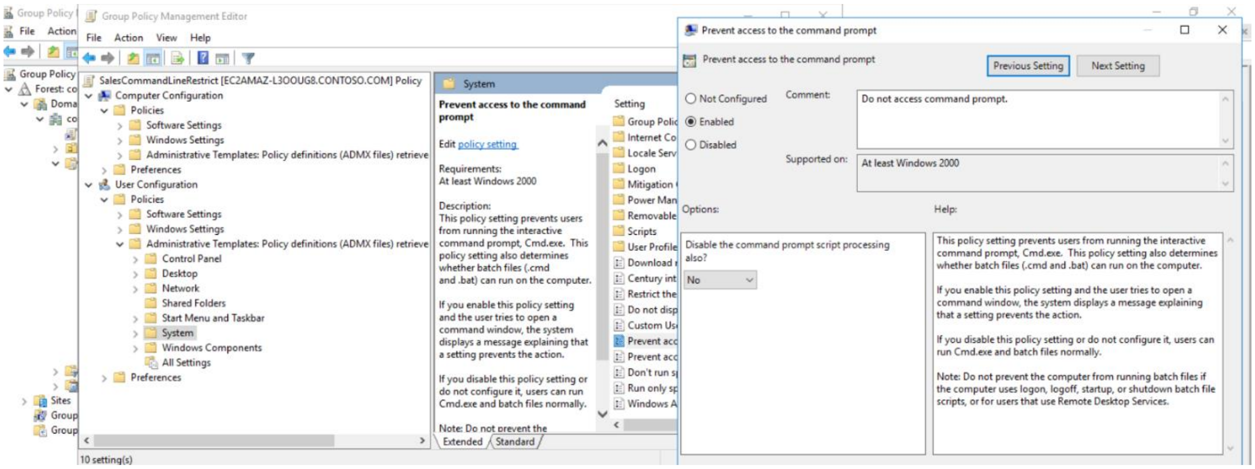
Security Policy Setting | Explain

Interactive logon: Message text for users attempting to log on

☑ Define this policy setting in the template

Do not install unauthorized programs.

Next we'll prevent the users access to command line. Navigate to User Configuration > Policies > Administrative Templates > System. Locate the "Prevent access to the command prompt" setting and double-click on it. Select the "Enabled" option to turn on the policy. Click "OK" to save the policy. Close the Group Policy Editor and link the GPO to the appropriate OU by right-clicking on the OU and selecting "Link an existing GPO." Select the GPO you just created and click "OK."



Prevent access to the command prompt

○ Not Configured
● Enabled
○ Disabled

Comment: Do not access command prompt.

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.

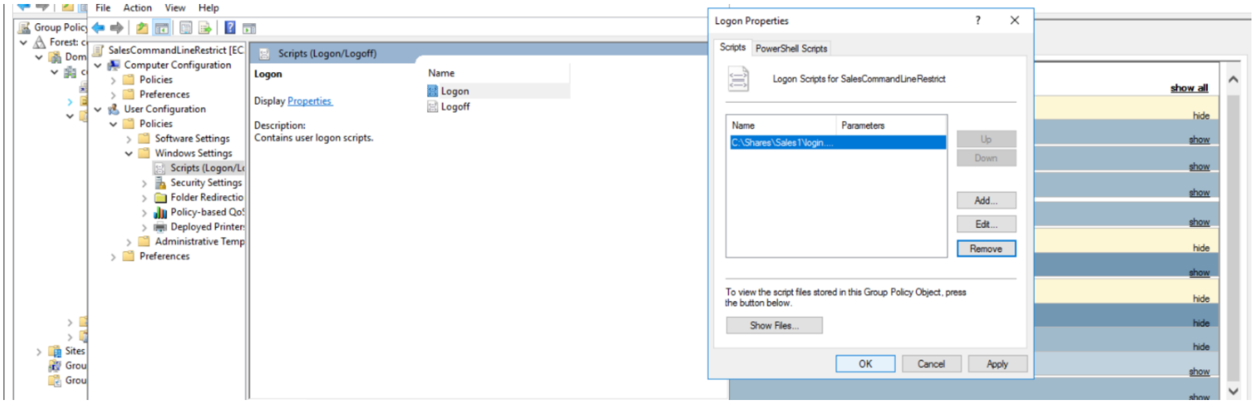
If you disable this policy setting or do not configure it, users can run Cmd.exe and batch files normally.

