New Zealand Diploma in System Administration Level 6

NET602: Network Services

Assessment/Aromatawai - Assessment 2 v2

Practical

Credits/Whiwhinga 7

	Submission	FER1	FER2
Result	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Date	Click or tap to enter a date.	Click or tap to enter a date.	Click or tap to enter a date.
Assessor's Signature			

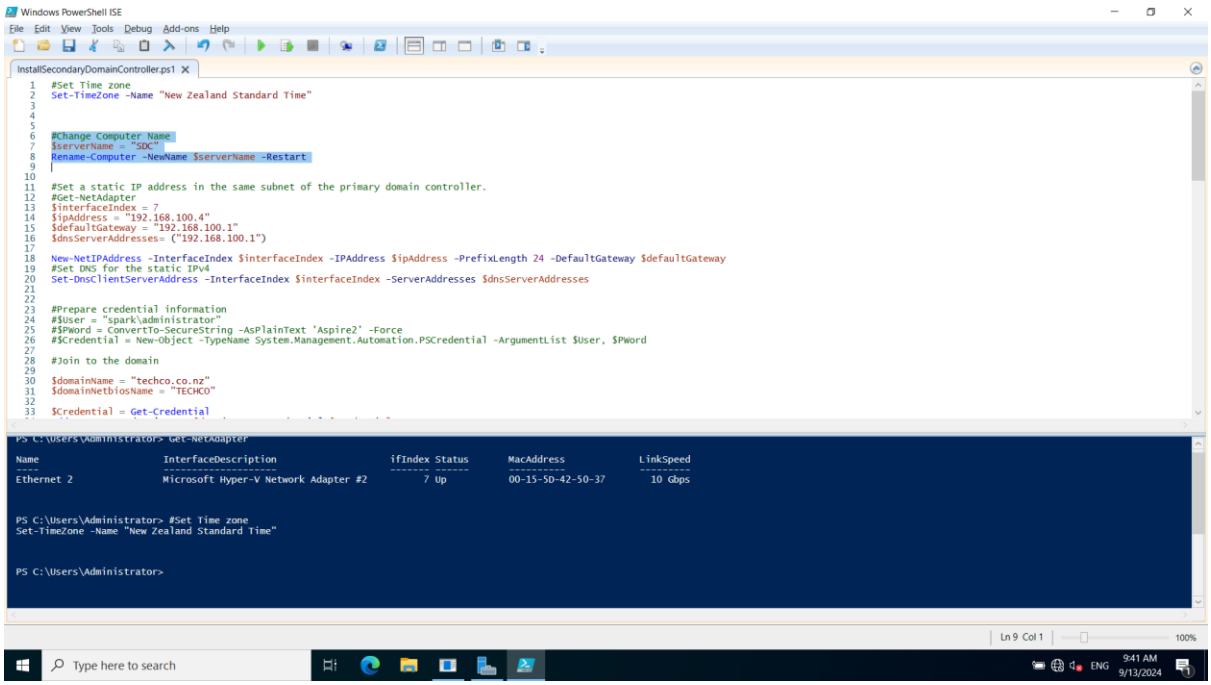
Student Name	Hui(Spark) ZHENG
Student ID	AEU3000774
Student Signature	Spark
Assessor	Click or tap here to enter text.

Contents

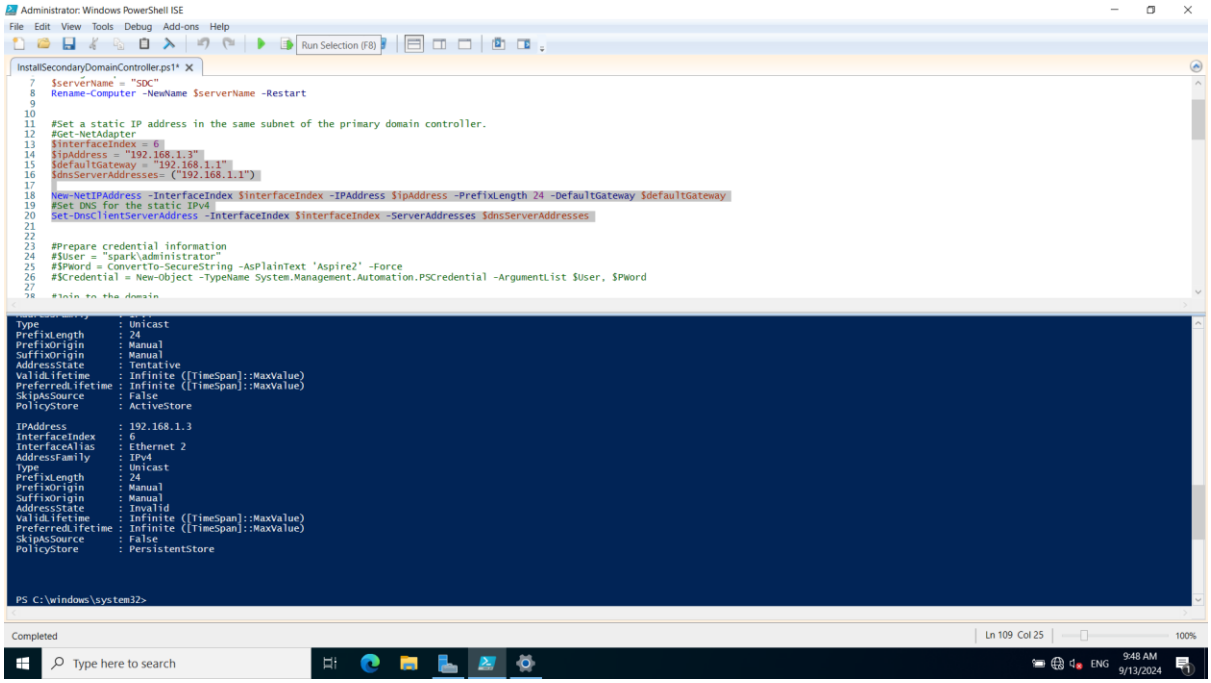
Task/Mahi 1: Second Domain Controller Integration & User Authorization

Task 1.1 Create a PowerShell script to set up and integrate a second domain controller

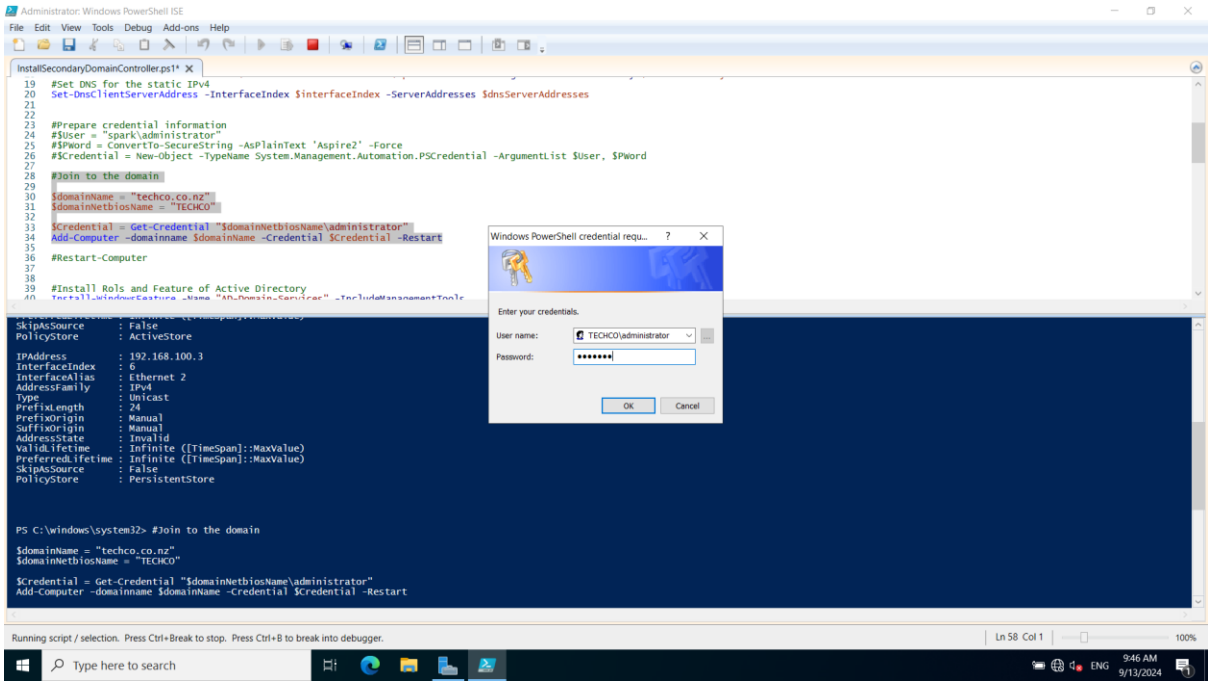
1. Change Computer Name

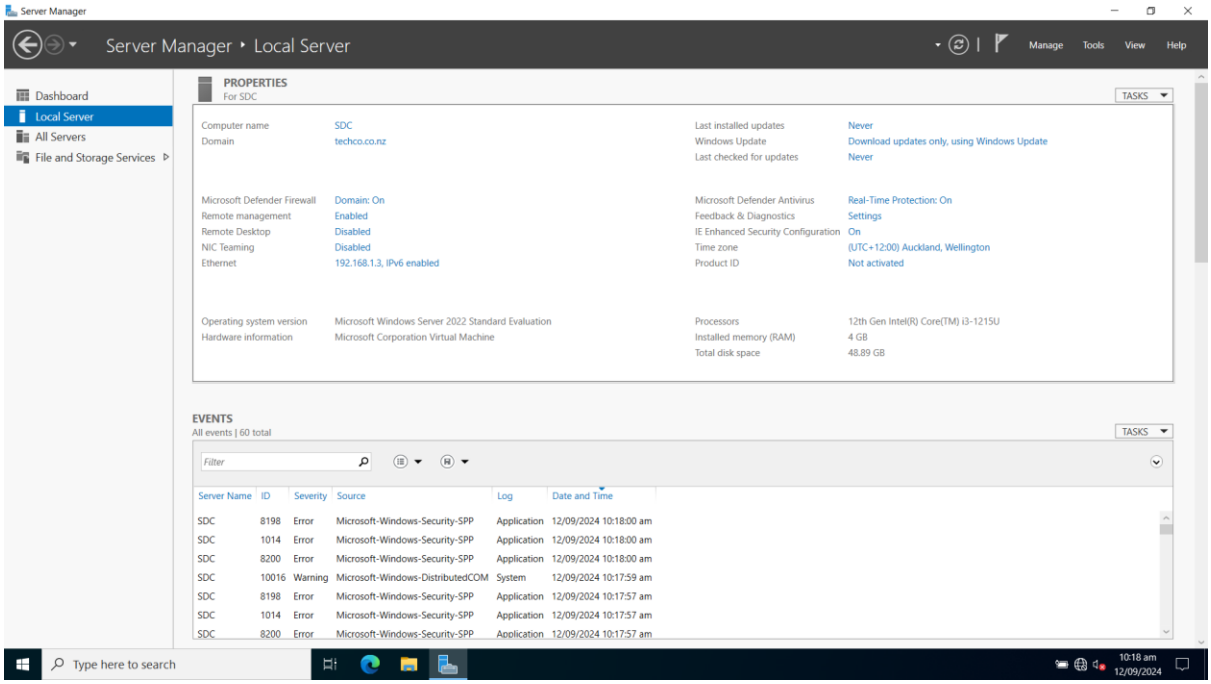


2. Set static IP address

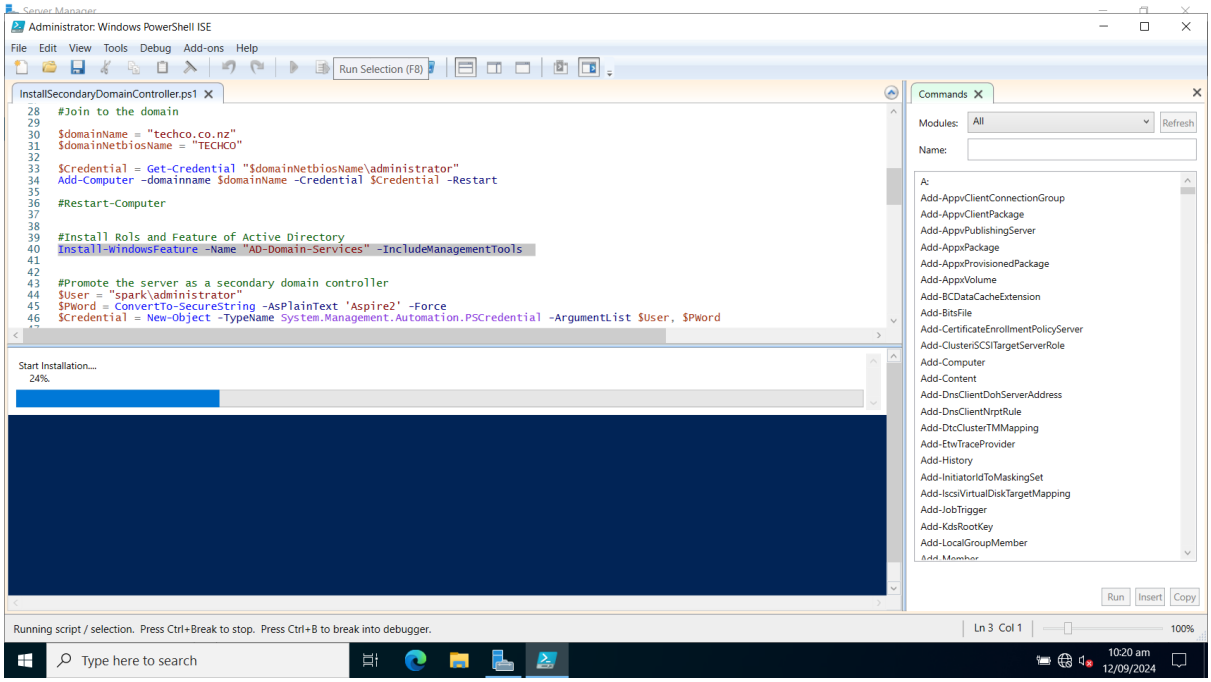


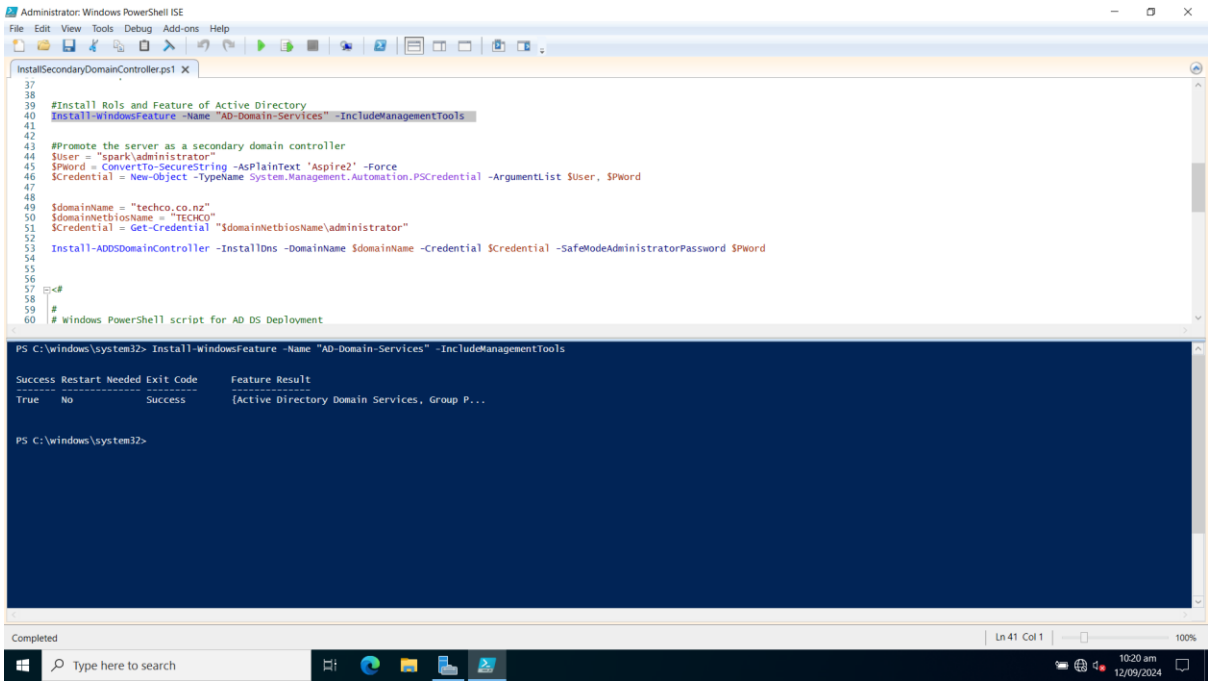
3. Join the domain techco.co.nz



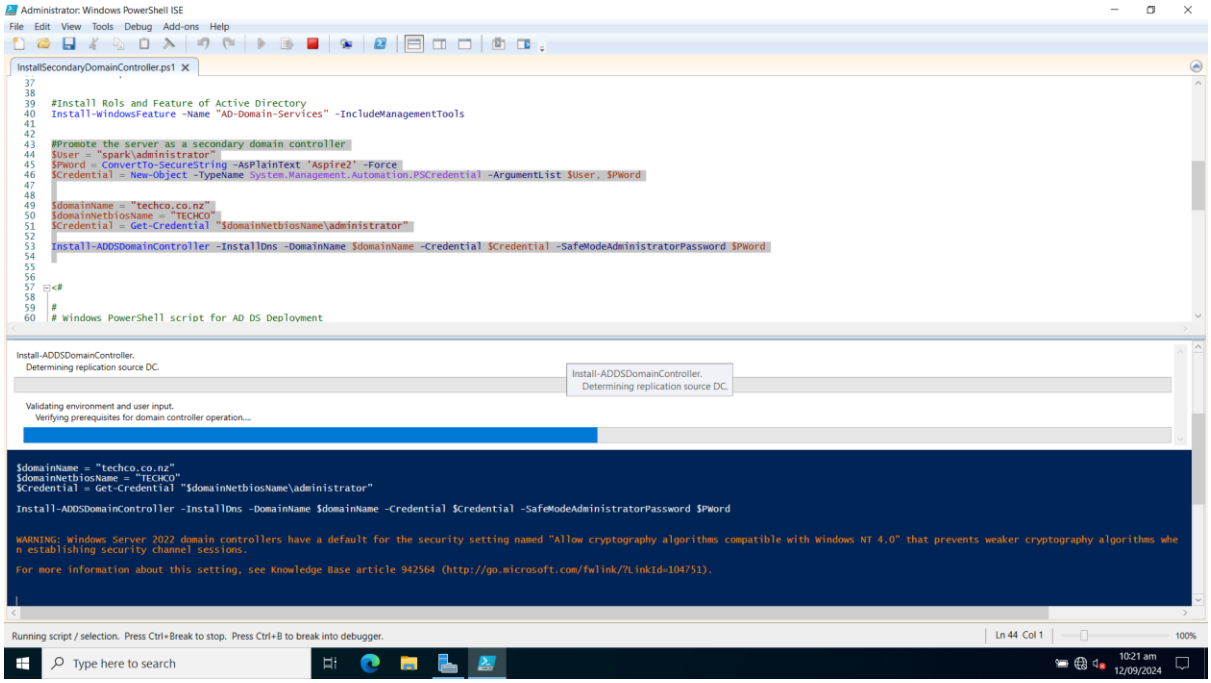

Server Manager
Server Manager ▸ Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
PROPERTIES
For SDC
TASKS
Computer name
SDC
Domain
techco.co.nz
Last installed updates
Never
Windows Update
Download updates only, using Windows Update
Last checked for updates
Never
Microsoft Defender Firewall
Domain: On
Remote management
Enabled
Remote Desktop
Disabled
NIC Teaming
Disabled
Ethernet
192.168.1.3, IPv6 enabled
Microsoft Defender Antivirus
Real-Time Protection: On
Feedback & Diagnostics
Settings
IE Enhanced Security Configuration
On
Time zone
(UTC+12:00) Auckland, Wellington
Product ID
Not activated
Operating system version
Microsoft Windows Server 2022 Standard Evaluation
Hardware information
Microsoft Corporation Virtual Machine
Processors
12th Gen Intel(R) Core(TM) i3-1215U
Installed memory (RAM)
4 GB
Total disk space
48.89 GB
EVENTS
All events | 60 total
TASKS
Filter
Server Name
ID
Severity
Source
Log
Date and Time
SDC 8198 Error Microsoft-Windows-Security-SPP Application 12/09/2024 10:18:00 am
SDC 1014 Error Microsoft-Windows-Security-SPP Application 12/09/2024 10:18:00 am
SDC 8200 Error Microsoft-Windows-Security-SPP Application 12/09/2024 10:18:00 am
SDC 10016 Warning Microsoft-Windows-DistributedCOM System 12/09/2024 10:17:59 am
SDC 8198 Error Microsoft-Windows-Security-SPP Application 12/09/2024 10:17:57 am
SDC 1014 Error Microsoft-Windows-Security-SPP Application 12/09/2024 10:17:57 am
SDC 8200 Error Microsoft-Windows-Security-SPP Application 12/09/2024 10:17:57 am
Type here to search
10:18 am
12/09/2024

4. Install Rols and Feature of Active Directory

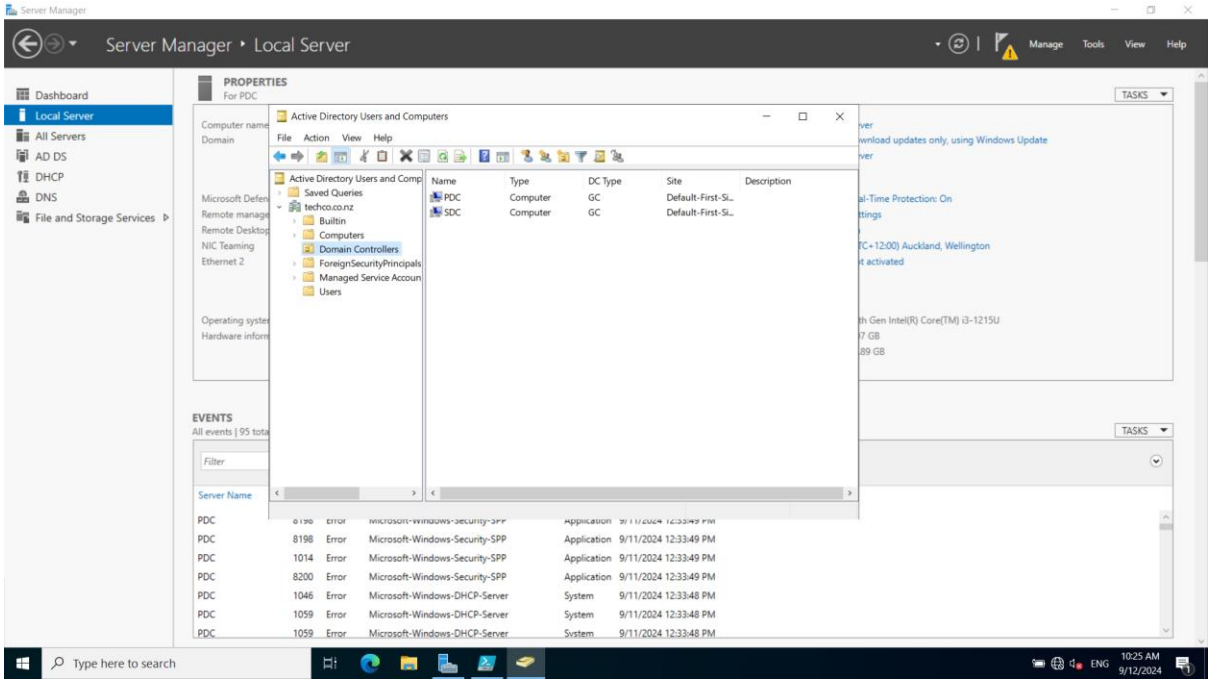


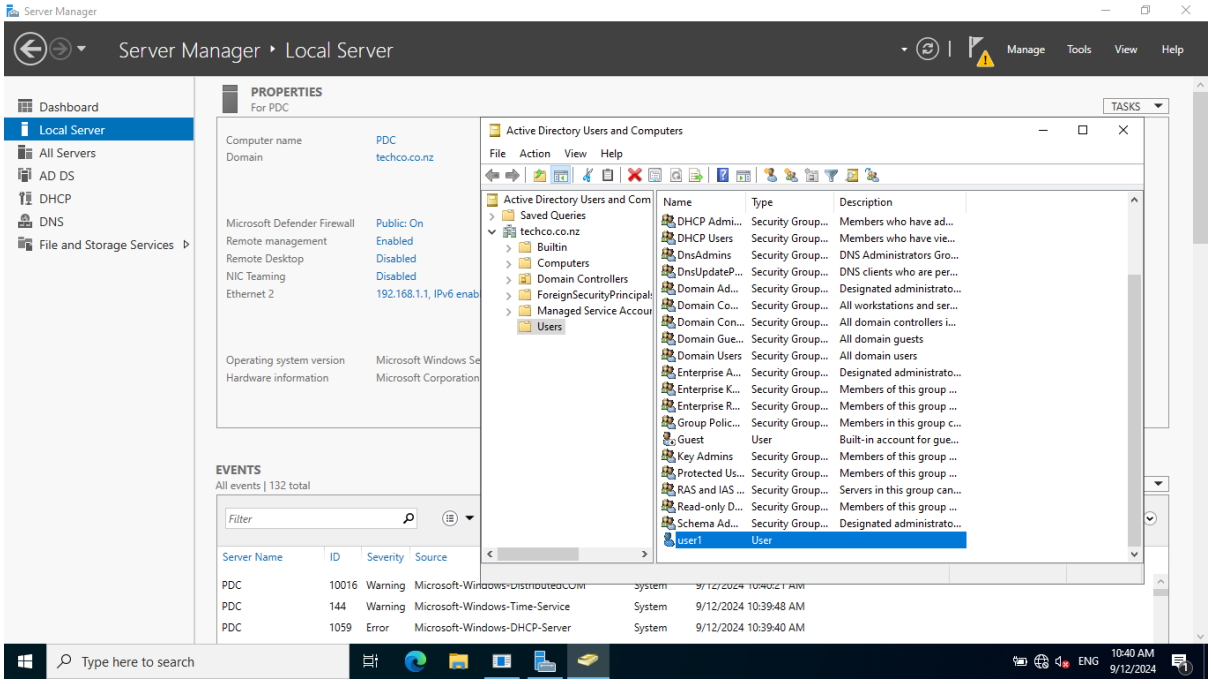


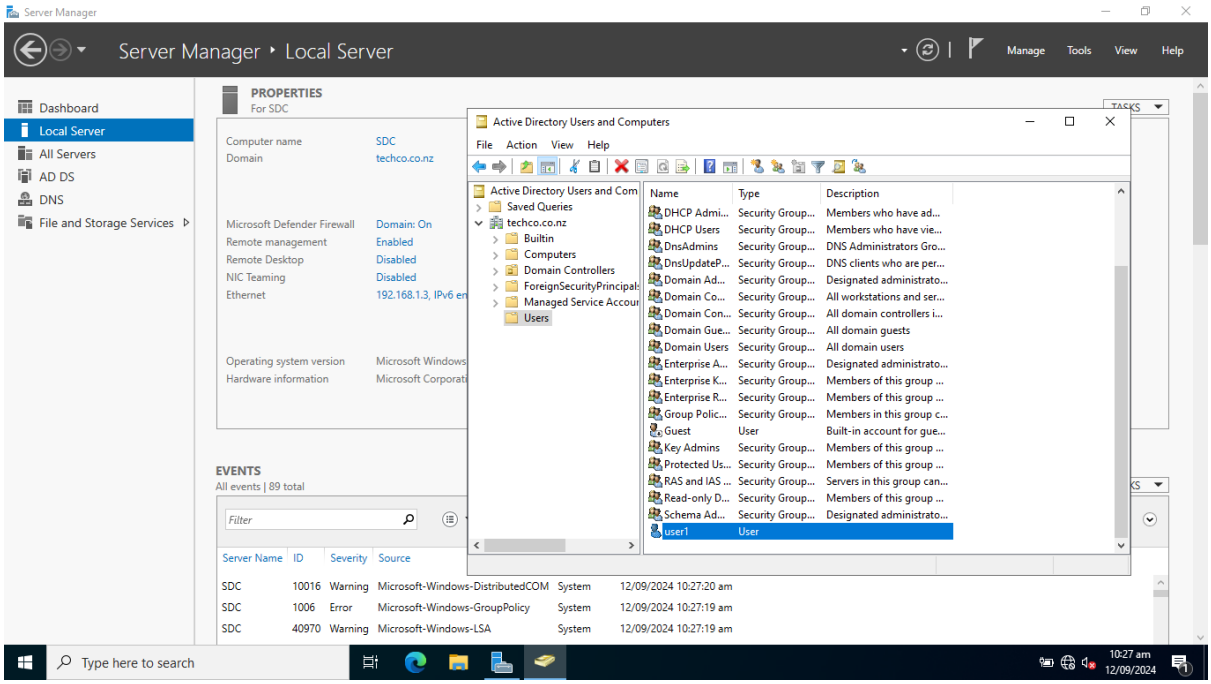
5. Promote the server as a secondary domain controller



6. Check the user “User1” created on PDC has been synchronized to SDC

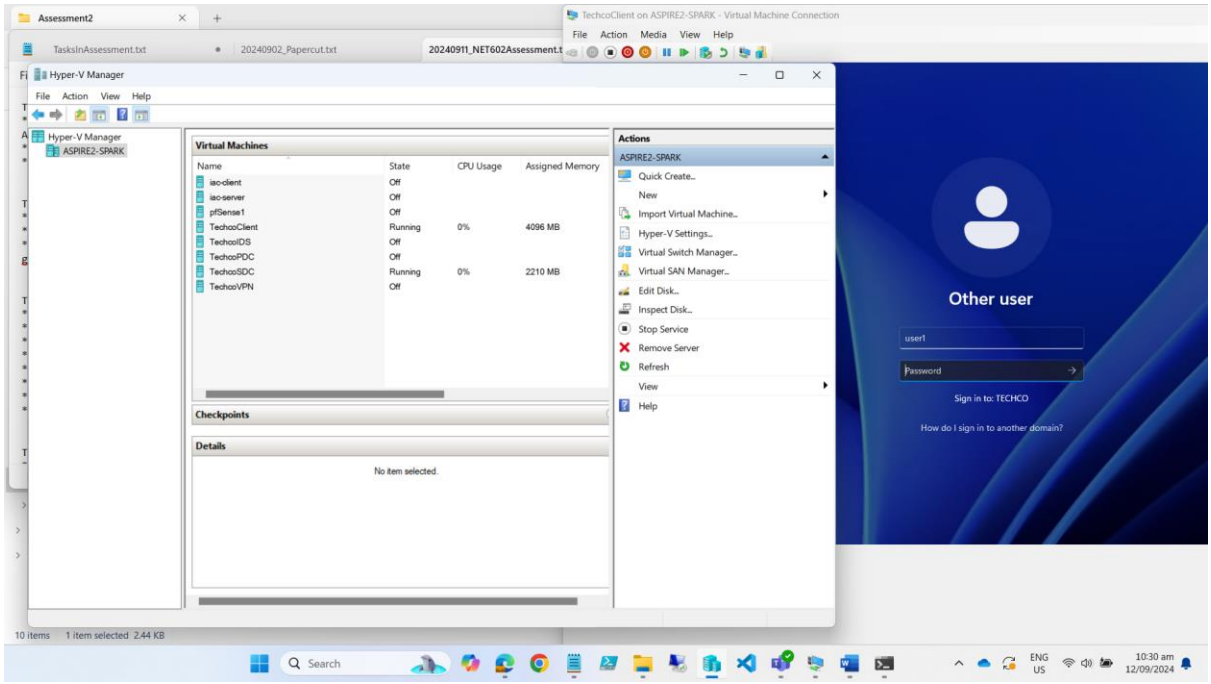


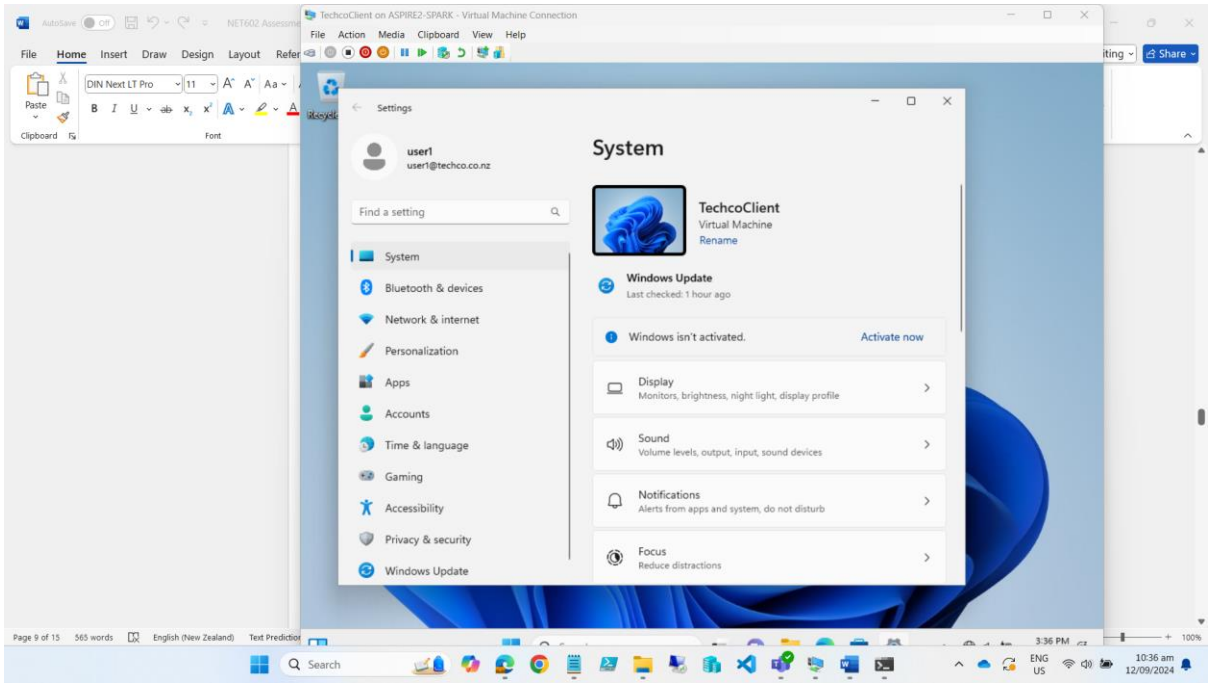



Server Manager
Server Manager ▸ Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
PROPERTIES
For SDC
Computer name
SDC
Domain
techco.co.nz
Microsoft Defender Firewall
Domain: On
Remote management
Enabled
Remote Desktop
Disabled
NIC Teaming
Disabled
Ethernet
Operating system version
Hardware information
EVENTS
All events | 89 total
Filter
Server Name
ID
Severity
Source
SDC 10016 Warning Microsoft-Windows-DistributedCOM System 12/09/2024 10:27:20 am
SDC 1006 Error Microsoft-Windows-GroupPolicy System 12/09/2024 10:27:19 am
SDC 40970 Warning Microsoft-Windows-LSA System 12/09/2024 10:27:19 am
Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
techco.co.nz
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name
Type
Description
DHCP Admi... Security Group... Members who have ad...
DHCP Users Security Group... Members who have vie...
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 ...
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...
user1 User
Type here to search
10:27 am
12/09/2024

AUE3000774

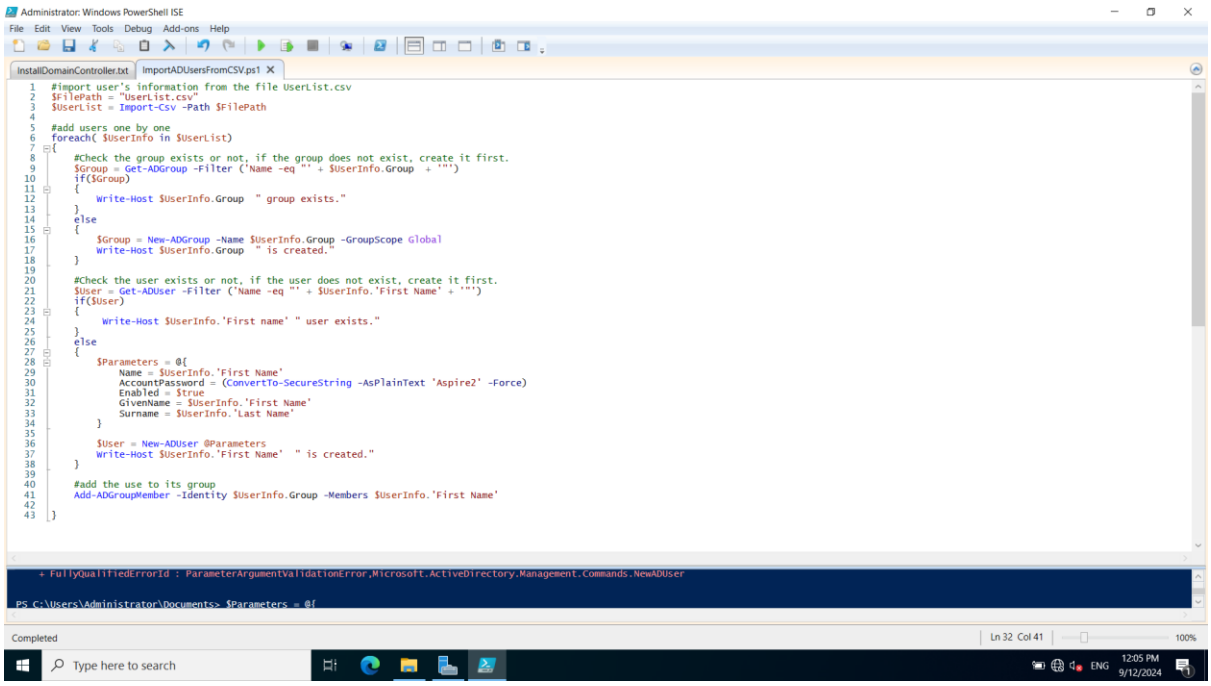
7. Test a client machine to login domain with PDC down.



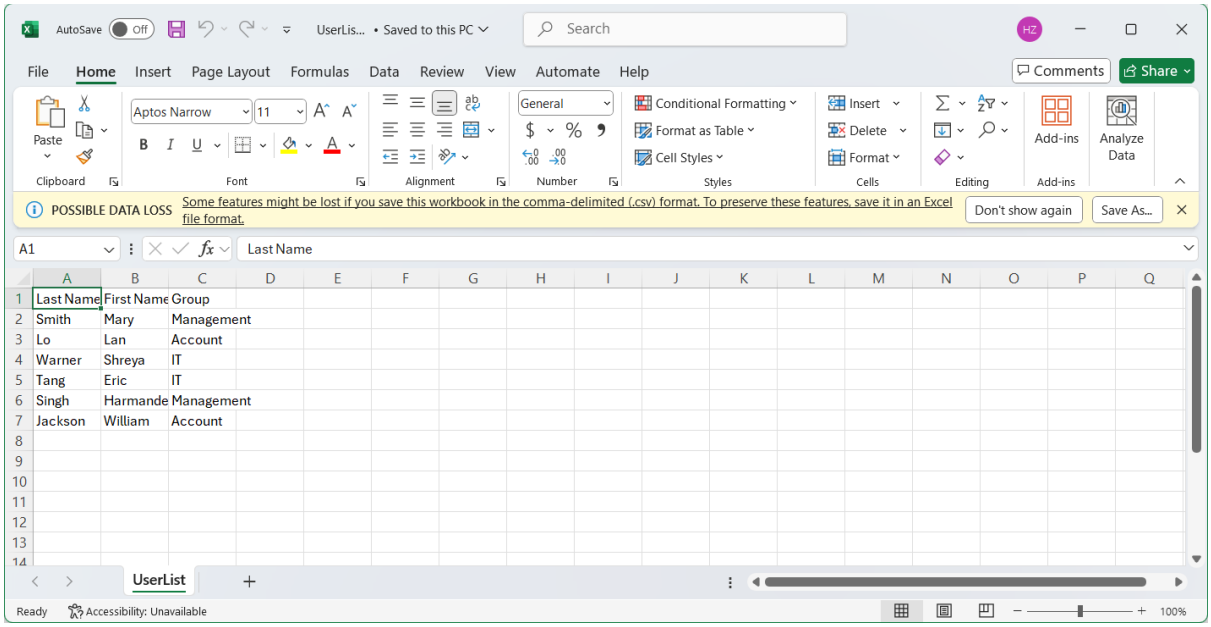


Task 1.2 Create a PowerShell script to automate user creation in Active Directory

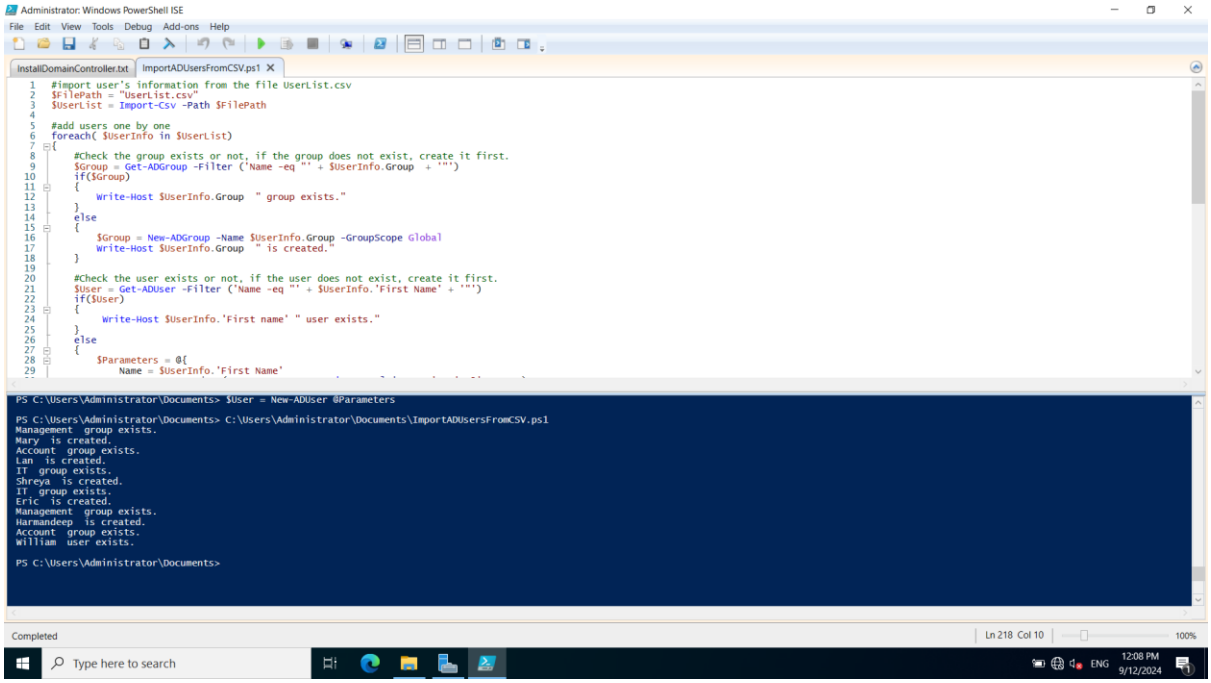
1. The PowerShell Script to add AD users