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.

Next we’ll make a script and tie it to the GPO. In the script we’ll use the command:

```
@echo off

net use X: \contoso.com\Shares\Sales /persistent:yes
```

Put this into a Notepad document and save it as login.bat in the shared folder \Shares\Sales. Next we’ll tie this script to our GPO. Navigate to User Configuration > Policies > Windows Settings > Scripts (Logon/Logoff). Double-click on "Logon" to open the "Logon Properties" dialog box. Click "Add" to add a new login script. In the "Script Name" field, enter the UNC path of the login script that you want to use (e.g. \Shares\Sales\login.bat). Click "OK" to save the script. In the "Logon Properties" dialog box, click "OK" to save the login script settings.



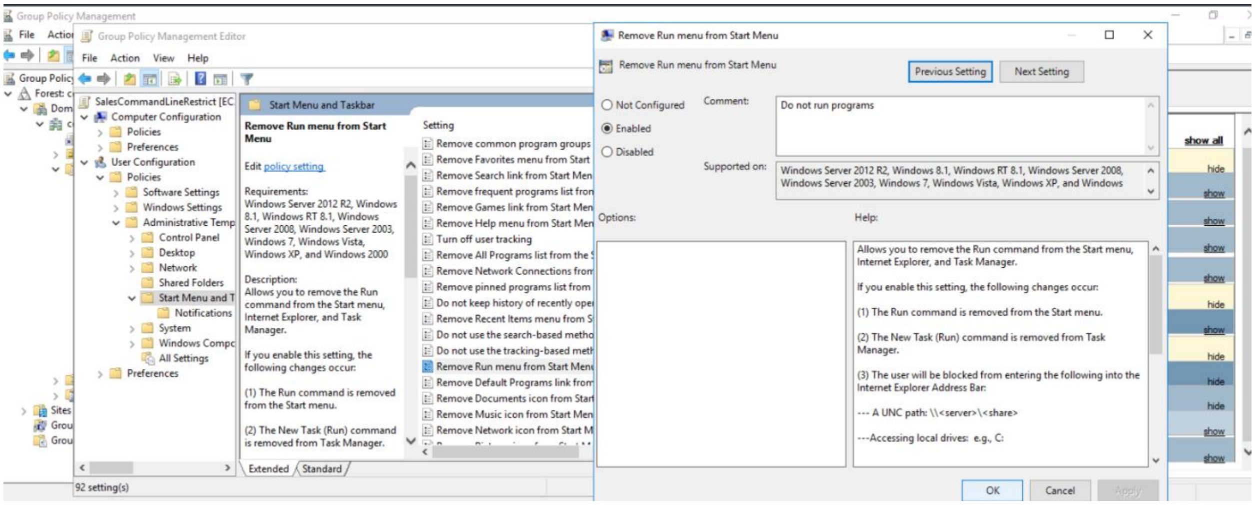
Description:
Contains user logon scripts.

Logon Scripts for SalesCommandLineRestrict

Name	Parameters
C:\Shares\Sales1\login....	

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

Next we’ll remove the run command from the start menu. Navigate to User Configuration > Administrative Templates > Start Menu and Taskbar. Locate the "Remove Run menu from Start Menu" setting and double-click on it. Select the "Enabled" option to turn on the policy. Click "OK" to save the policy. Close the Group Policy Editor and link the GPO to the appropriate OU by right-clicking on the OU and selecting "Link an existing GPO." Select the GPO you just created and click "OK."