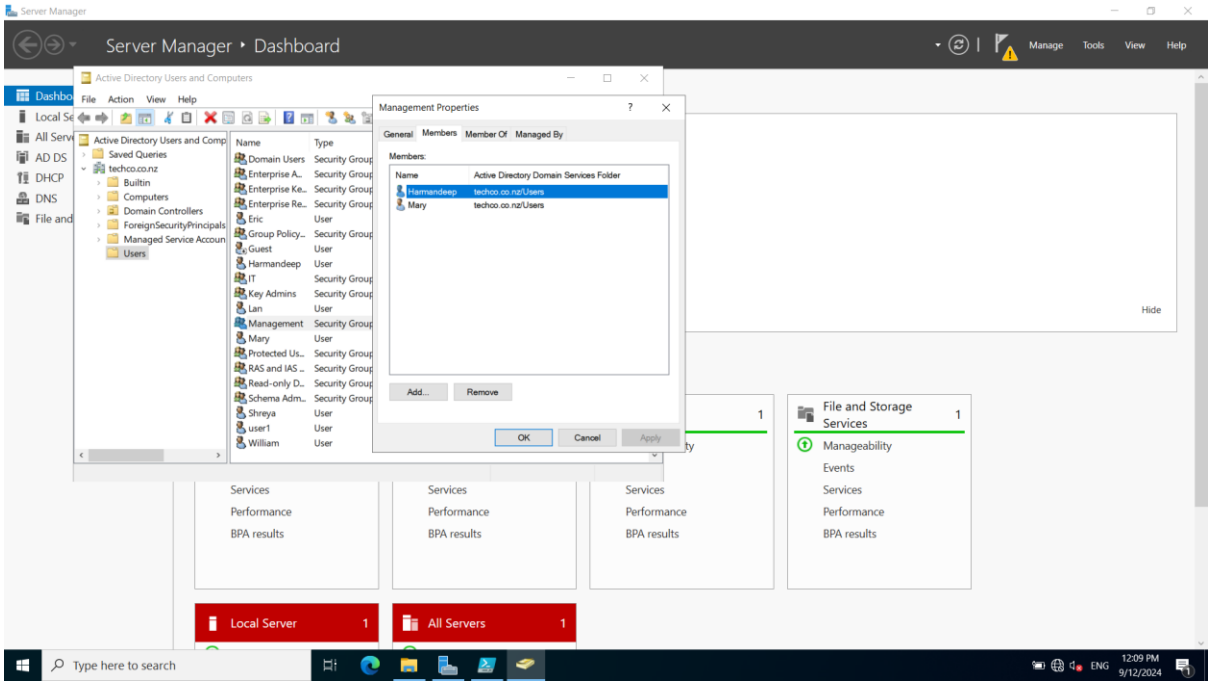


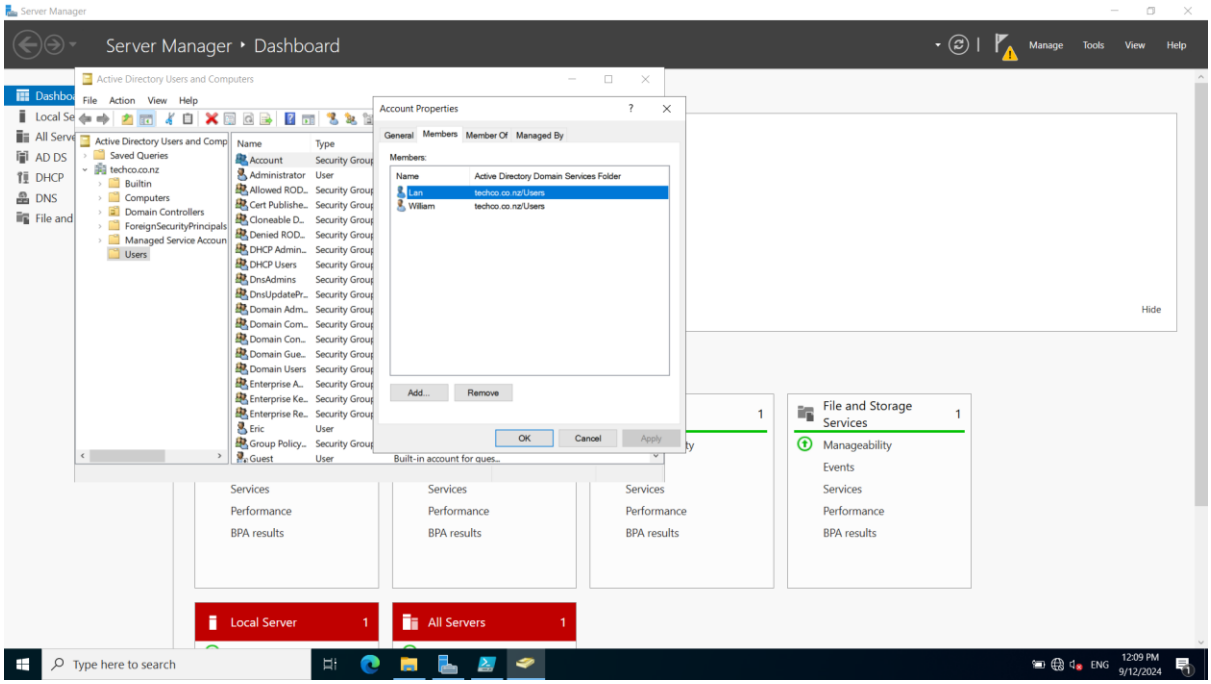
2. Users in userlist.csv file

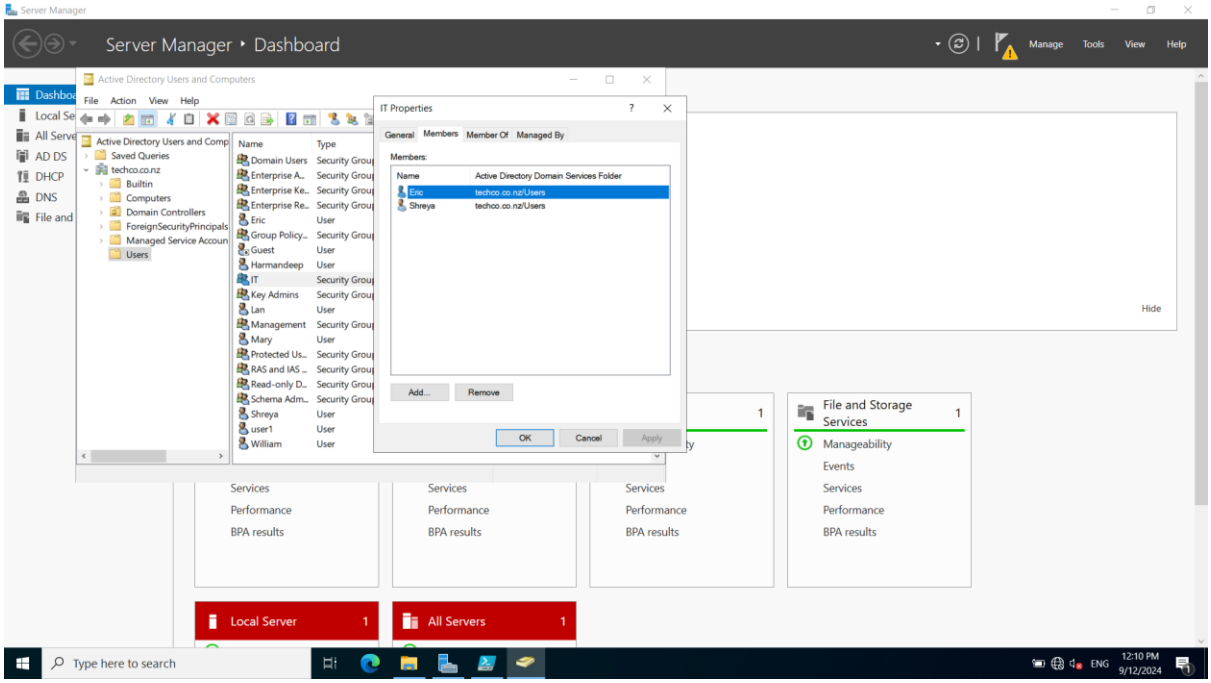


3. Run the PowerShell script

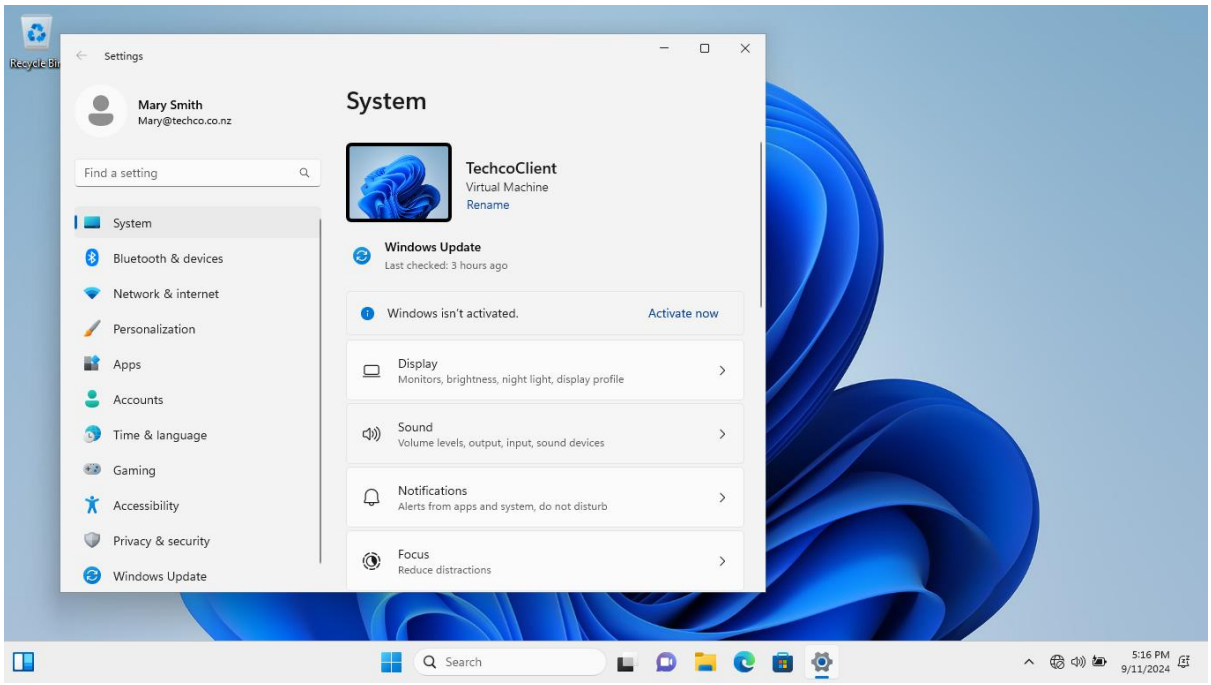


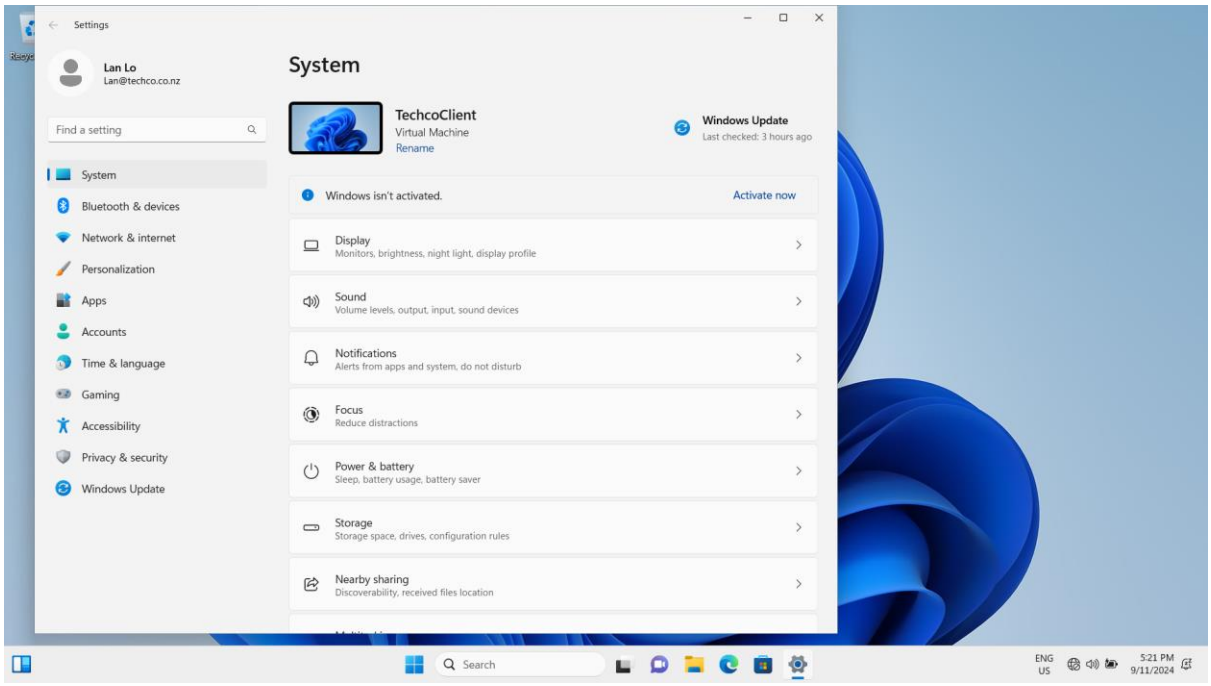


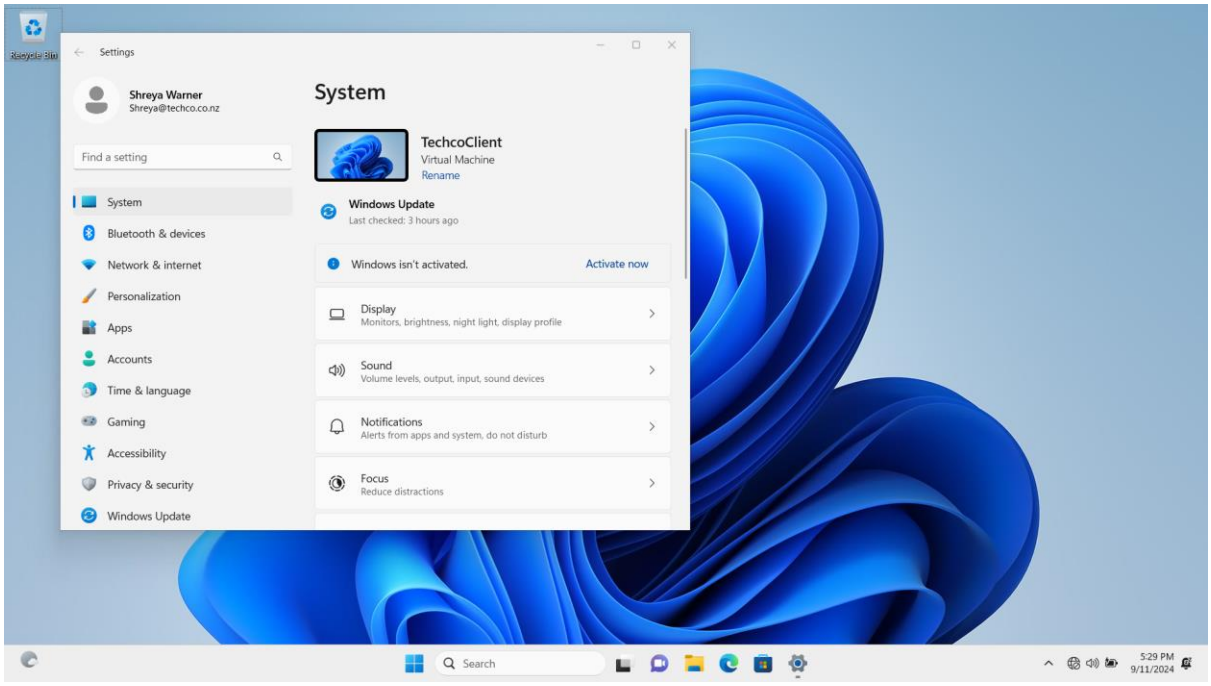

Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Active Directory Users and Computers
File Action View Help
Account Properties
General Members Member Of Managed By
Members:
Name
Active Directory Domain Services Folder
Lan
techco.co.nz/Users
William
techco.co.nz/Users
Add...
Remove
OK
Cancel
Apply
Hide
File and Storage Services
Manageability
Events
Services
Performance
BPA results
Local Server
All Servers
Type here to search
ENG
12:09 PM
9/12/2024


Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Active Directory Users and Computers
File Action View Help
IT Properties
General Members Member Of Managed By
Members:
Name
Active Directory Domain Services Folder
Eric
techco.co.nz/Users
Shreya
techco.co.nz/Users
Add...
Remove
OK
Cancel
Apply
Hide
File and Storage Services
Manageability
Events
Services
Performance
BPA results
Local Server
All Servers
Type here to search
ENG
12:10 PM
9/12/2024

4. Test users created to login on the client machine






Recycle Bin
Settings
Shreya Warner
Shreya@techco.co.nz
Find a setting
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Windows Update
System
TechcoClient
Virtual Machine
Rename
Windows Update
Last checked: 3 hours ago
Windows isn't activated.
Activate now
Display
Monitors, brightness, night light, display profile
Sound
Volume levels, output, input, sound devices
Notifications
Alerts from apps and system, do not disturb
Focus
Reduce distractions
Search
5:29 PM
9/11/2024

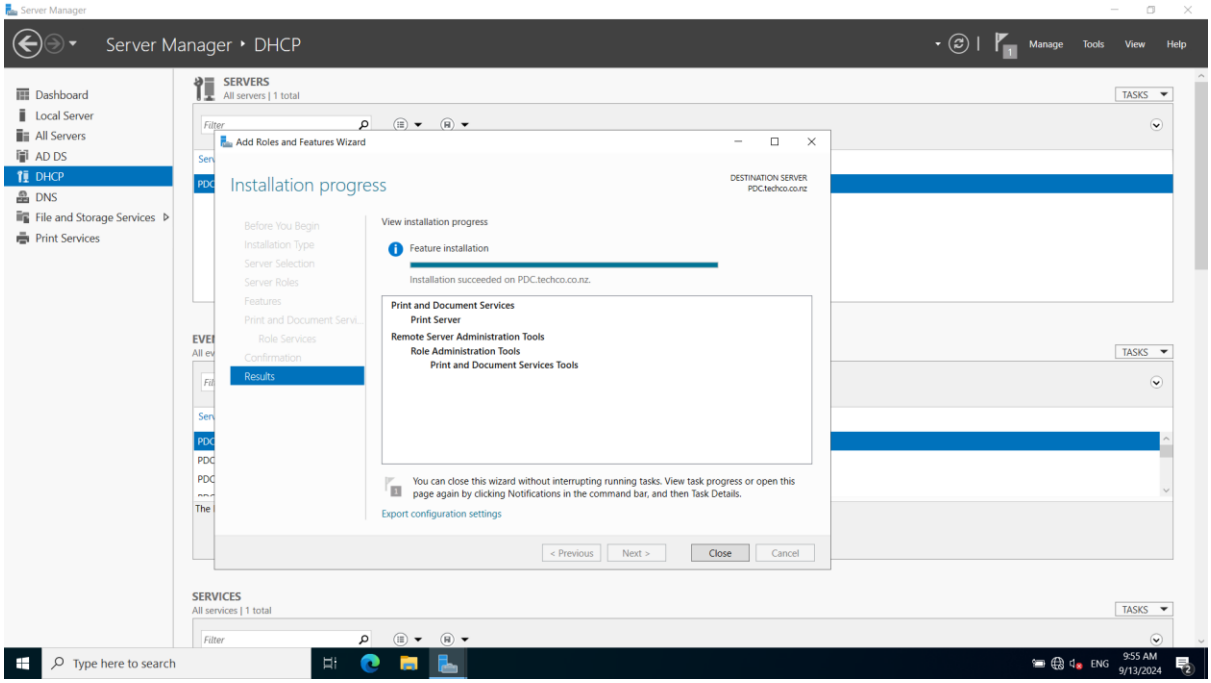
Task/Mahi 2: Deploying Print Management Solution via Group Policy Object

1. PaperCut is chosen as our print management solution

PaperCut provides tools to monitor and control printing activities centrally across the Media Labs network. And PaperCut provides effective ways to manage and reduce printing costs. In our print management solution, PaperCut management system will be deployed on the primary domain controller and PaperCut client software will be deployed to the user client machines through Group Policy Objects (GPO).

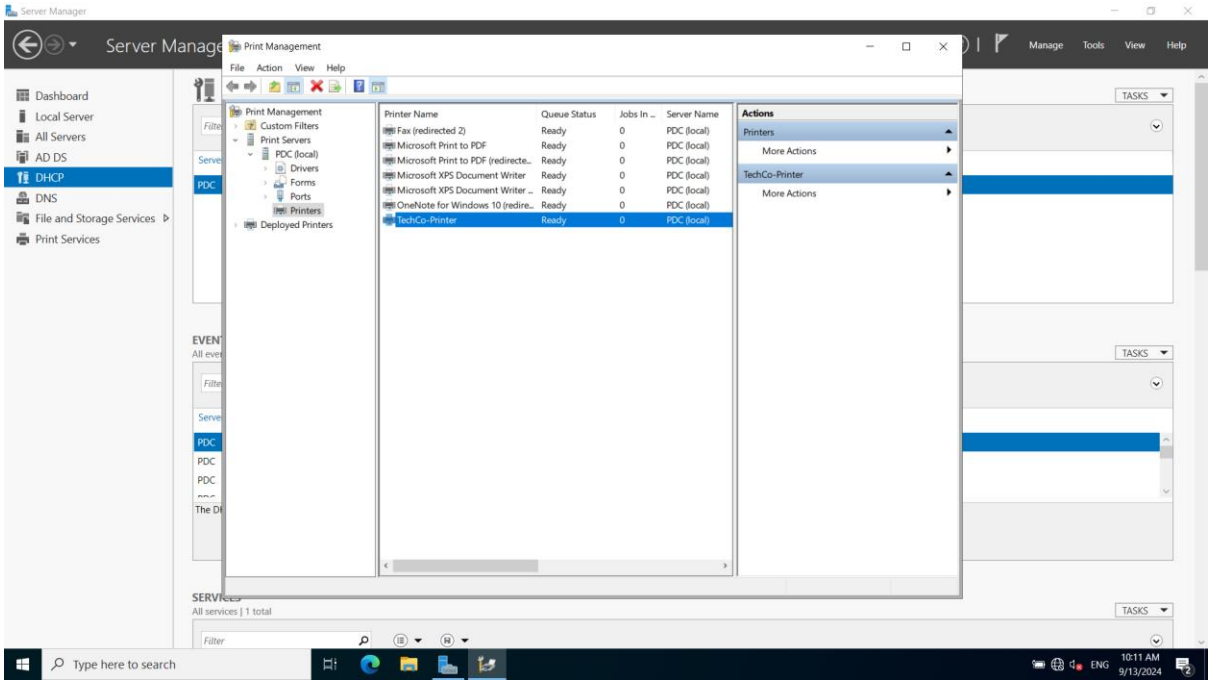
2. Prepare and install Papercut software

2.1 Install Printer service role on DC



2.2 Install Lexmark printer driver on DC

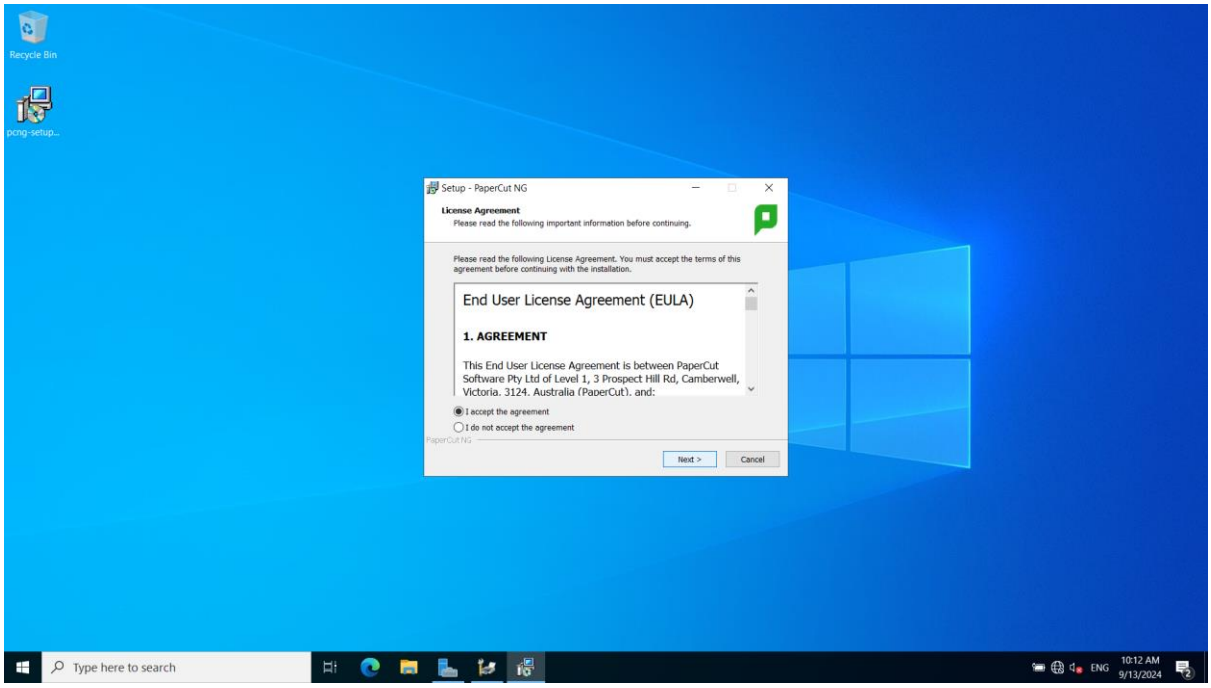
Download Lexmark Printer Drivers from https://downloads.lexmark.com/downloads/drivers/Lexmark_Universal_v2_UD1_Installation_Package_02092023.exe

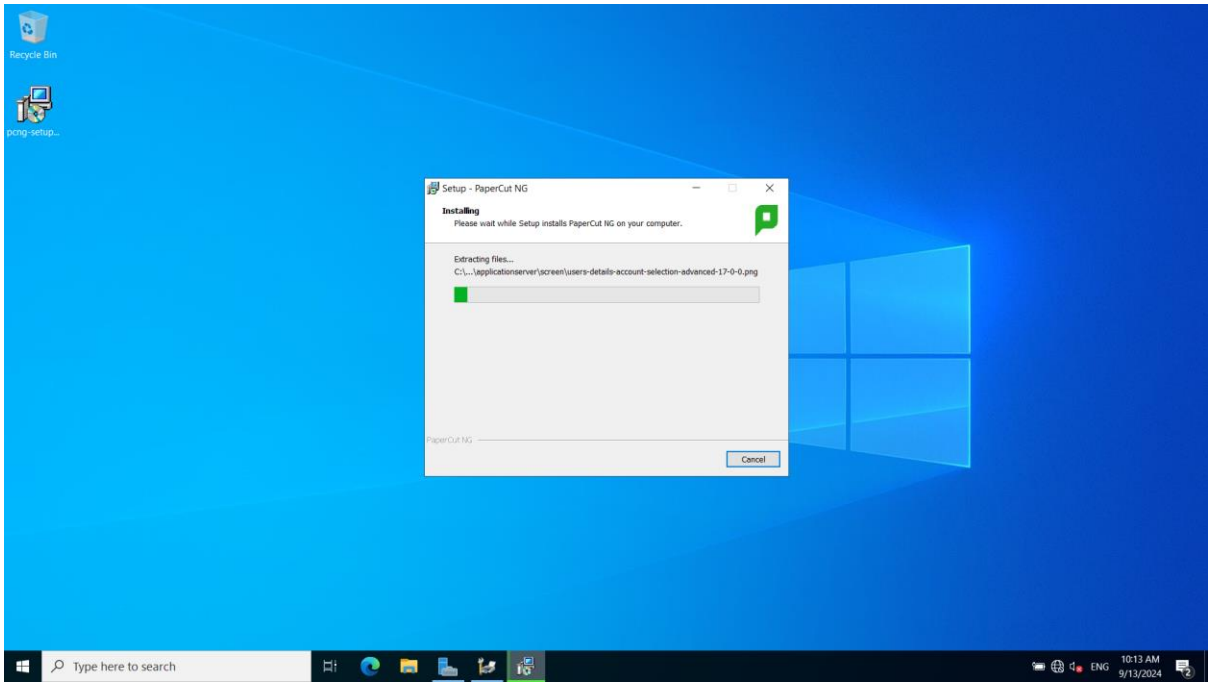


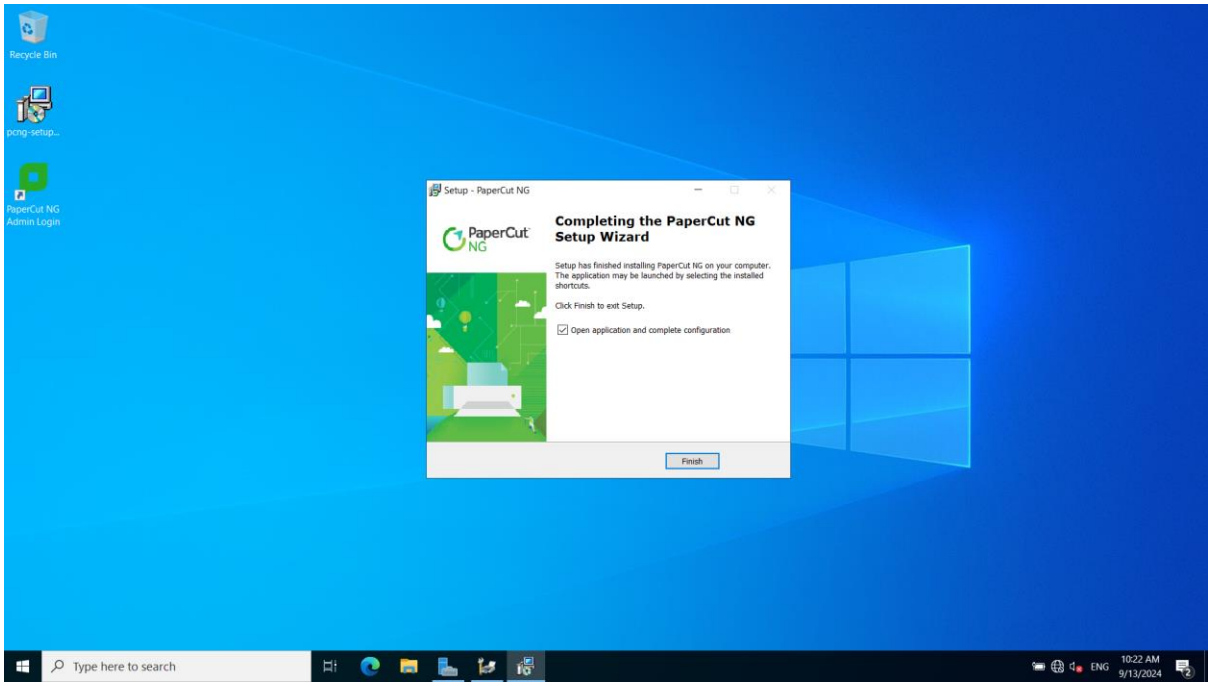
2.3 Download Papercut software.

https://cdn.papercut.com/web/products/ng-mf/installers/ng/24.x/pcng-setup-24.0.4.70157.exe

2.4 Install Papercut software on DC. (Admin/Spark@Aspire2)

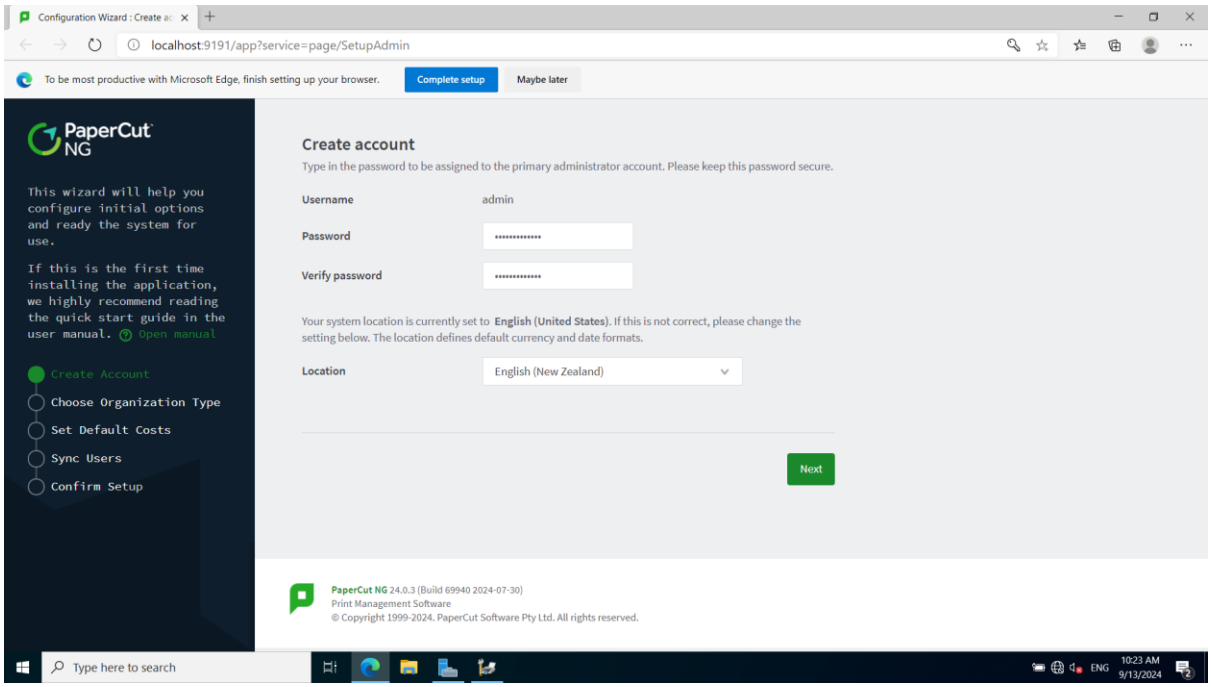



Recycle Bin
pcng-setup...
Setup - PaperCut NG
Installing
Please wait while Setup installs PaperCut NG on your computer.
Extracting files...
C:\...\applicationserver\screen\users-details-account-selection-advanced-17-0-0.png
PaperCut NG
Cancel
Type here to search
ENG
10:13 AM
9/13/2024

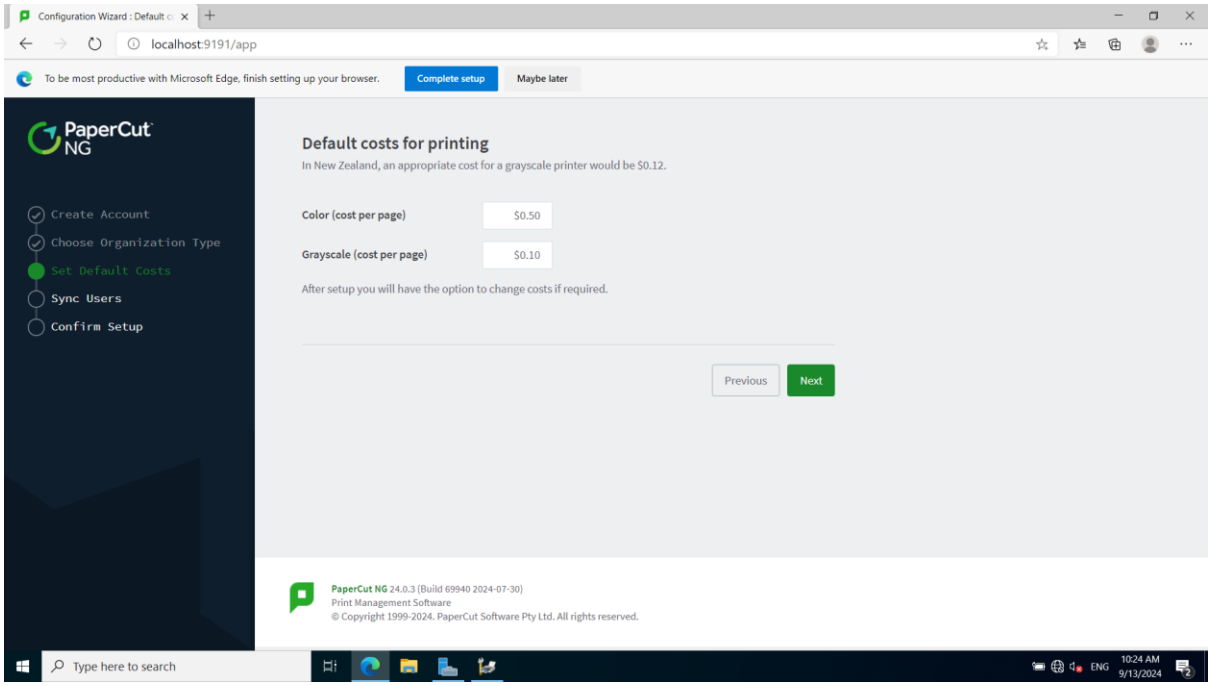

Recycle Bin
pcng-setup...
PaperCut NG
Admin Login
Setup - PaperCut NG
PaperCut NG
Completing the PaperCut NG Setup Wizard
Setup has finished installing PaperCut NG on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Open application and complete configuration
Finish
Type here to search
ENG
10:22 AM
9/13/2024

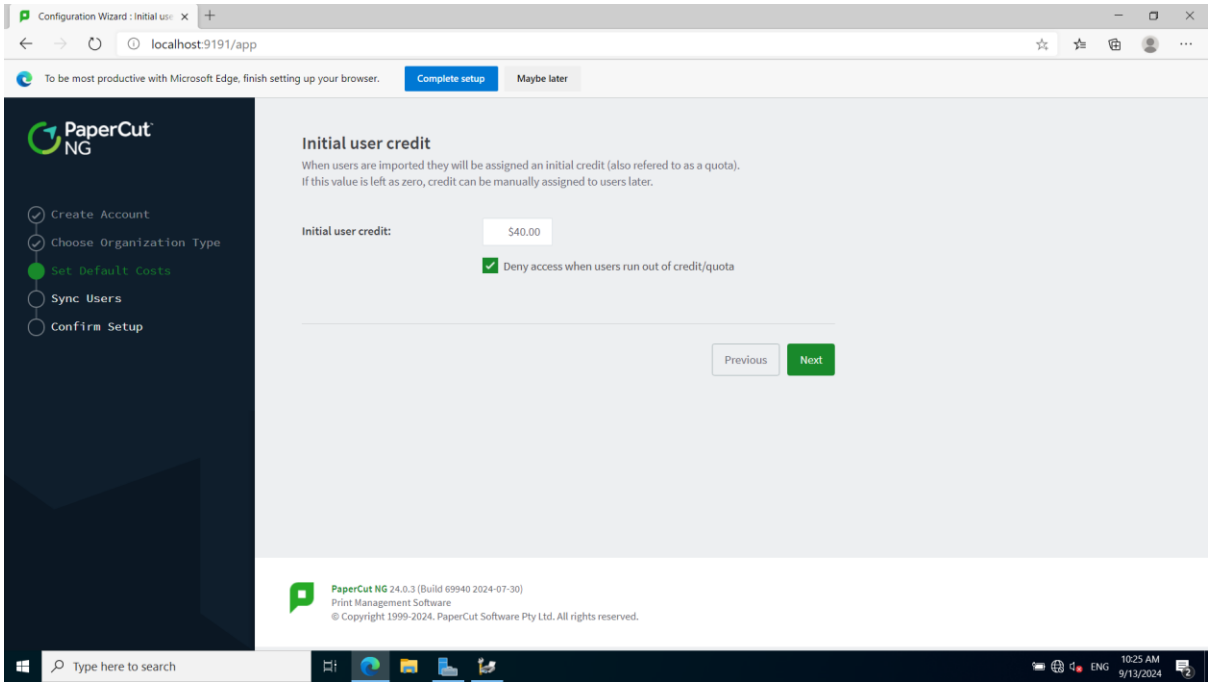
3. Configure PaperCut

3.1 Login to Admin portal.

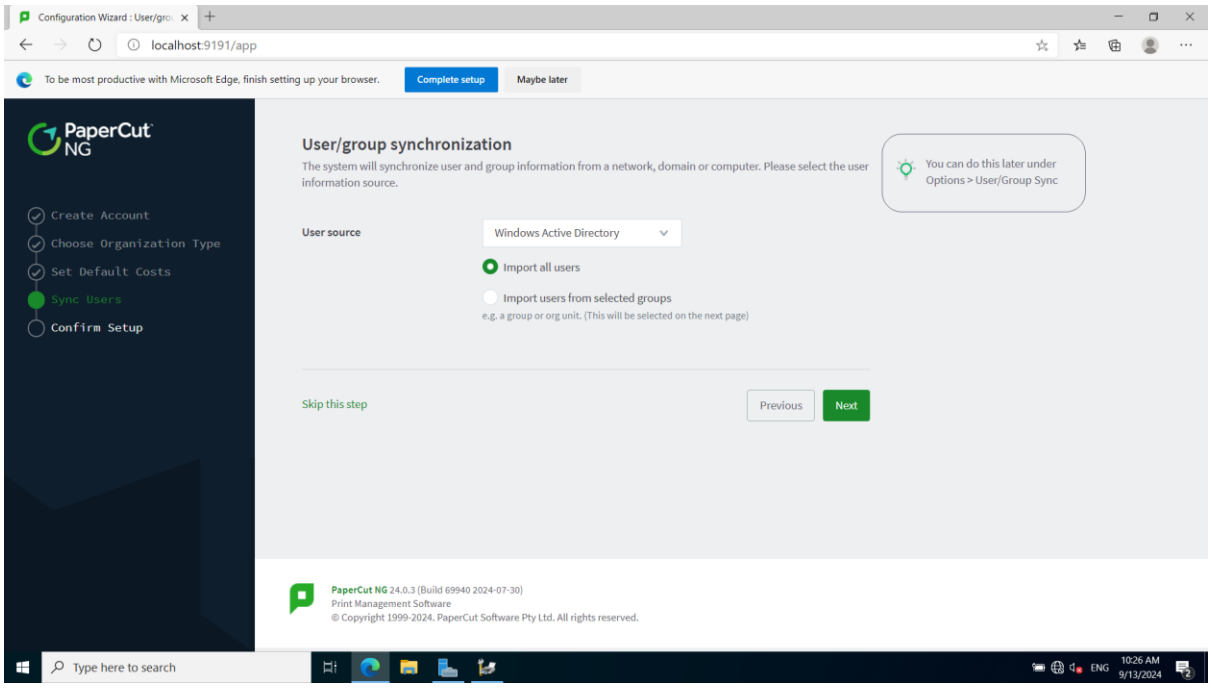


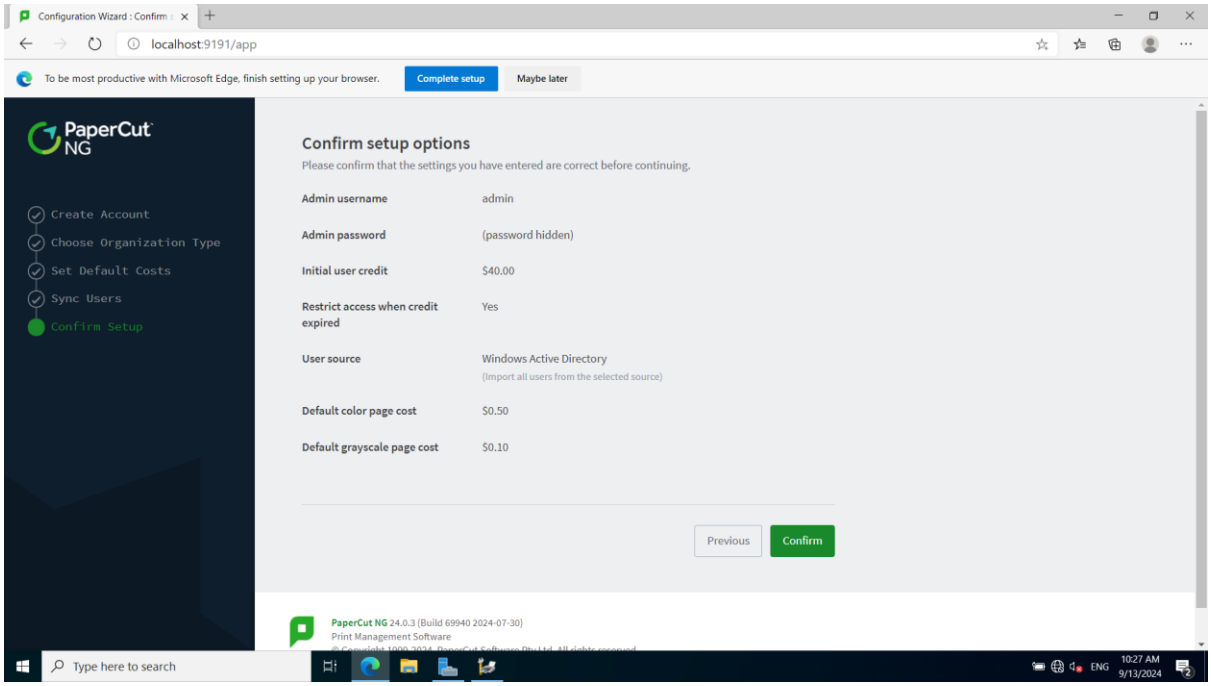
3.2 Set printing price

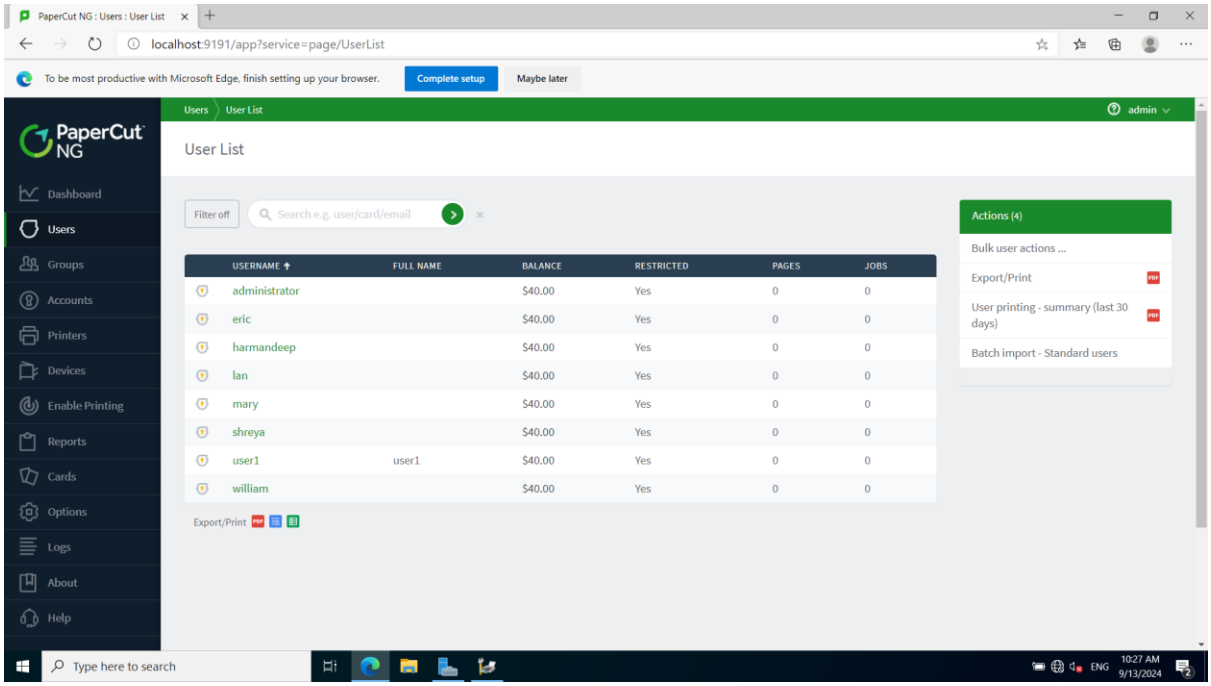




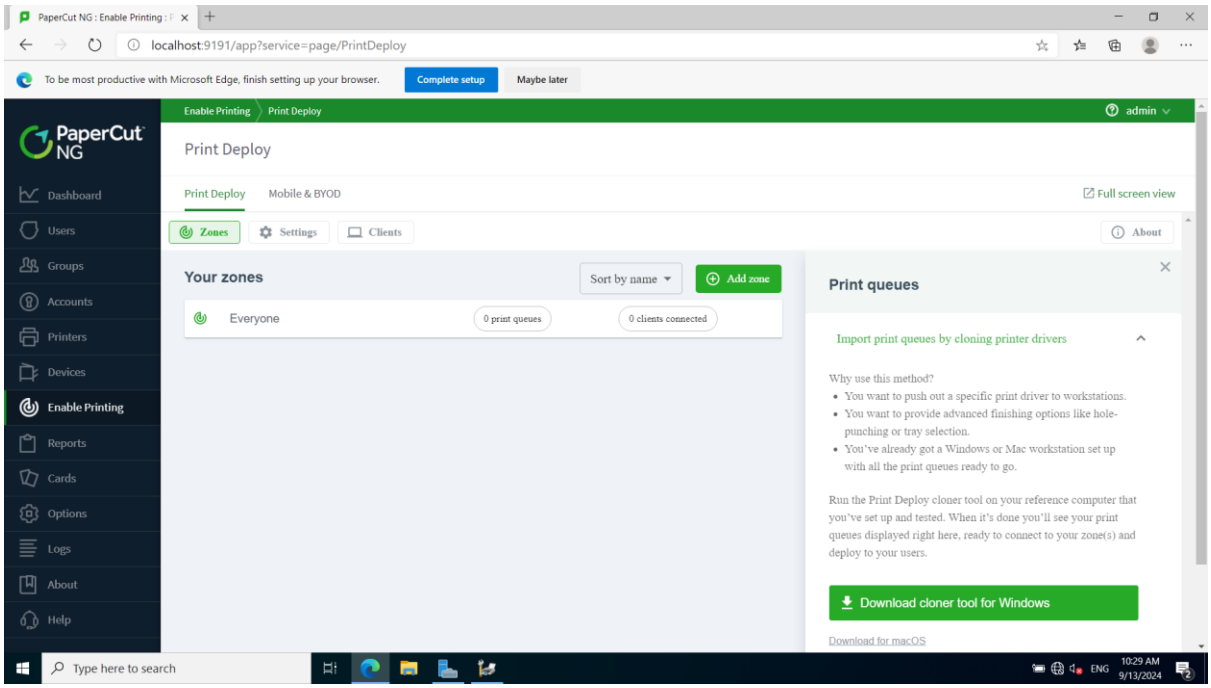
3.3 Sync users with AD

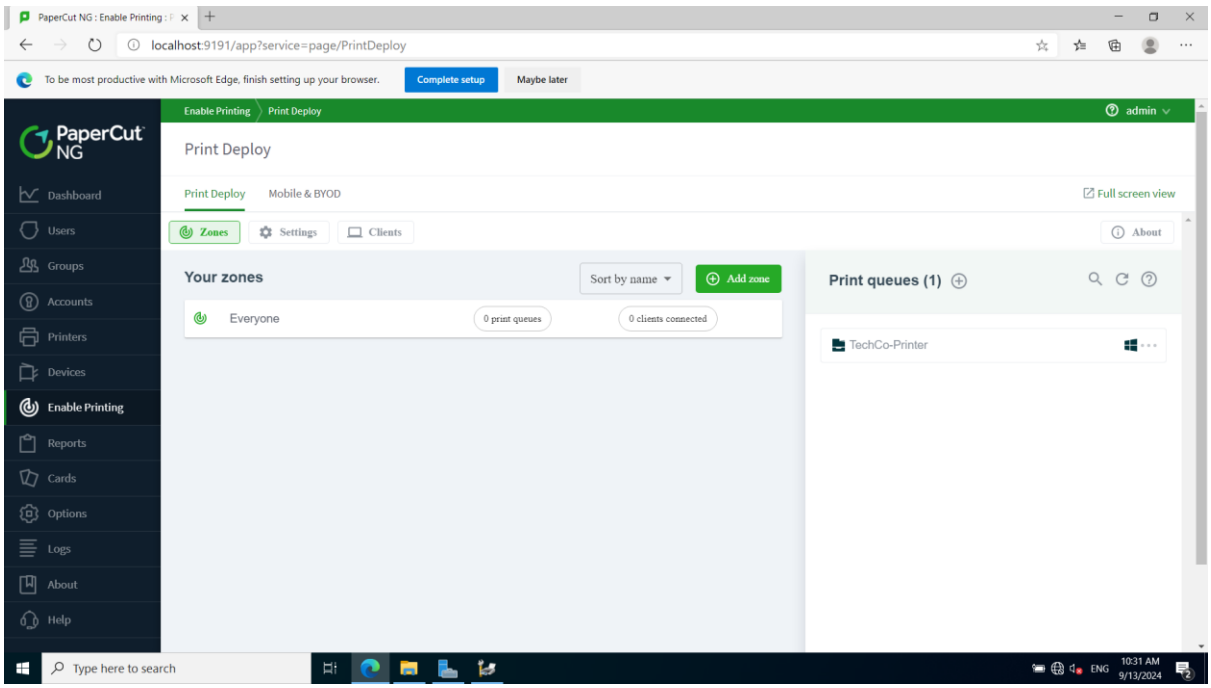



Configuration Wizard : Confirm
localhost:9191/app
To be most productive with Microsoft Edge, finish setting up your browser.
Complete setup
Maybe later
PaperCut NG
Create Account
Choose Organization Type
Set Default Costs
Sync Users
Confirm Setup
Confirm setup options
Please confirm that the settings you have entered are correct before continuing.
Admin username
admin
Admin password
(password hidden)
Initial user credit
$40.00
Restrict access when credit expired
Yes
User source
Windows Active Directory
(Import all users from the selected source)
Default color page cost
$0.50
Default grayscale page cost
$0.10
Previous
Confirm
PaperCut NG 24.0.3 (Build 69940 2024-07-30)
Print Management Software
Type here to search
ENG
10:27 AM
9/13/2024

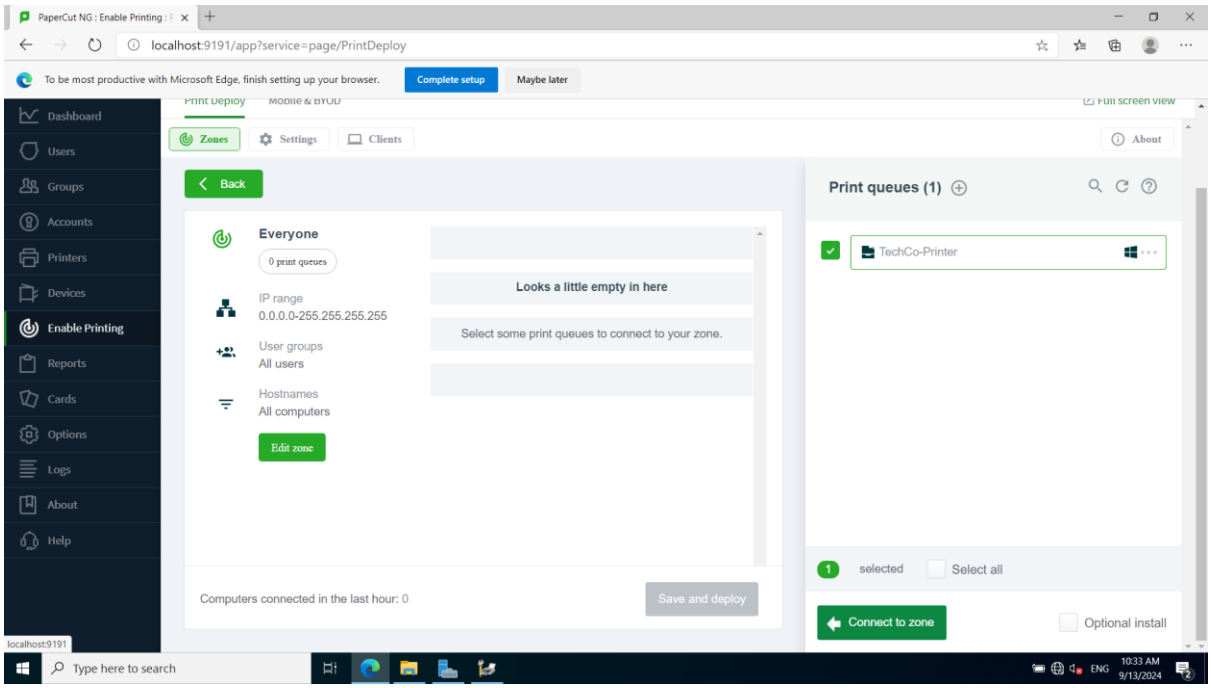

PaperCut NG : Users : User List
localhost:9191/app?service=page/UserList
To be most productive with Microsoft Edge, finish setting up your browser.
Complete setup
Maybe later
PaperCut NG
Users
User List
admin
Dashboard
Users
Groups
Accounts
Printers
Devices
Enable Printing
Reports
Cards
Options
Logs
About
Help
User List
Filter off
Search e.g. user/card/email
USERNAME
FULL NAME
BALANCE
RESTRICTED
PAGES
JOBS
administrator
$40.00
Yes
0
0
eric
$40.00
Yes
0
0
harmandeep
$40.00
Yes
0
0
lan
$40.00
Yes
0
0
mary
$40.00
Yes
0
0
shreya
$40.00
Yes
0
0
user1
user1
$40.00
Yes
0
0
william
$40.00
Yes
0
0
Export/Print
Actions (4)
Bulk user actions ...
Export/Print
User printing - summary (last 30 days)
Batch import - Standard users
Type here to search
ENG
10:27 AM
9/13/2024

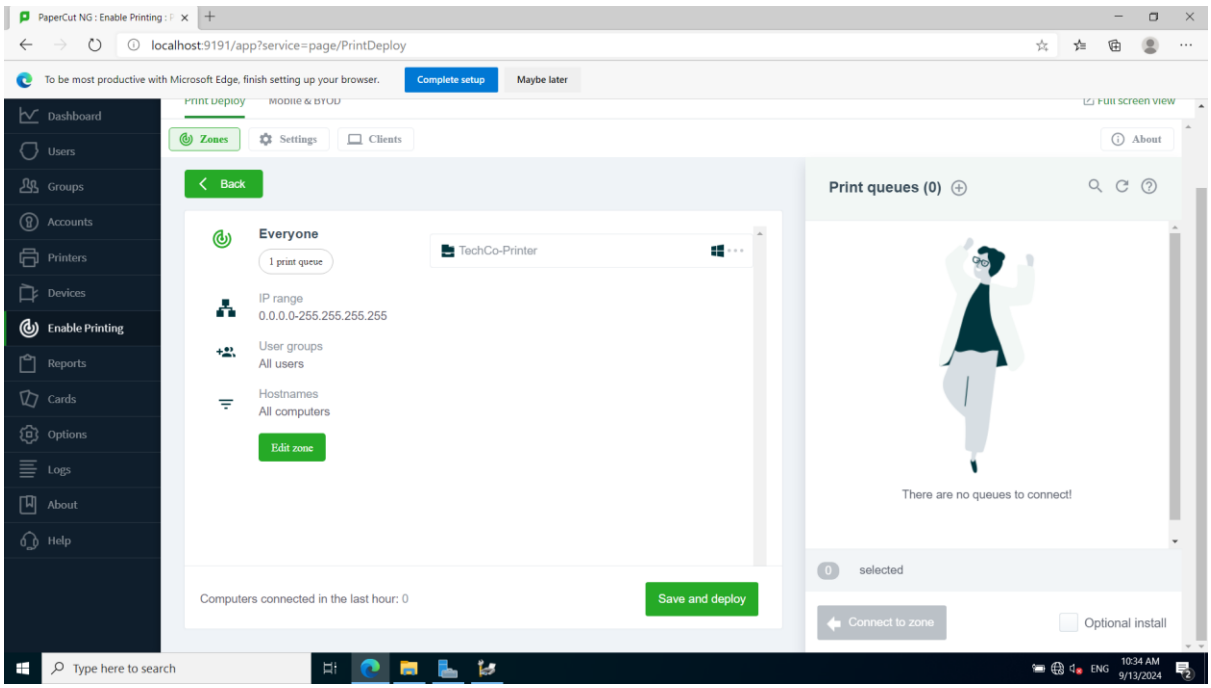
4. Add printer with cloner to portal in "Enable Printing" option.

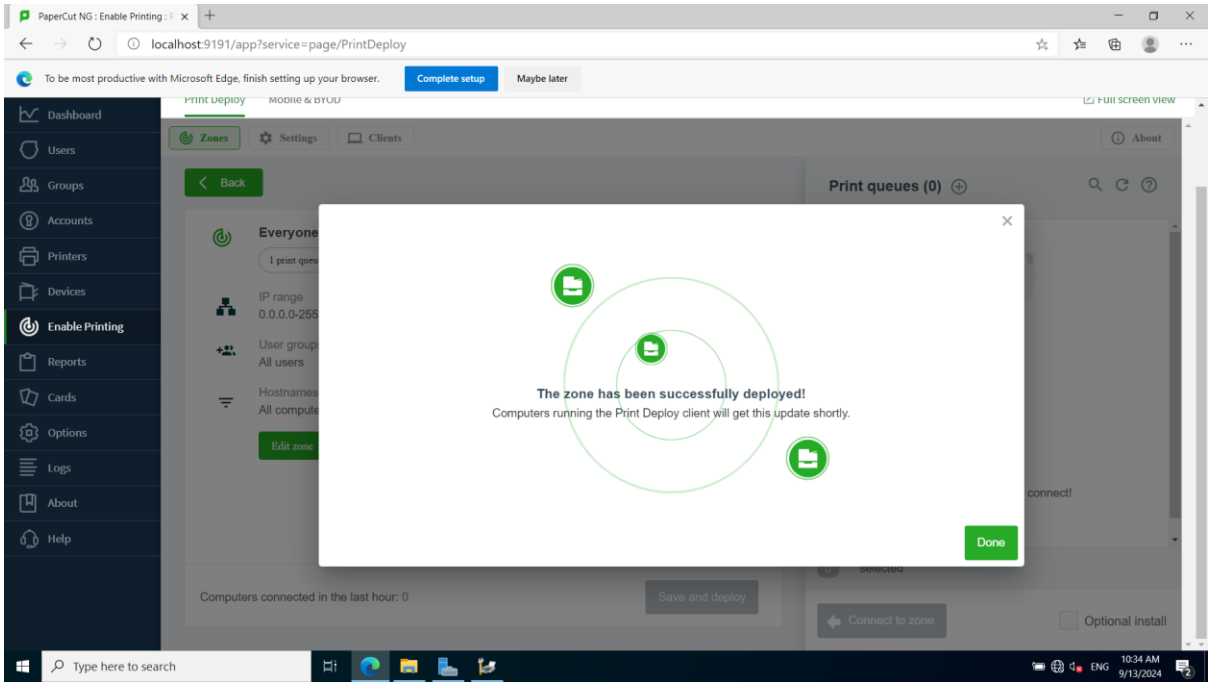




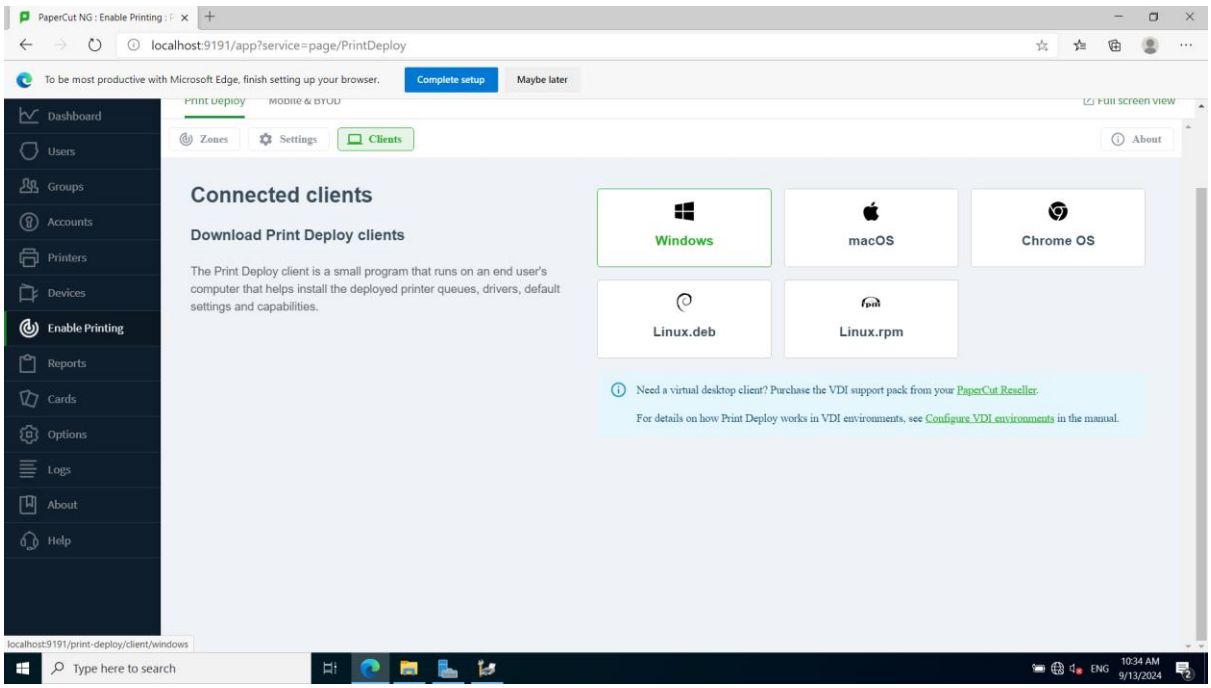
5. Add printer to Zone.





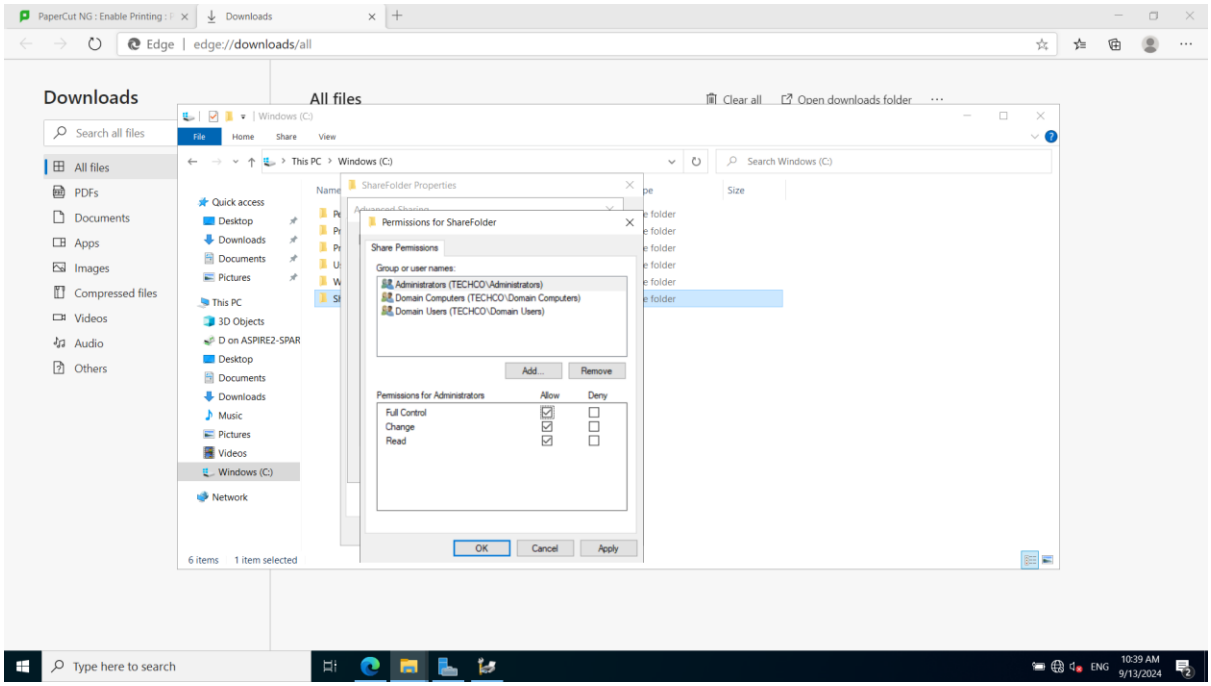


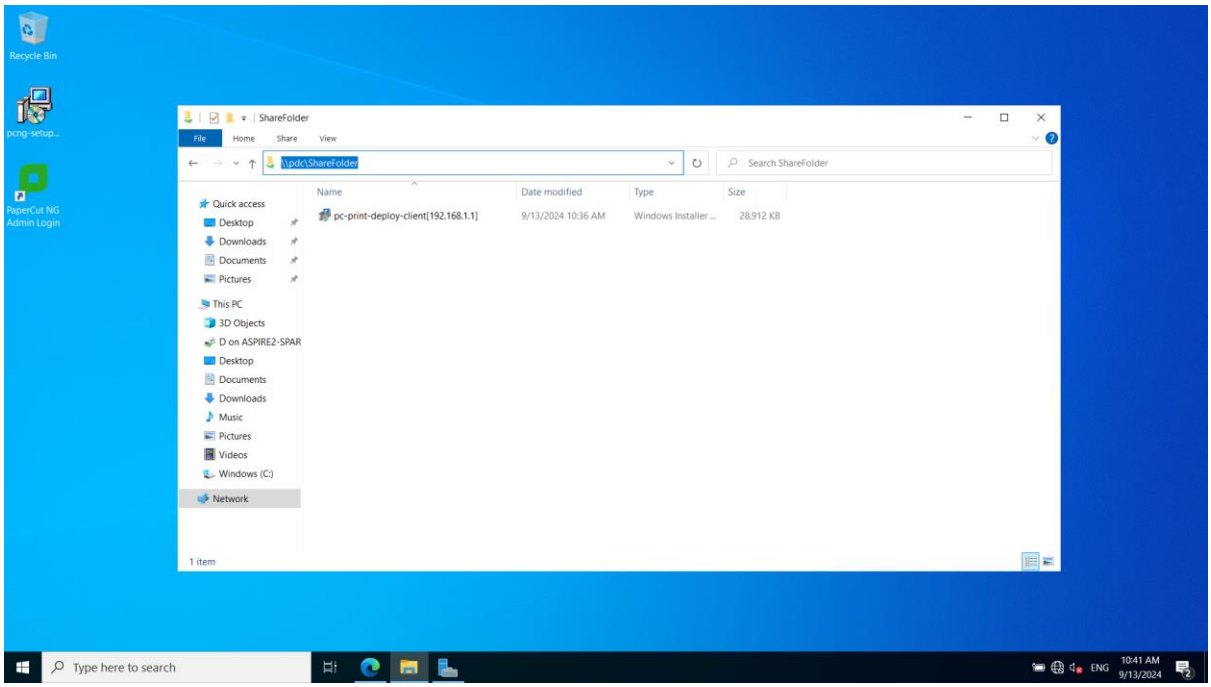
6. Generate a client software in "Zone->Client->Windows"



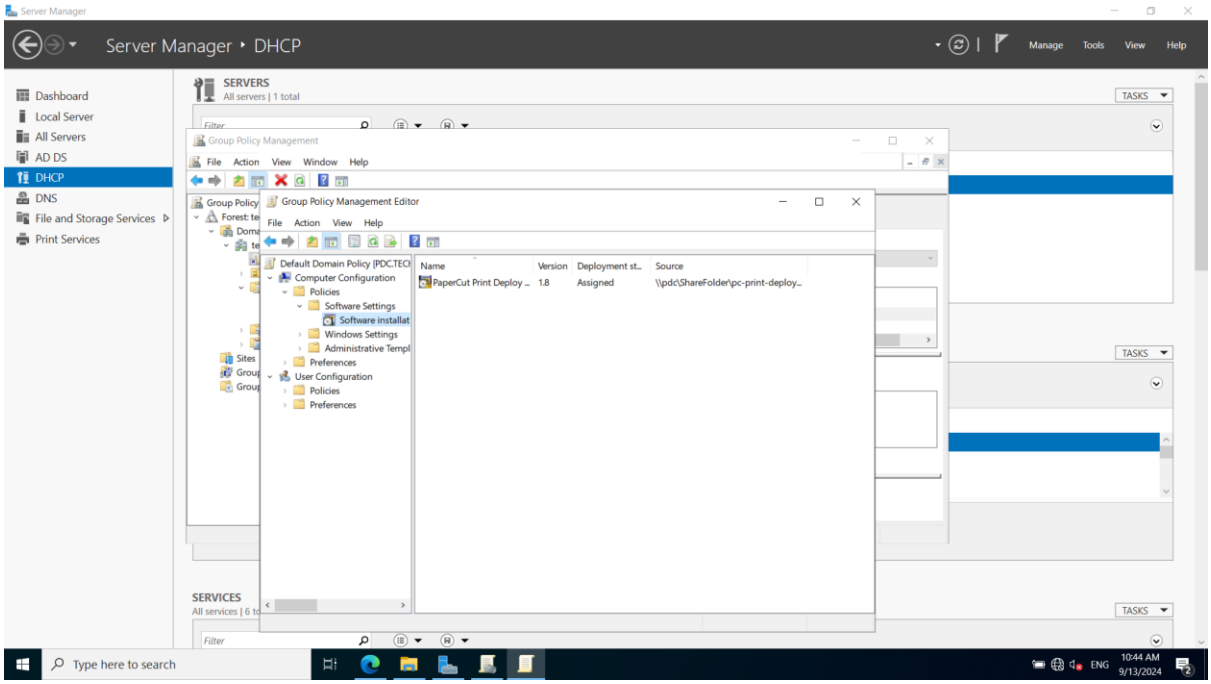
7. Create a Papercut Group Policy to deploy the client software to the client machine.

- Set up shared folder (Administrators, Domain Computers, Domain Users)

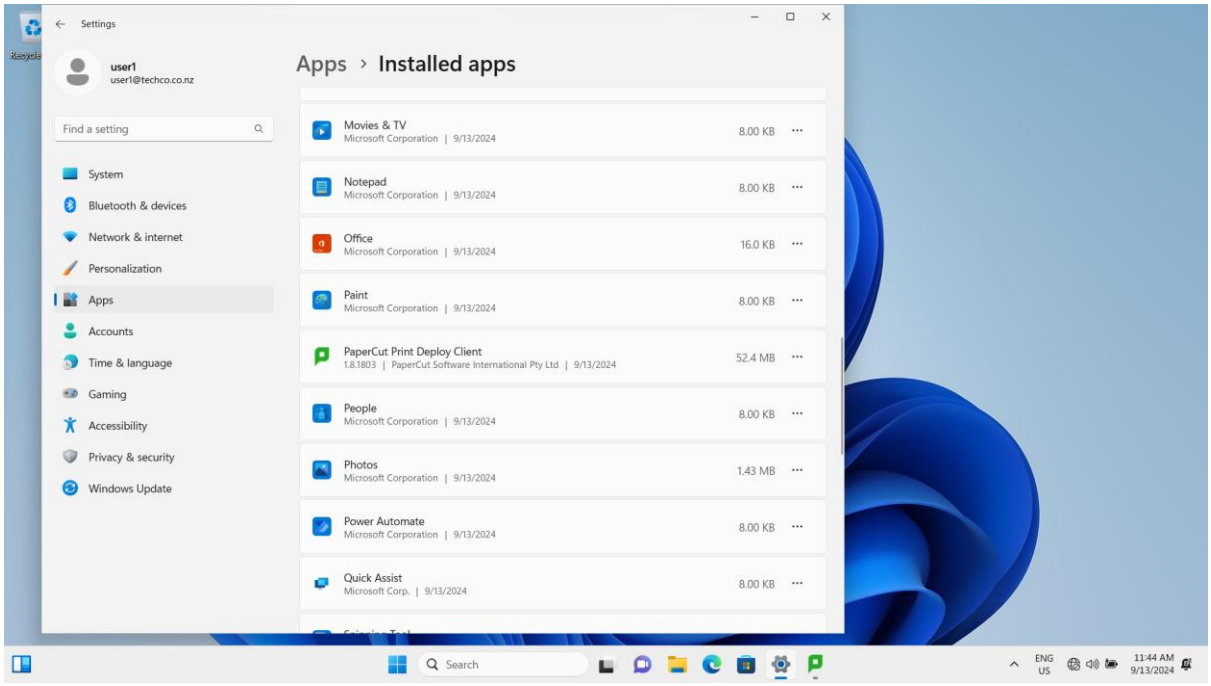


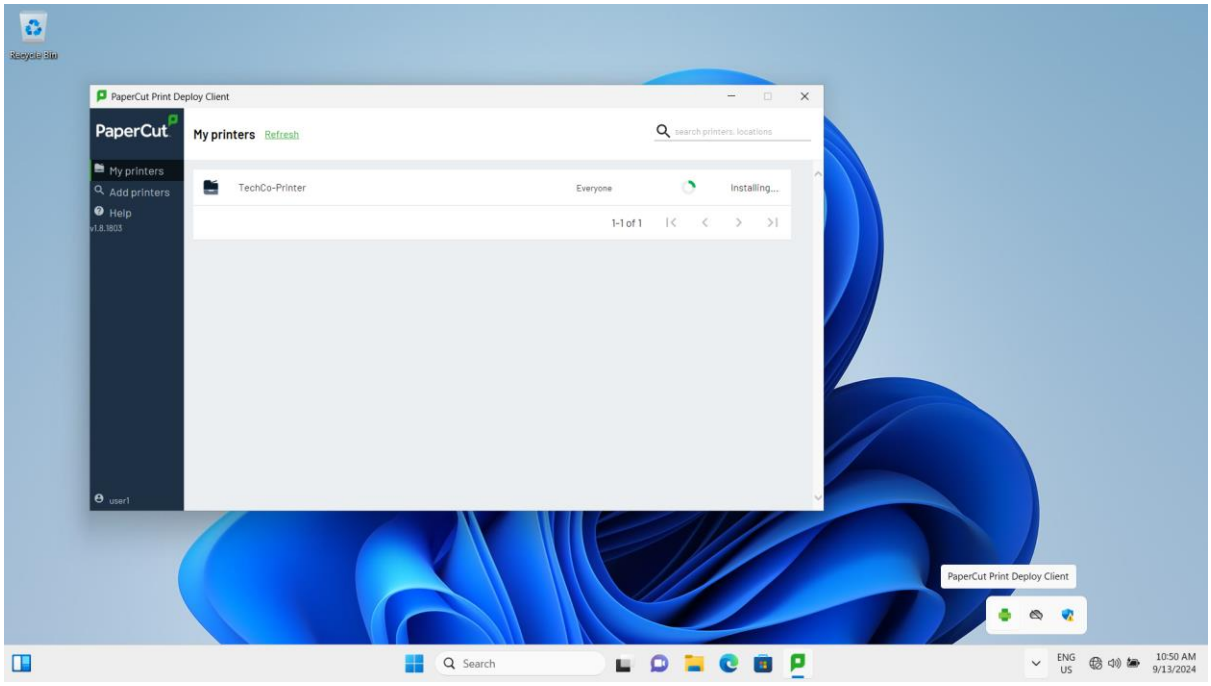


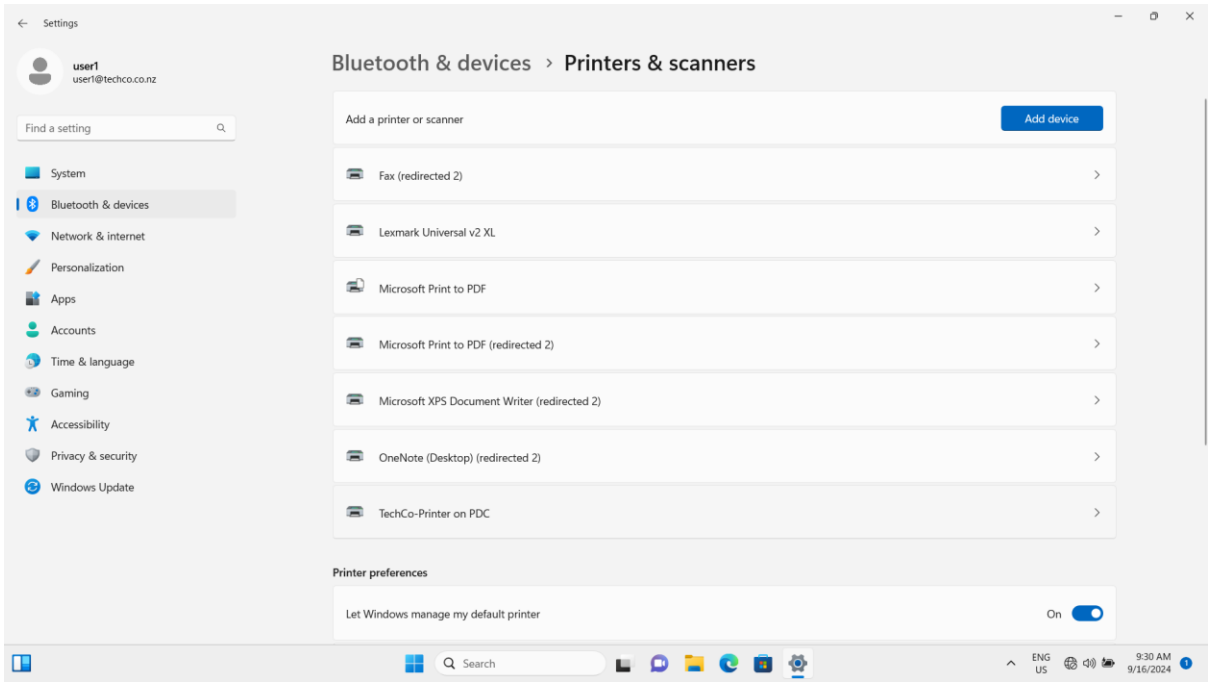
- Deploy client version of Papercut to client machine using GPO.



8. Login to the Client machine to check the client software is deployed correctly.




Recycle Bin
PaperCut Print Deploy Client
PaperCut
My printers
Refresh
My printers
Add printers
Help
v1.8.1803
TechCo-Printer
Everyone
Installing...
1-1 of 1
user1
PaperCut Print Deploy Client
Search
ENG
US
10:50 AM
9/13/2024

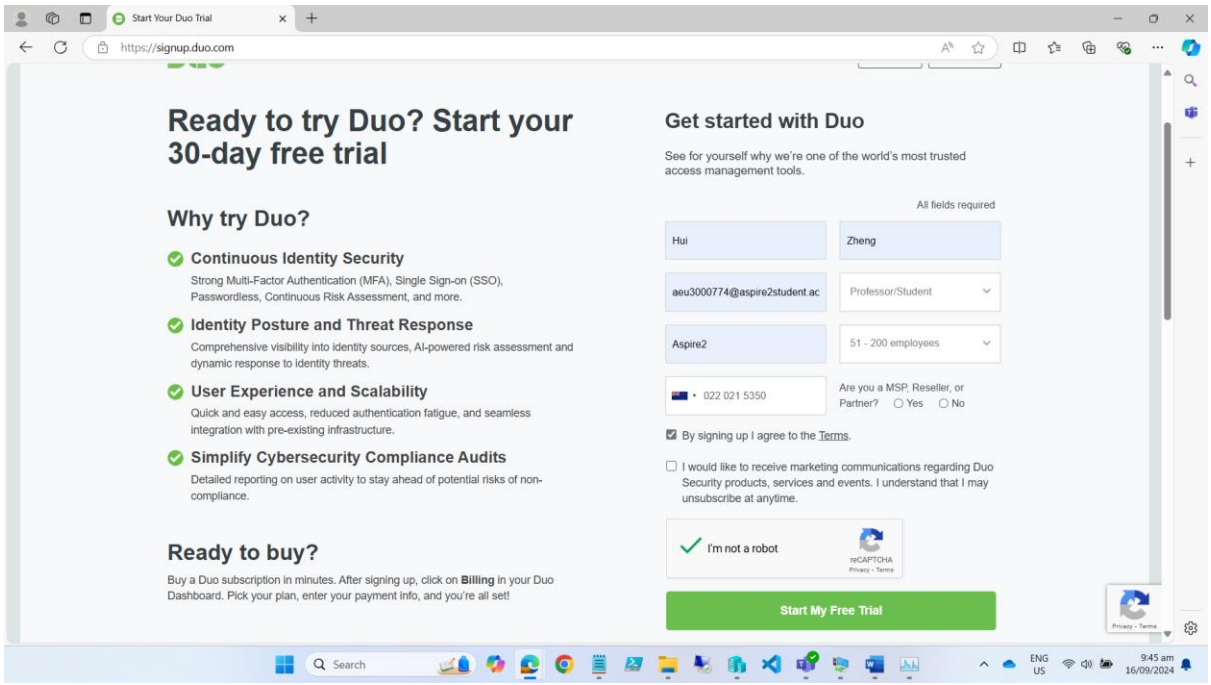

Settings
user1
user1@techco.co.nz
Find a setting
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Windows Update
Bluetooth & devices › Printers & scanners
Add a printer or scanner
Add device
Fax (redirected 2)
Lexmark Universal v2 XL
Microsoft Print to PDF
Microsoft Print to PDF (redirected 2)
Microsoft XPS Document Writer (redirected 2)
OneNote (Desktop) (redirected 2)
TechCo-Printer on PDC
Printer preferences
Let Windows manage my default printer
On
Search
ENG
US
9:30 AM
9/16/2024

Task/Mahi 3: Implementing & Managing Multi-Factor Authentication (MFA) for Network Access

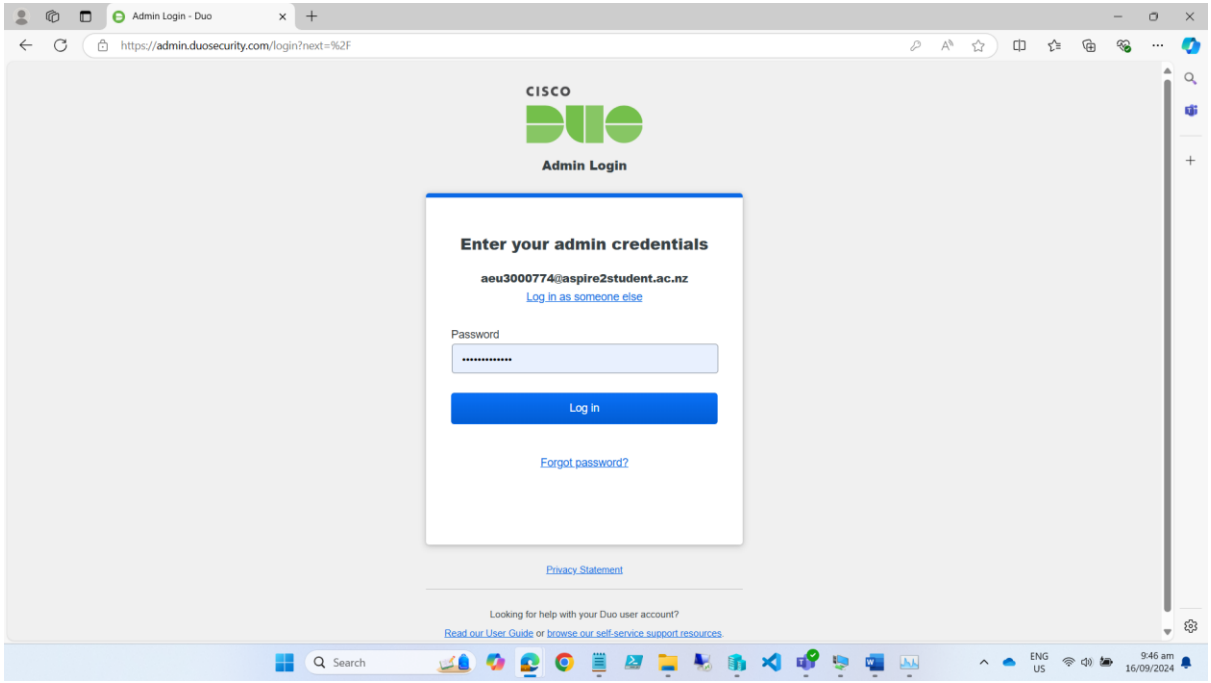
Task 3.1 Set up the MFA platform on a server and automate the deployment of MFA to the client machines

Cisco DUO provides the MFA platform which support the multiple factors authentication not only for users but also for applications on Windows, MacOS, and Android. DUO is chosen as MFA platform to strengthen TechCo Solutions network security.

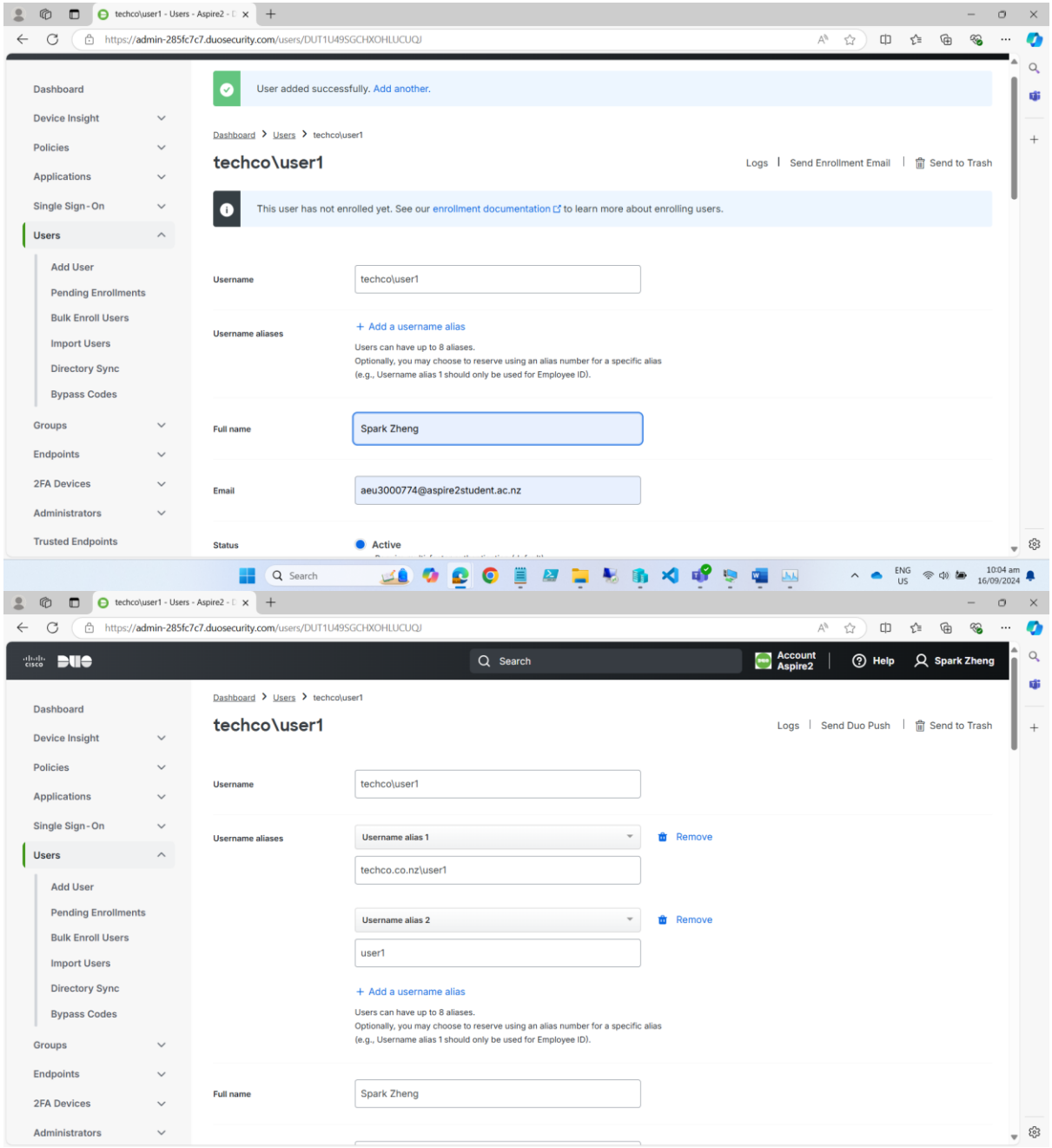
1. Sign up a new account on DUO website



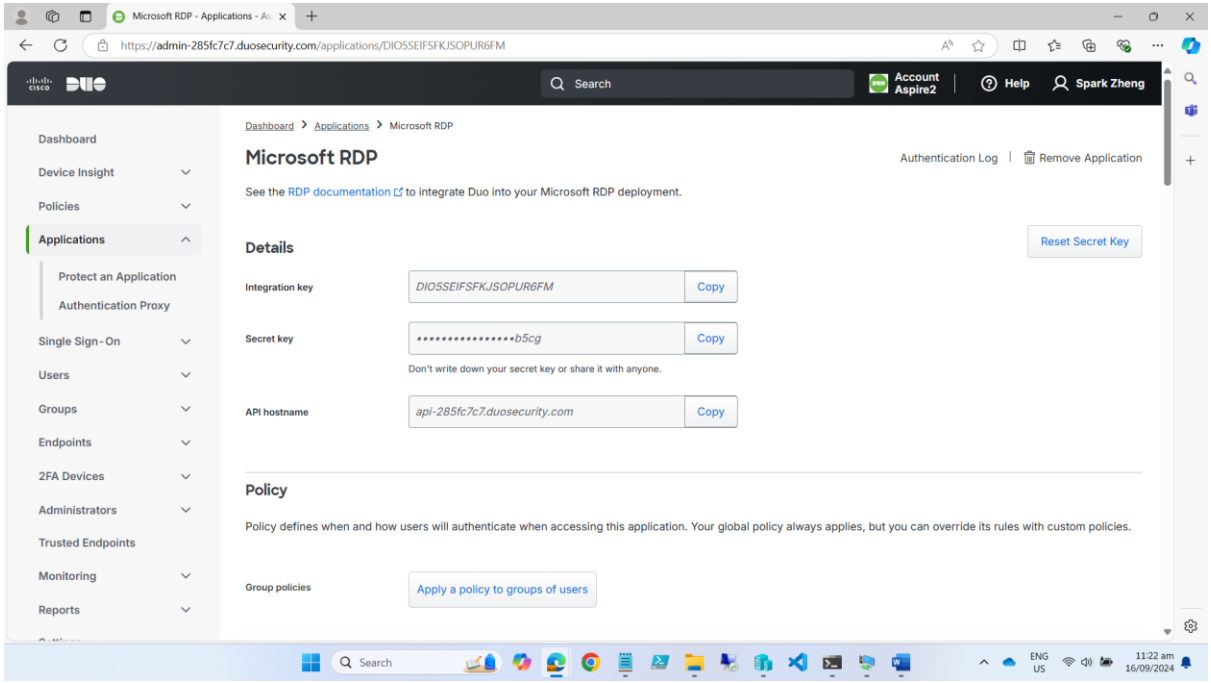
2. Log in to Admin Console



3. Add a new user “techco\user1” and send enrolment email



4. Add a new protected application: RDP and keep the credentials information



Integration key: DIO5SEIFSFKJSOPUR6FM

Secret key: bdNS18FAuPlTDCCgsz59N25IA5SfwEynPqCLb5cg

API hostname: api-285fc7c7.duosecurity.com

5. Download GPO file from DUO website

https://dl.duosecurity.com/DuoWinLogon_MSIs_Policies_and_Documentation-latest.zip

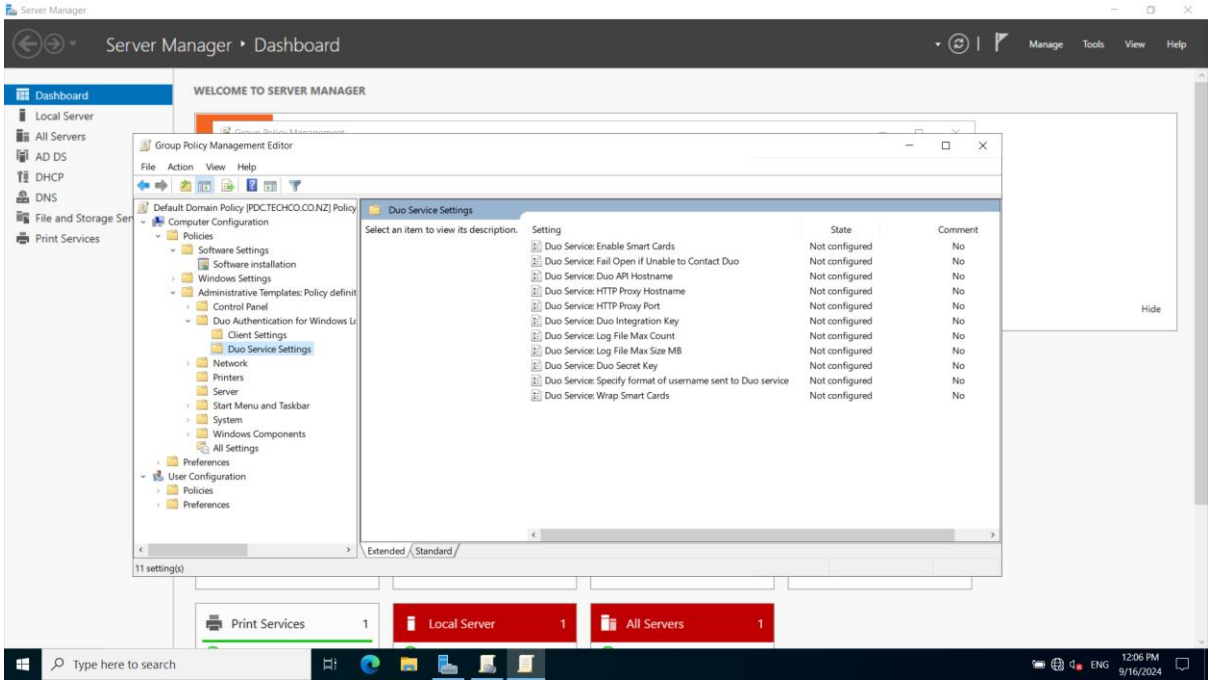
6. Copy GPO file to policy folder on the Domain Controller Server

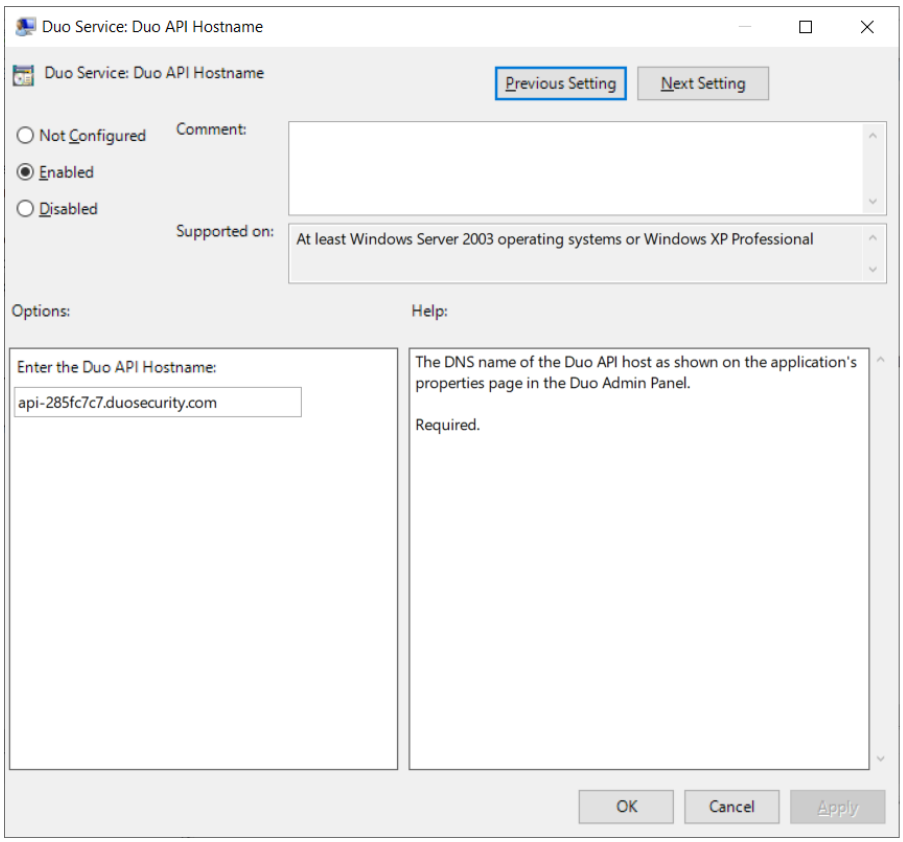
DuoWindowsLogon.admx -> C:\Windows\PolicyDefinitions\

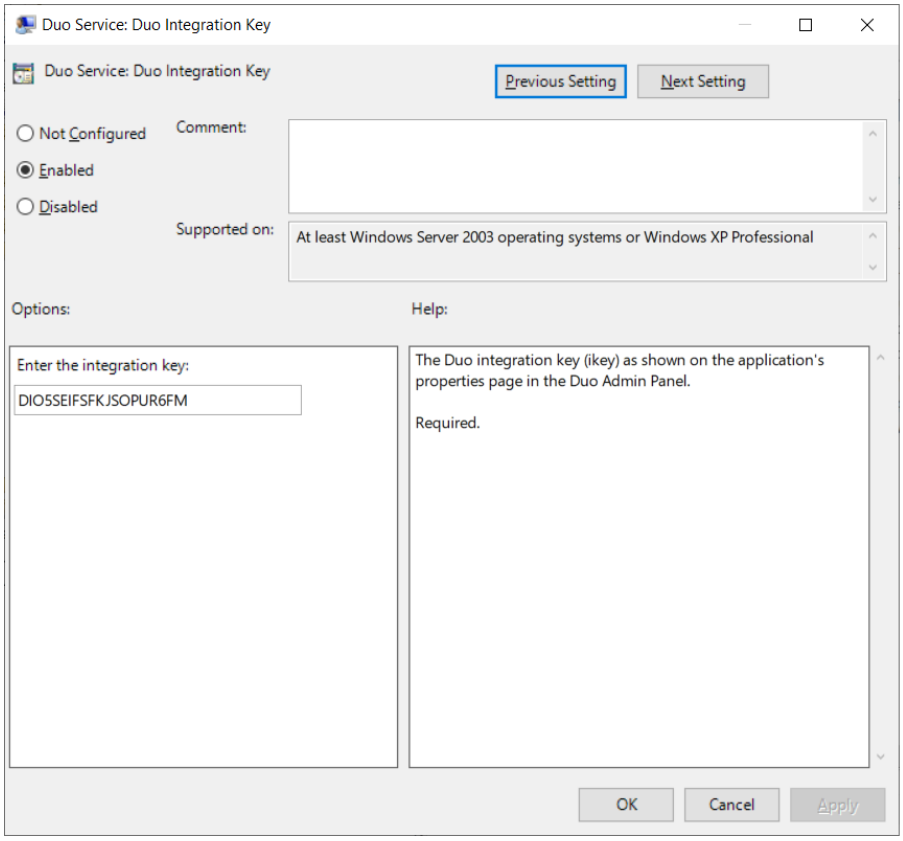
DuoWindowsLogon.adml -> C:\Windows\PolicyDefinitions\en-US\

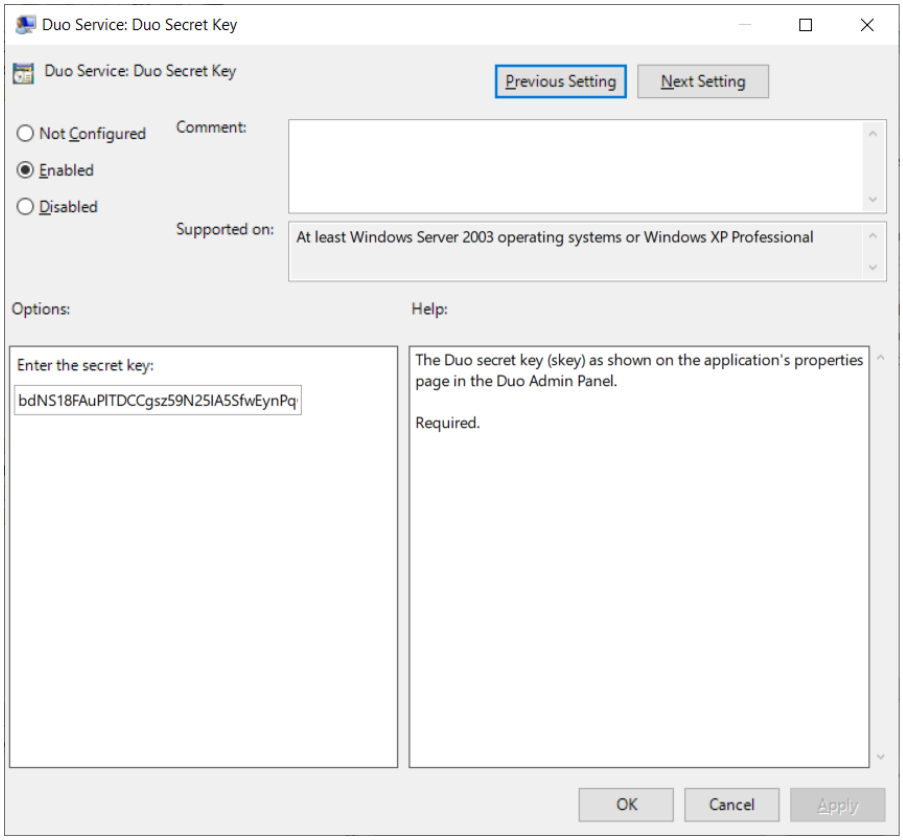
DuoWindowsLogon64.msi -> \\VMWINDOWSSERVER\ShareFolder\

7. Edit DUO related parameters in GPO of Domain Controller

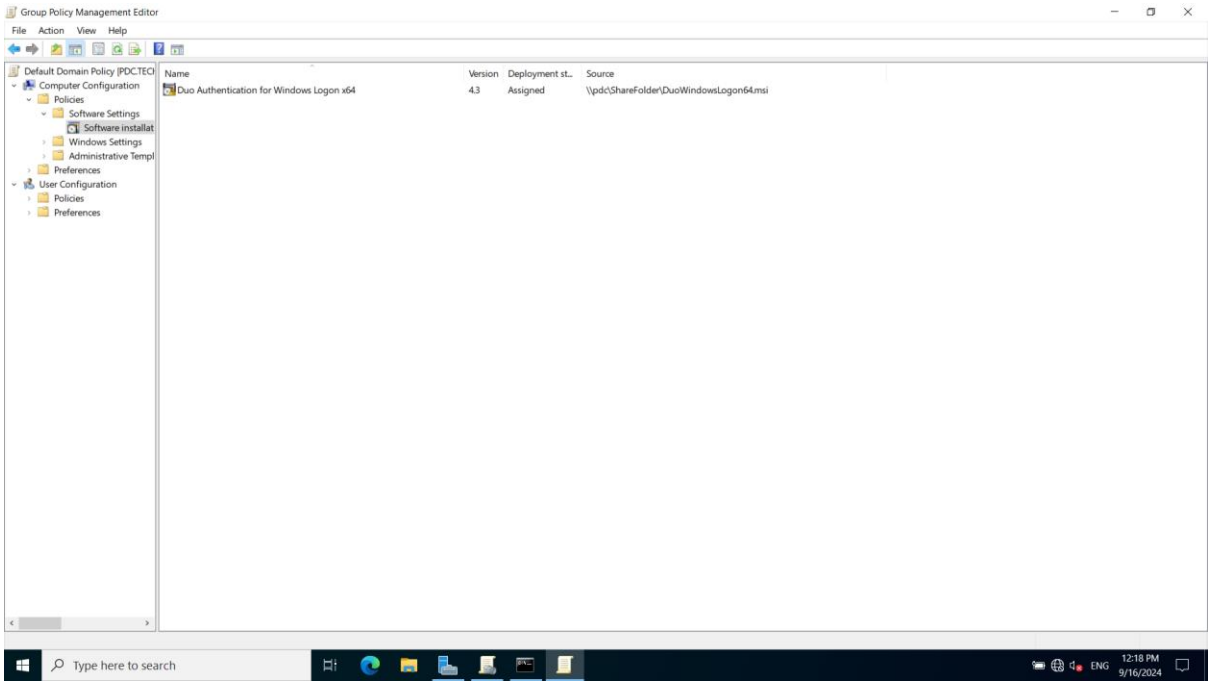




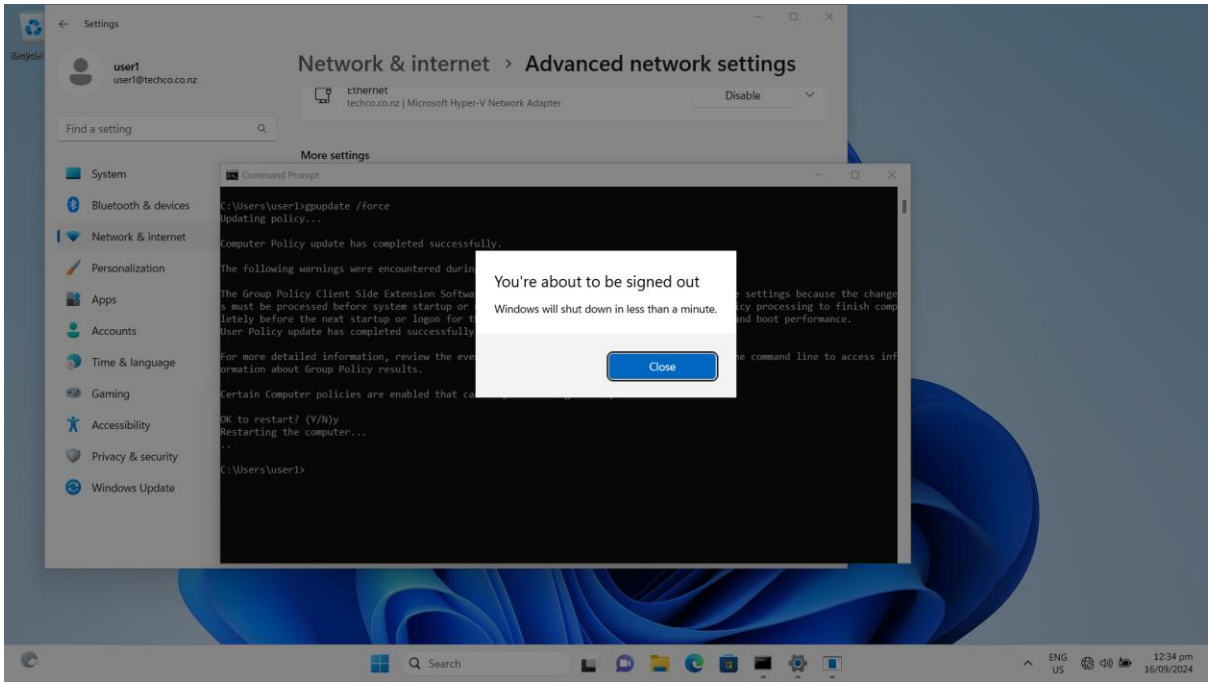

Duo Service: Duo Integration Key
Duo Service: Duo Integration Key
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Server 2003 operating systems or Windows XP Professional
Options:
Help:
Enter the integration key:
DIO5SEIFSFKJSOPUR6FM
The Duo integration key (ikey) as shown on the application's properties page in the Duo Admin Panel.
Required.
OK
Cancel
Apply