Group Policy Management
File Action
Group Policy Management Editor
File Action View Help
SalesCommandLineRestrict [EC
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Temp
Control Panel
Desktop
Network
Shared Folders
Start Menu and T
Notifications
System
Windows Compc
All Settings
Preferences
Sites
Start Menu and Taskbar
Setting
Remove common program groups
Remove Favorites menu from Start
Remove Search link from Start Men
Remove frequent programs list fron
Remove Games link from Start Men
Remove Help menu from Start Men
Turn off user tracking
Remove All Programs list from the S
Remove Network Connections from
Remove pinned programs list from
Do not keep history of recently ope
Remove Recent Items menu from S
Do not use the search-based metho
Do not use the tracking-based meth
Remove Run menu from Start Menu
Remove Default Programs link from
Remove Documents icon from Start
Remove Music icon from Start Men
Remove Network icon from Start M
Extended
Standard
92 setting(s)
show all
hide
show
Previous Setting
Next Setting
OK
Cancel
Apply

Remove Run menu from Start Menu

Edit policy setting

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

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

If you enable this setting, the following changes occur:

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

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

Remove Run menu from Start Menu

○ Not Configured
● Enabled
○ Disabled

Comment: Do not run programs

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

Options:

Help:

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

If you enable this setting, the following changes occur:

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

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

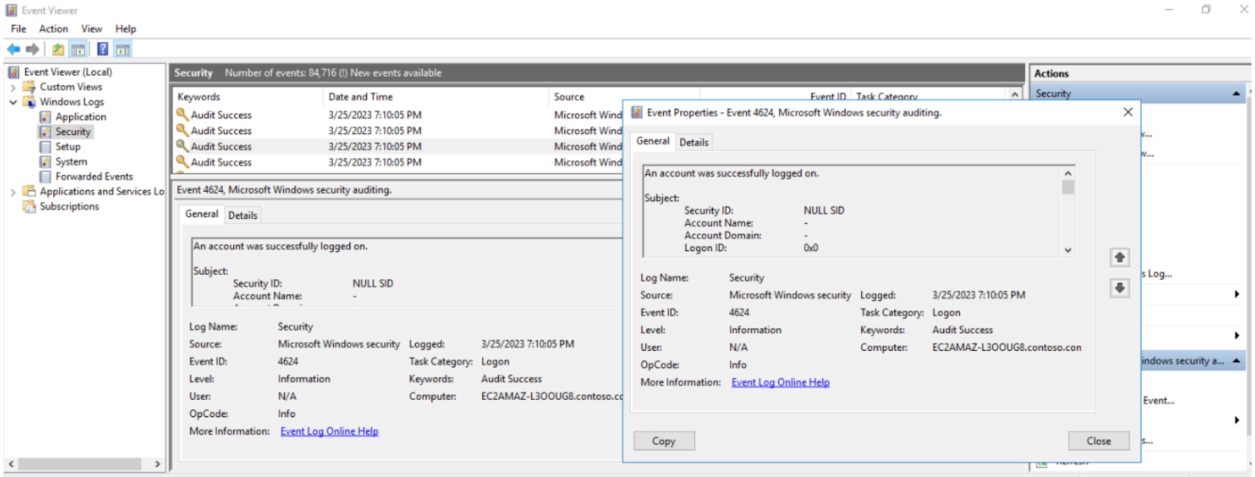
(3) The user will be blocked from entering the following into the Internet Explorer Address Bar:

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

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

Close the Group Policy Editor and link the GPO to the appropriate OU by right-clicking on the OU called “Sales” and selecting "Link an existing GPO." Select the GPO you just created called “SalesCommandLineRestrict” and click "OK." This will link the GPO to the OU.