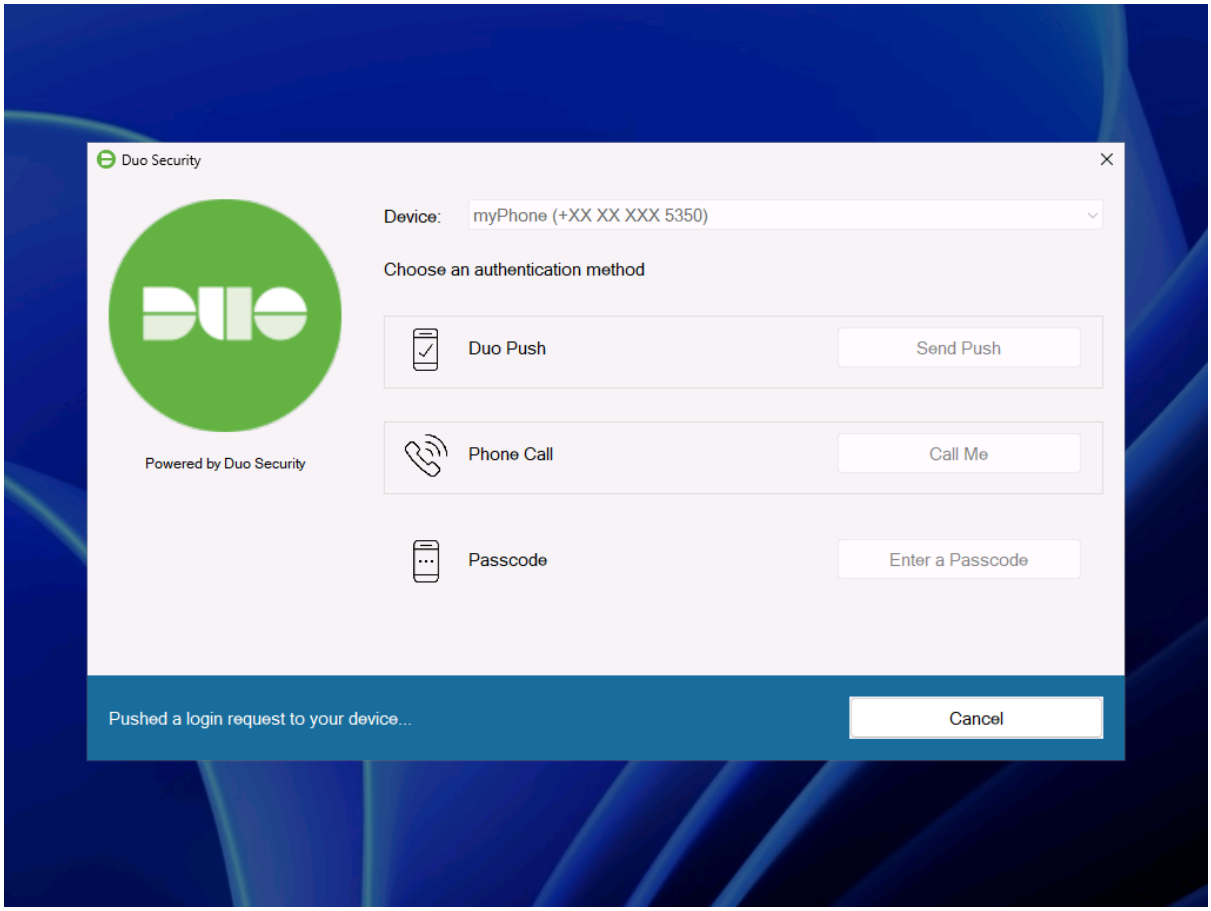

Duo Service: Duo Secret Key
Duo Service: Duo Secret Key
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Server 2003 operating systems or Windows XP Professional
Options:
Help:
Enter the secret key:
bdNS18FAuPITDCCgsz59N25IA5SfwEynPq
The Duo secret key (skey) as shown on the application's properties page in the Duo Admin Panel.
Required.
OK
Cancel
Apply

8. Add new Software installation to the GPO policy



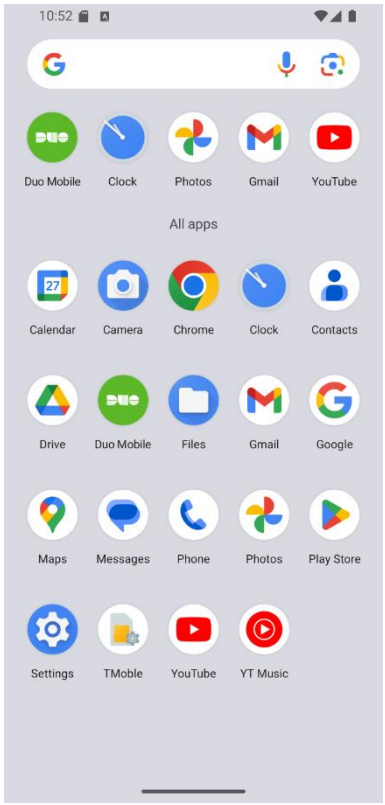
9. Login on Client machine and update group policy

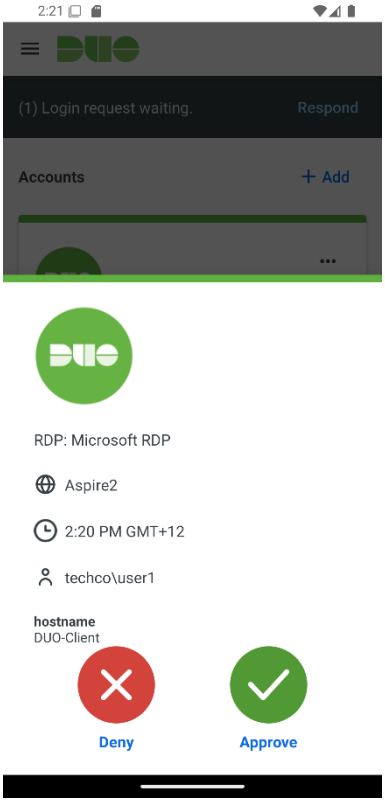



Duo Security
Device:
myPhone (+XX XX XXX 5350)
Choose an authentication method
Duo Push
Send Push
Phone Call
Call Me
Passcode
Enter a Passcode
Powered by Duo Security
Pushed a login request to your device...
Cancel

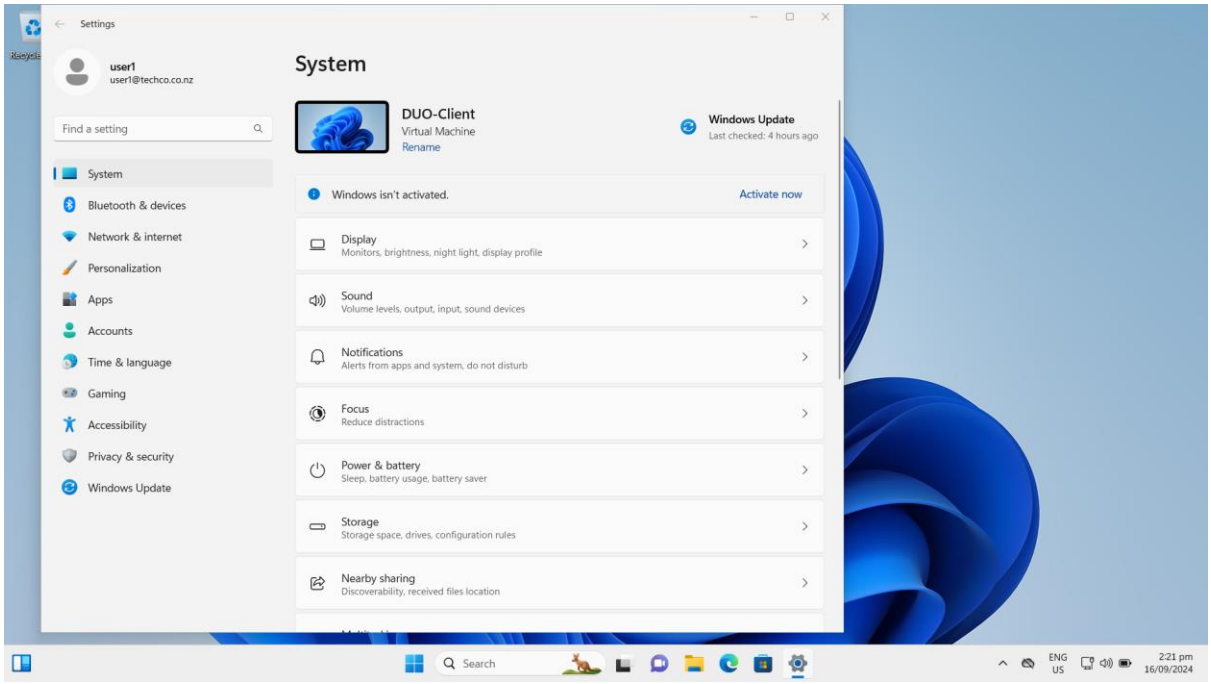
10. Active mobile phone and approve the client login request

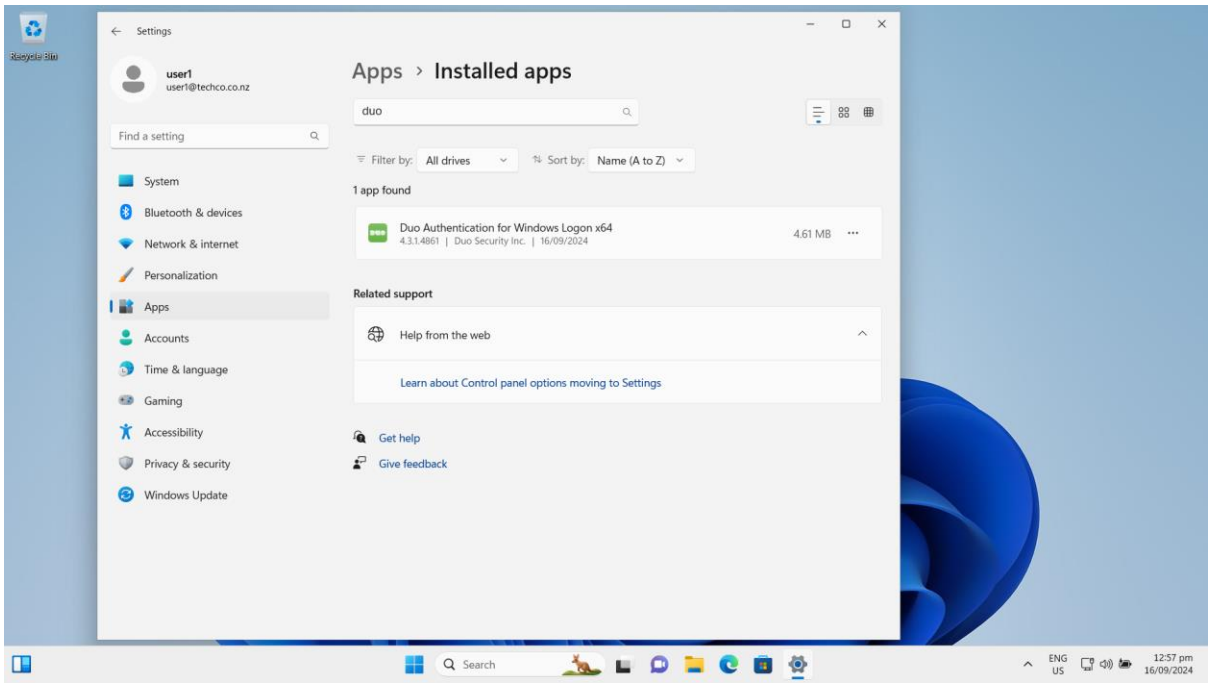
- copy and paste active link into Duo Mobile manually: https://m-285fc7c7.duosecurity.com/activate/83nFnX6BN7Aj7pBIOmAw





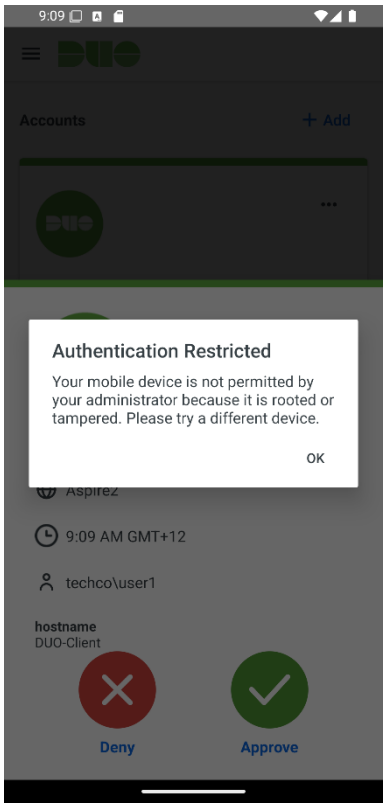
11. Client machine logged in with DUO app installed.



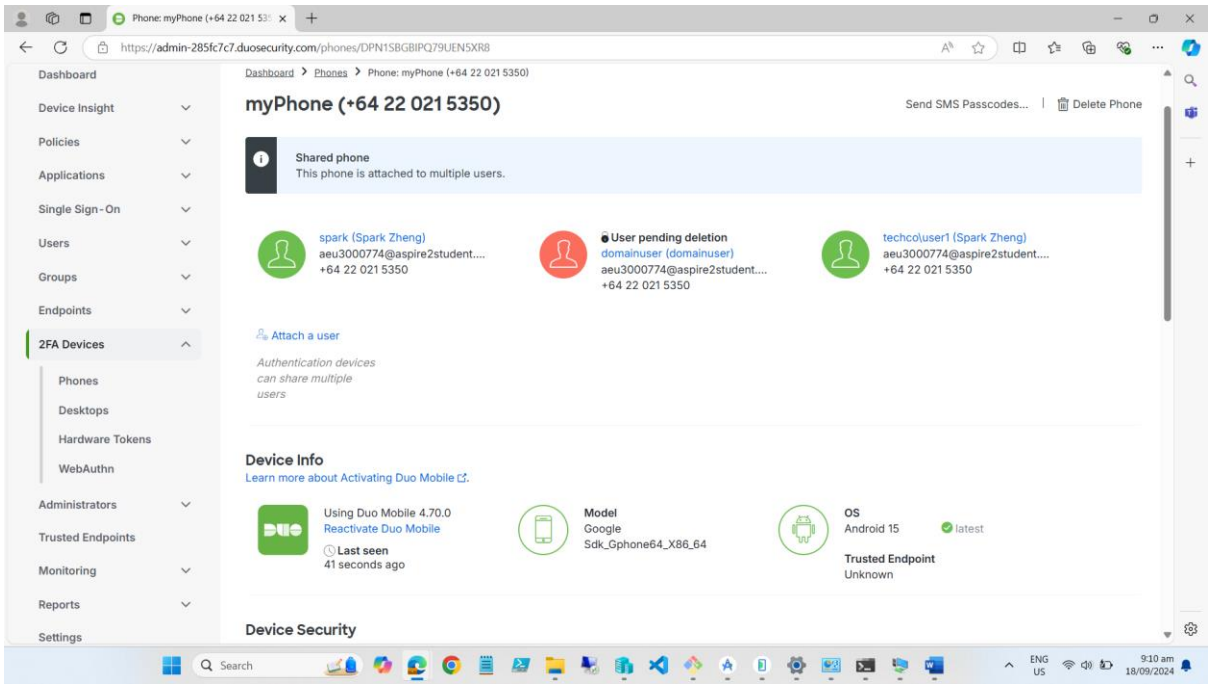


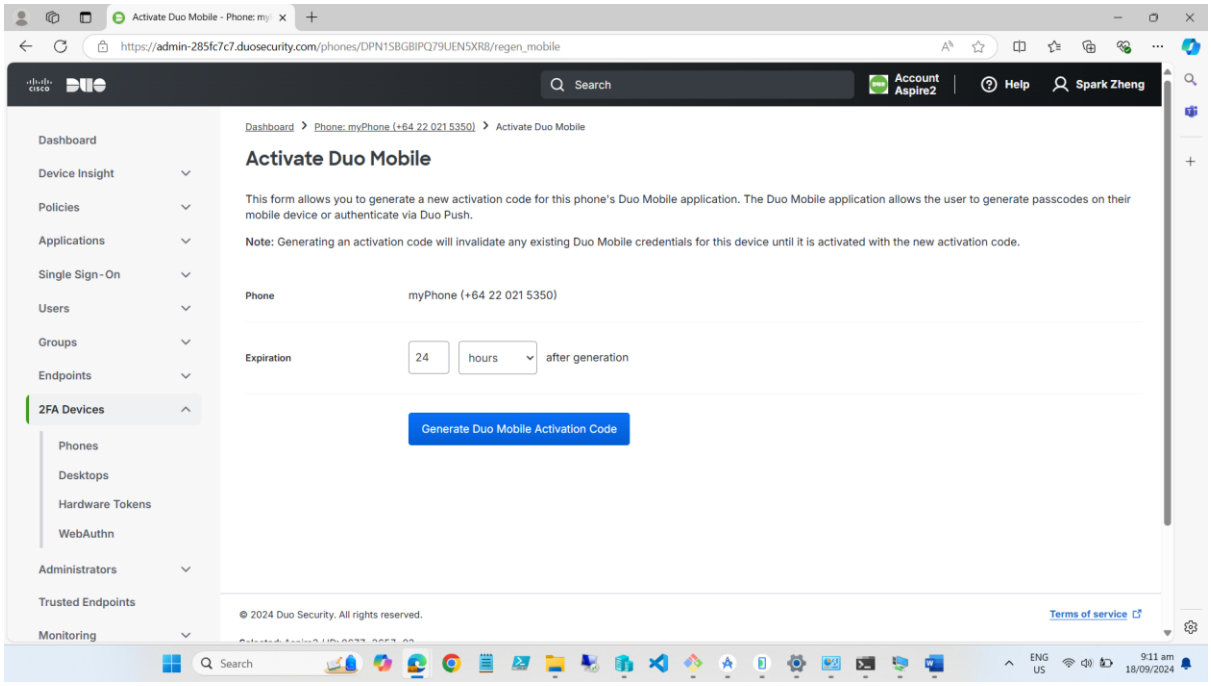
Task 3.2 Troubleshooting the MFA configurations on a client machine and MFA Admin App

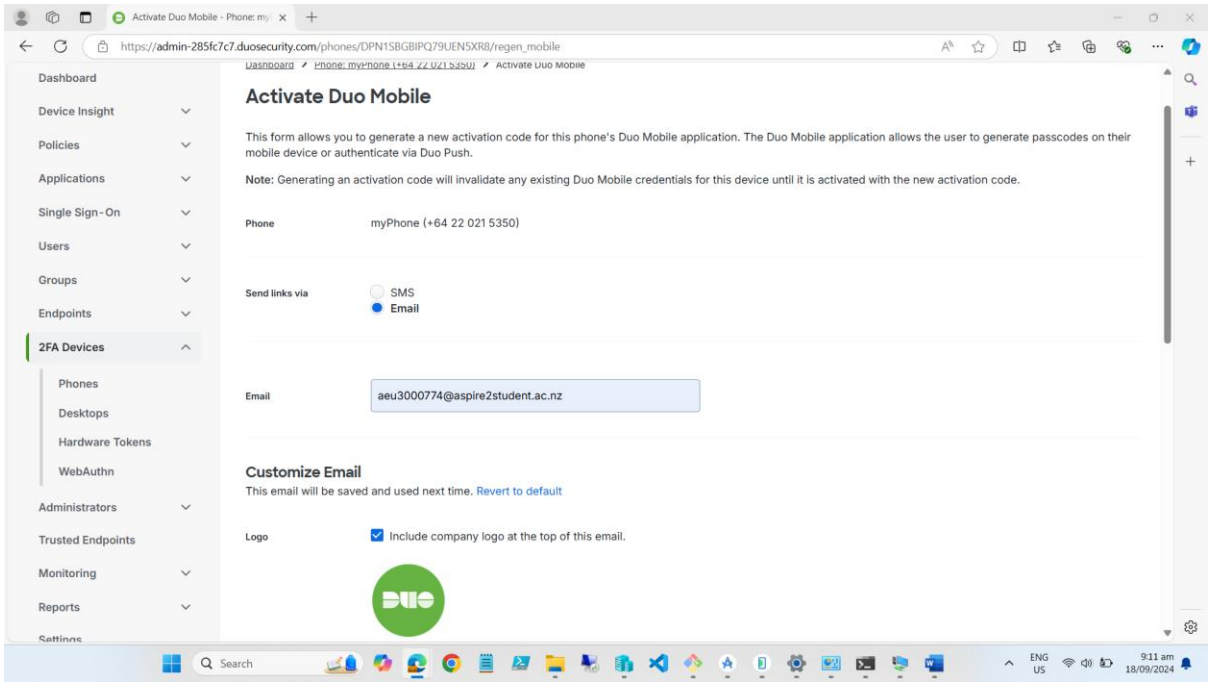
1. Mobile device is restricted for the privilege of approvement and needs to be reactivated.

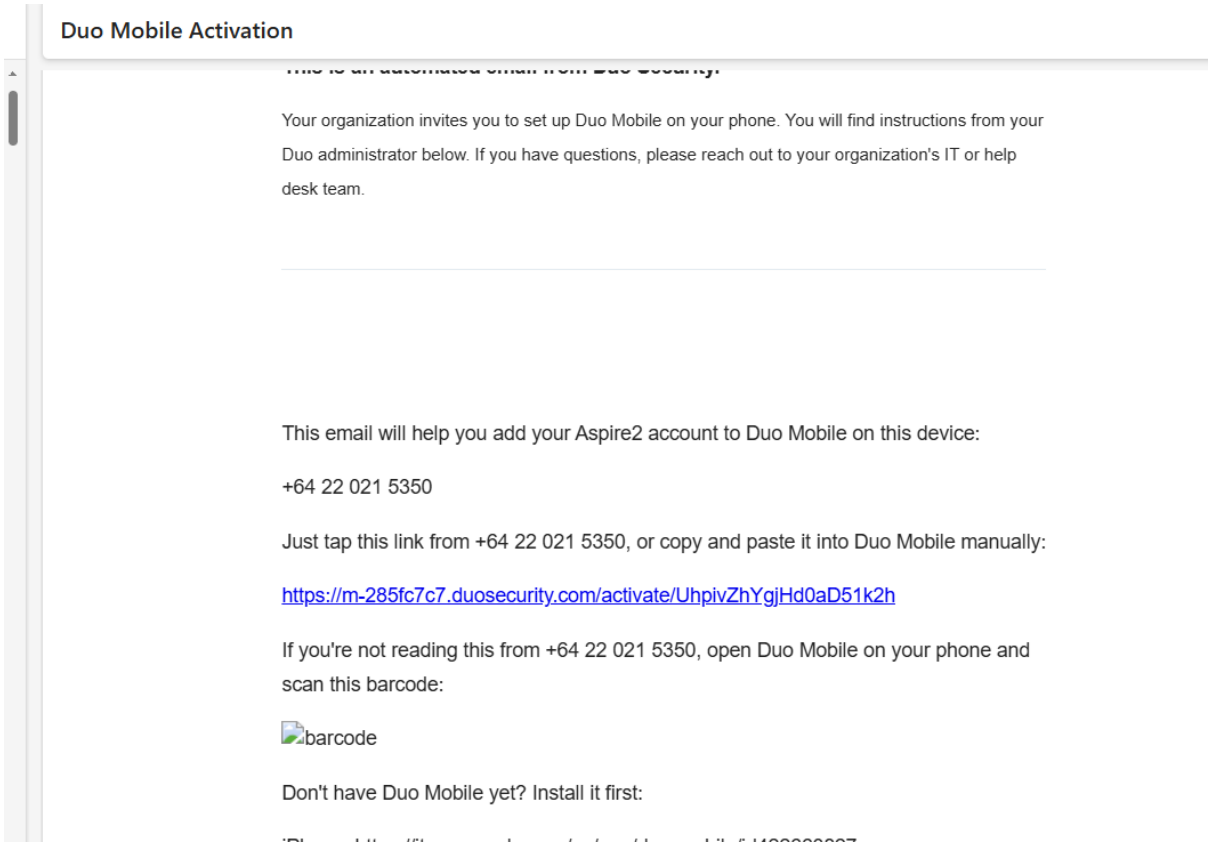


2. Reactivate the mobile device and send notification email









Duo Mobile Activation

Your organization invites you to set up Duo Mobile on your phone. You will find instructions from your Duo administrator below. If you have questions, please reach out to your organization's IT or help desk team.

This email will help you add your Aspire2 account to Duo Mobile on this device:

+64 22 021 5350

Just tap this link from +64 22 021 5350, or copy and paste it into Duo Mobile manually:

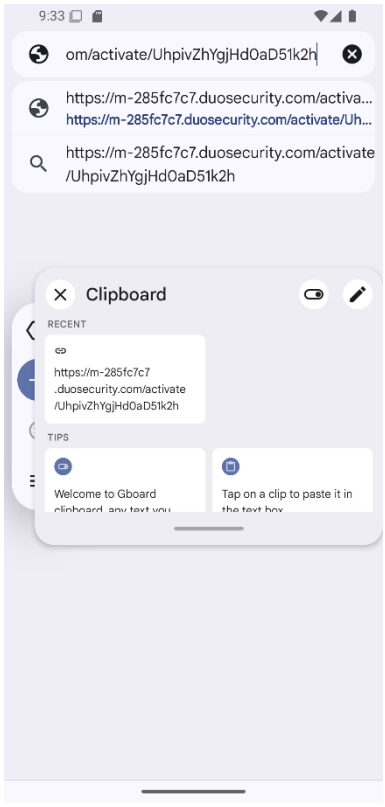
https://m-285fc7c7.duosecurity.com/activate/UhpivZhYgjHd0aD51k2h

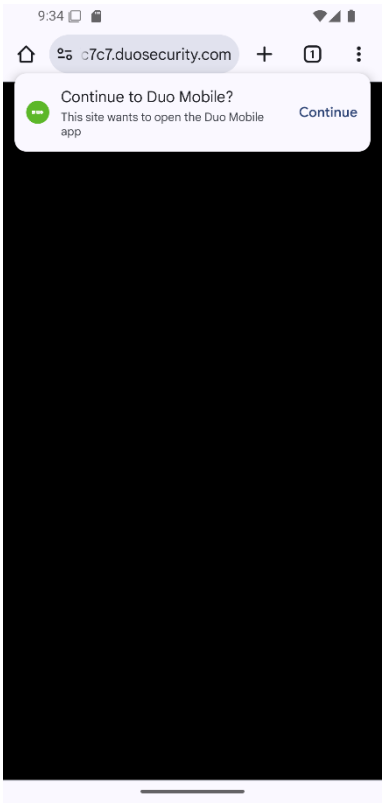
If you're not reading this from +64 22 021 5350, open Duo Mobile on your phone and scan this barcode:

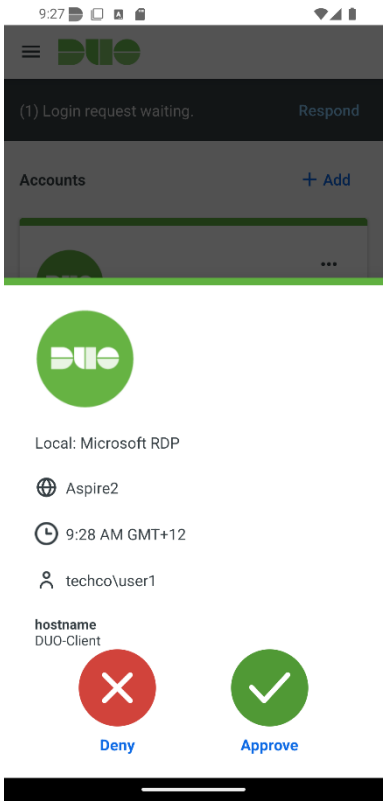
barcode

Don't have Duo Mobile yet? Install it first:

3. Access reactivating link on the mobile device and the issue is resolved.



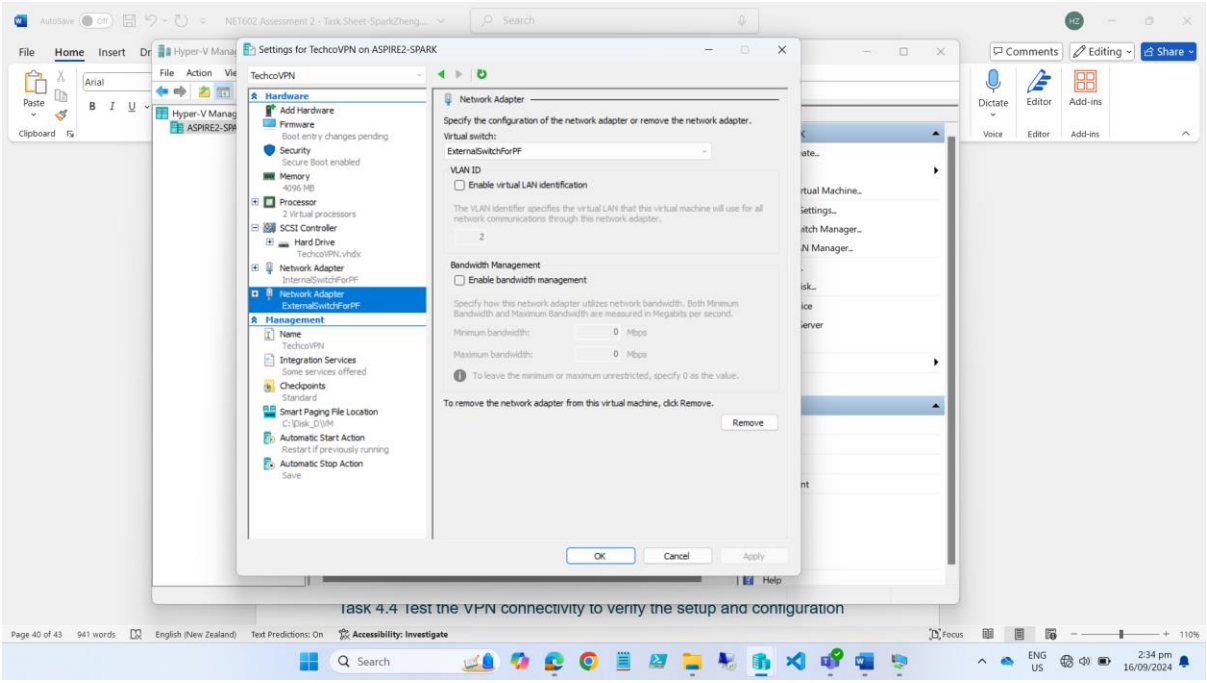




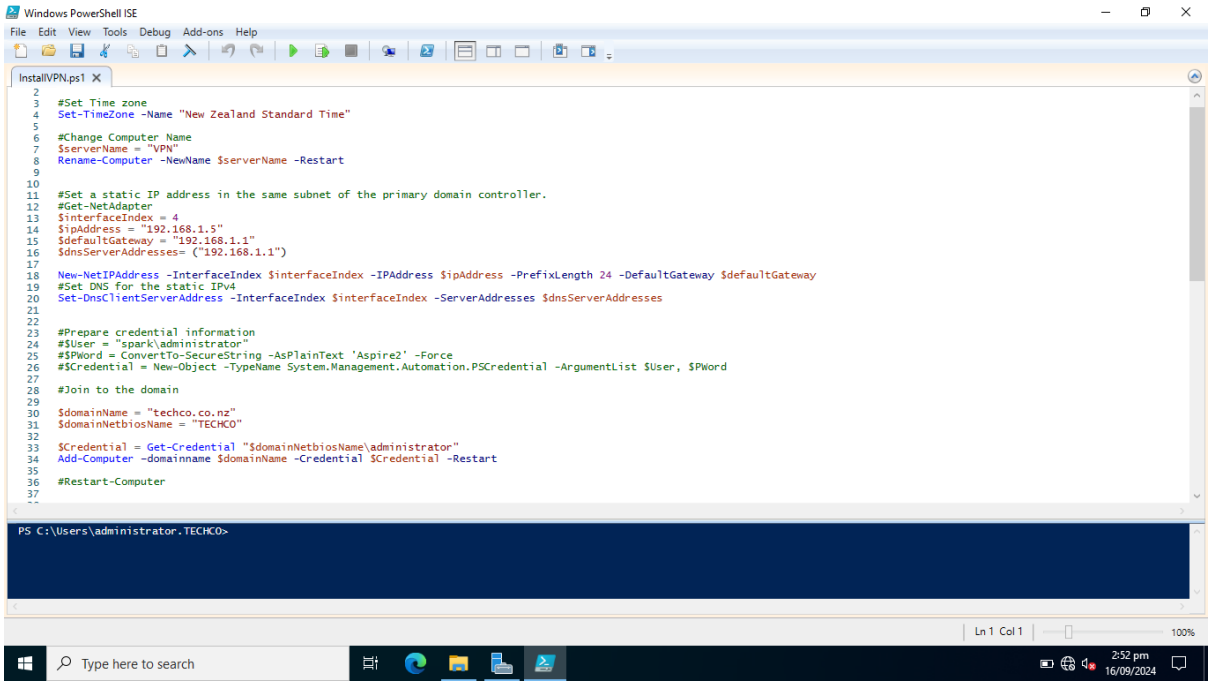
Task/Mahi 4: Manage the remote access via VPN

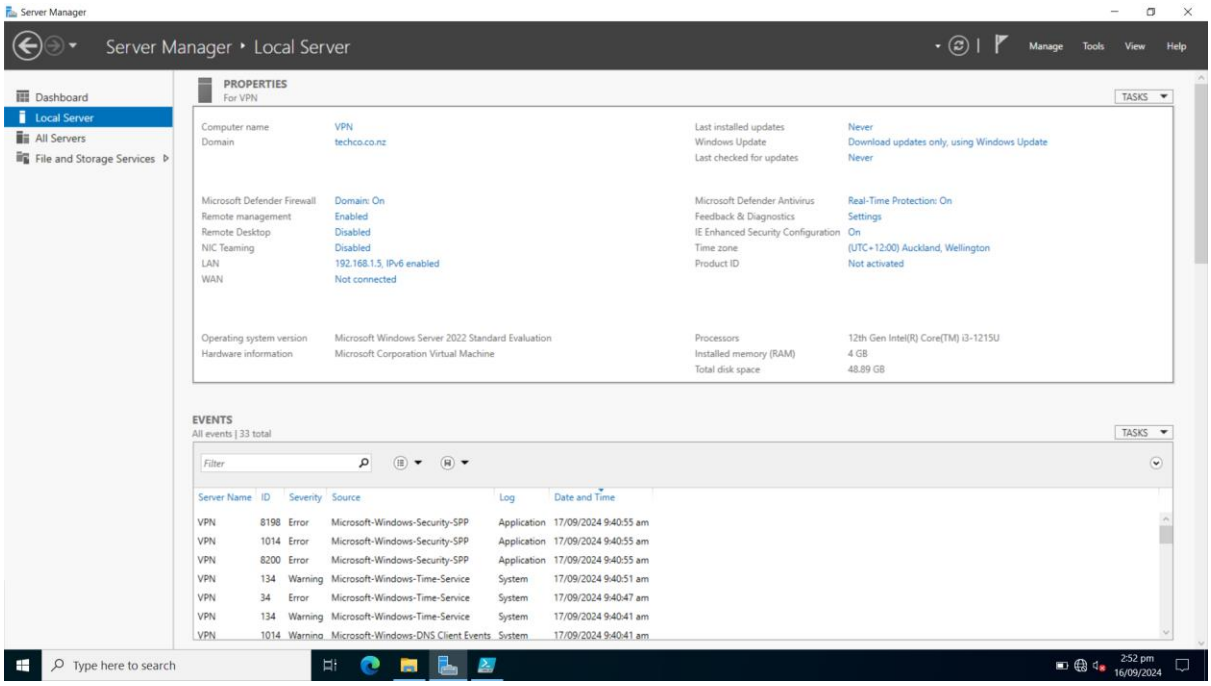
Task 4.1 Set up and configure a member server of the domain to act as a VPN server

1. Create a new virtual machine with 2 network adapters

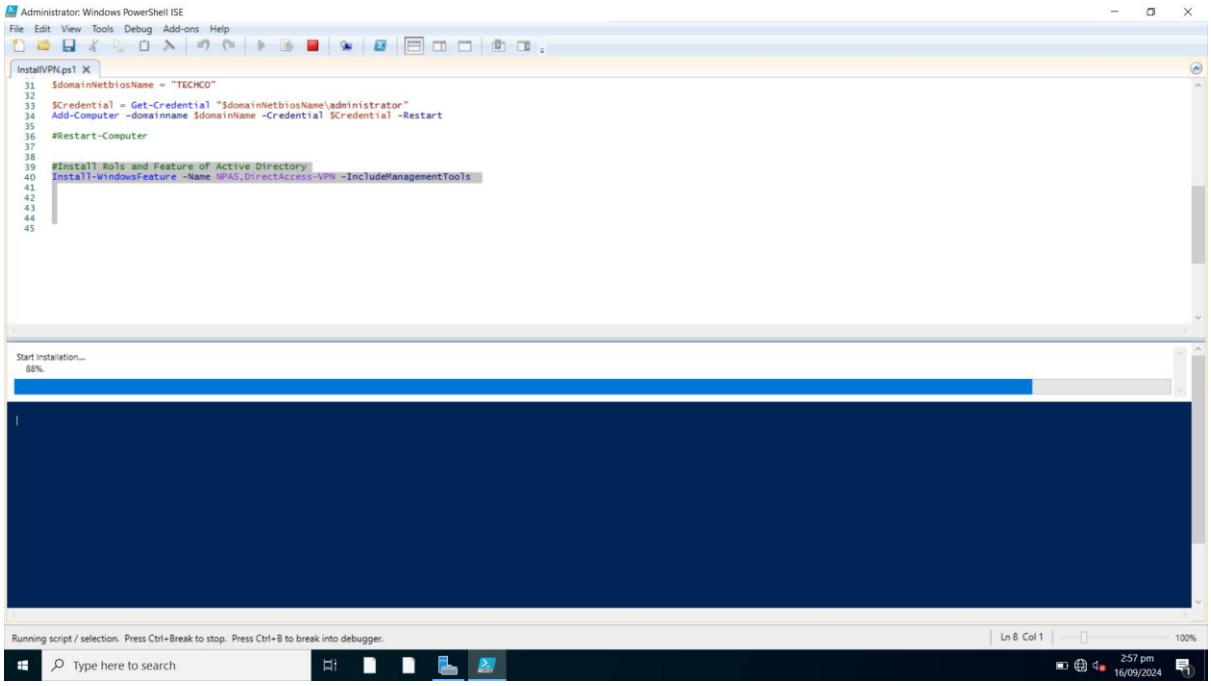


2. Add the new virtual machine to domain “techco.co.nz”

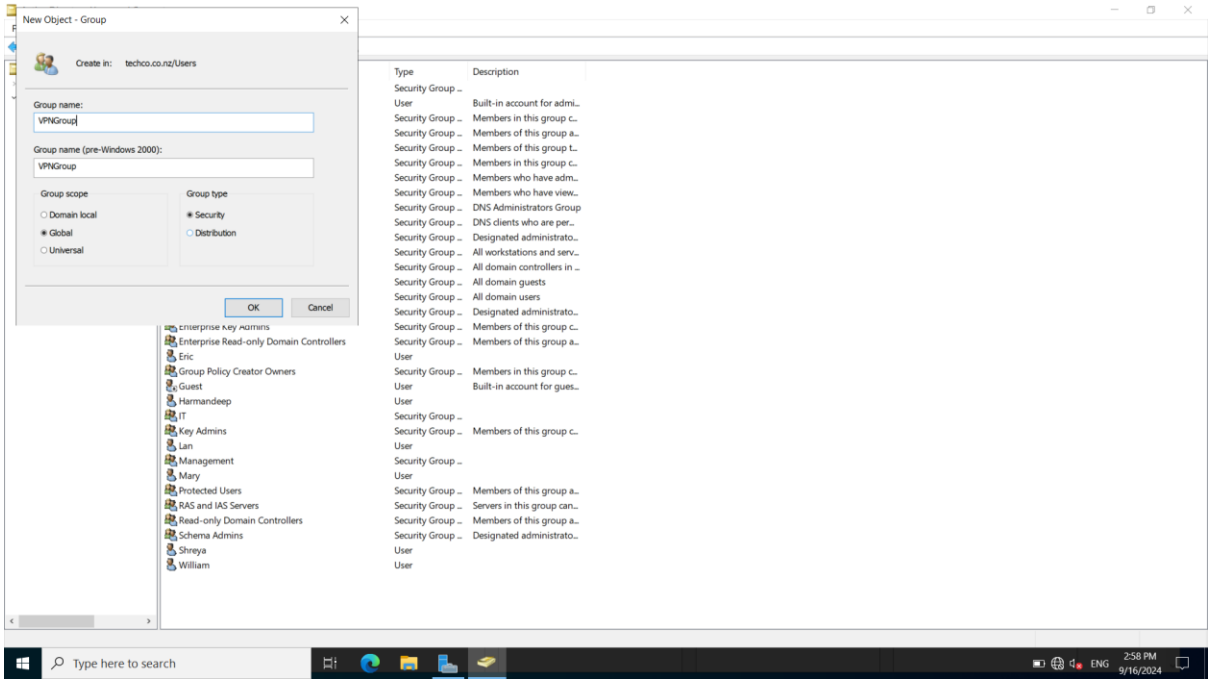


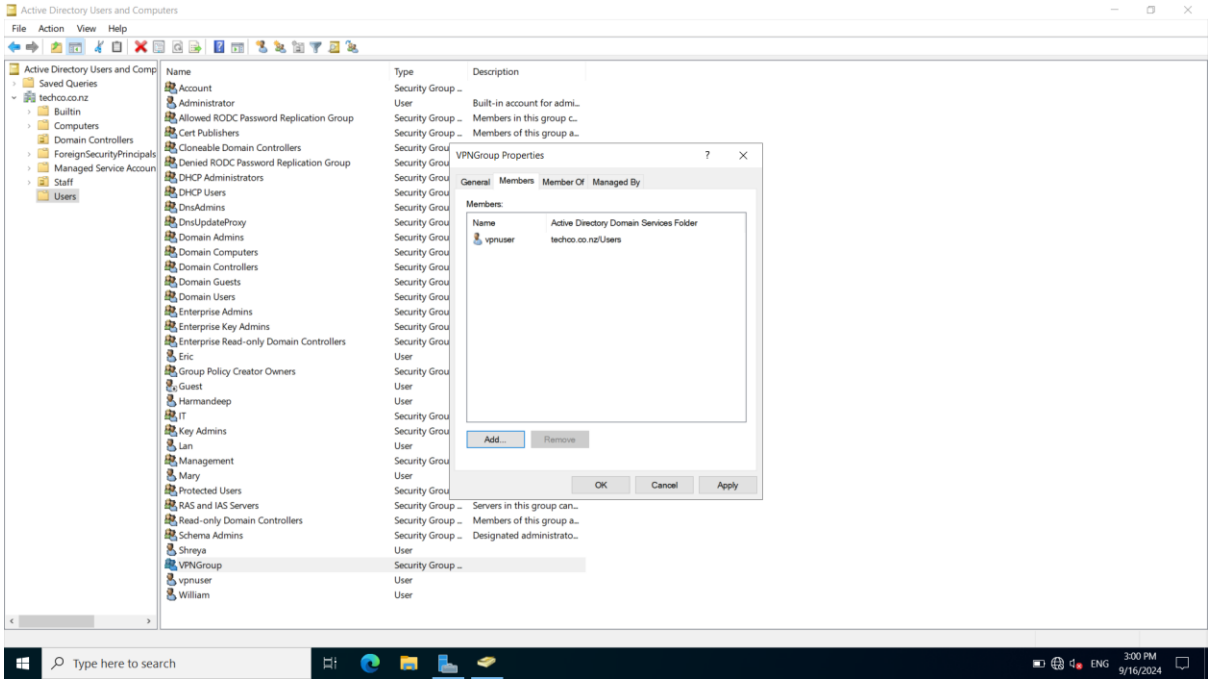


3. Add Roles and Features of NPAS and DirectAccess-VPN

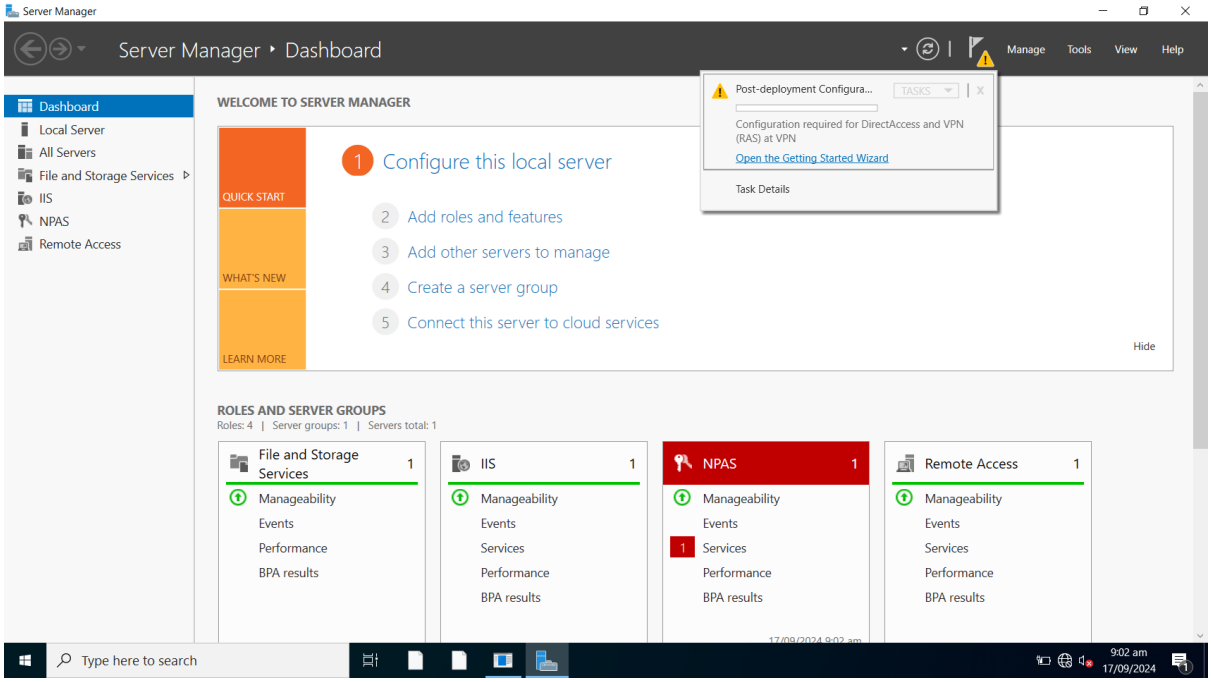


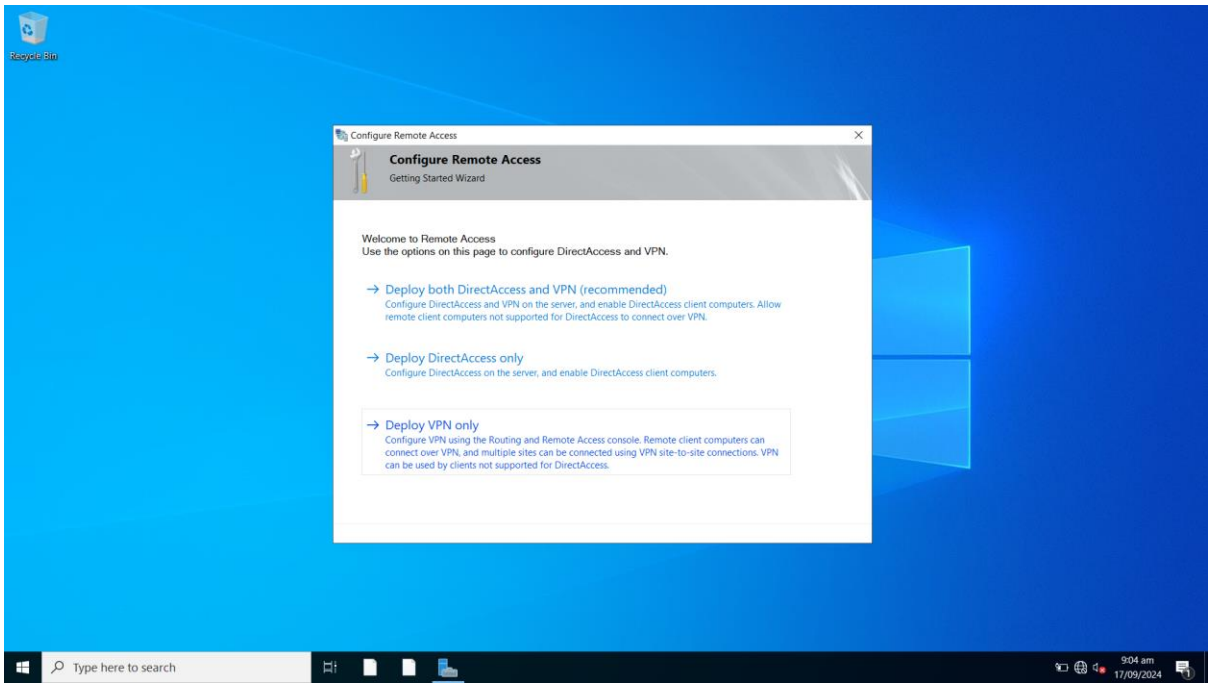
4. Create new VPN group and VPN users

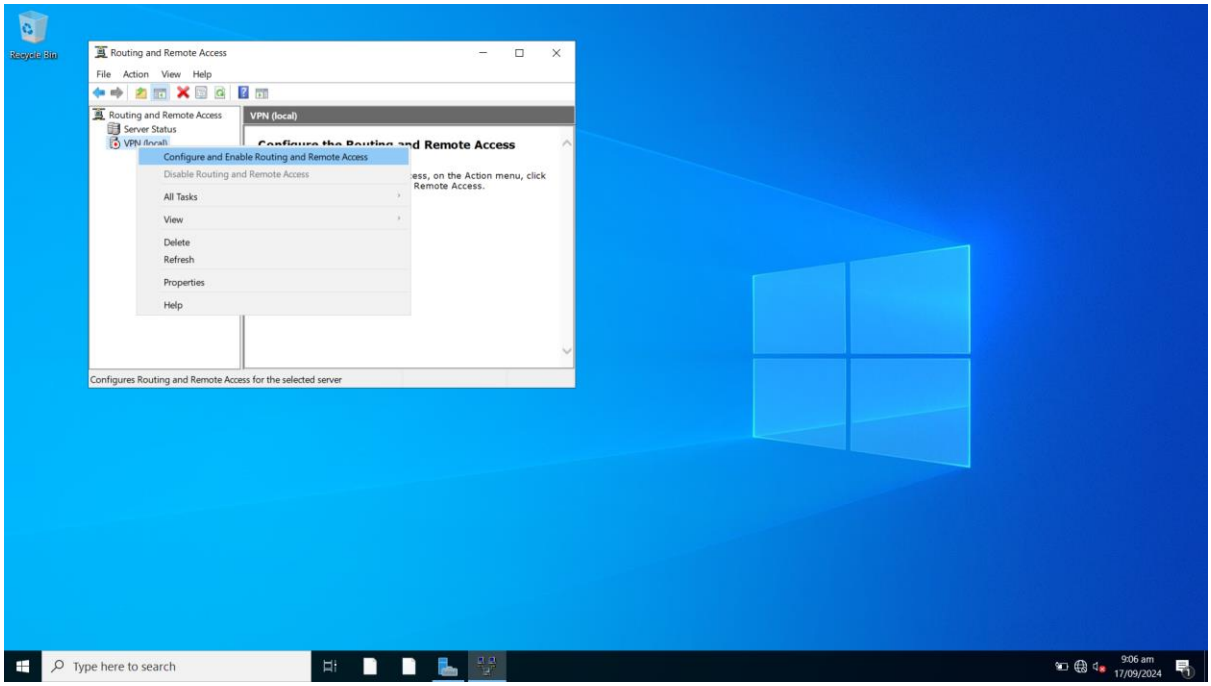


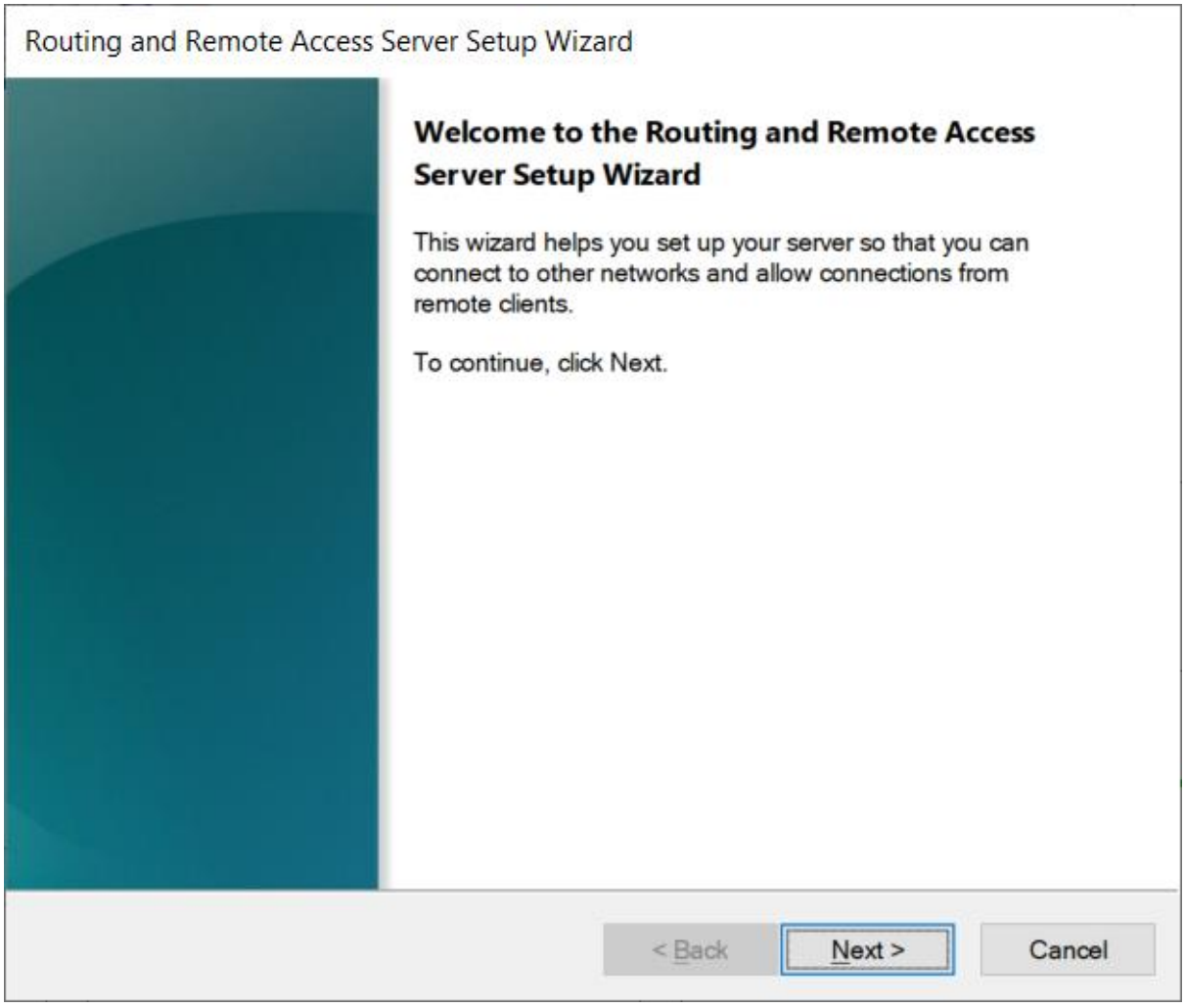


5. Configure DirectAccess and VPN

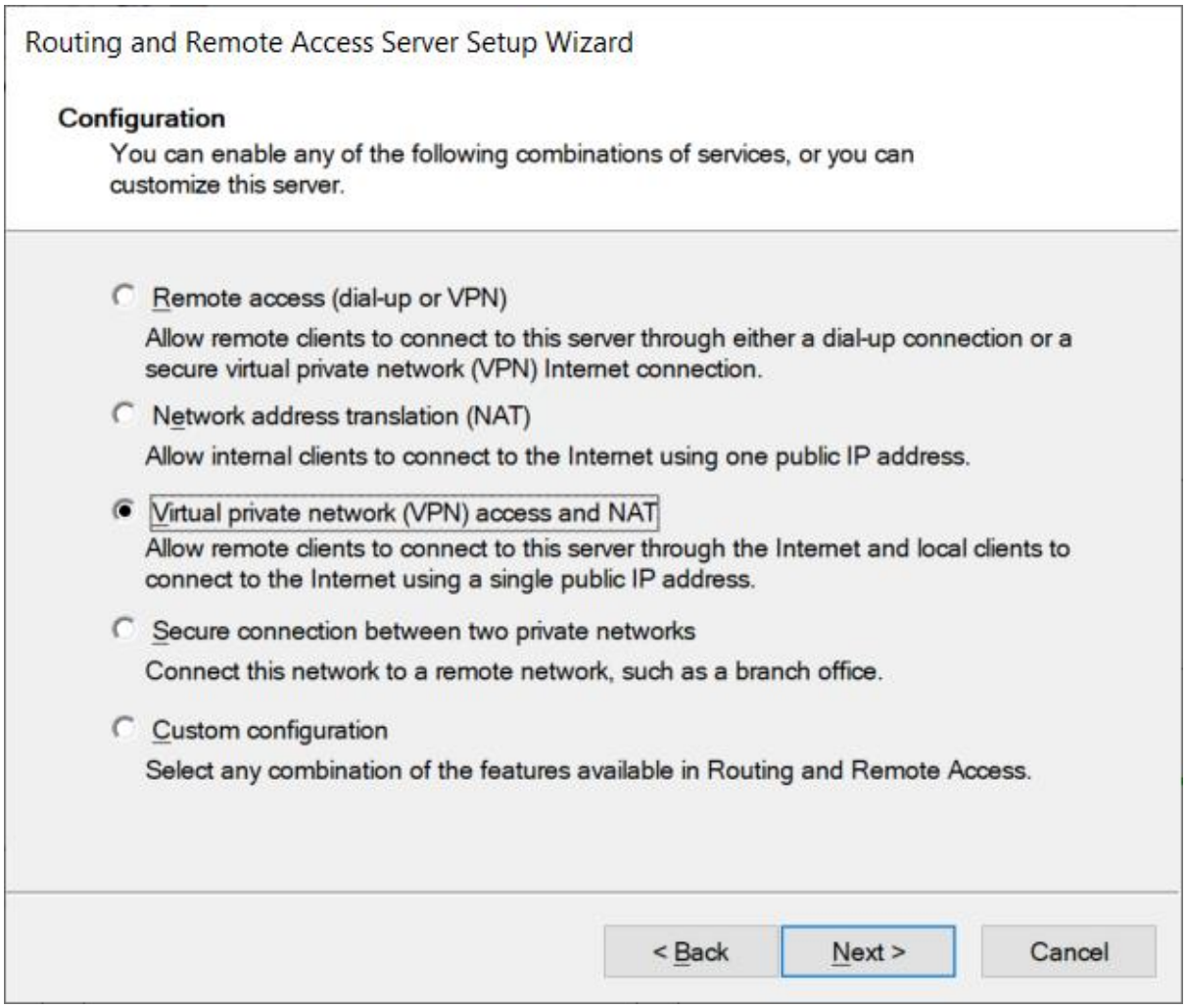


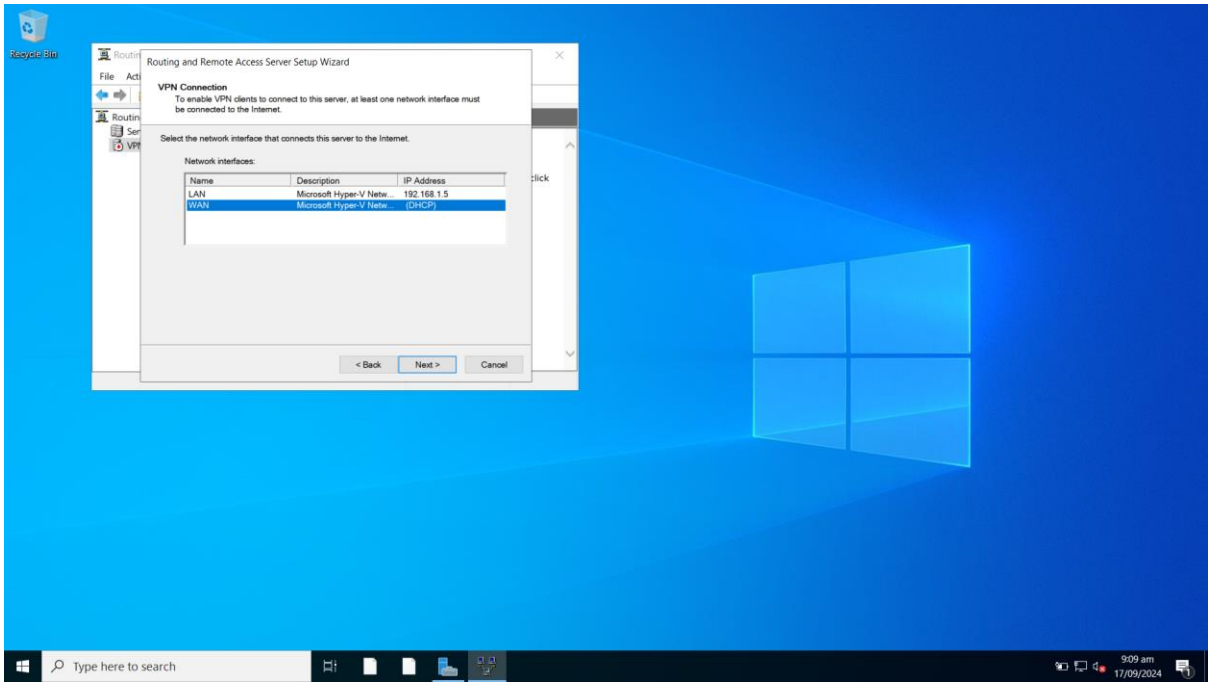


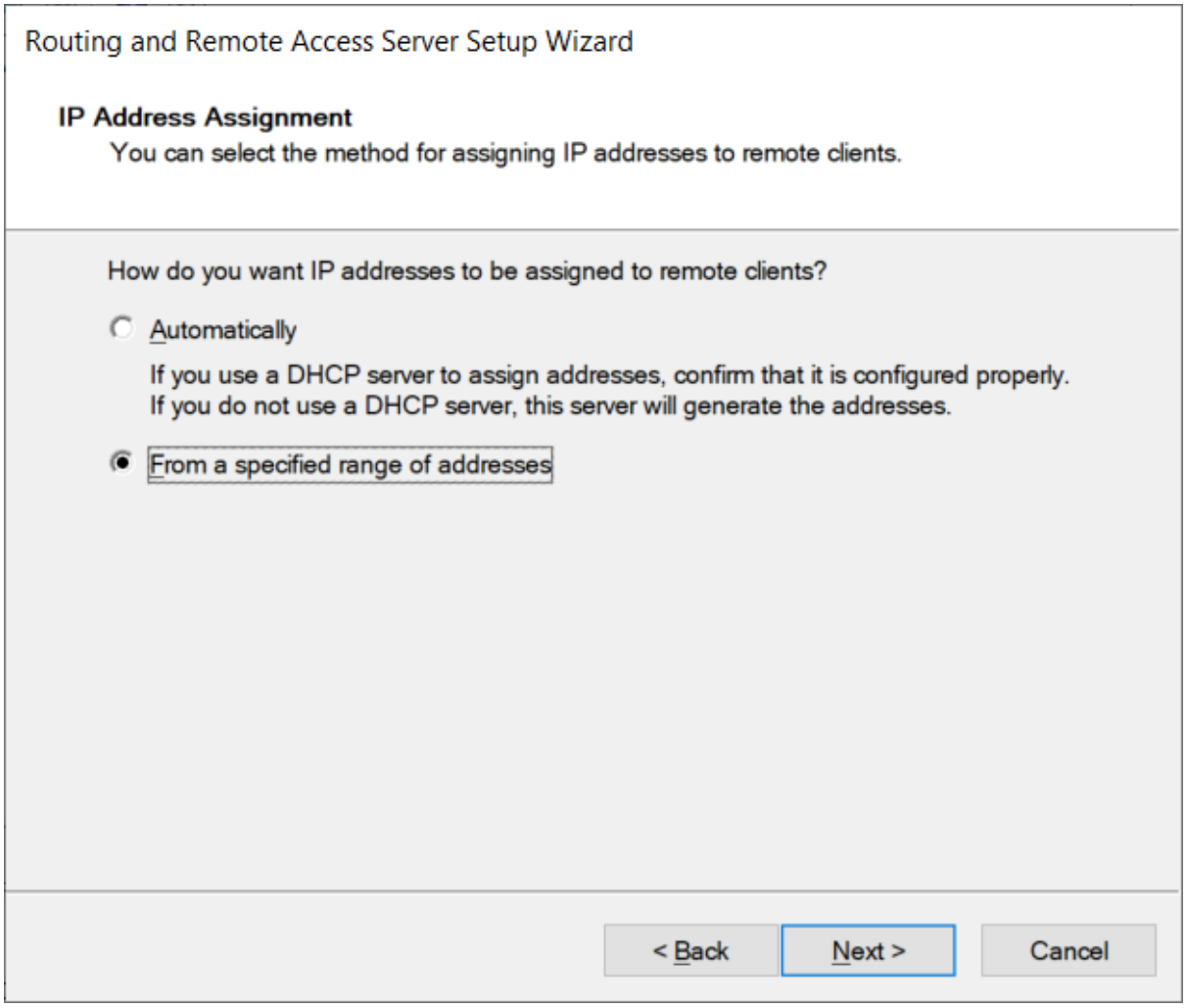

Recycle Bin
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
VPN (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help
Configures Routing and Remote Access for the selected server
Type here to search
9:06 am
17/09/2024


Routing and Remote Access Server Setup Wizard
Welcome to the Routing and Remote Access Server Setup Wizard
This wizard helps you set up your server so that you can connect to other networks and allow connections from remote clients.
To continue, click Next.
< Back
Next >
Cancel

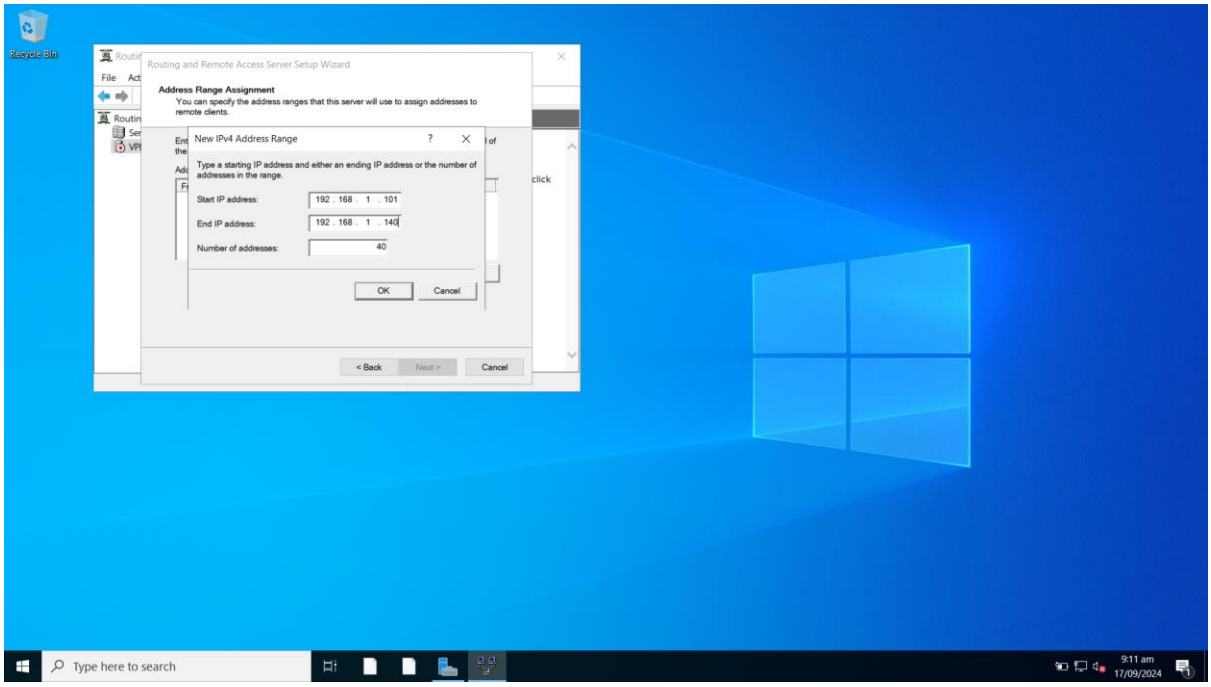
Choose Virtual Private Network(VPN) access and NAT.

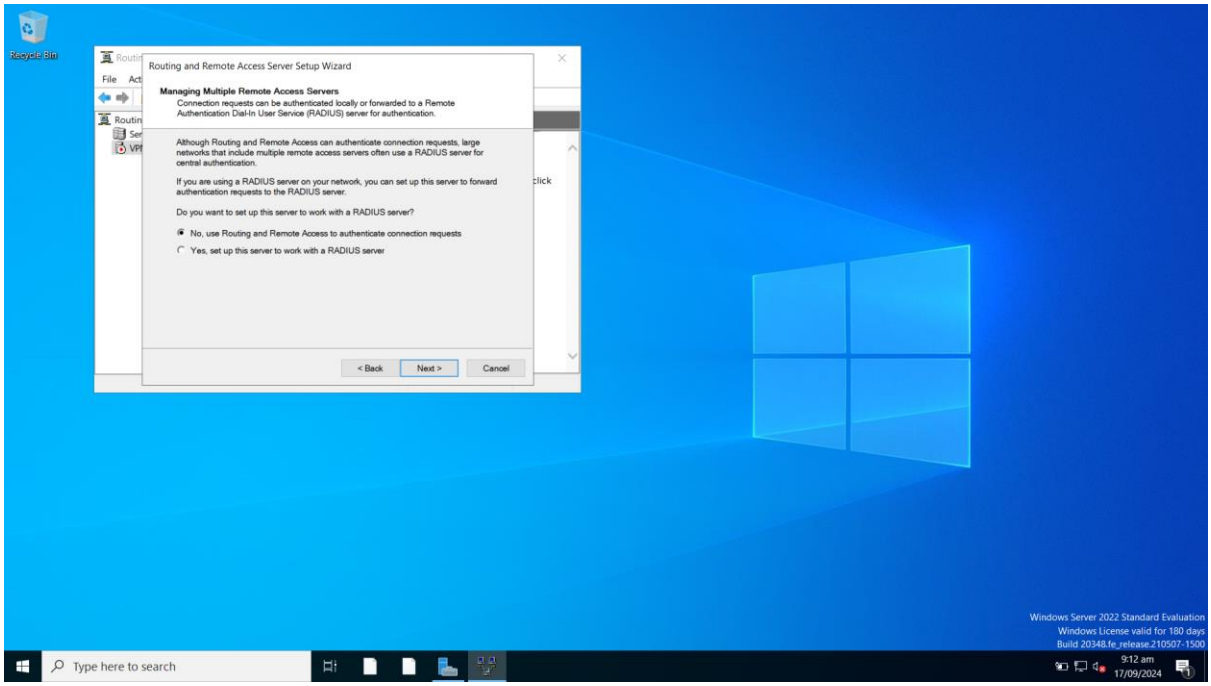


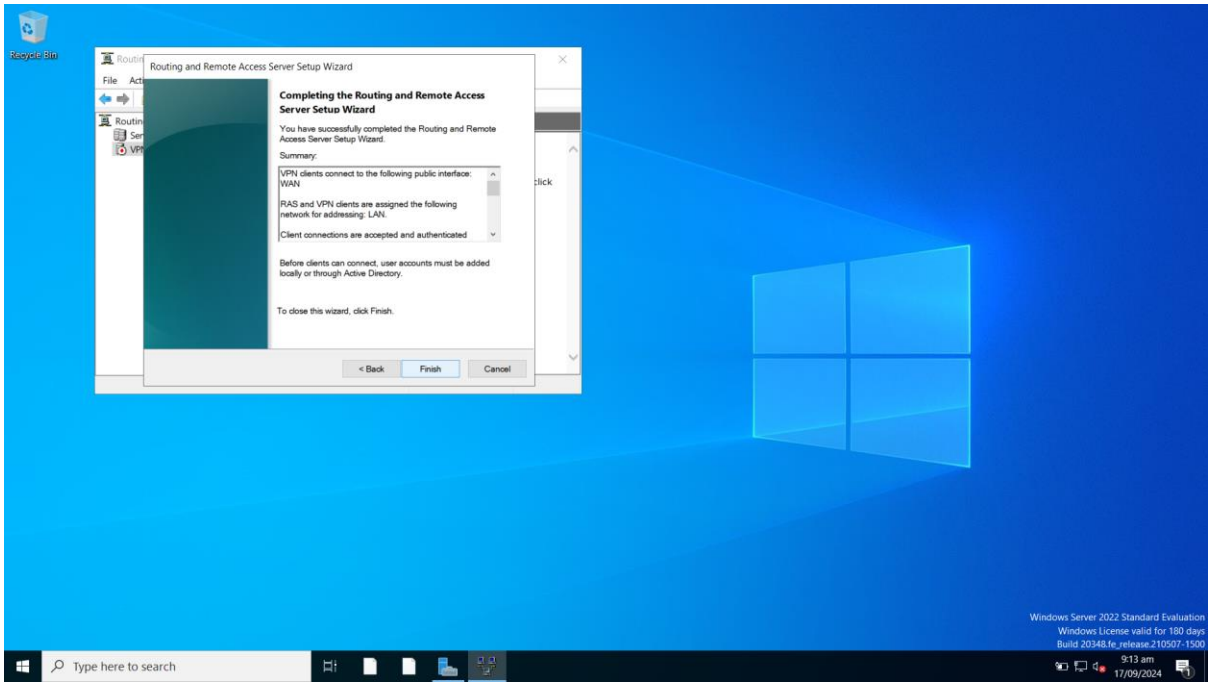


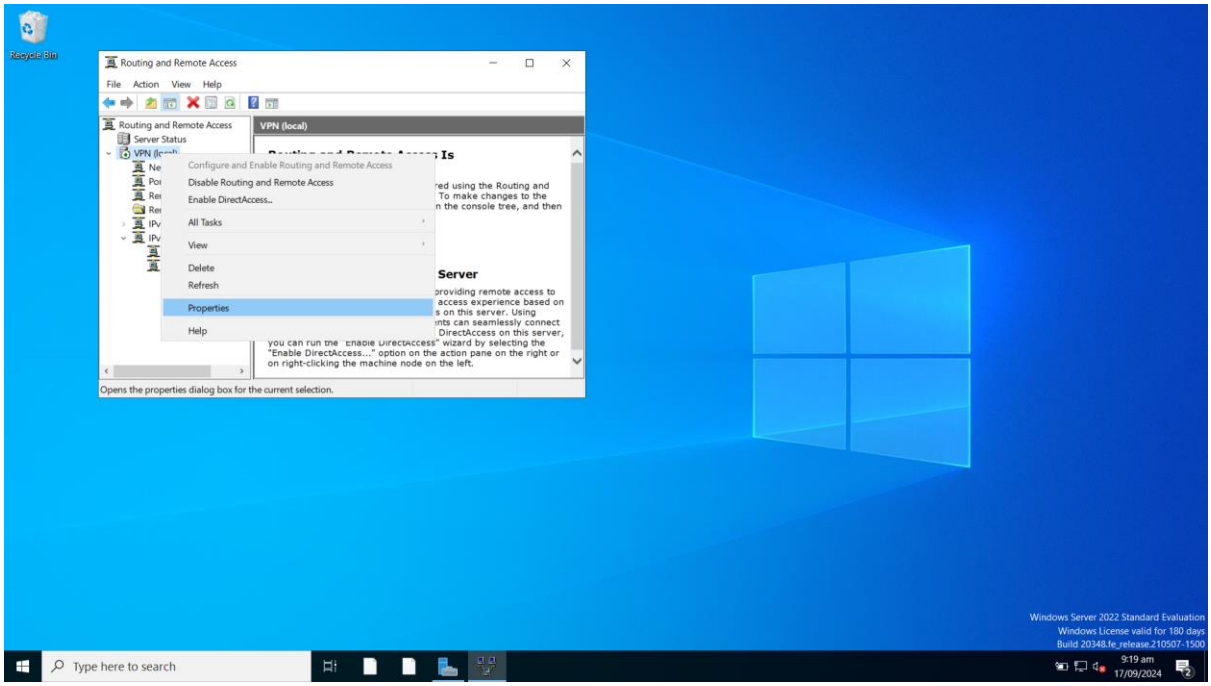


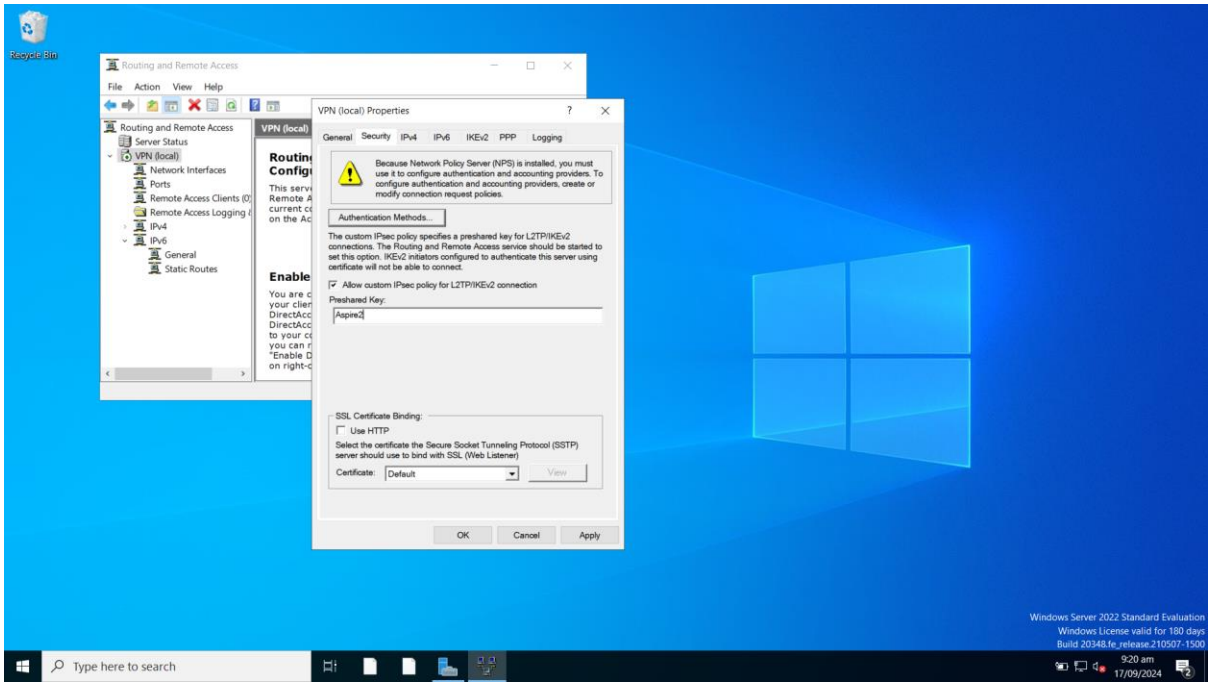
40 IP addresses assigned to VPN users. (192.168.1.101~140/24)

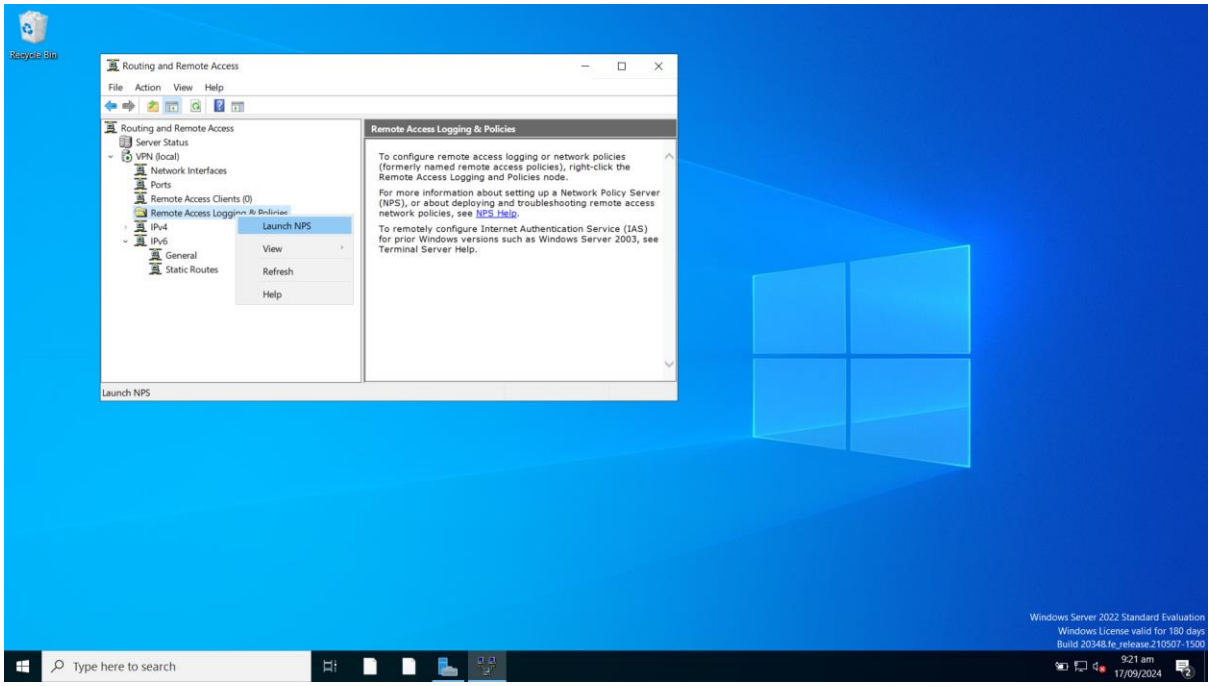


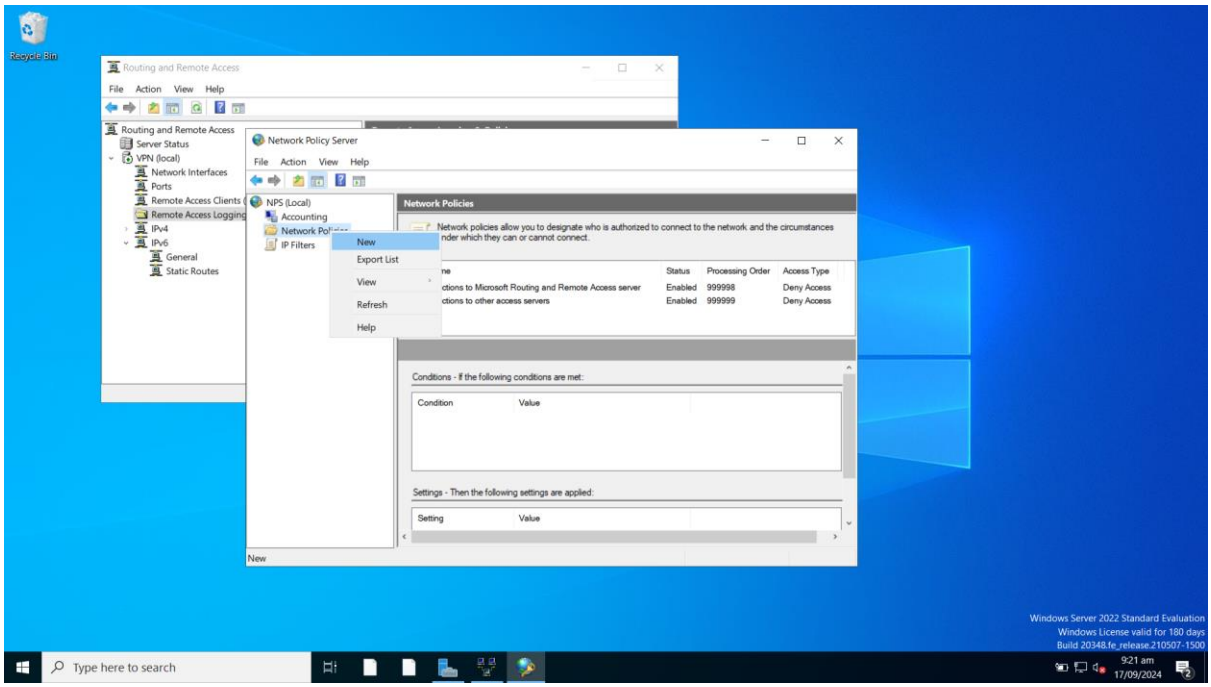

Recycle Bin
Routing and Remote Access Server Setup Wizard
Managing Multiple Remote Access Servers
Connection requests can be authenticated locally or forwarded to a Remote Authentication Dial-In User Service (RADIUS) server for authentication.
Although Routing and Remote Access can authenticate connection requests, large networks that include multiple remote access servers often use a RADIUS server for central authentication.
If you are using a RADIUS server on your network, you can set up this server to forward authentication requests to the RADIUS server.
Do you want to set up this server to work with a RADIUS server?
No, use Routing and Remote Access to authenticate connection requests
Yes, set up this server to work with a RADIUS server
< Back
Next >
Cancel
Type here to search
Windows Server 2022 Standard Evaluation
Windows License valid for 180 days
Build 20348.fe_release.210507-1500
9:12 am
17/09/2024

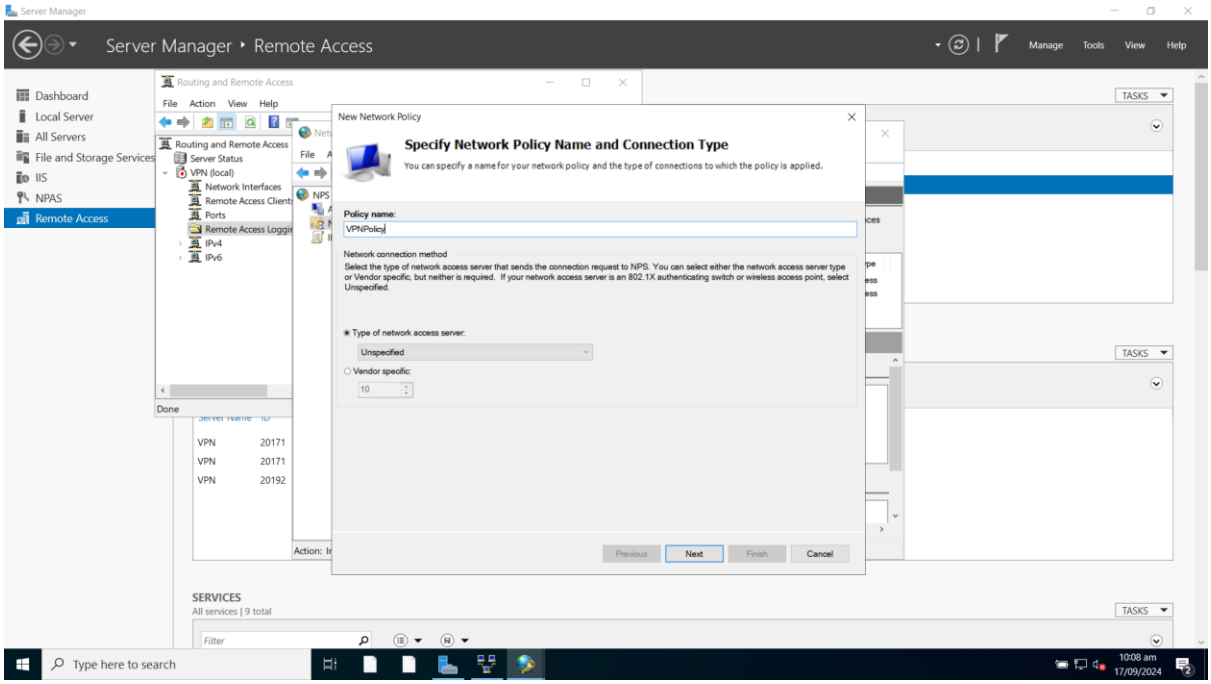

Recycle Bin
Routing and Remote Access Server Setup Wizard
Completing the Routing and Remote Access Server Setup Wizard
You have successfully completed the Routing and Remote Access Server Setup Wizard.
Summary:
VPN clients connect to the following public interface: WAN
RAS and VPN clients are assigned the following network for addressing: LAN.
Client connections are accepted and authenticated
Before clients can connect, user accounts must be added locally or through Active Directory.
To close this wizard, click Finish.
< Back
Finish
Cancel
Type here to search
Windows Server 2022 Standard Evaluation
Windows License valid for 180 days
Build 20348.fe_release.210507-1500
9:13 am
17/09/2024

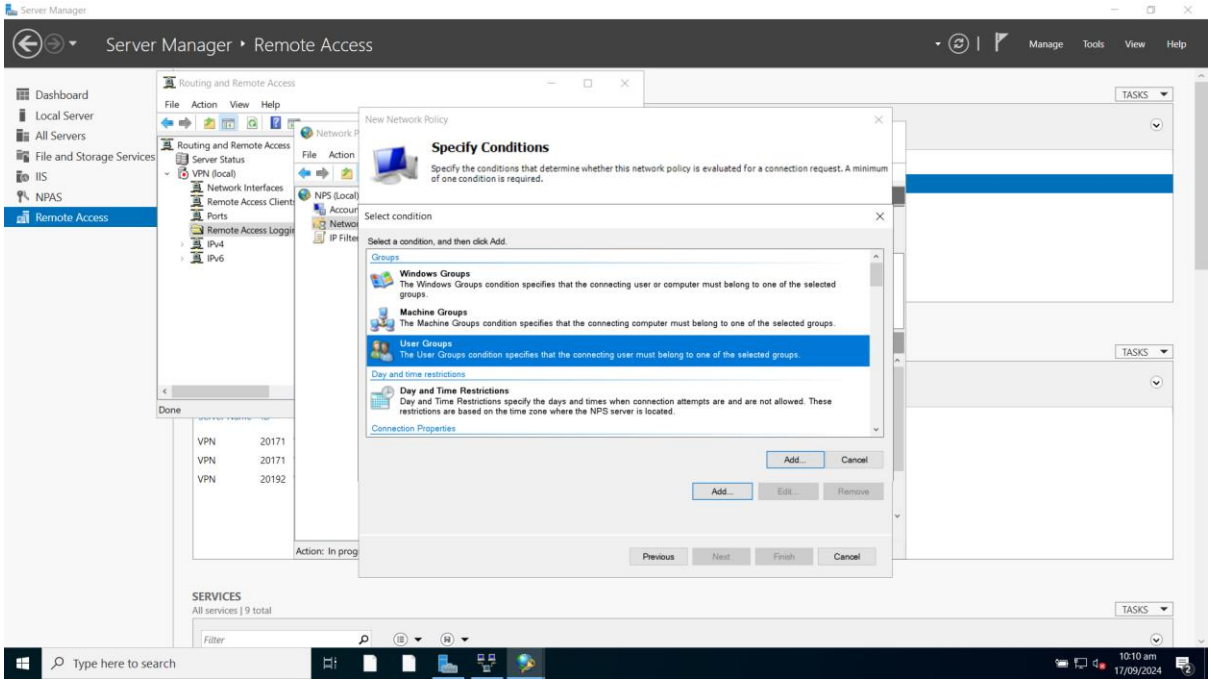

Recycle Bin
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
VPN (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
Enable DirectAccess...
All Tasks
View
Delete
Refresh
Properties
Help
Server
Opens the properties dialog box for the current selection.
Type here to search
Windows Server 2022 Standard Evaluation
Windows License valid for 180 days
Build 20348.fe_release.210507-1500
9:19 am
17/09/2024

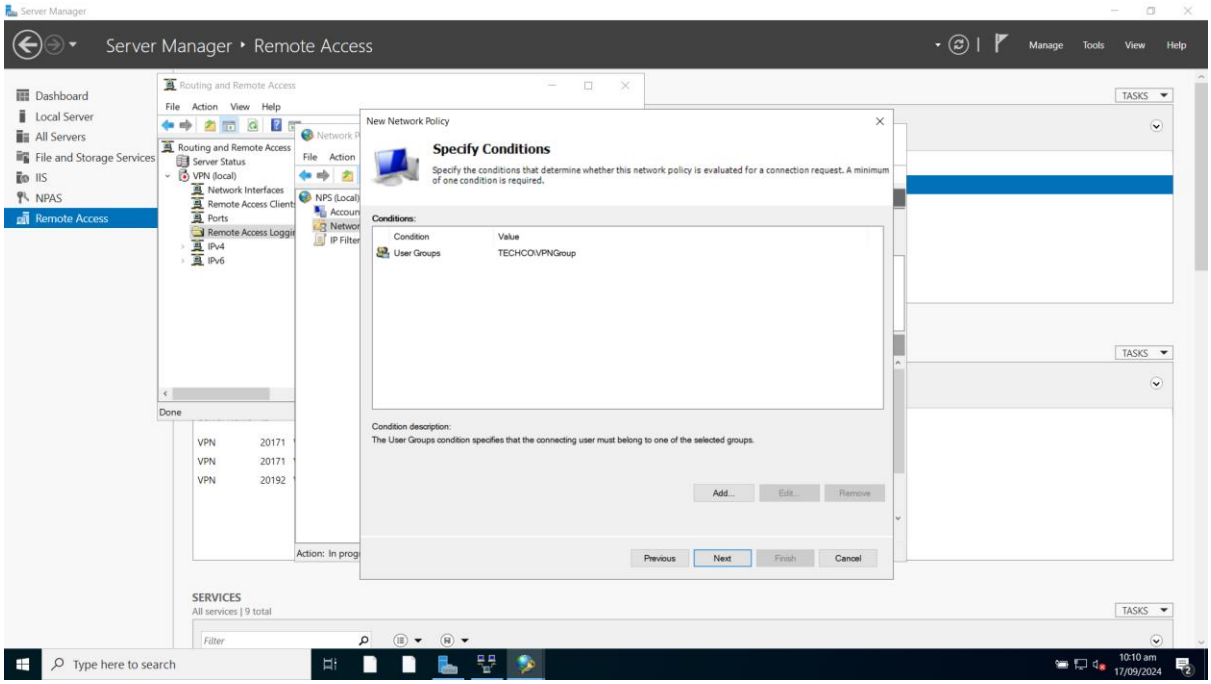

Recycle Bin
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
VPN (local)
Network Interfaces
Ports
Remote Access Clients
Remote Access Logging
IPv4
IPv6
General
Static Routes
VPN (local) Properties
General Security IPv4 IPv6 IKEv2 PPP Logging
Because Network Policy Server (NPS) is installed, you must use it to configure authentication and accounting providers. To configure authentication and accounting providers, create or modify connection request policies.
Authentication Methods...
The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.
Allow custom IPsec policy for L2TP/IKEv2 connection
Preshared Key:
Aspire2
SSL Certificate Binding:
Use HTTP
Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)
Certificate:
Default
View
OK
Cancel
Apply
Type here to search
Windows Server 2022 Standard Evaluation
Windows License valid for 180 days
Build 20348.fe_release.210507-1500
9:20 am
17/09/2024

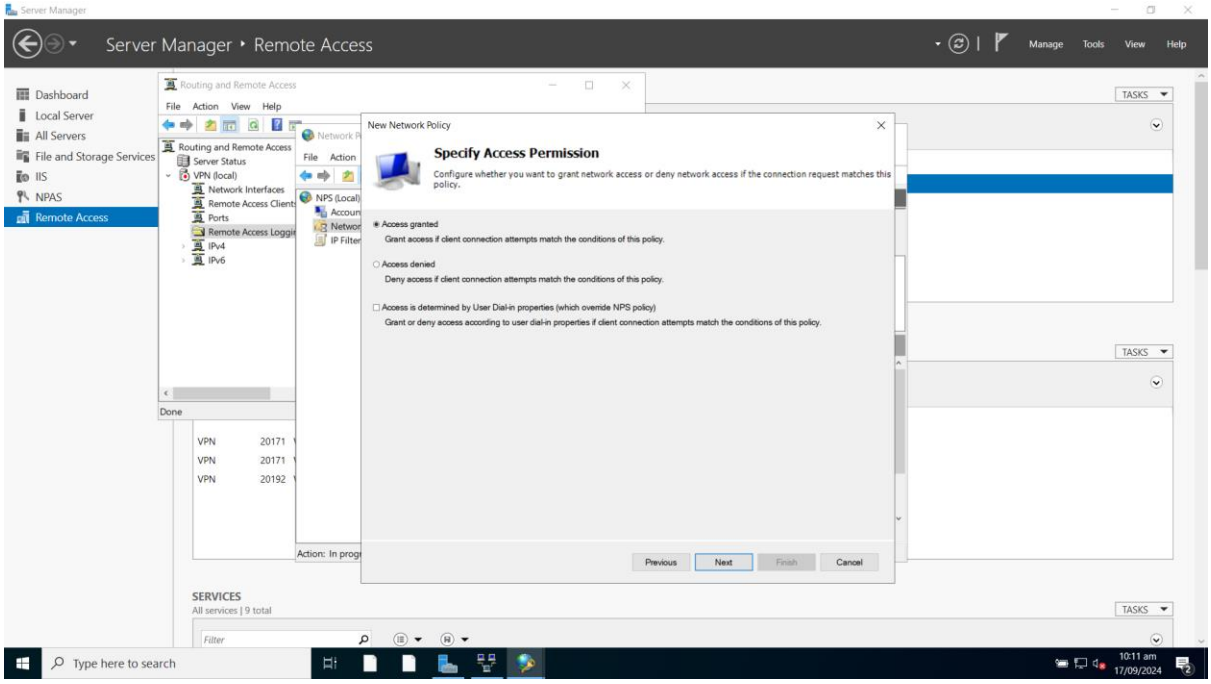

Recycle Bin
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
VPN (local)
Network Interfaces
Ports
Remote Access Clients (0)
Remote Access Logging & Policies
IPv4
IPv6
General
Static Routes
Launch NPS
View
Refresh
Help
Remote Access Logging & Policies
To configure remote access logging or network policies (formerly named remote access policies), right-click the Remote Access Logging and Policies node.
For more information about setting up a Network Policy Server (NPS), or about deploying and troubleshooting remote access network policies, see NPS Help.
To remotely configure Internet Authentication Service (IAS) for prior Windows versions such as Windows Server 2003, see Terminal Server Help.
Launch NPS
Windows Server 2022 Standard Evaluation
Windows License valid for 180 days
Build 20348.fe_release.210507-1500
Type here to search
9:21 am
17/09/2024