Step 7: Next we'll check the Event Viewer and see the last successful login from a user. Make sure you're logged in to the server machine with administrative privileges. Open the Event Viewer by clicking on the Start menu, typing "event viewer," and selecting the "Event Viewer" app. In the Event Viewer, click on "Windows Logs" in the left-hand pane. Click on "Security" in the left-hand pane. In the middle pane, you will see a list of security events. Look for event ID 4624, which is the Windows event ID for a successful login. You can use the "Find" feature in the "Actions" pane on the right-hand side to search for event ID 4624. Alternatively, you can simply scroll through the list of events until you find the one you are looking for. Double-click on the event to open the event details. In the event details, look for the "Account Name" field to see the username of the user who logged in successfully. You can also find additional information about the successful login, such as the date and time of the event, the computer name, and the logon type. To write down the last successful login from your user, simply note the date and time of the event and the username of the user who logged in successfully.



Security Number of events: 84,716 (!) New events available

Keywords	Date and Time	Source
Audit Success	3/25/2023 7:10:05 PM	Microsoft Wind
Audit Success	3/25/2023 7:10:05 PM	Microsoft Wind
Audit Success	3/25/2023 7:10:05 PM	Microsoft Wind
Audit Success	3/25/2023 7:10:05 PM	Microsoft Wind

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:
Security ID: NULL SID
Account Name: -

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	3/25/2023 7:10:05 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	EC2AMAZ-L3OOUG8.contoso.cc
OpCode:	Info		
More Information:	Event Log Online Help		

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

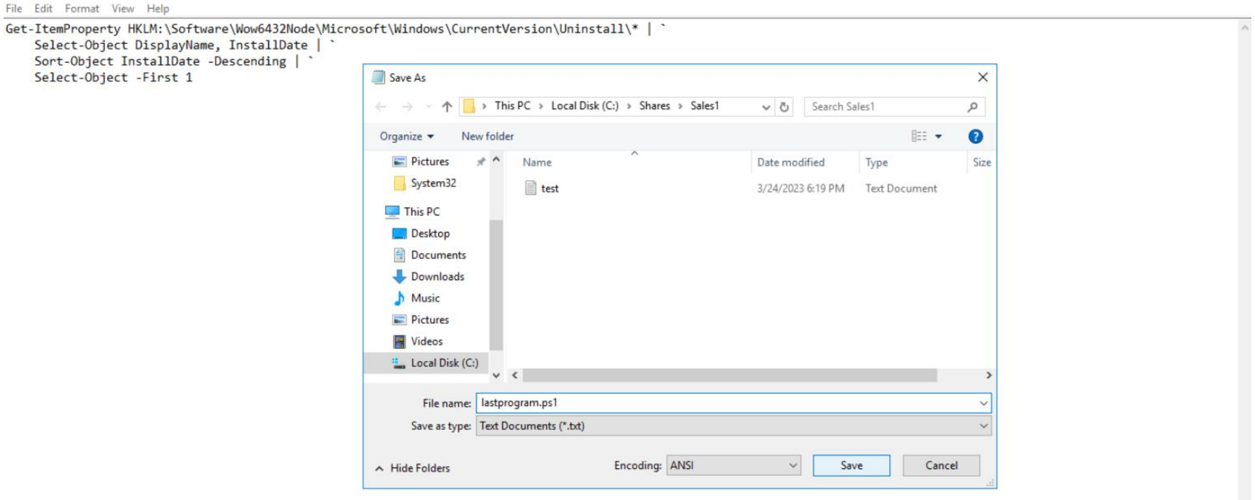
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	3/25/2023 7:10:05 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	EC2AMAZ-L3OOUG8.contoso.con
OpCode:	Info		
More Information:	Event Log Online Help		

Step 8: Next we'll create a PowerShell script to see what the last program installed on the machine was. We'll use this command:

```
Get-ItemProperty
HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* | `
  Select-Object DisplayName, InstallDate | `
  Sort-Object InstallDate -Descending | `
  Select-Object -First 1
```

Take this command and save it to a file called lastprogram.ps1 in the shared folder we created.



```
Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* | `
    Select-Object DisplayName, InstallDate | `
    Sort-Object InstallDate -Descending | `
    Select-Object -First 1
```

This PC › Local Disk (C:) › Shares › Sales1

Name	Date modified	Type	Size
test	3/24/2023 6:19 PM	Text Document	

File name: lastprogram.ps1

Save as type: Text Documents (*.txt)