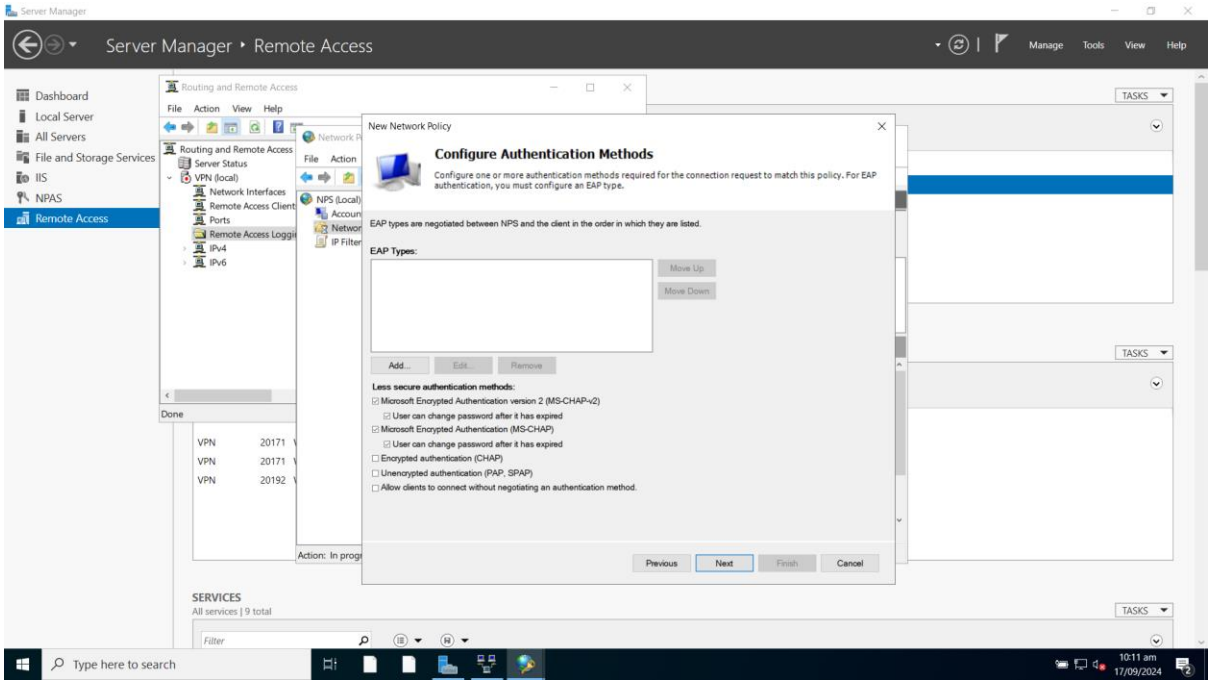

Recycle Bin
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
VPN (local)
Network Interfaces
Ports
Remote Access Clients
Remote Access Logging
IPv4
IPv6
General
Static Routes
Network Policy Server
File Action View Help
NPS (Local)
Accounting
Network Policies
IP Filters
New
Export List
View
Refresh
Help
Network Policies
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.
Status
Processing Order
Access Type
Enabled
999998
Deny Access
Enabled
999999
Deny Access
Conditions - If the following conditions are met:
Condition
Value
Settings - Then the following settings are applied:
Setting
Value
New
Windows Server 2022 Standard Evaluation
Windows License valid for 180 days
Build 20348.fe_release.210507-1500
Type here to search
9:21 am
17/09/2024


Server Manager
Server Manager ‣ Remote Access
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
NPAS
Remote Access
Routing and Remote Access
File Action View Help
Server Status
VPN (local)
Network Interfaces
Remote Access Clients
Ports
Remote Access Logging
IPv4
IPv6
New Network Policy
Specify Network Policy Name and Connection Type
You can specify a name for your network policy and the type of connections to which the policy is applied.
Policy name:
VPNPolicy
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.
Type of network access server:
Unspecified
Vendor specific:
10
Previous
Next
Finish
Cancel
VPN 20171
VPN 20171
VPN 20192
SERVICES
All services | 9 total
TASKS
Type here to search
10:08 am
17/09/2024

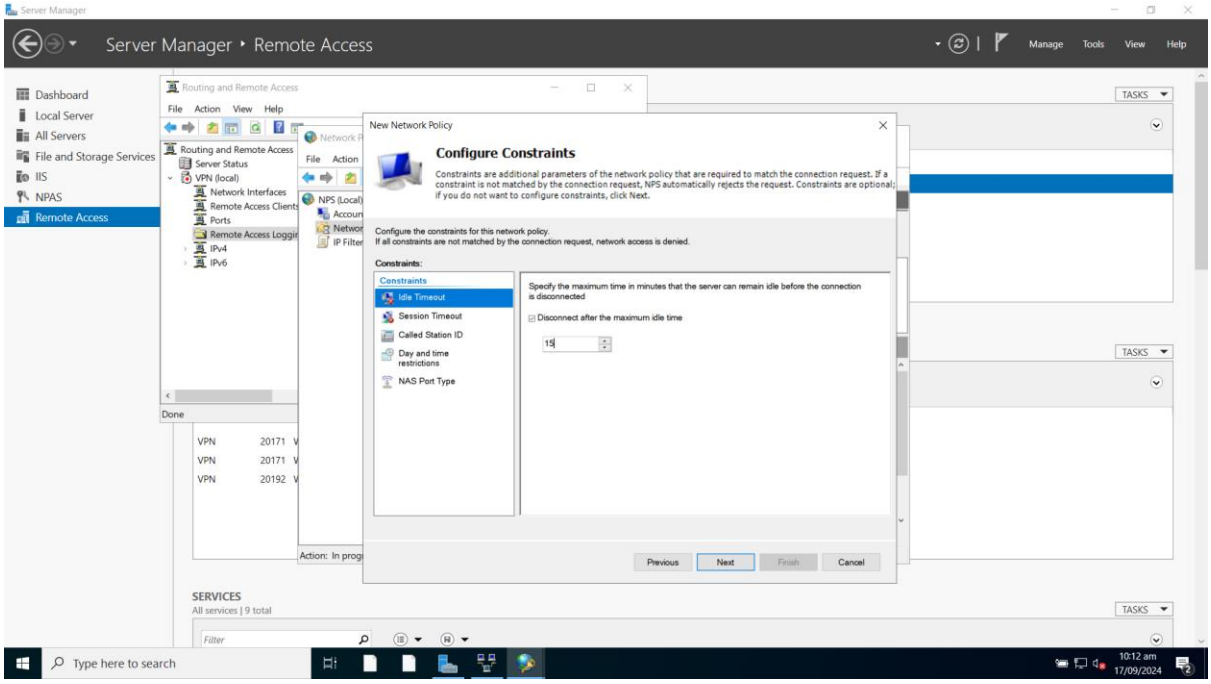

Server Manager
Server Manager ‣ Remote Access
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
NPAS
Remote Access
Routing and Remote Access
File Action View Help
Server Status
VPN (local)
Network Interfaces
Remote Access Clients
Ports
Remote Access Logging
IPv4
IPv6
New Network Policy
Specify Conditions
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.
Select condition
Select a condition, and then click Add.
Groups
Windows Groups
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.
Machine Groups
The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.
User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.
Day and time restrictions
Day and Time Restrictions
Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.
Connection Properties
Add...
Cancel
Add...
Edit...
Remove
Previous
Next
Finish
Cancel
VPN 20171
VPN 20171
VPN 20192
SERVICES
All services | 9 total
TASKS
Type here to search
10:10 am
17/09/2024

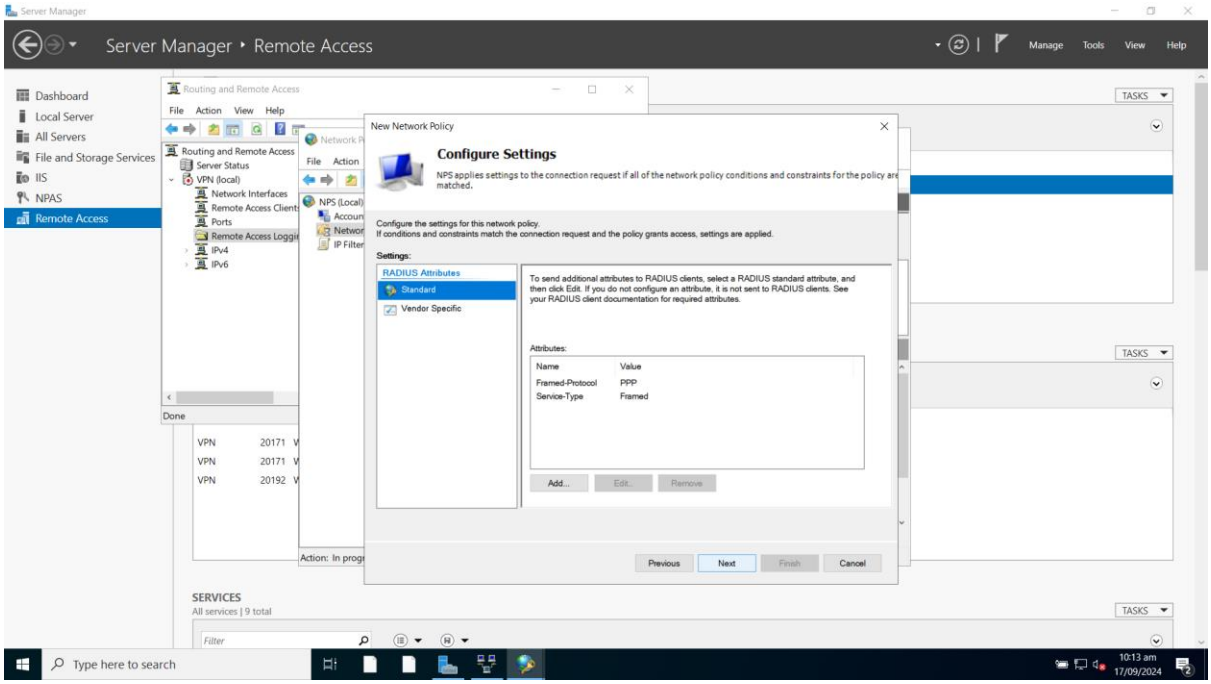

Server Manager
Server Manager ‣ Remote Access
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
NPAS
Remote Access
Routing and Remote Access
File Action View Help
Server Status
VPN (local)
Network Interfaces
Remote Access Clients
Ports
Remote Access Logging
IPv4
IPv6
New Network Policy
Specify Conditions
Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.
Conditions:
Condition
Value
User Groups
TECHCO\VPNGroup
Condition description:
The User Groups condition specifies that the connecting user must belong to one of the selected groups.
Add...
Edit...
Remove
Previous
Next
Finish
Cancel
Done
VPN 20171
VPN 20171
VPN 20192
SERVICES
All services | 9 total
TASKS
Filter
Type here to search
10:10 am
17/09/2024

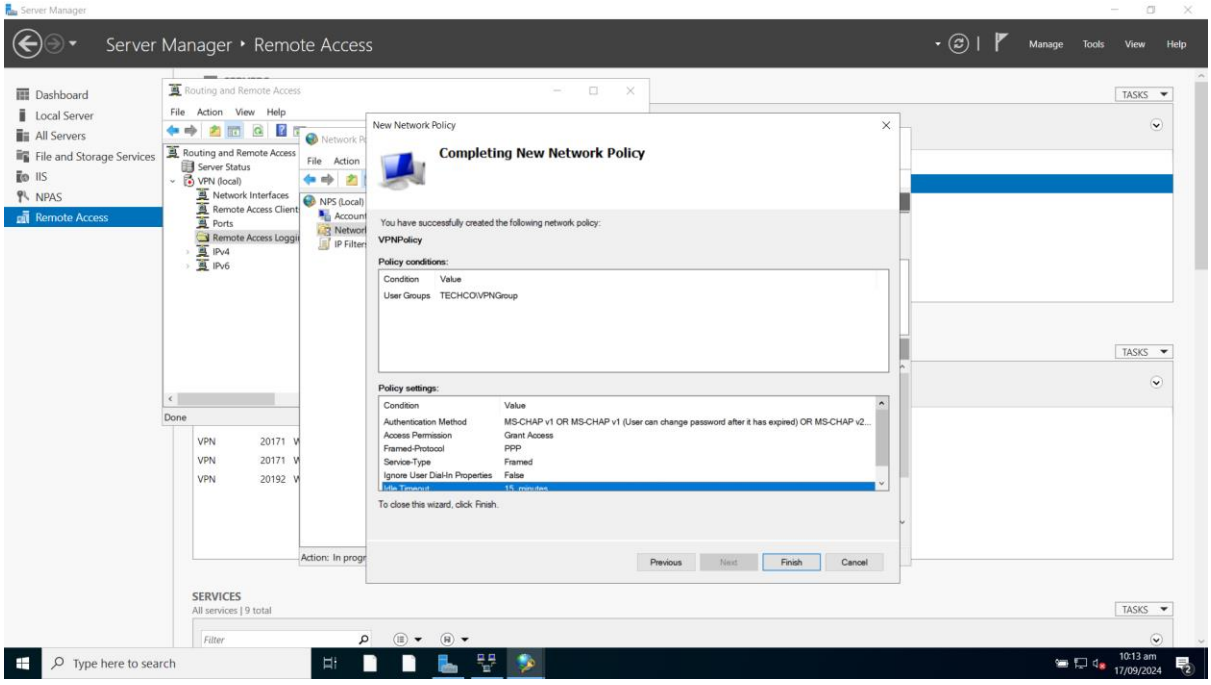

Server Manager
Server Manager ‣ Remote Access
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
NPAS
Remote Access
Routing and Remote Access
File Action View Help
Server Status
VPN (local)
Network Interfaces
Remote Access Clients
Ports
Remote Access Logging
IPv4
IPv6
New Network Policy
Specify Access Permission
Configure whether you want to grant network access or deny network access if the connection request matches this policy.
Access granted
Grant access if client connection attempts match the conditions of this policy.
Access denied
Deny access if client connection attempts match the conditions of this policy.
Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.
Previous
Next
Finish
Cancel
Done
VPN 20171
VPN 20171
VPN 20192
SERVICES
All services | 9 total
TASKS
Filter
Type here to search
10:11 am
17/09/2024

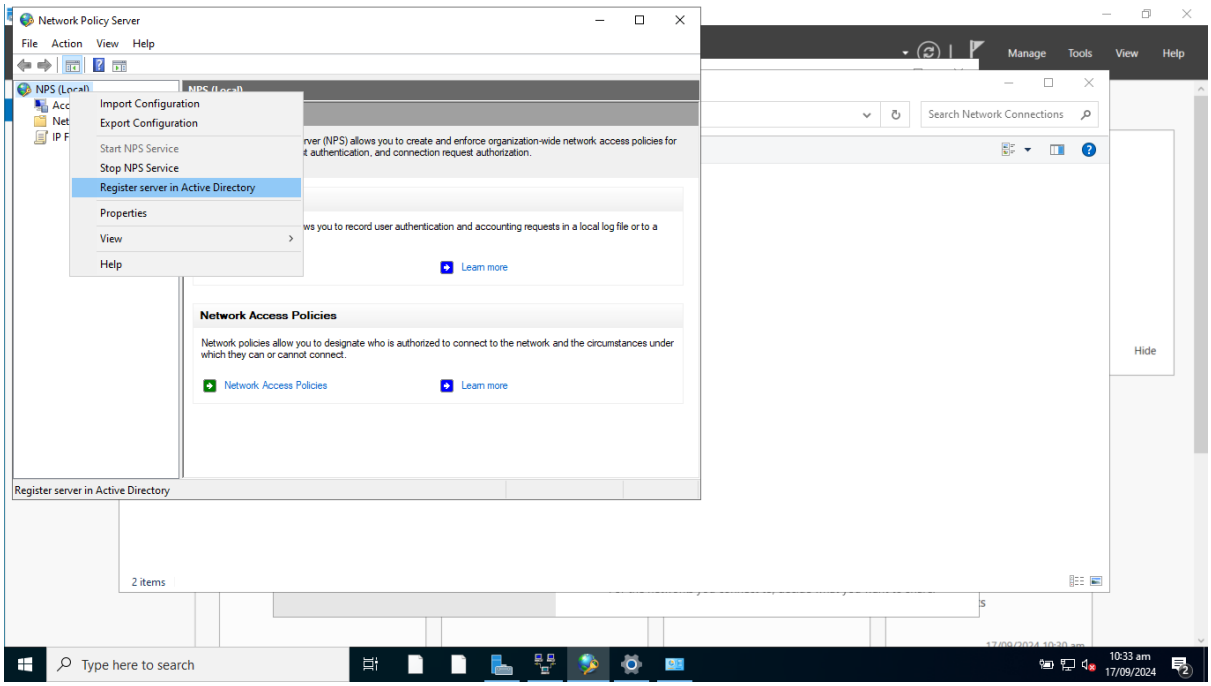


Set the default idle timeout for VPN connections to 15 minutes.

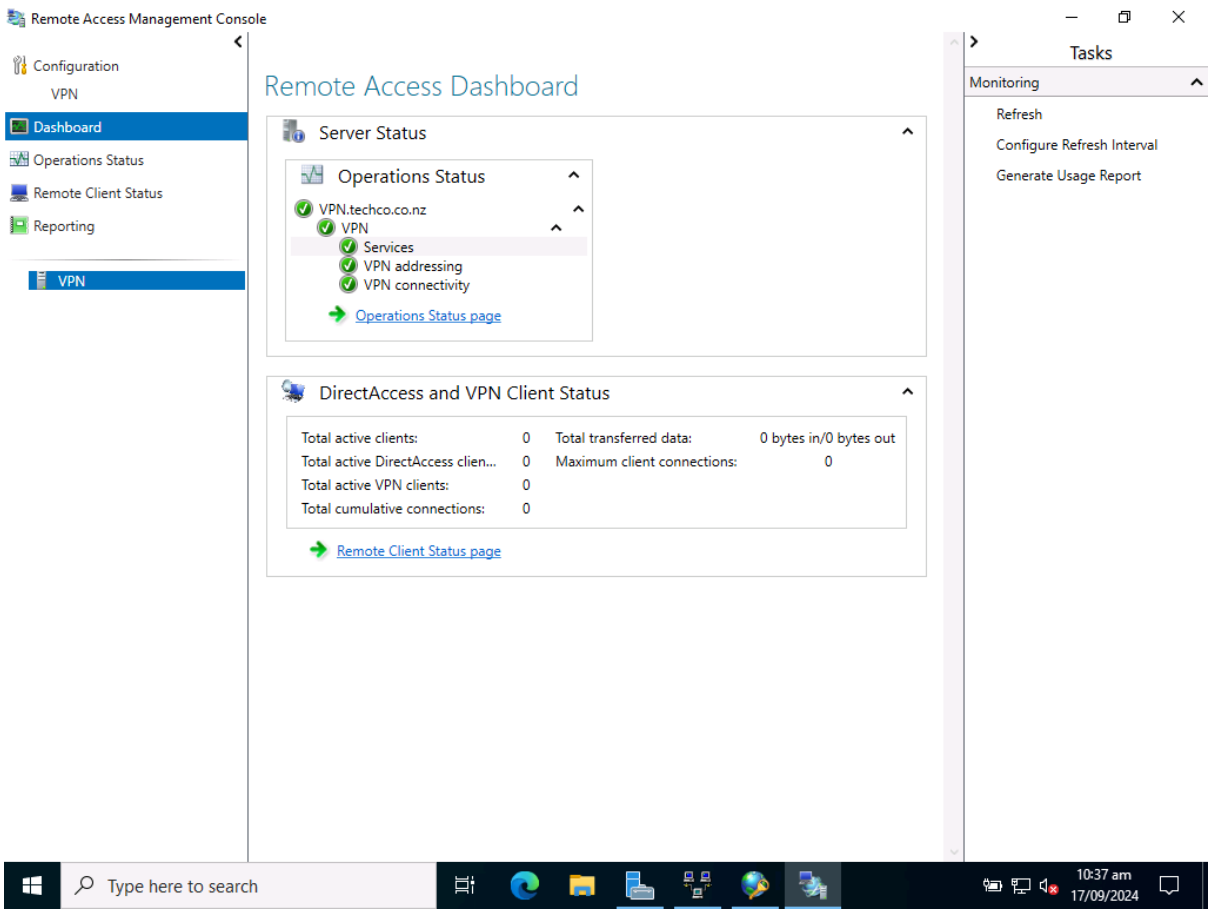



Server Manager
Server Manager ‣ Remote Access
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
NPAS
Remote Access
Routing and Remote Access
File Action View Help
Server Status
VPN (local)
Network Interfaces
Remote Access Clients
Ports
Remote Access Logging
IPv4
IPv6
NPS (Local)
New Network Policy
Configure Settings
NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
RADIUS Attributes
Standard
Vendor Specific
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Value
Framed-Protocol
PPP
Service-Type
Framed
Add...
Edit...
Remove
Previous
Next
Finish
Cancel
SERVICES
All services | 9 total
TASKS
Type here to search
10:13 am
17/09/2024


Server Manager
Server Manager ‣ Remote Access
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
NPAS
Remote Access
Routing and Remote Access
File Action View Help
Server Status
VPN (local)
Network Interfaces
Remote Access Clients
Ports
Remote Access Logging
IPv4
IPv6
NPS (Local)
New Network Policy
Completing New Network Policy
You have successfully created the following network policy:
VPNPolicy
Policy conditions:
Condition
Value
User Groups
TECHCO\VPNGroup
Policy settings:
Condition
Value
Authentication Method
MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2...
Access Permission
Grant Access
Framed-Protocol
PPP
Service-Type
Framed
Ignore User Dial-In Properties
False
To close this wizard, click Finish.
Previous
Next
Finish
Cancel
SERVICES
All services | 9 total
TASKS
Type here to search
10:13 am
17/09/2024

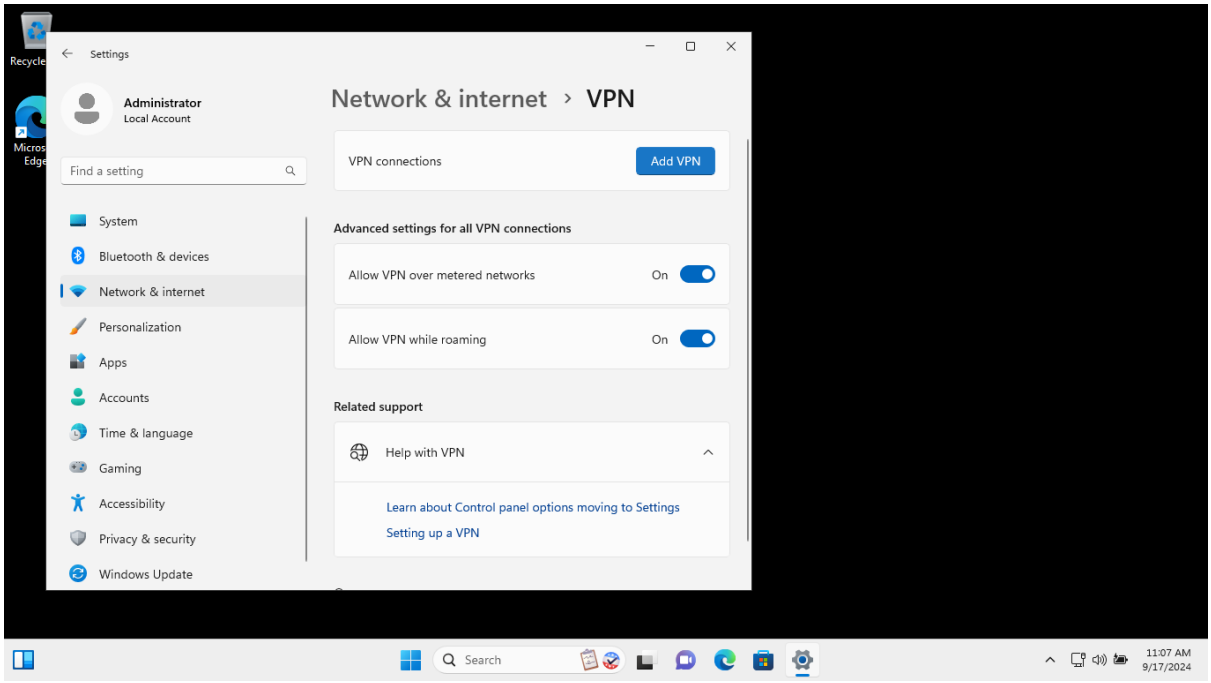


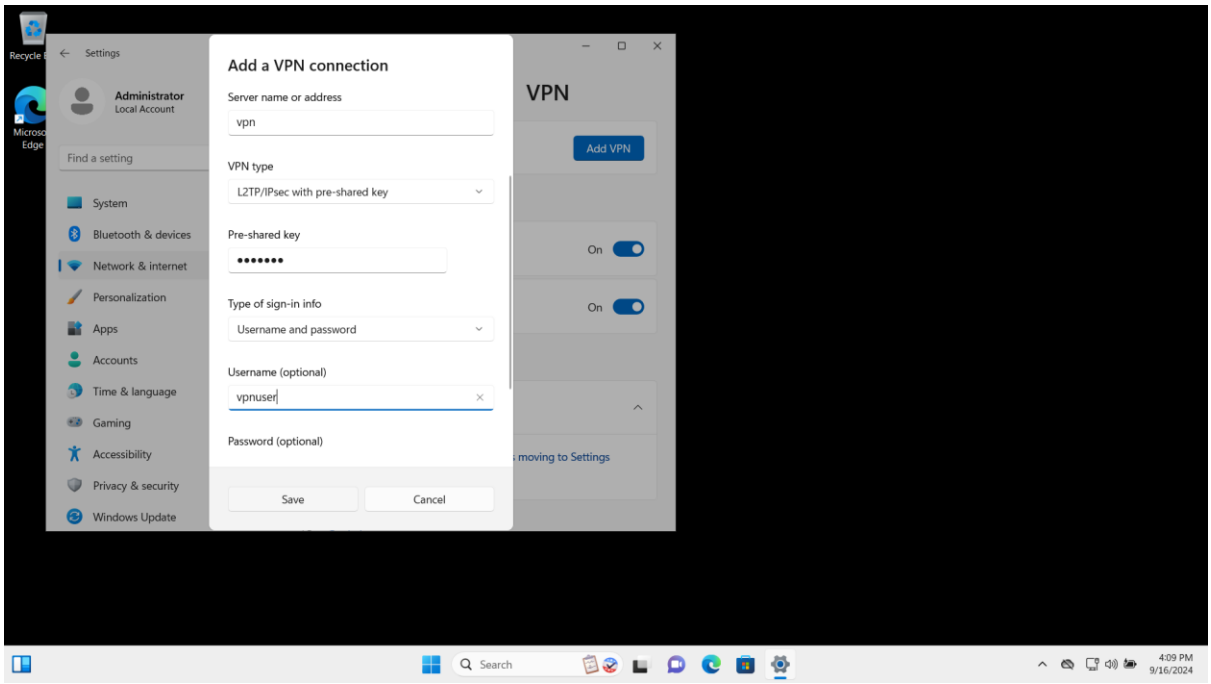
VPN server is ready.



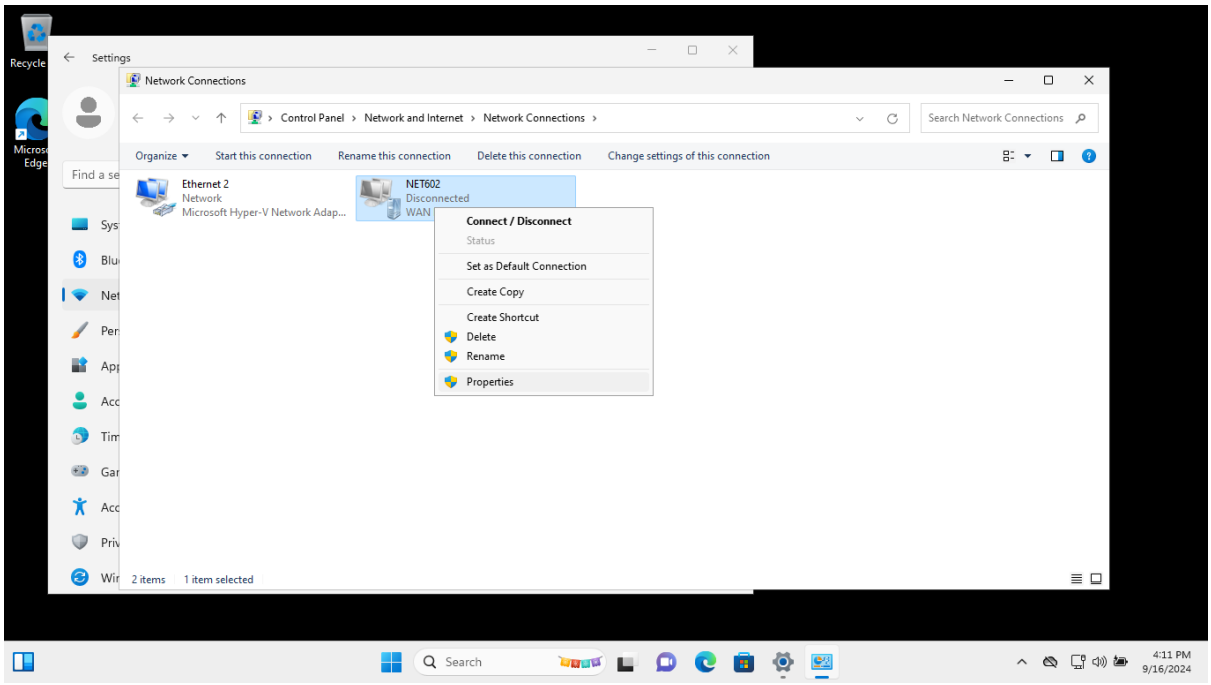
Task 4.2 Set up a secure VPN connection

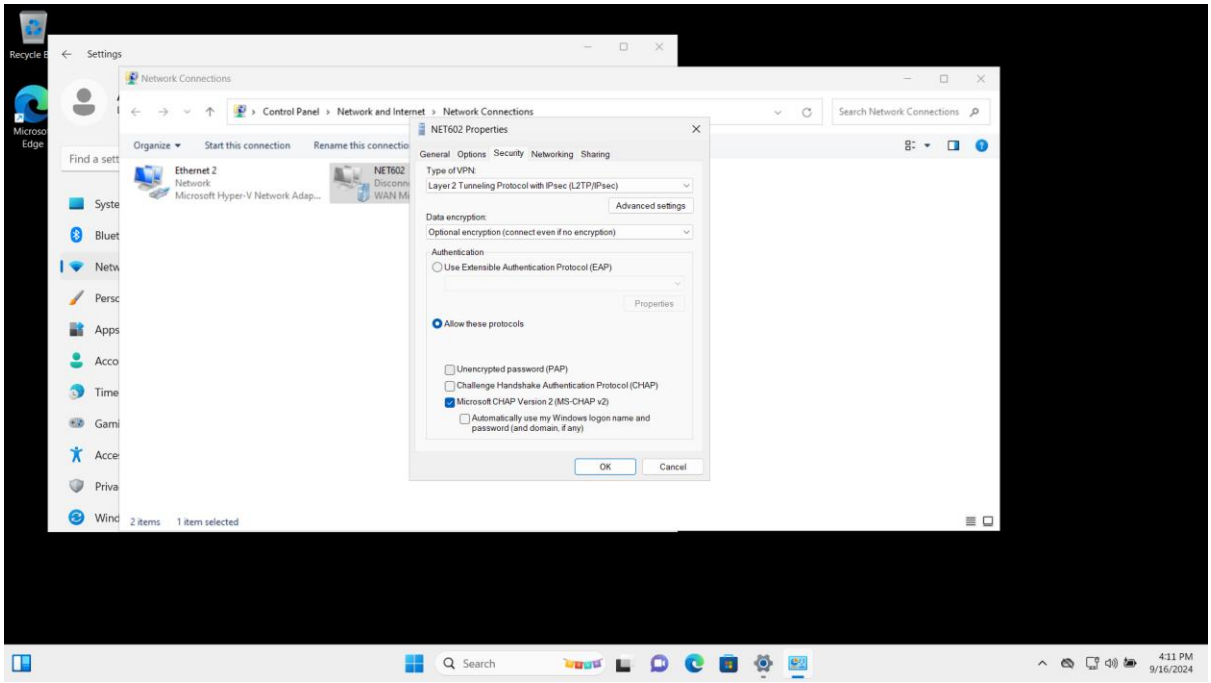
1. Login a client machine with a WAN network adapter and create a VPN connection





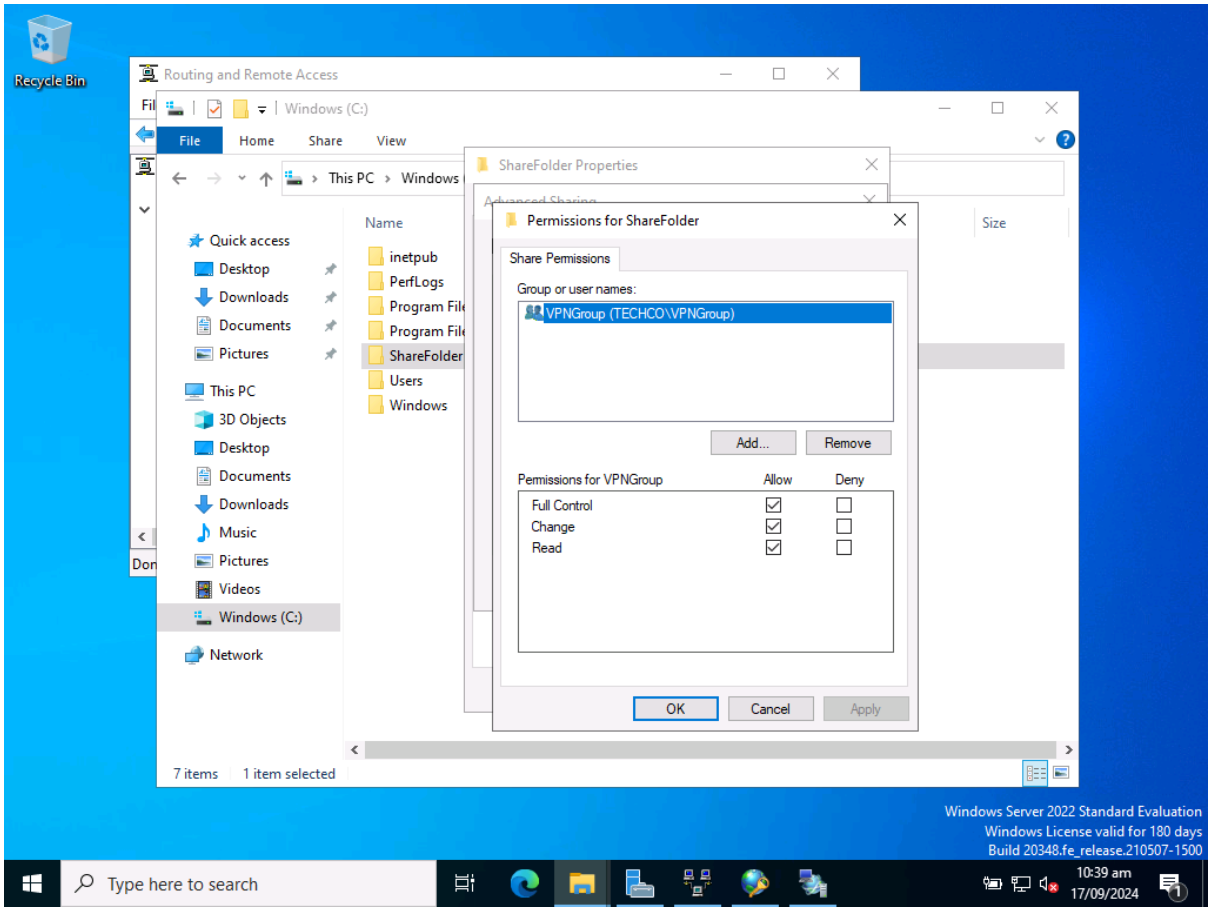
2. Modify the properties of VPN to allow MS CHAP v2.



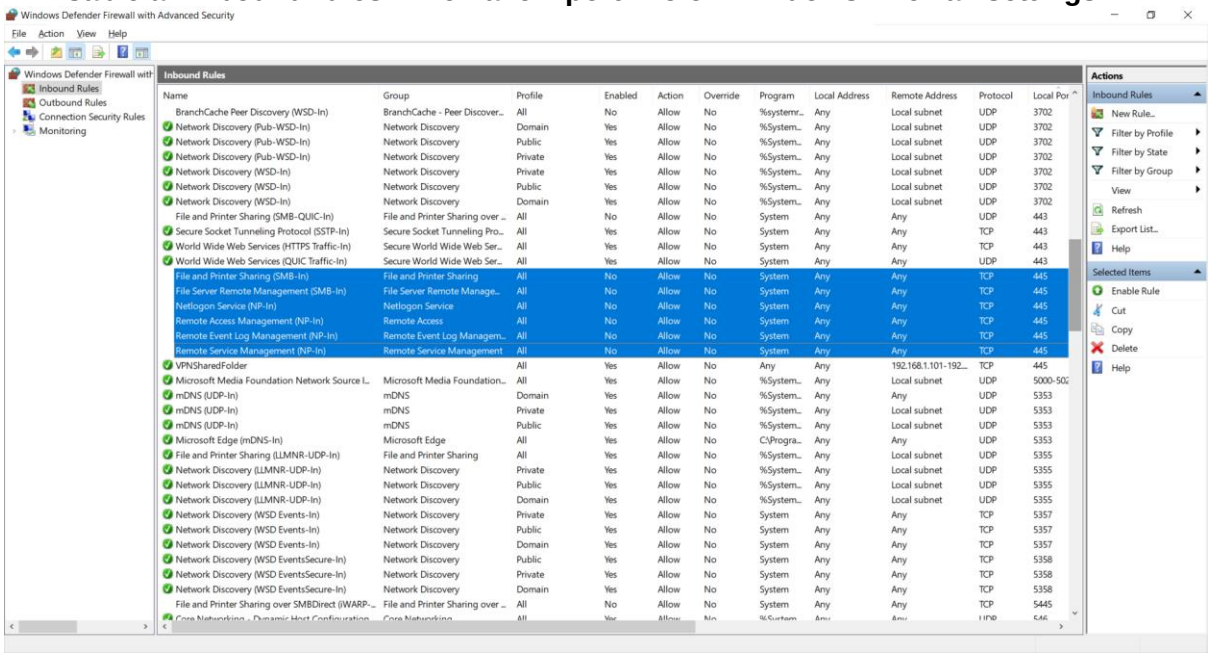


Task 4.3 Allow file sharing for a shared folder

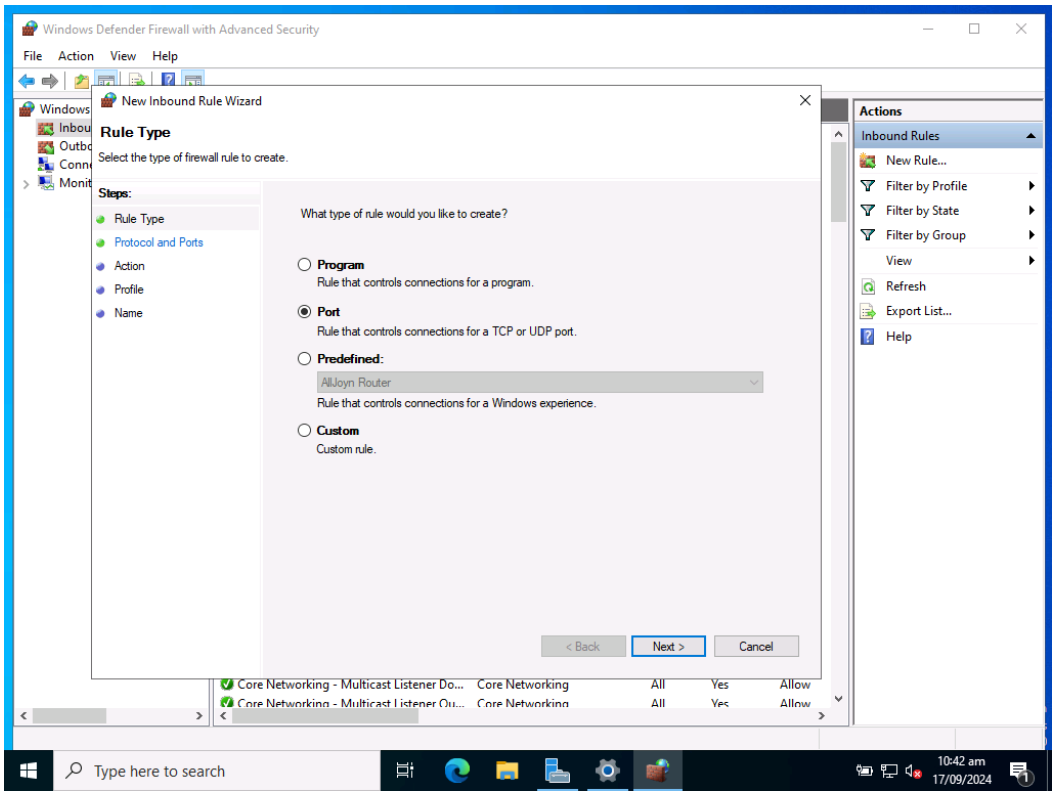
1. Create a shared folder on VPN server

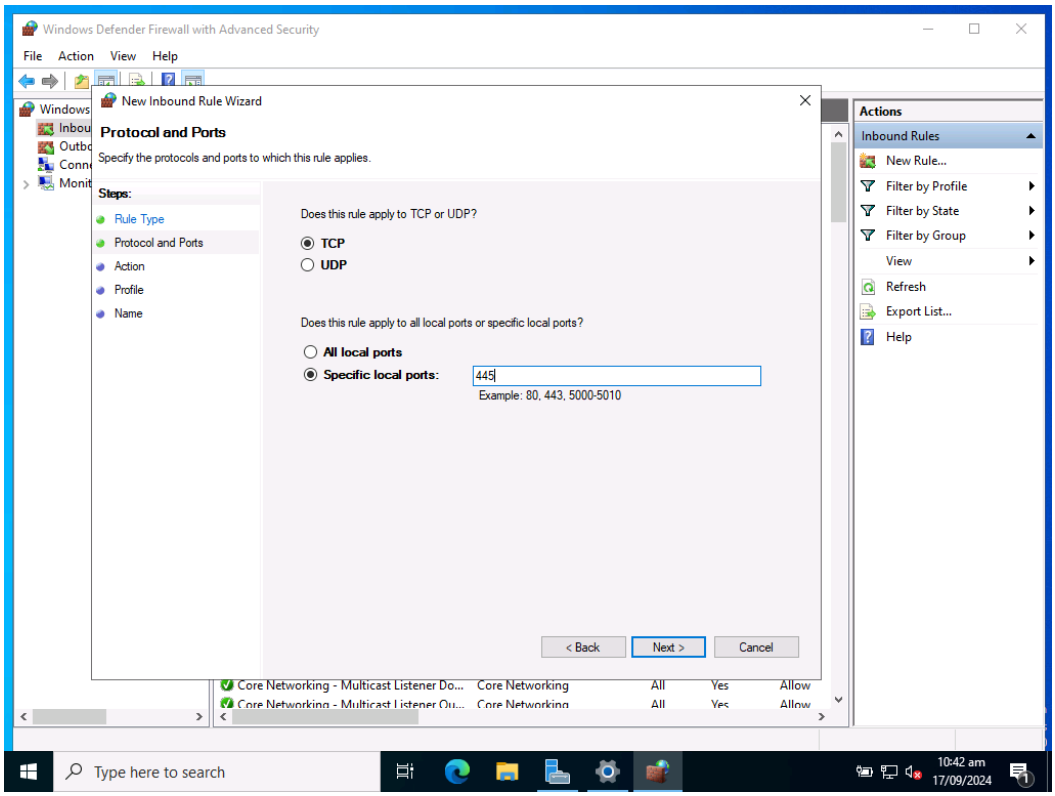


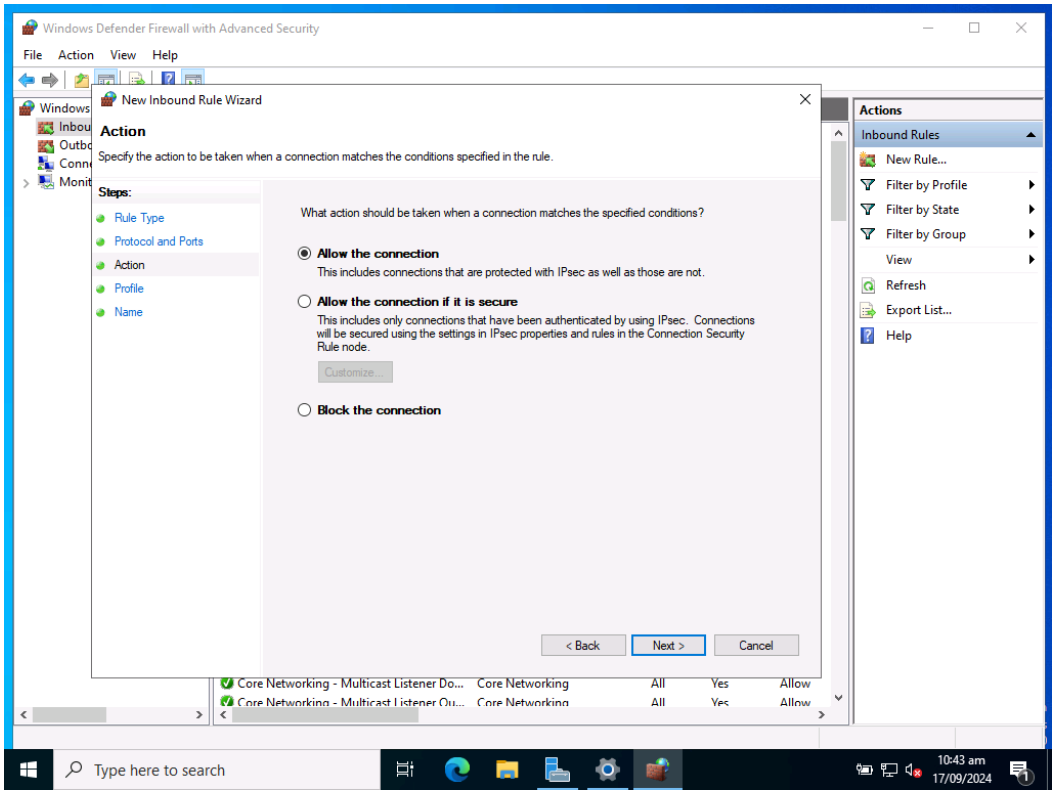
2. Disable all inbound rules which allow port 445 on Windows Firewall settings

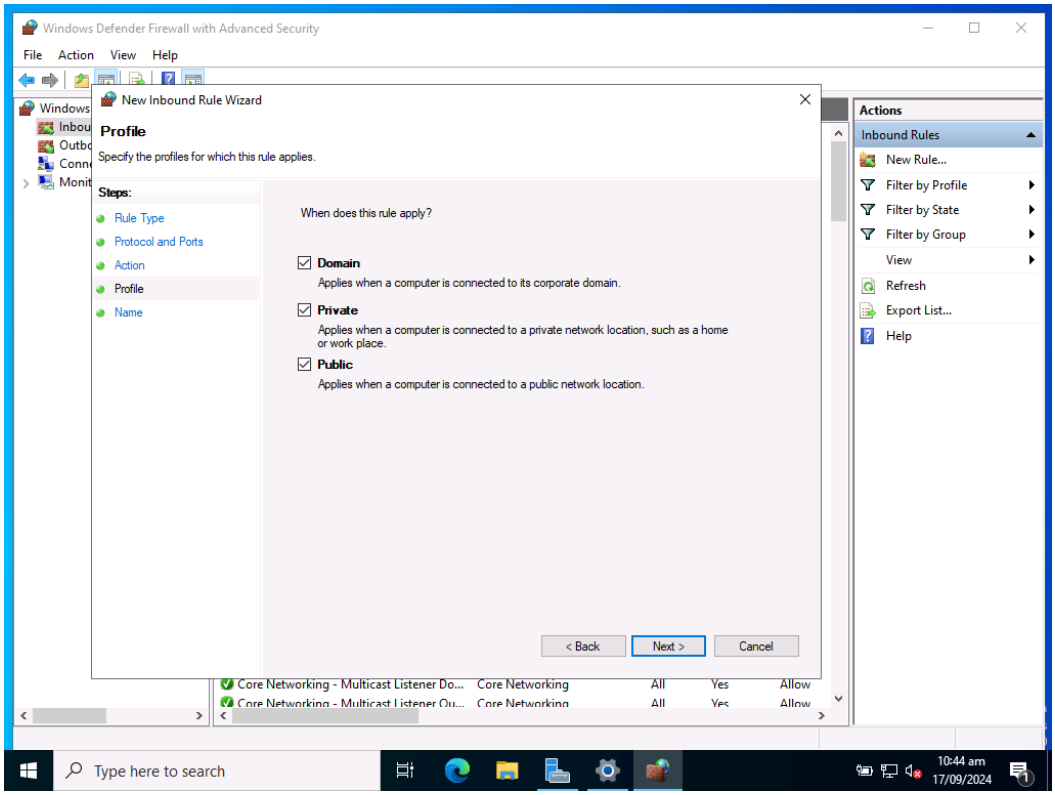


3. Create a new inbound rule which allows port 445

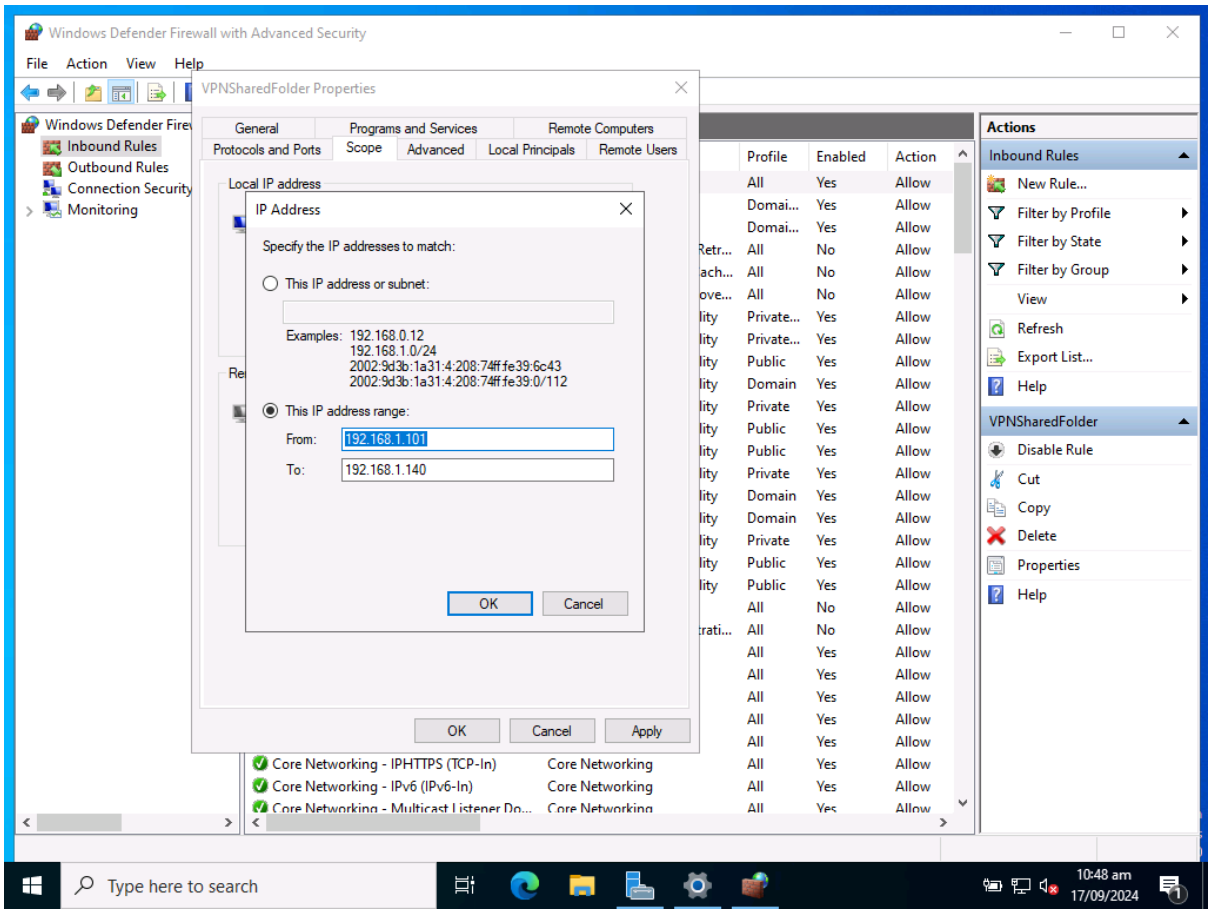





Windows Defender Firewall with Advanced Security
File Action View Help
New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Core Networking - Multicast Listener Do... Core Networking All Yes Allow
Type here to search
10:43 am
17/09/2024

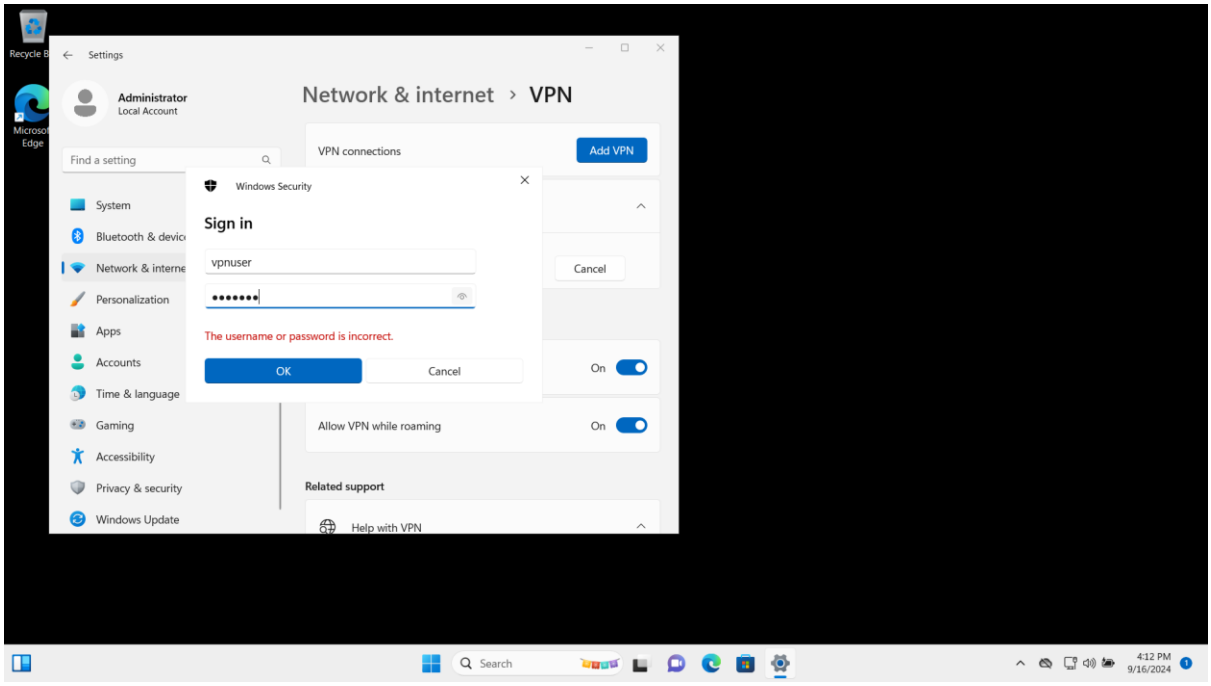

Windows Defender Firewall with Advanced Security
File Action View Help
New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Next >
Cancel
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Core Networking - Multicast Listener Do... Core Networking All Yes Allow
Type here to search
10:44 am
17/09/2024

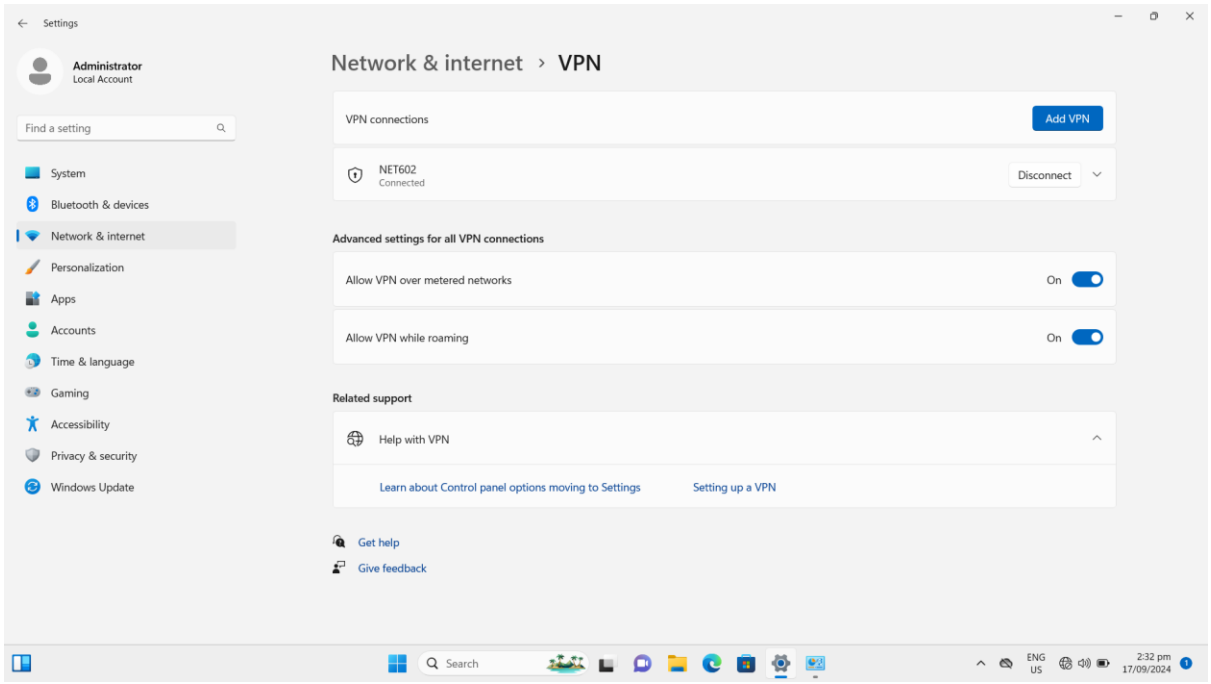
4. Set the inbound rule properties, and set remote IP addresses scope same as VPN settings.

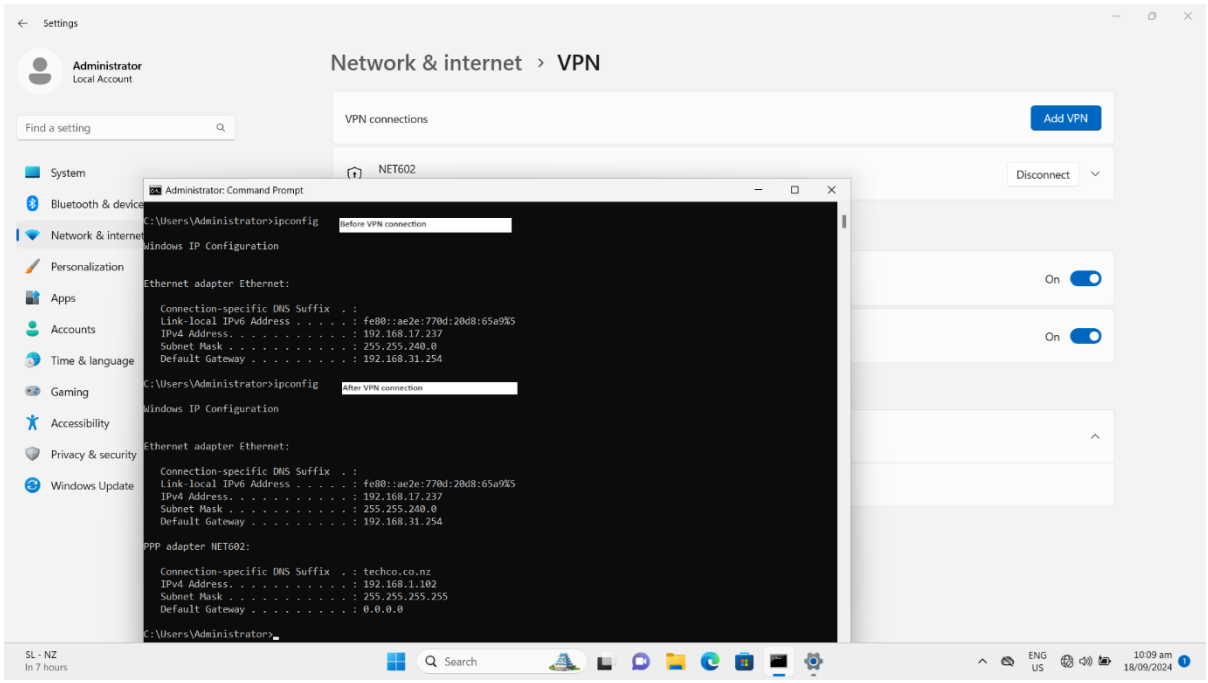


Task 4.4 Test the VPN connectivity to verify the setup and configuration

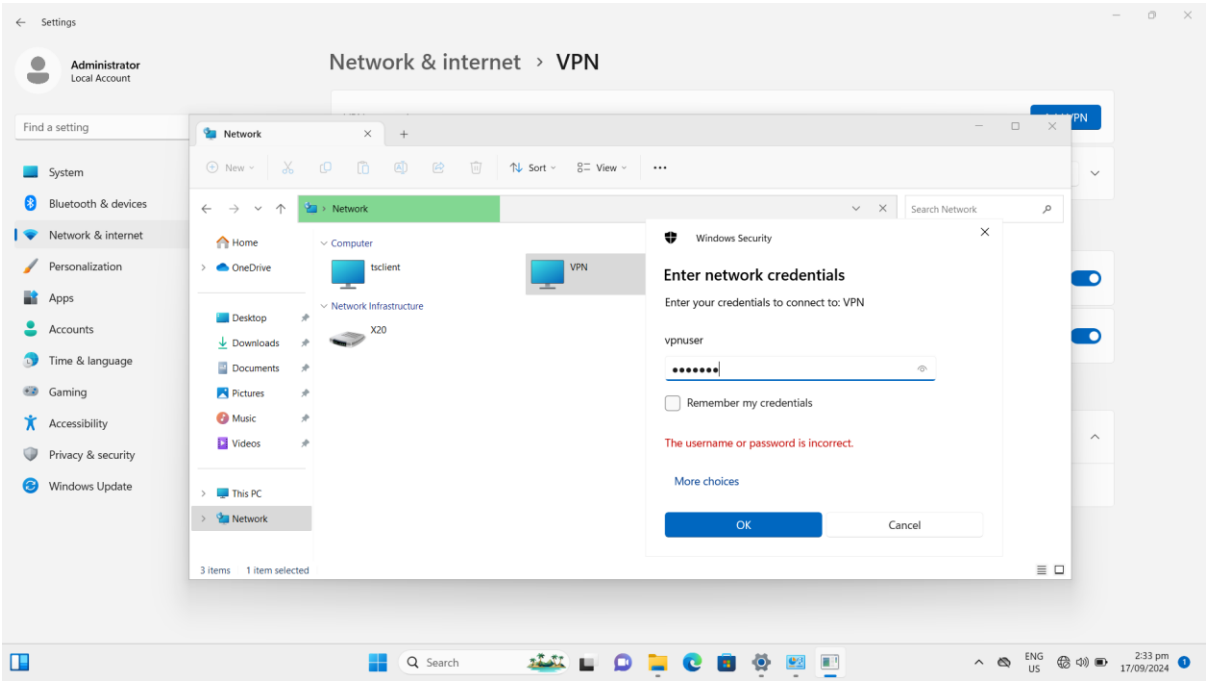
1. Connect the client machine VPN

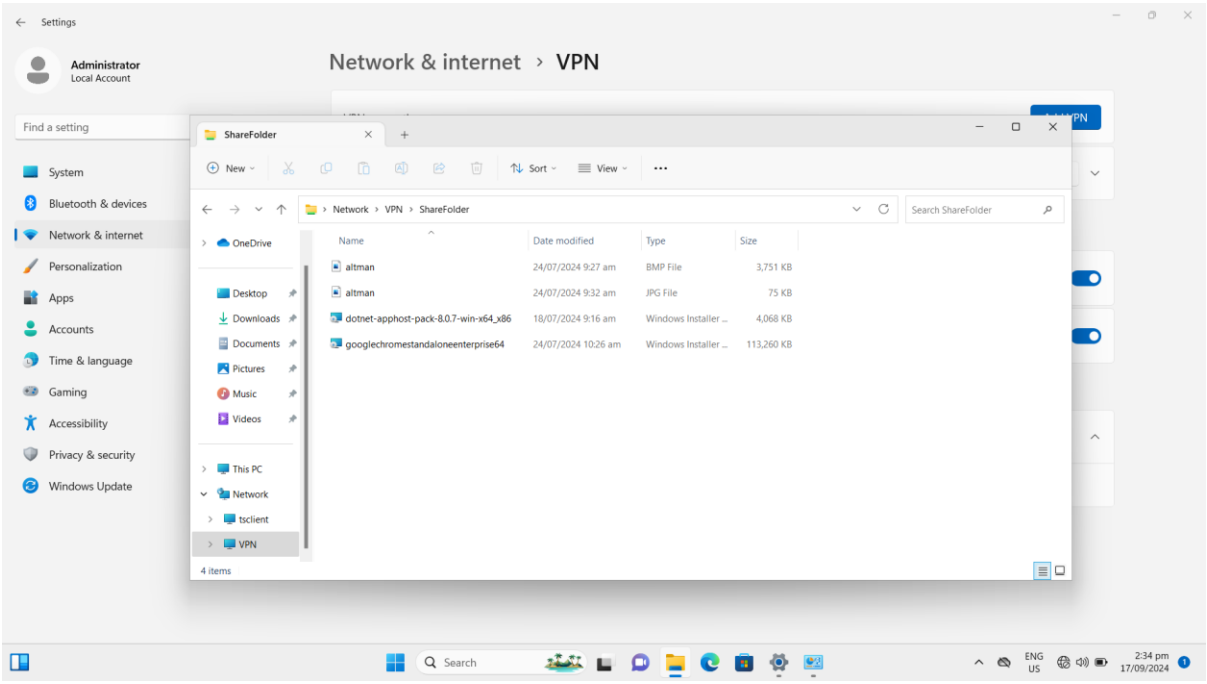





Settings
Administrator
Local Account
Find a setting
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Windows Update
Network & internet › VPN
VPN connections
Add VPN
NET602
Disconnect
On
On
Administrator: Command Prompt
C:\Users\Administrator>ipconfig
Before VPN connection
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::ae2e:770d:20d8:65a9%5
IPv4 Address. . . . . : 192.168.17.237
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . : 192.168.31.254
C:\Users\Administrator>ipconfig
After VPN connection
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::ae2e:770d:20d8:65a9%5
IPv4 Address. . . . . : 192.168.17.237
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . : 192.168.31.254
PPP adapter NET602:
Connection-specific DNS Suffix . : techco.co.nz
IPv4 Address. . . . . : 192.168.1.102
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 0.0.0.0
C:\Users\Administrator>
SL - NZ
In 7 hours
Search
ENG
US
10:09 am
18/09/2024

2. The VPN user “vpnuser” can access the shared folder on the VPN server:

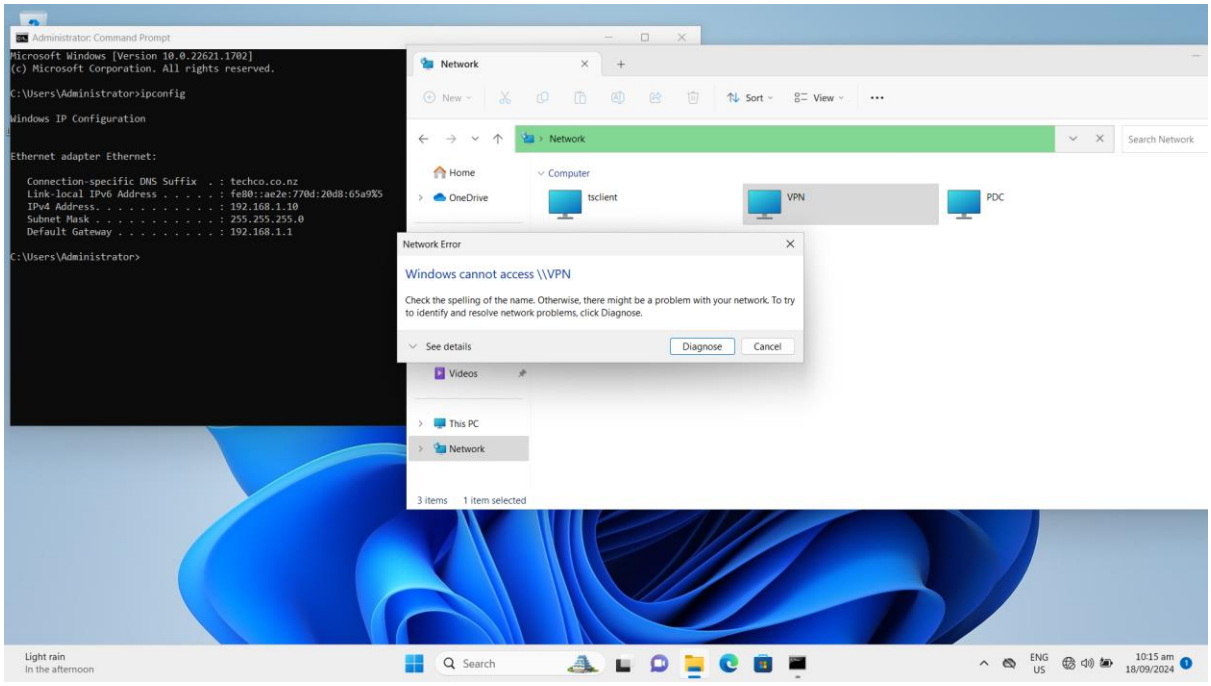




3. The shared folder cannot be accessed from the client machine since the IP address of the client machine is not in the range of firewall Inbound rules.

The IP address of the client machine is: 192.168.1.10

The range of firewall Inbound rules: 192.168.1.101~192.168.1.140

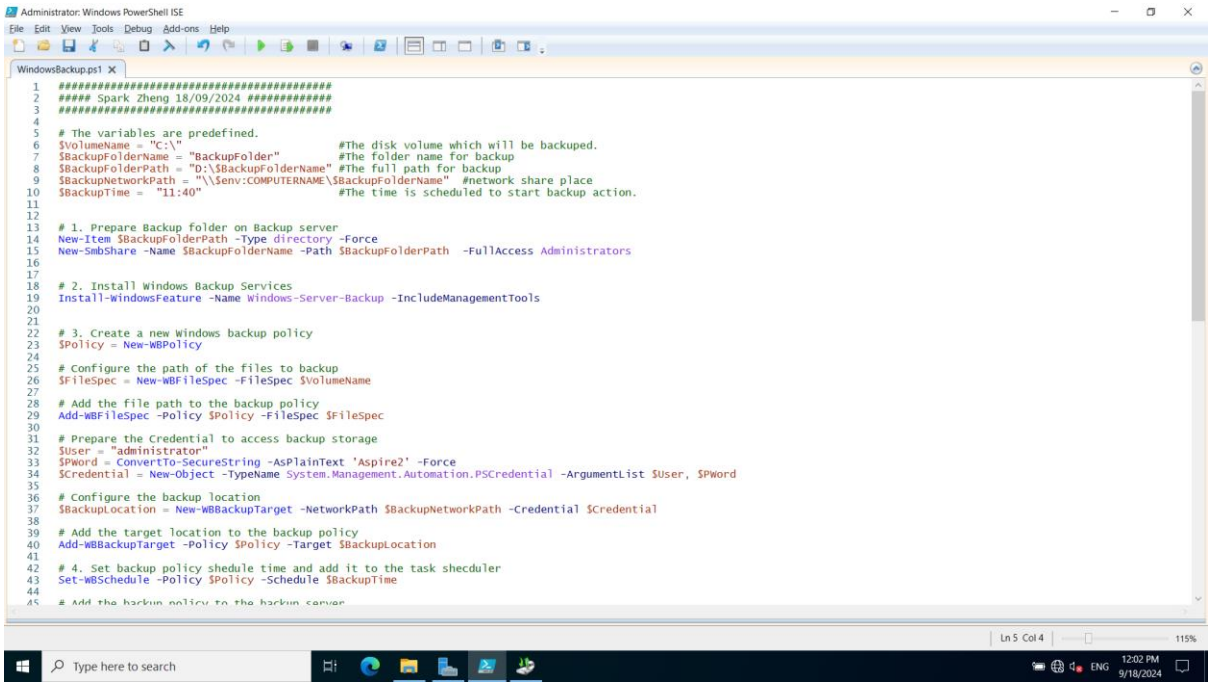


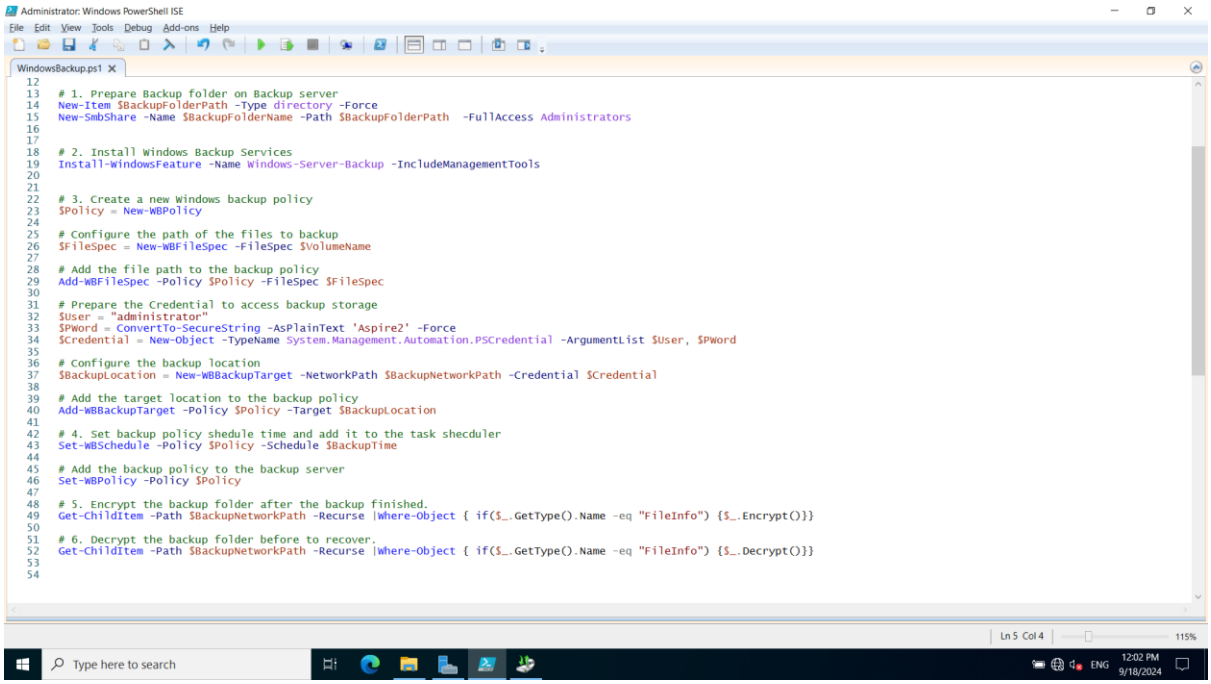
Task/Mahi 5: Implementing Server Backup

Task 5.1 Create a complete backup policy using PowerShell Scripts to automate the backup process

```
##########################################

##### Spark Zheng 18/09/2024 #############

##########################################


# The variables are predefined.

$VolumeName = "C:\"                    #The disk volume which will be backuped.

$BackupFolderName = "BackupFolder"         #The folder name for backup

$BackupFolderPath = "D:\$BackupFolderName" #The full path for backup

$BackupNetworkPath = "\\$env:COMPUTERNAME\$BackupFolderName"  #network share place

$BackupTime =  "11:40"                 #The time is scheduled to start backup action.


# 1. Prepare Backup folder on Backup server

New-Item $BackupFolderPath -Type directory -Force

New-SmbShare -Name $BackupFolderName -Path $BackupFolderPath  -FullAccess Administrators


# 2. Install Windows Backup Services

Install-WindowsFeature -Name Windows-Server-Backup -IncludeManagementTools


# 3. Create a new Windows backup policy

$Policy = New-WBPolicy


# Configure the path of the files to backup

$FileSpec = New-WBFileSpec -FileSpec $VolumeName


# Add the file path to the backup policy
```

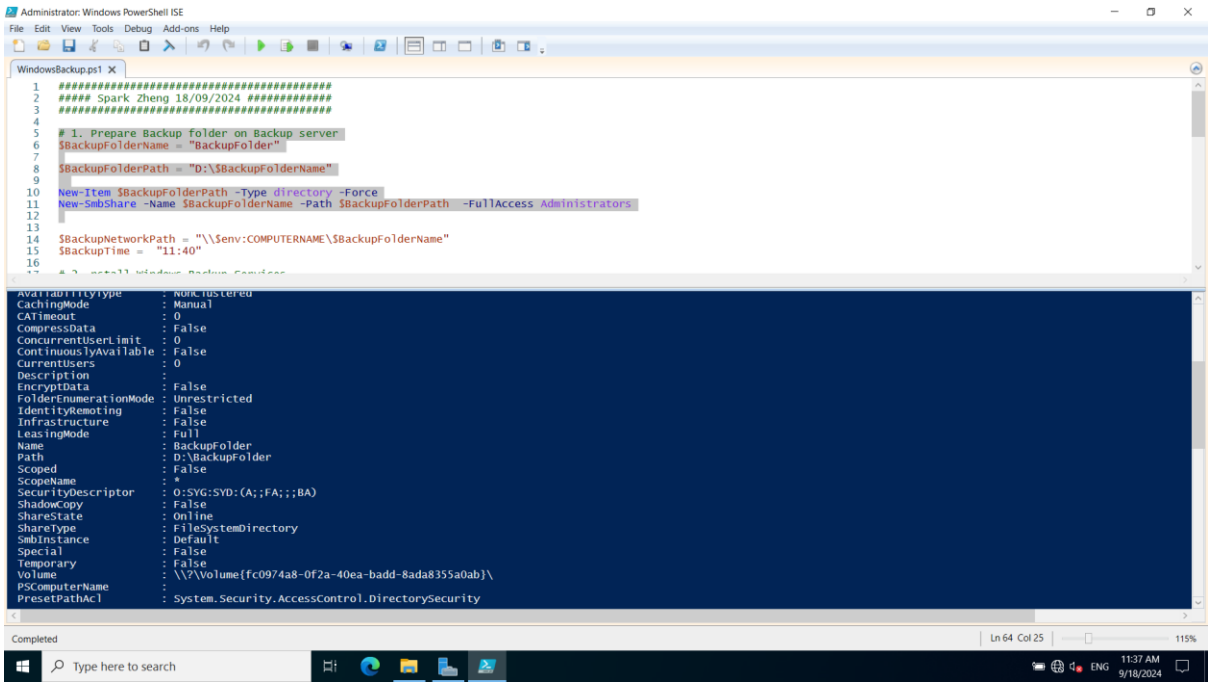
```
Add-WBFileSpec -Policy $Policy -FileSpec $FileSpec


# Prepare the Credential to access backup storage

$User = "administrator"

$PWord = ConvertTo-SecureString -AsPlainText 'Aspire2' -Force

$Credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $User, $PWord


# Configure the backup location

$BackupLocation = New-WBBackupTarget -NetworkPath $BackupNetworkPath -Credential $Credential


# Add the target location to the backup policy

Add-WBBackupTarget -Policy $Policy -Target $BackupLocation


# 4. Set backup policy schedule time and add it to the task scheduler

Set-WBSchedule -Policy $Policy -Schedule $BackupTime


# Add the backup policy to the backup server

Set-WBPolicy -Policy $Policy


# 5. Encrypt the backup folder after the backup finished.

Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_.Encrypt()}}


# 6. Decrypt the backup folder before to recover.

Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_.Decrypt()}}
```


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
WindowsBackup.ps1
##
Spark Zheng 18/09/2024
##
The variables are predefined.
$VolumeName = "C:\"   #The disk volume which will be backuped.
$BackupFolderName = "BackupFolder"   #The folder name for backup
$BackupFolderPath = "D:\$BackupFolderName" #The full path for backup
$BackupNetworkPath = "\\$env:COMPUTERNAME\$BackupFolderName" #network share place
$BackupTime = "11:40"   #The time is scheduled to start backup action.
1. Prepare Backup folder on Backup server
New-Item $BackupFolderPath -Type directory -Force
New-SmbShare -Name $BackupFolderName -Path $BackupFolderPath -FullAccess Administrators
2. Install Windows Backup Services
Install-WindowsFeature -Name Windows-Server-Backup -IncludeManagementTools
3. Create a new Windows backup policy
$Policy = New-WBPolicy
Configure the path of the files to backup
$FileSpec = New-WBFileSpec -FileSpec $VolumeName
Add the file path to the backup policy
Add-WBFileSpec -Policy $Policy -FileSpec $FileSpec
Prepare the Credential to access backup storage
$User = "administrator"
$PWord = ConvertTo-SecureString -AsPlainText 'Aspire2' -Force
$Credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $User, $PWord
Configure the backup location
$BackupLocation = New-WBBackupTarget -NetworkPath $BackupNetworkPath -Credential $Credential
Add the target location to the backup policy
Add-WBBackupTarget -Policy $Policy -Target $BackupLocation
4. Set backup policy shedule time and add it to the task shecduler
Set-WBSchedule -Policy $Policy -Schedule $BackupTime
Ln 5 Col 4
115%
Type here to search
ENG
12:02 PM
9/18/2024

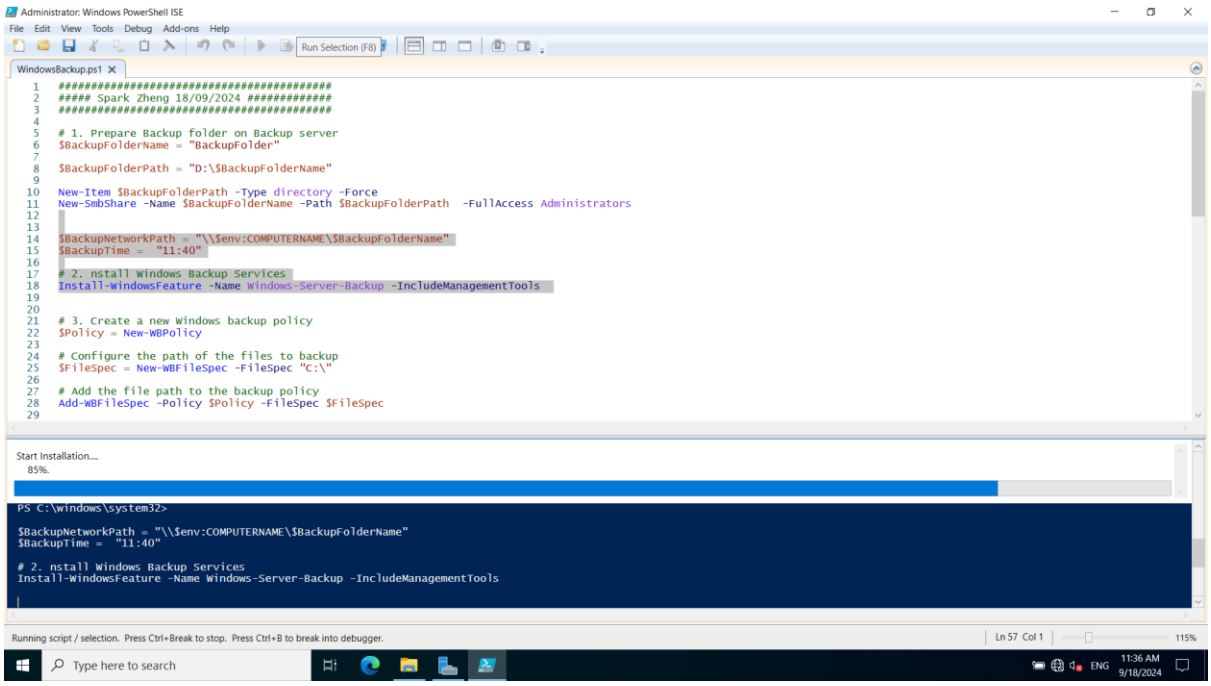

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
WindowsBackup.ps1
1. Prepare Backup folder on Backup server
New-Item $BackupFolderPath -Type directory -Force
New-SmbShare -Name $BackupFolderName -Path $BackupFolderPath -FullAccess Administrators
2. Install Windows Backup Services
Install-WindowsFeature -Name Windows-Server-Backup -IncludeManagementTools
3. Create a new Windows backup policy
$Policy = New-WBPolicy
Configure the path of the files to backup
$FileSpec = New-WBFileSpec -FileSpec $VolumeName
Add the file path to the backup policy
Add-WBFileSpec -Policy $Policy -FileSpec $FileSpec
Prepare the Credential to access backup storage
$User = "administrator"
$PWord = ConvertTo-SecureString -AsPlainText 'Aspire2' -Force
$Credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $User, $PWord
Configure the backup location
$BackupLocation = New-WBBackupTarget -NetworkPath $BackupNetworkPath -Credential $Credential
Add the target location to the backup policy
Add-WBBackupTarget -Policy $Policy -Target $BackupLocation
4. Set backup policy shedule time and add it to the task shecduler
Set-WBSchedule -Policy $Policy -Schedule $BackupTime
Add the backup policy to the backup server
Set-WBPolicy -Policy $Policy
5. Encrypt the backup folder after the backup finished.
Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_.Encrypt()}}
6. Decrypt the backup folder before to recover.
Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_.Decrypt()}}
Ln 5 Col 4
115%
Type here to search
ENG
12:02 PM
9/18/2024

Task 5.2 Configure Windows backup using the PowerShell Script

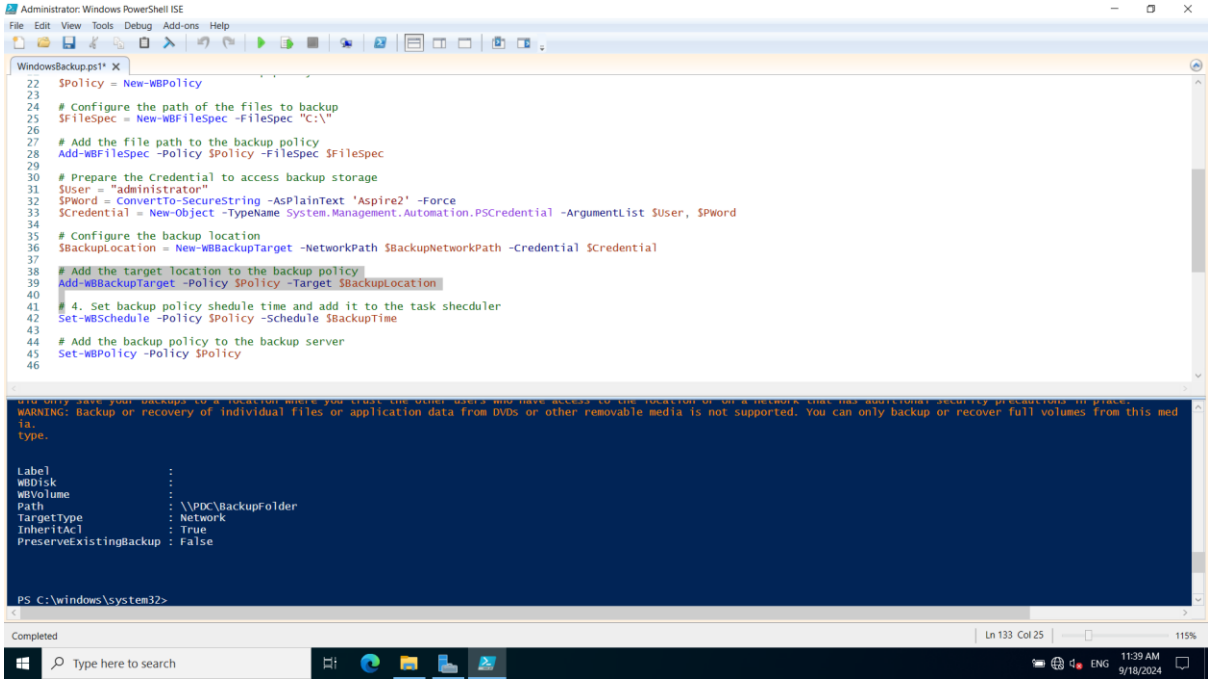
1. Prepare Backup folder on Backup server



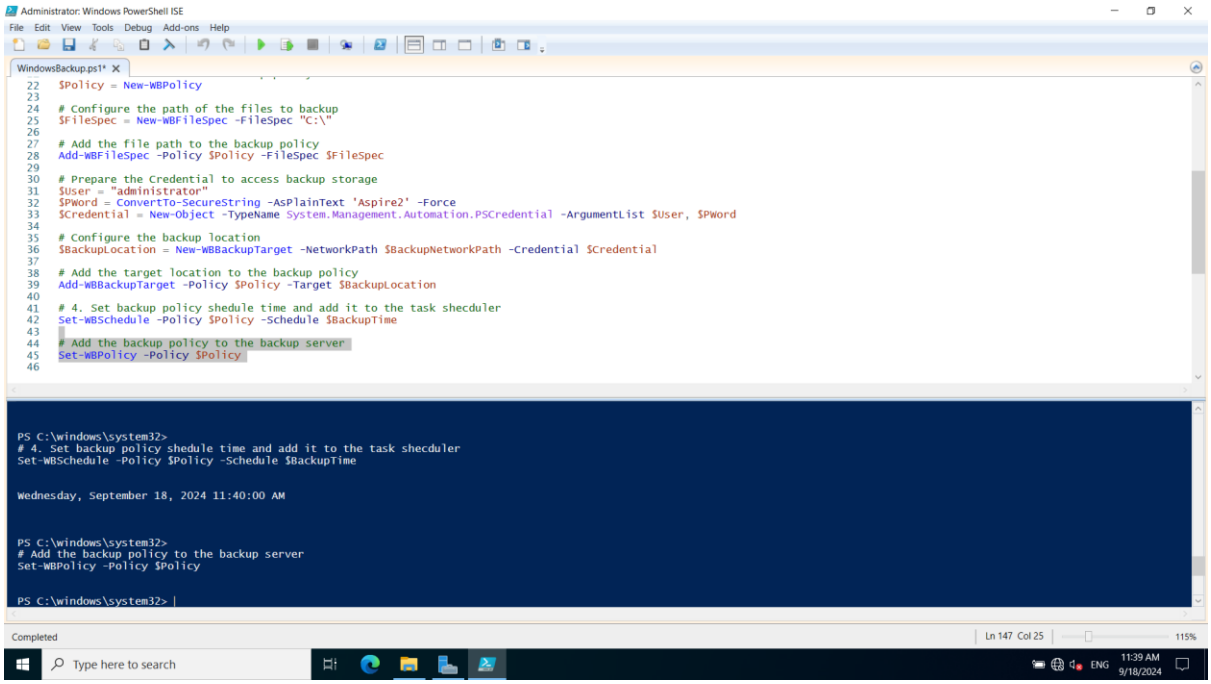
2. Install Windows Backup Services



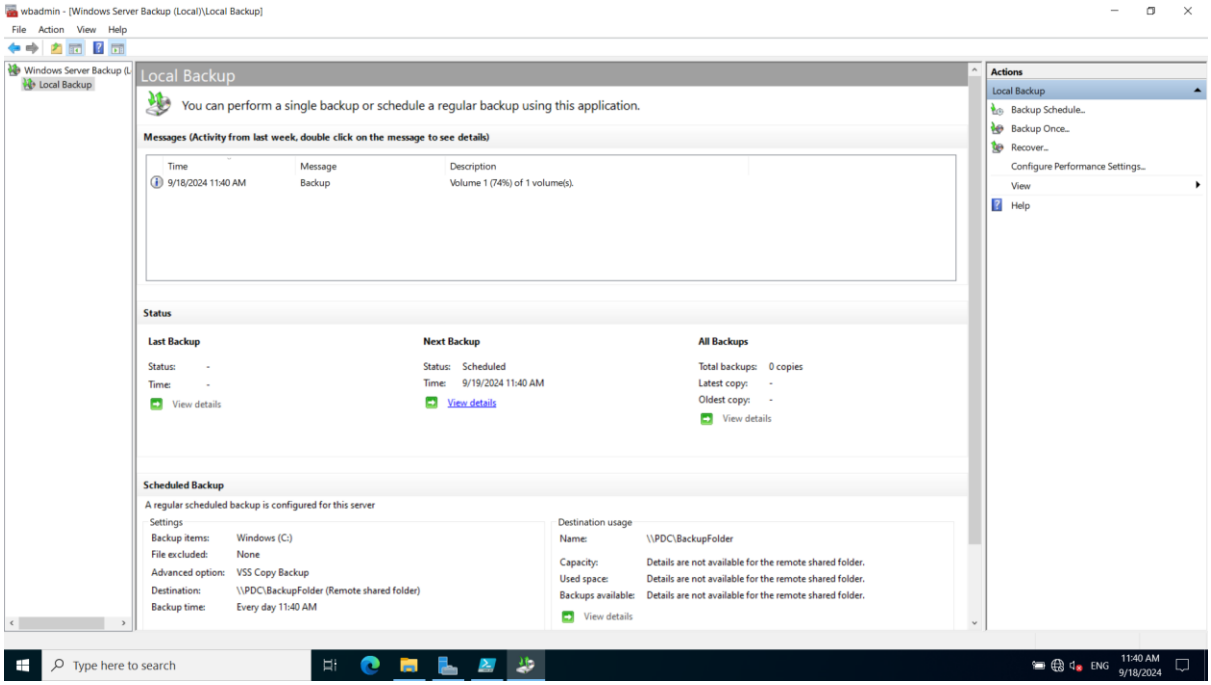
3. Create a new Windows backup policy

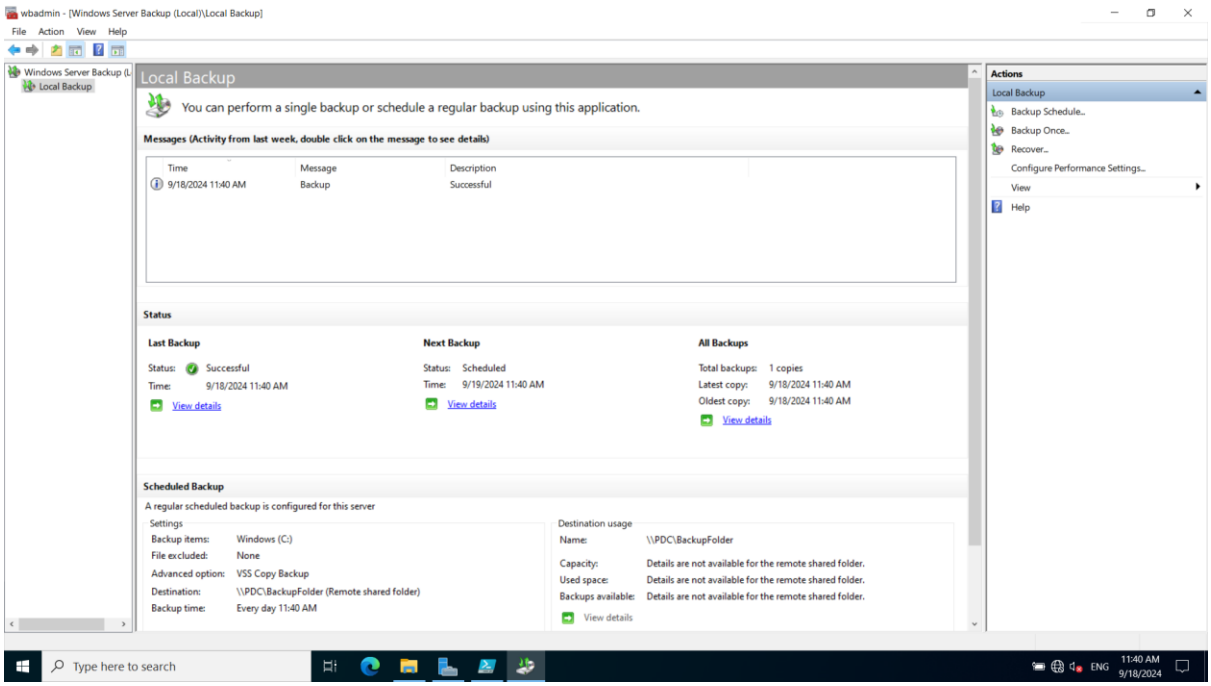


4. Set backup policy schedule time and add it to the task scheduler

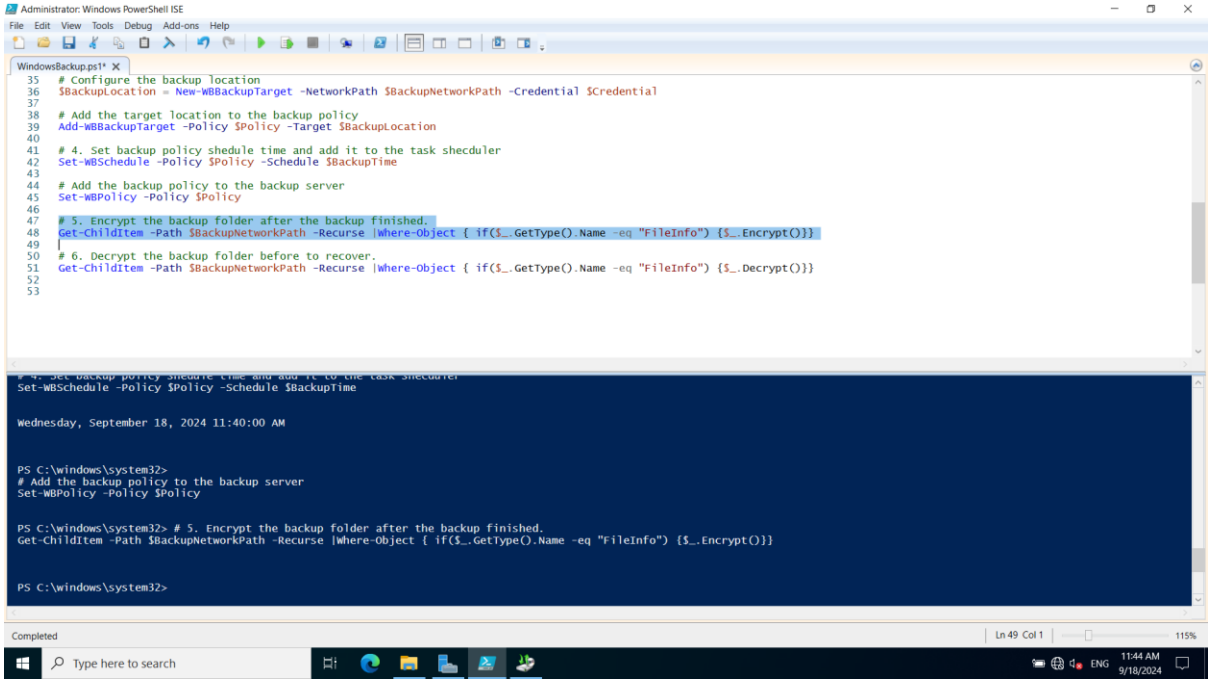


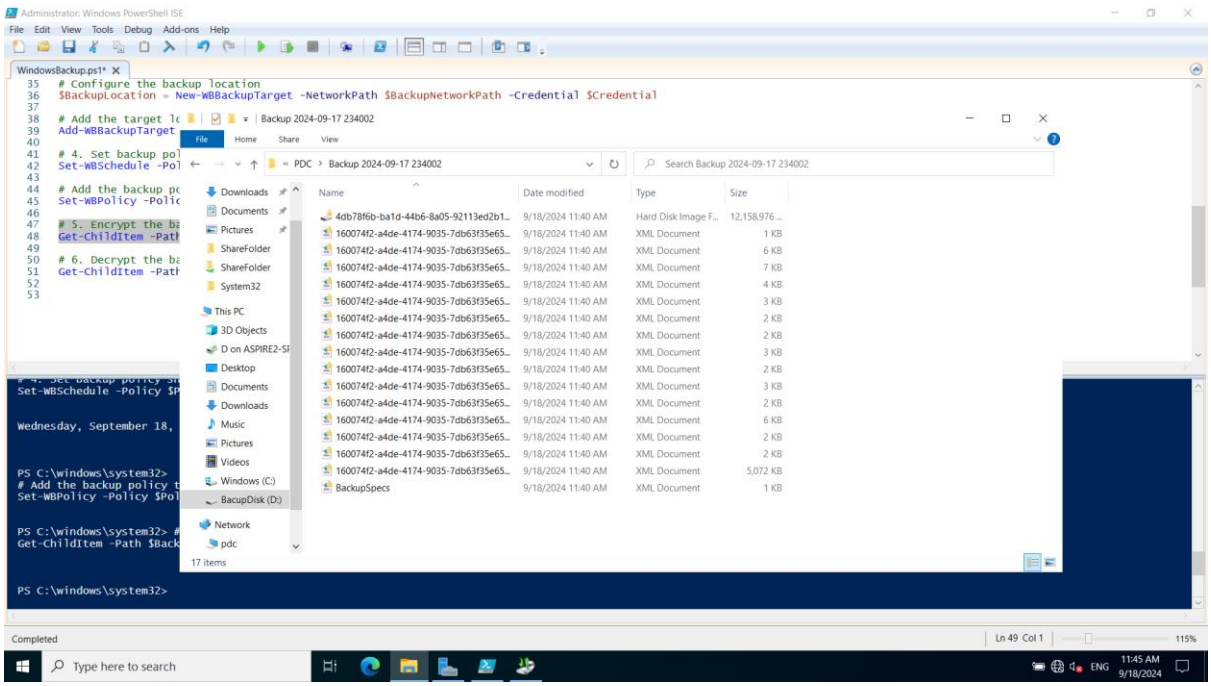
5. Check Backup status on Windows Server Backup console



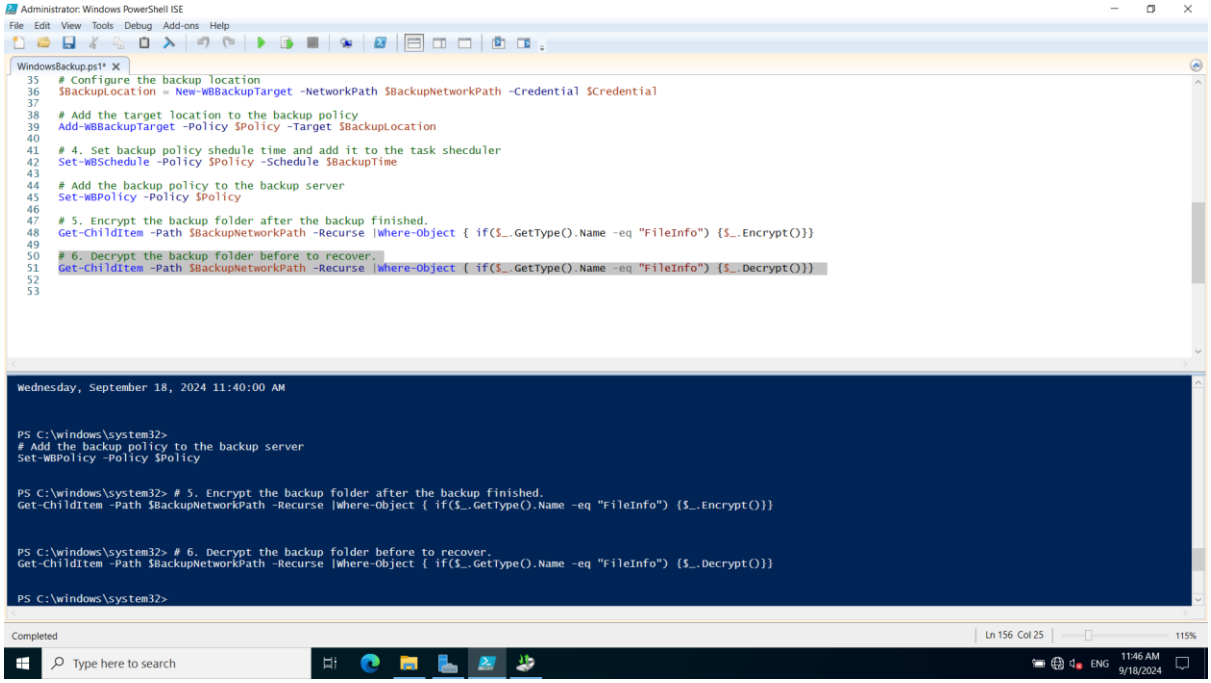


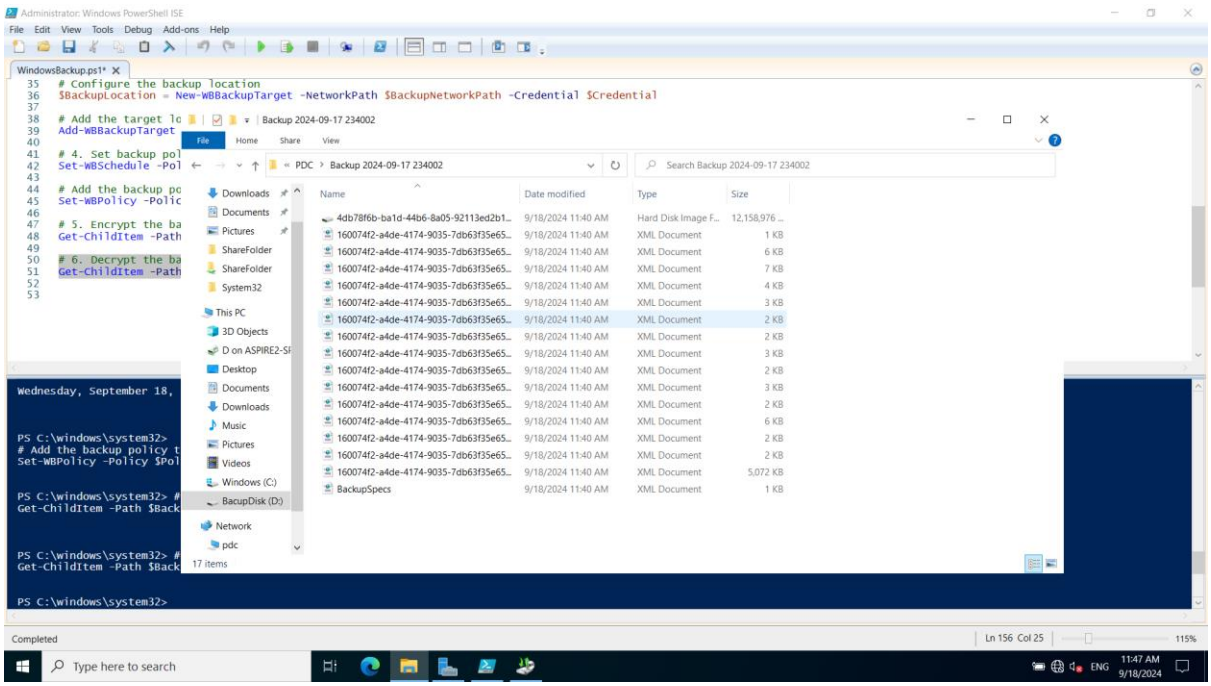
6. Encrypt the backup folder after the backup finished.