Encoding: ANSI

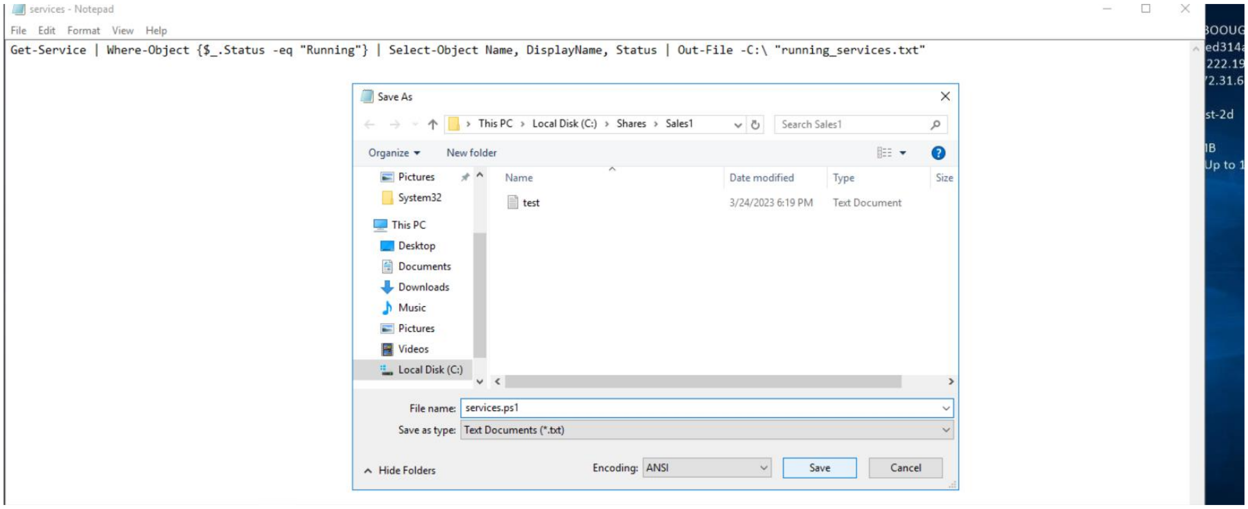
This script will look in the registry under the Uninstall key for all installed programs, and then select the DisplayName and InstallDate properties for each program. It will then sort the list by InstallDate in descending order, so that the most recently installed program is at the top, and select the first item in the list.

To run the script, open PowerShell and copy and paste the script into the PowerShell window. Press Enter to run the script and it will output the name and installation date of the most recently installed program on the computer. Making this command a script will enable ease of access later for anyone who needs to run it.

Step 9: For our last step, we’ll create a PowerShell script that lists all running services and puts the output into a file called “running_services.txt”. We’ll do this using the following command:

```
Get-Service | Where-Object {$_.Status -eq "Running"} | Select-Object Name, DisplayName, Status | Out-File -FilePath "running_services.txt"
```

Save this command to a notepad document and call it “services.ps1” since it’s a PowerShell script. We’ll be saving this to the shared folder we created earlier. Our script can now be used by the group so see running services if needed.



```
Get-Service | Where-Object {$_.Status -eq "Running"} | Select-Object Name, DisplayName, Status | Out-File -C:\ "running_services.txt"
```

Save As

This PC › Local Disk (C:) › Shares › Sales1

Name	Date modified	Type	Size
test	3/24/2023 6:19 PM	Text Document	

File name: services.ps1

Save as type: Text Documents (*.txt)

Encoding: ANSI

Conclusion

All of these steps will help to set up users and groups with appropriate restrictions so that we can have an effective and efficiently trained team following all best practices with security so that we minimize risks. Using these methods we can establish a good foundation to set ourselves up for success. All of these steps will set up our accounts as well as giving everyone some tools needed to achieve our goals. Please see the IT Security Manager if you have a persisting user (Which is Damen) otherwise this guide should walk you through everything you need. Good luck!