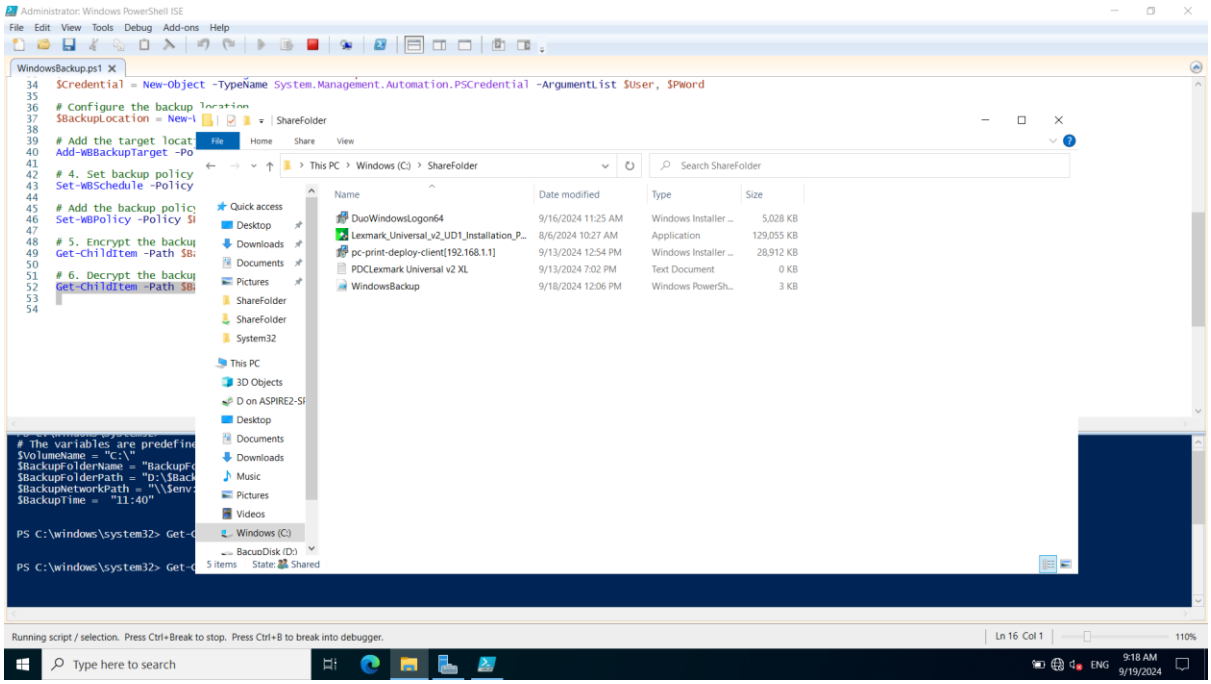
7. Decrypt the backup folder before to recover.



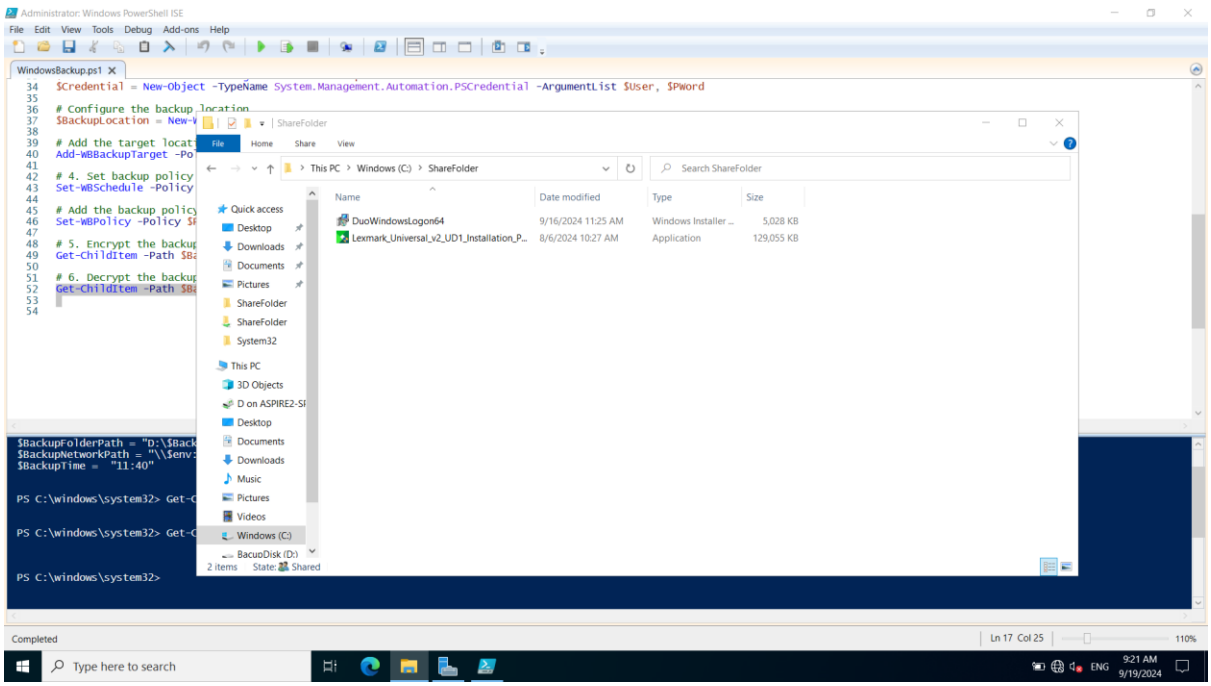


8. Recover a specified folder from a backup

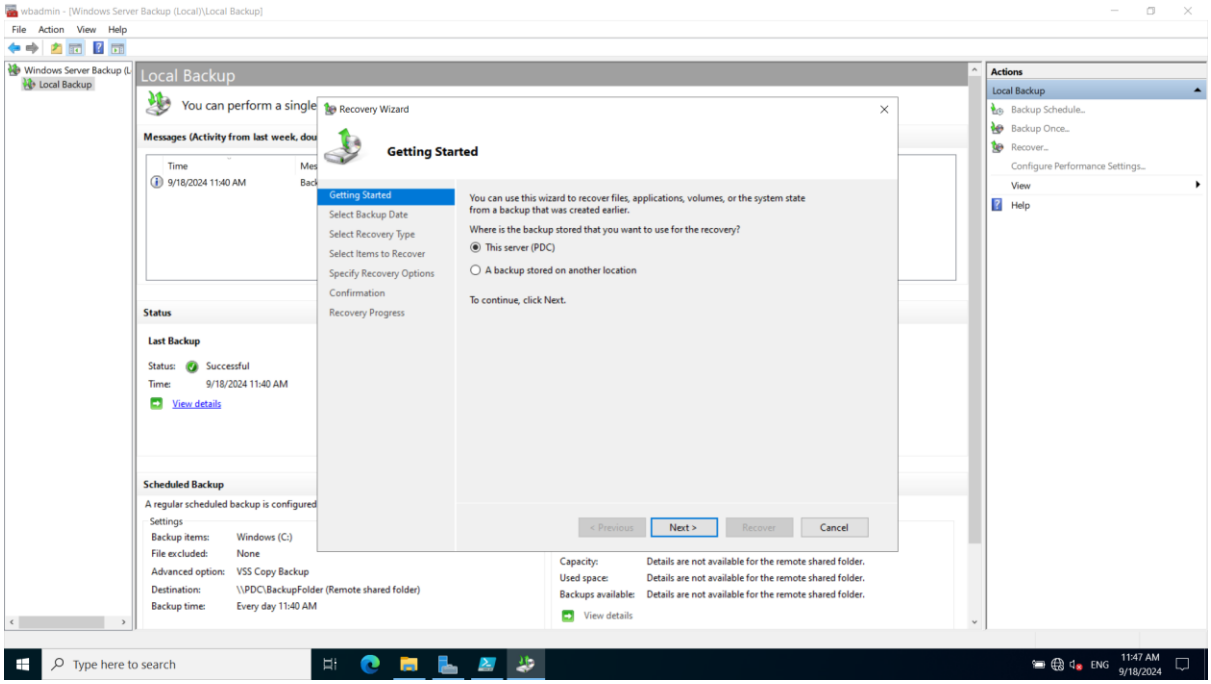
There are 5 files in C:\Sharefolder at the beginning of test.

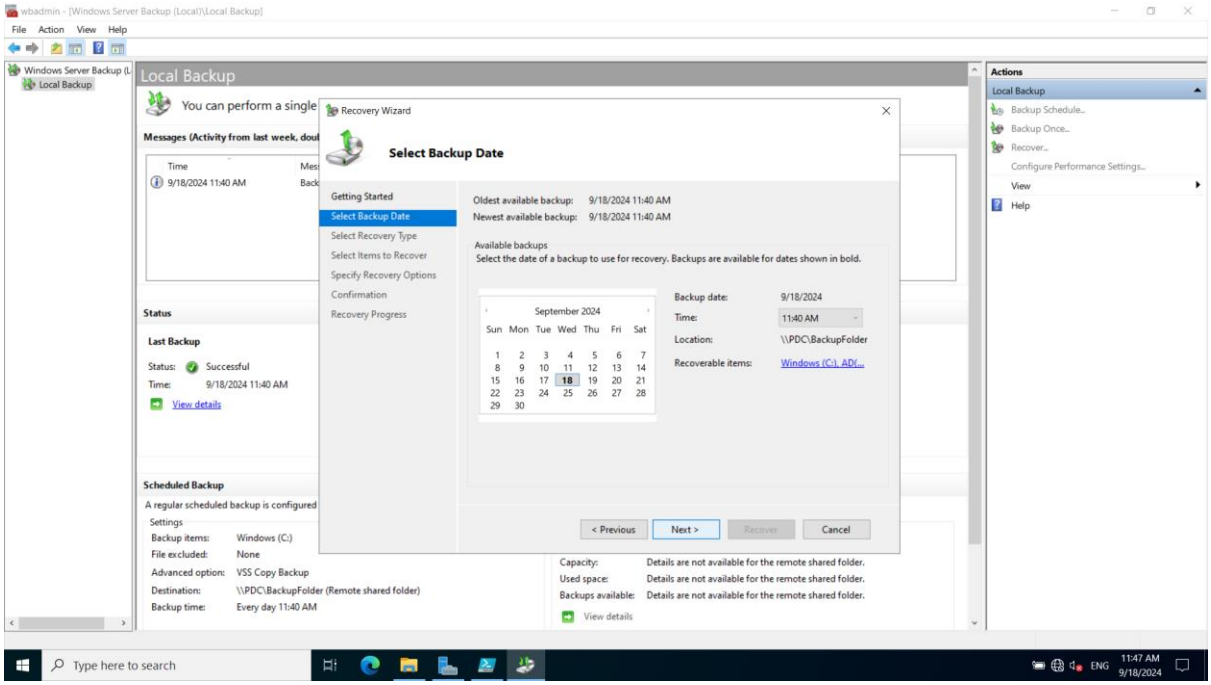


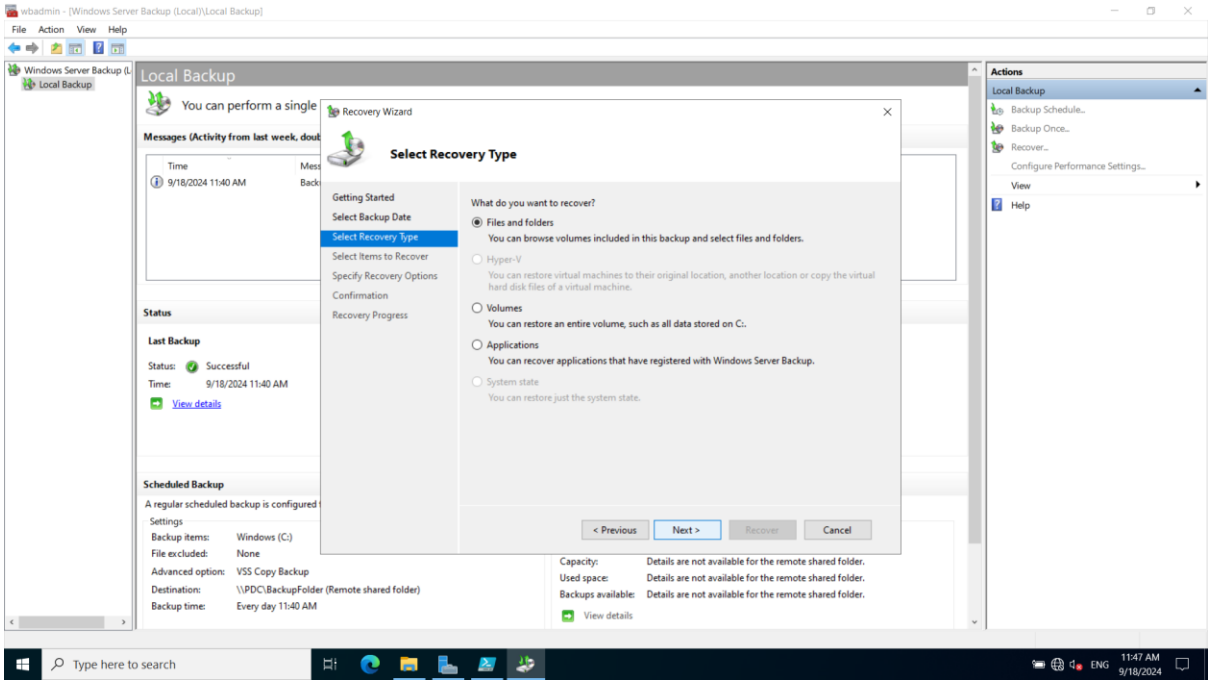
Then 3 files are deleted accidentally:

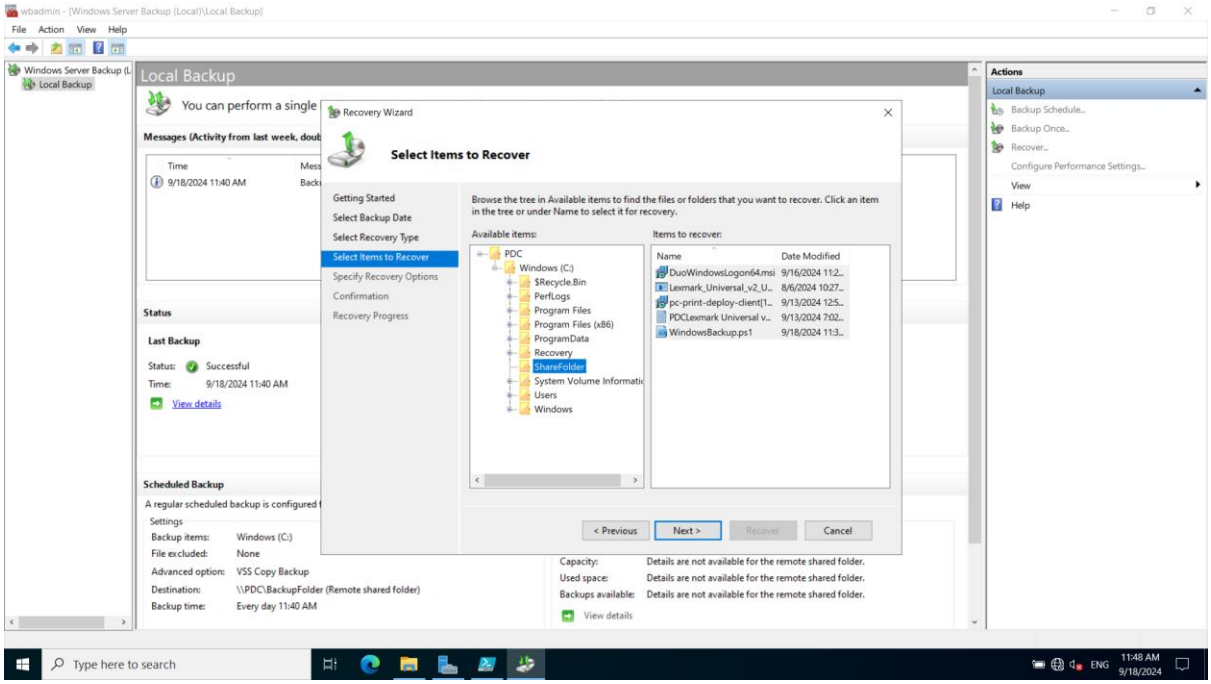


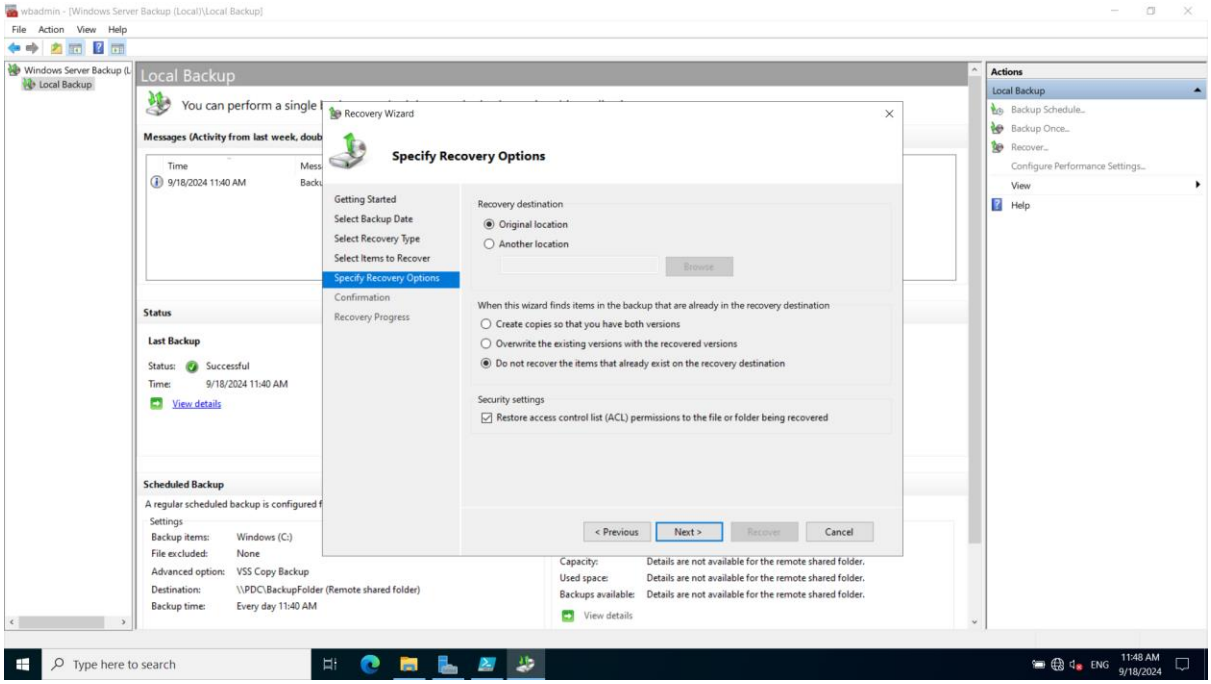
Start a new recover process:

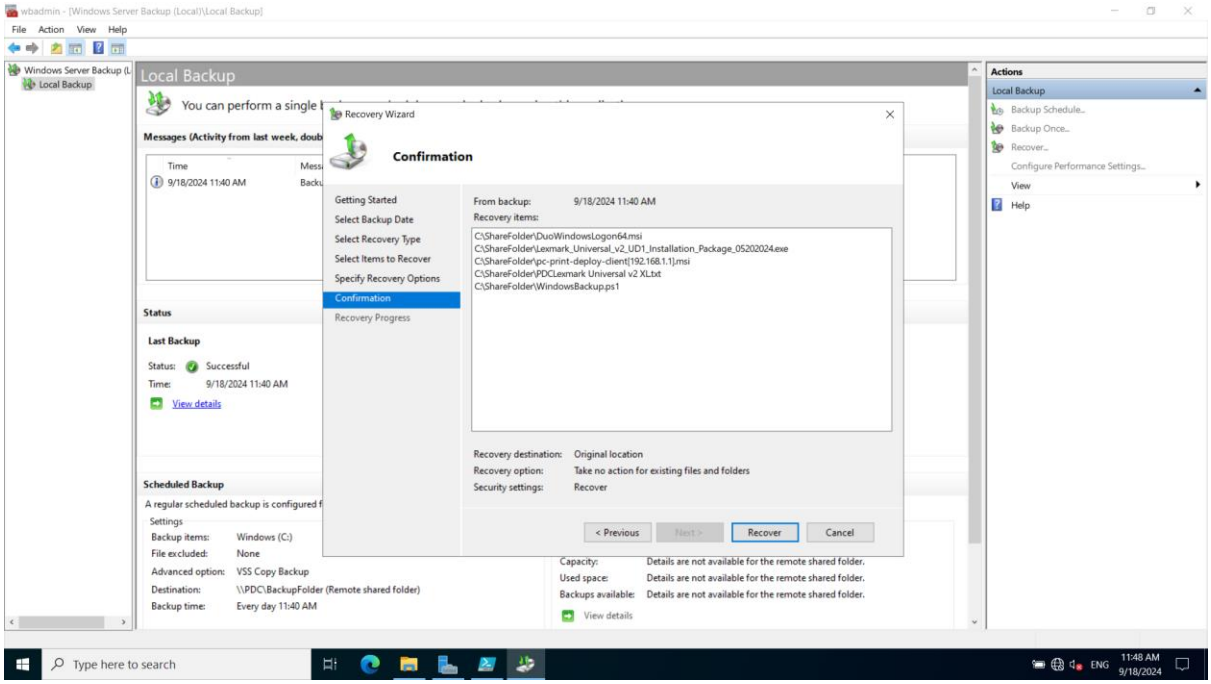


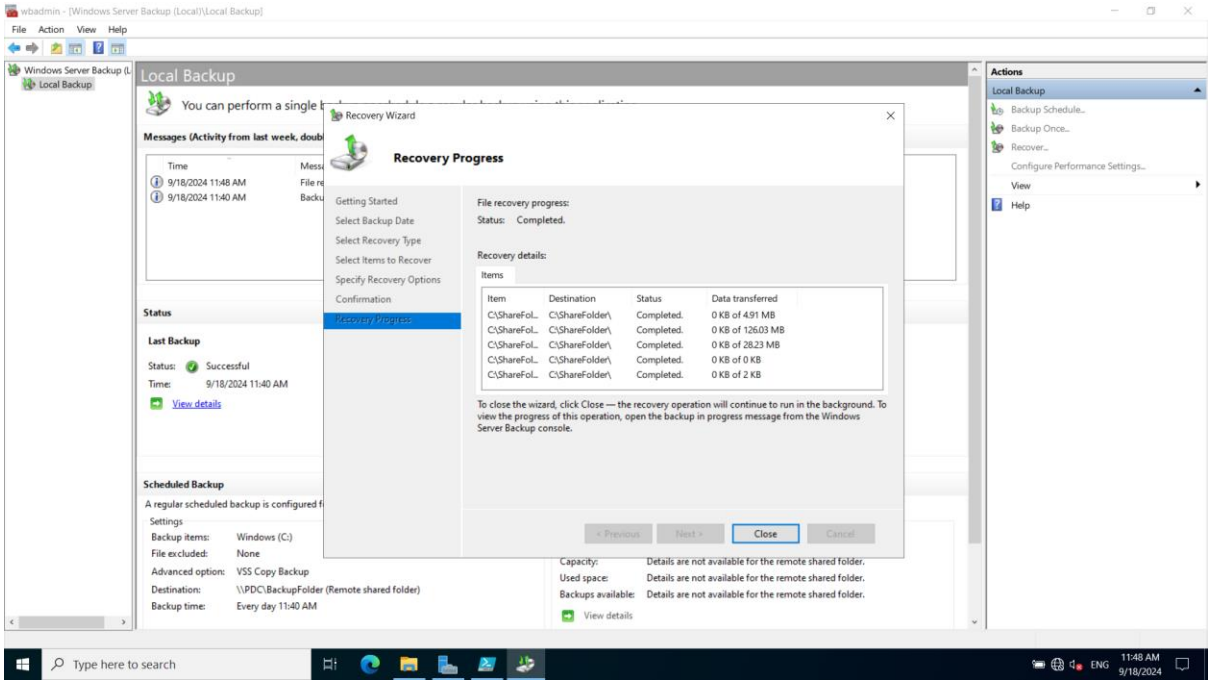


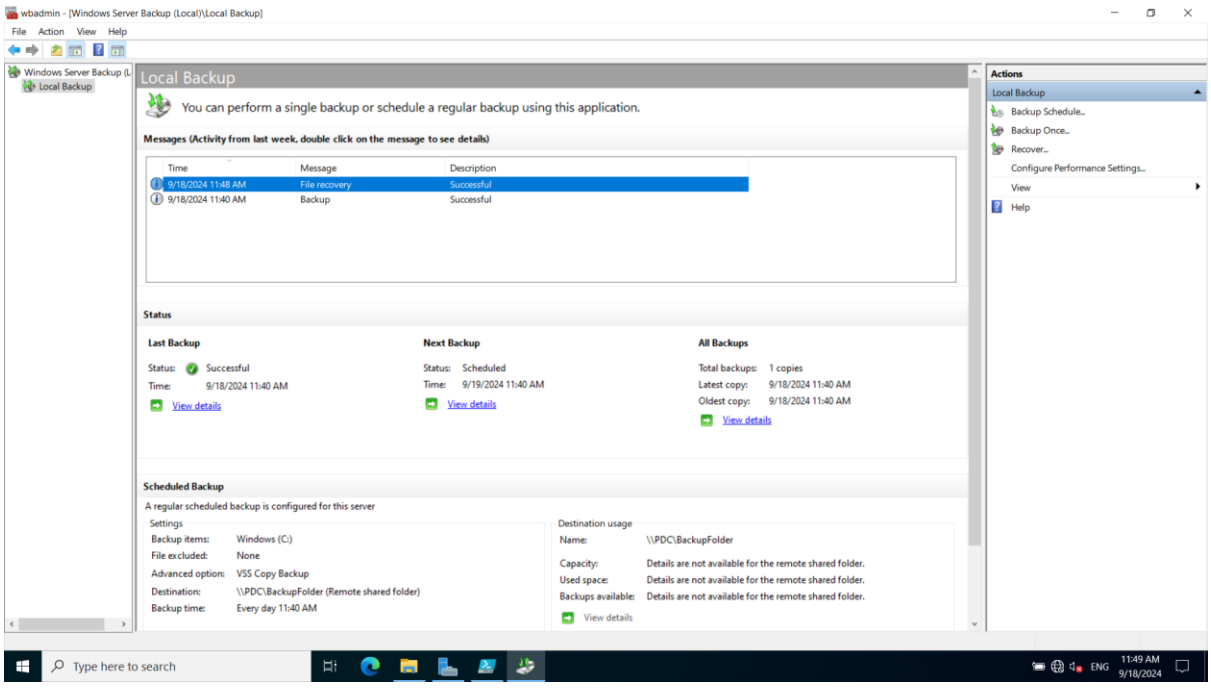

wbadmin - [Windows Server Backup (Local)\Local Backup]
File Action View Help
Windows Server Backup (L
Local Backup
Local Backup
You can perform a single
Messages (Activity from last week, doub
Time
9/18/2024 11:40 AM
Status
Last Backup
Status: Successful
Time: 9/18/2024 11:40 AM
View details
Scheduled Backup
A regular scheduled backup is configured
Settings
Backup items: Windows (C:)
File excluded: None
Advanced option: VSS Copy Backup
Destination: \\PDC\BackupFolder (Remote shared folder)
Backup time: Every day 11:40 AM
Capacity: Details are not available for the remote shared folder.
Used space: Details are not available for the remote shared folder.
Backups available: Details are not available for the remote shared folder.
View details
Actions
Local Backup
Backup Schedule...
Backup Once...
Recover...
Configure Performance Settings...
View
Help
Recovery Wizard
Select Recovery Type
Getting Started
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
What do you want to recover?
Files and folders
You can browse volumes included in this backup and select files and folders.
Hyper-V
You can restore virtual machines to their original location, another location or copy the virtual hard disk files of a virtual machine.
Volumes
You can restore an entire volume, such as all data stored on C:.
Applications
You can recover applications that have registered with Windows Server Backup.
System state
You can restore just the system state.
< Previous
Next >
Recover
Cancel
Type here to search
ENG
11:47 AM
9/18/2024


wbadmin - [Windows Server Backup (Local)\Local Backup]
File Action View Help
Windows Server Backup (L
Local Backup
Local Backup
You can perform a single
Messages (Activity from last week, doub
Time
9/18/2024 11:40 AM
Status
Last Backup
Status: Successful
Time: 9/18/2024 11:40 AM
View details
Scheduled Backup
A regular scheduled backup is configured
Settings
Backup items: Windows (C:)
File excluded: None
Advanced option: VSS Copy Backup
Destination: \\PDC\BackupFolder (Remote shared folder)
Backup time: Every day 11:40 AM
Capacity: Details are not available for the remote shared folder.
Used space: Details are not available for the remote shared folder.
Backups available: Details are not available for the remote shared folder.
View details
Actions
Local Backup
Backup Schedule...
Backup Once...
Recover...
Configure Performance Settings...
View
Help
Recovery Wizard
Select Items to Recover
Getting Started
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
Browse the tree in Available items to find the files or folders that you want to recover. Click an item in the tree or under Name to select it for recovery.
Available items:
Items to recover:
PDC
Windows (C:)
$Recycle.Bin
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
ShareFolder
System Volume Informatic
Users
Windows
Name
Date Modified
DuoWindowsLogon64.msi 9/16/2024 11:2...
Lexmark_Universal_v2_U... 8/6/2024 10:27...
pc-print-deploy-client[1... 9/13/2024 12:5...
PDCLexmark Universal v... 9/13/2024 7:02...
WindowsBackup.ps1 9/18/2024 11:3...
< Previous
Next >
Recover
Cancel
Type here to search
ENG
11:48 AM
9/18/2024

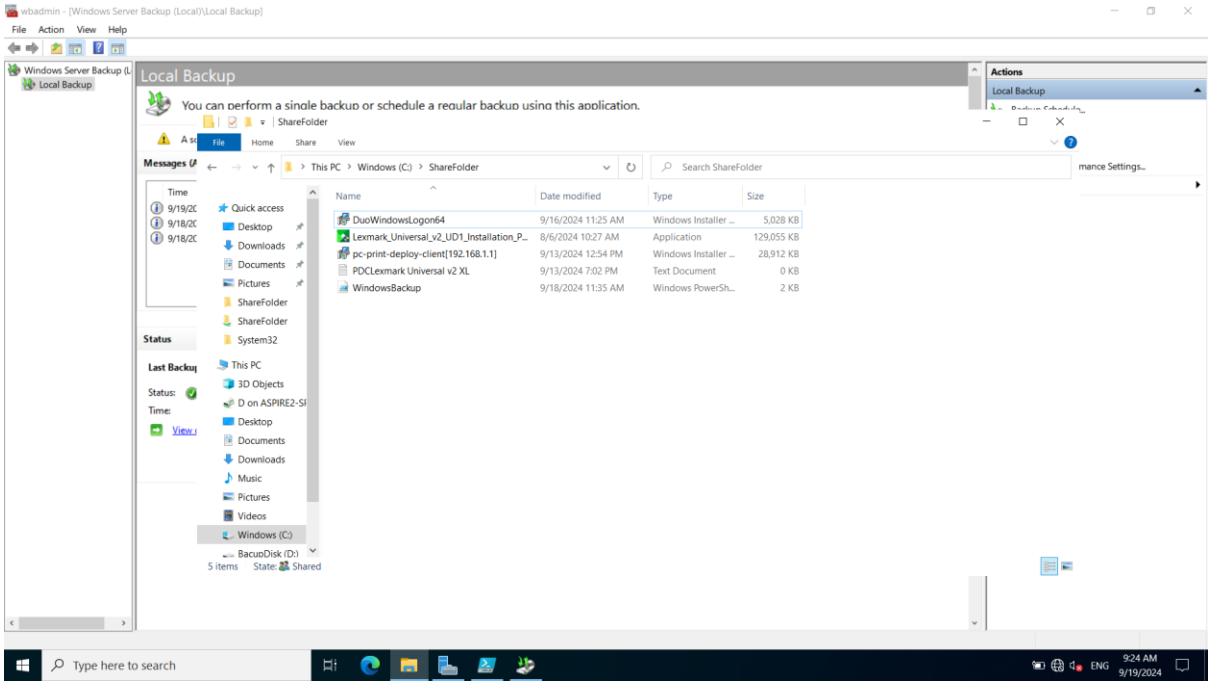

wbadmin - [Windows Server Backup (Local)\Local Backup]
File Action View Help
Windows Server Backup (L
Local Backup
Local Backup
You can perform a single
Messages (Activity from last week, doub
Time
9/18/2024 11:40 AM
Status
Last Backup
Status: Successful
Time: 9/18/2024 11:40 AM
View details
Scheduled Backup
A regular scheduled backup is configured
Settings
Backup items: Windows (C:)
File excluded: None
Advanced option: VSS Copy Backup
Destination: \\PDC\BackupFolder (Remote shared folder)
Backup time: Every day 11:40 AM
Capacity: Details are not available for the remote shared folder.
Used space: Details are not available for the remote shared folder.
Backups available: Details are not available for the remote shared folder.
View details
Actions
Local Backup
Backup Schedule...
Backup Once...
Recover...
Configure Performance Settings...
View
Help
Recovery Wizard
Specify Recovery Options
Getting Started
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
Recovery destination
Original location
Another location
Browse
When this wizard finds items in the backup that are already in the recovery destination
Create copies so that you have both versions
Overwrite the existing versions with the recovered versions
Do not recover the items that already exist on the recovery destination
Security settings
Restore access control list (ACL) permissions to the file or folder being recovered
< Previous
Next >
Recover
Cancel
Type here to search
ENG
11:48 AM
9/18/2024


wbadmin - [Windows Server Backup (Local)\Local Backup]
File Action View Help
Windows Server Backup (L
Local Backup
Local Backup
You can perform a single
Messages (Activity from last week, doub
Time
9/18/2024 11:40 AM
Status
Last Backup
Status: Successful
Time: 9/18/2024 11:40 AM
View details
Scheduled Backup
A regular scheduled backup is configured
Settings
Backup items: Windows (C:)
File excluded: None
Advanced option: VSS Copy Backup
Destination: \\PDC\BackupFolder (Remote shared folder)
Backup time: Every day 11:40 AM
Capacity: Details are not available for the remote shared folder.
Used space: Details are not available for the remote shared folder.
Backups available: Details are not available for the remote shared folder.
View details
Actions
Local Backup
Backup Schedule...
Backup Once...
Recover...
Configure Performance Settings...
View
Help
Recovery Wizard
Confirmation
Getting Started
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
From backup: 9/18/2024 11:40 AM
Recovery items:
C:\ShareFolder\DuoWindowsLogon64.msi
C:\ShareFolder\Lexmark_Universal_v2_UD1_Installation_Package_05202024.exe
C:\ShareFolder\pc-print-deploy-client[192.168.1.1].msi
C:\ShareFolder\PDCLexmark Universal v2 XL.txt
C:\ShareFolder\WindowsBackup.ps1
Recovery destination: Original location
Recovery option: Take no action for existing files and folders
Security settings: Recover
< Previous
Next >
Recover
Cancel
Type here to search
ENG
11:48 AM
9/18/2024


wbadmin - [Windows Server Backup (Local)\Local Backup]
File Action View Help
Windows Server Backup (L
Local Backup
Local Backup
You can perform a single b
Messages (Activity from last week, doub
Time
9/18/2024 11:48 AM
9/18/2024 11:40 AM
Status
Last Backup
Status: Successful
Time: 9/18/2024 11:40 AM
View details
Scheduled Backup
A regular scheduled backup is configured f
Settings
Backup items: Windows (C:)
File excluded: None
Advanced option: VSS Copy Backup
Destination: \\PDC\BackupFolder (Remote shared folder)
Backup time: Every day 11:40 AM
Recovery Wizard
Recovery Progress
Getting Started
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
File recovery progress:
Status: Completed.
Recovery details:
Items
Item
Destination
Status
Data transferred
C:\ShareFol...
C:\ShareFolder\
Completed.
0 KB of 4.91 MB
0 KB of 126.03 MB
0 KB of 28.23 MB
0 KB of 0 KB
0 KB of 2 KB
To close the wizard, click Close — the recovery operation will continue to run in the background. To view the progress of this operation, open the backup in progress message from the Windows Server Backup console.
< Previous
Next >
Close
Cancel
Capacity: Details are not available for the remote shared folder.
Used space: Details are not available for the remote shared folder.
Backups available: Details are not available for the remote shared folder.
View details
Actions
Local Backup
Backup Schedule...
Backup Once...
Recover...
Configure Performance Settings...
View
Help
Type here to search
ENG
11:48 AM
9/18/2024


wbadmin - [Windows Server Backup (Local)\Local Backup]
File Action View Help
Windows Server Backup (L
Local Backup
Local Backup
You can perform a single backup or schedule a regular backup using this application.
Messages (Activity from last week, double click on the message to see details)
Time
Message
Description
9/18/2024 11:48 AM
File recovery
Successful
9/18/2024 11:40 AM
Backup
Successful
Status
Last Backup
Status: Successful
Time: 9/18/2024 11:40 AM
View details
Next Backup
Status: Scheduled
Time: 9/19/2024 11:40 AM
View details
All Backups
Total backups: 1 copies
Latest copy: 9/18/2024 11:40 AM
Oldest copy: 9/18/2024 11:40 AM
View details
Scheduled Backup
A regular scheduled backup is configured for this server
Settings
Backup items: Windows (C:)
File excluded: None
Advanced option: VSS Copy Backup
Destination: \\PDC\BackupFolder (Remote shared folder)
Backup time: Every day 11:40 AM
Destination usage
Name: \\PDC\BackupFolder
Capacity: Details are not available for the remote shared folder.
Used space: Details are not available for the remote shared folder.
Backups available: Details are not available for the remote shared folder.
View details
Actions
Local Backup
Backup Schedule...
Backup Once...
Recover...
Configure Performance Settings...
View
Help
Type here to search
ENG
11:49 AM
9/18/2024

The 3 files deleted accidentally have been recovered to the original place:



Task/Mahi 6: Implementing and Managing Intrusion Detection System (IDS)

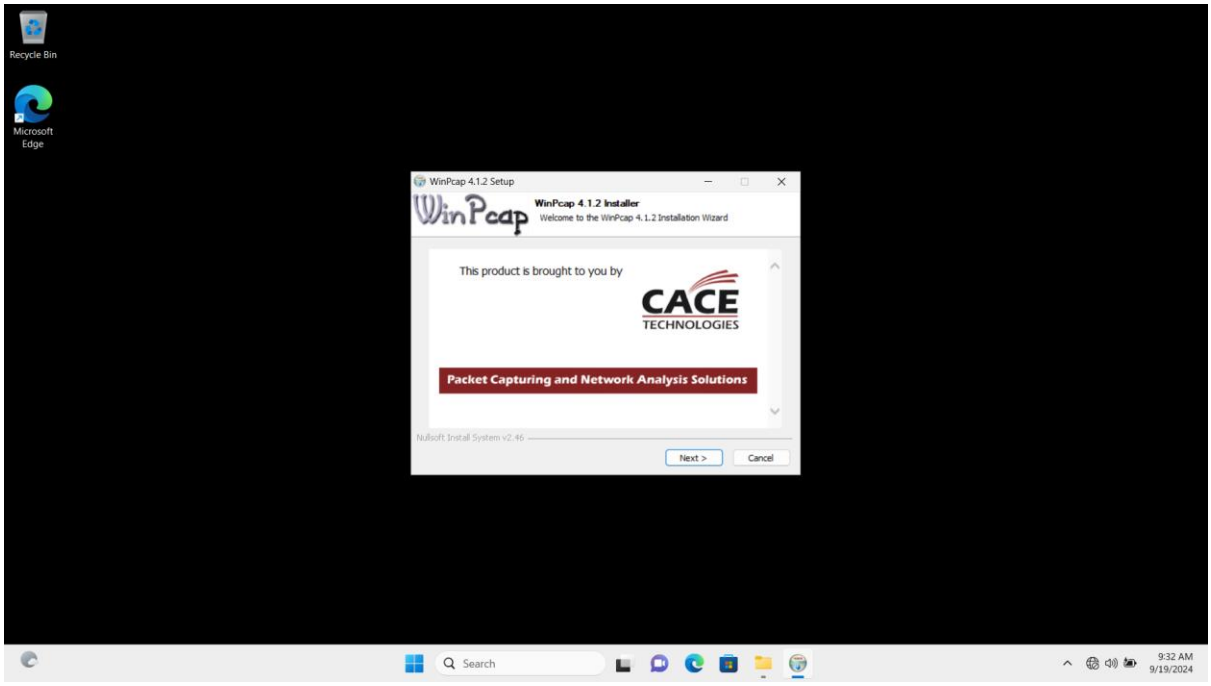
Task 6.1: IDS Deployment and Configuration

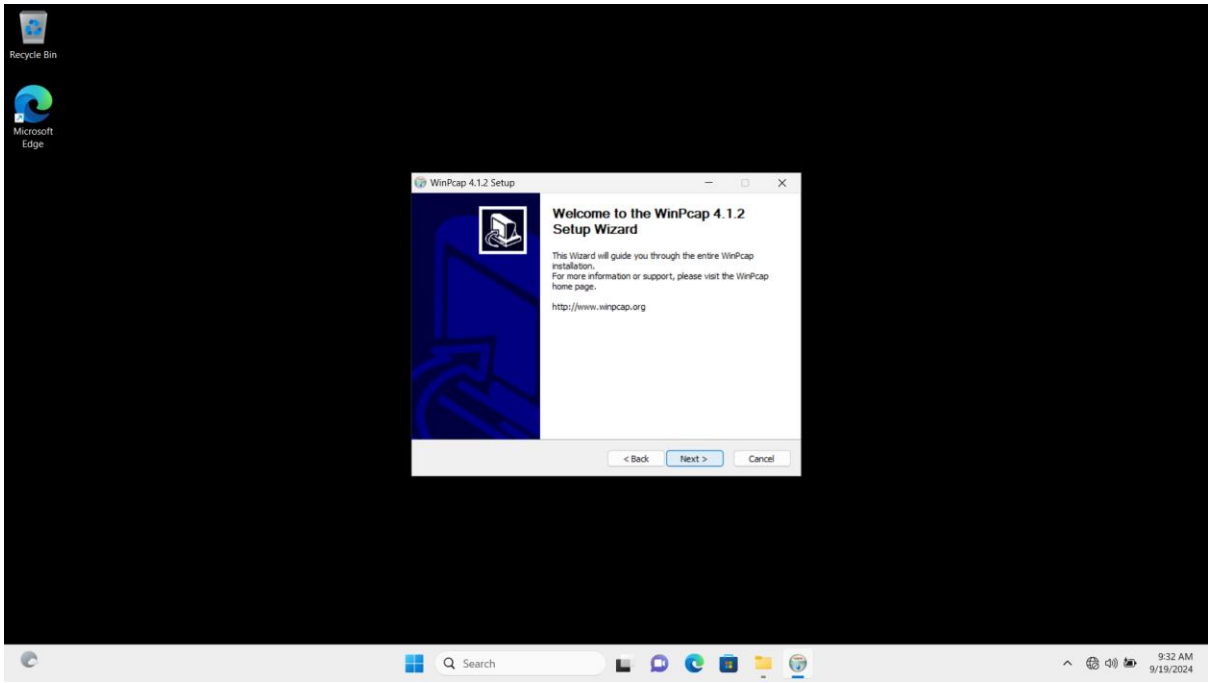
Snort is chosen as IDS solution for TechCo Solutions because it is cost effective, flexibility and strong community support.

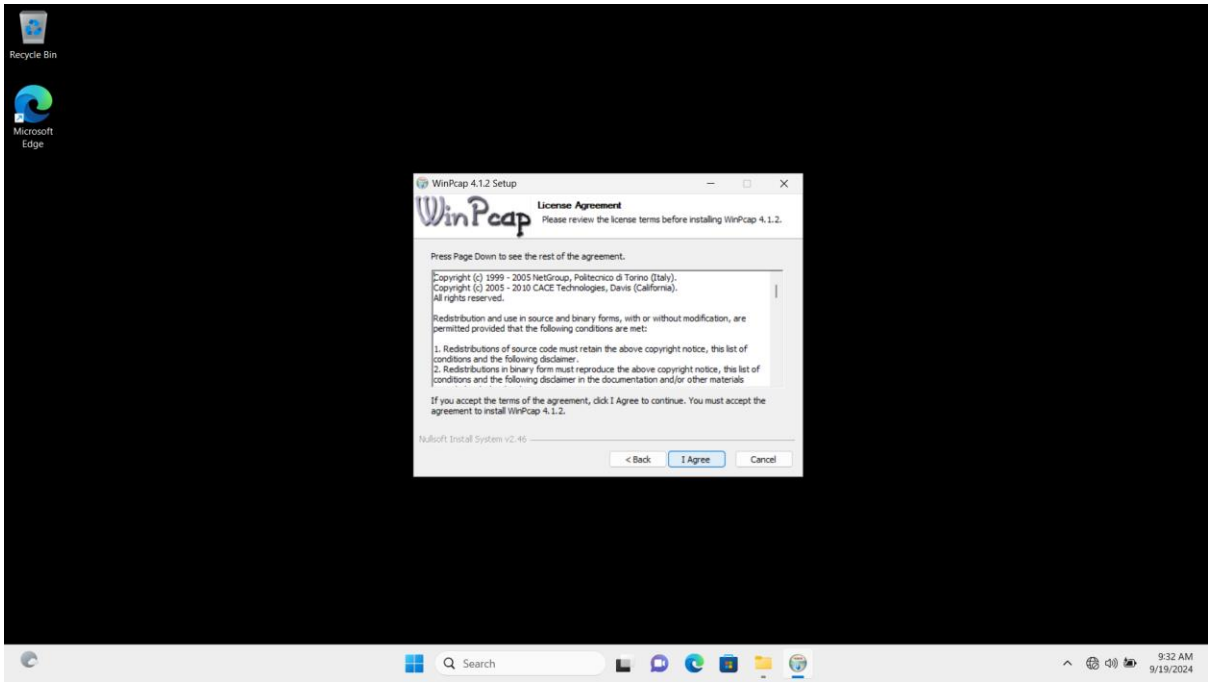
- Low cost. Snort is an open-source software, and it is free and no license fee.
- Ease of use and deployment. Snort has good documentation and strong community support.
- Completed rules sets. Snort provides a lot of detection rules and update rules set regularly.

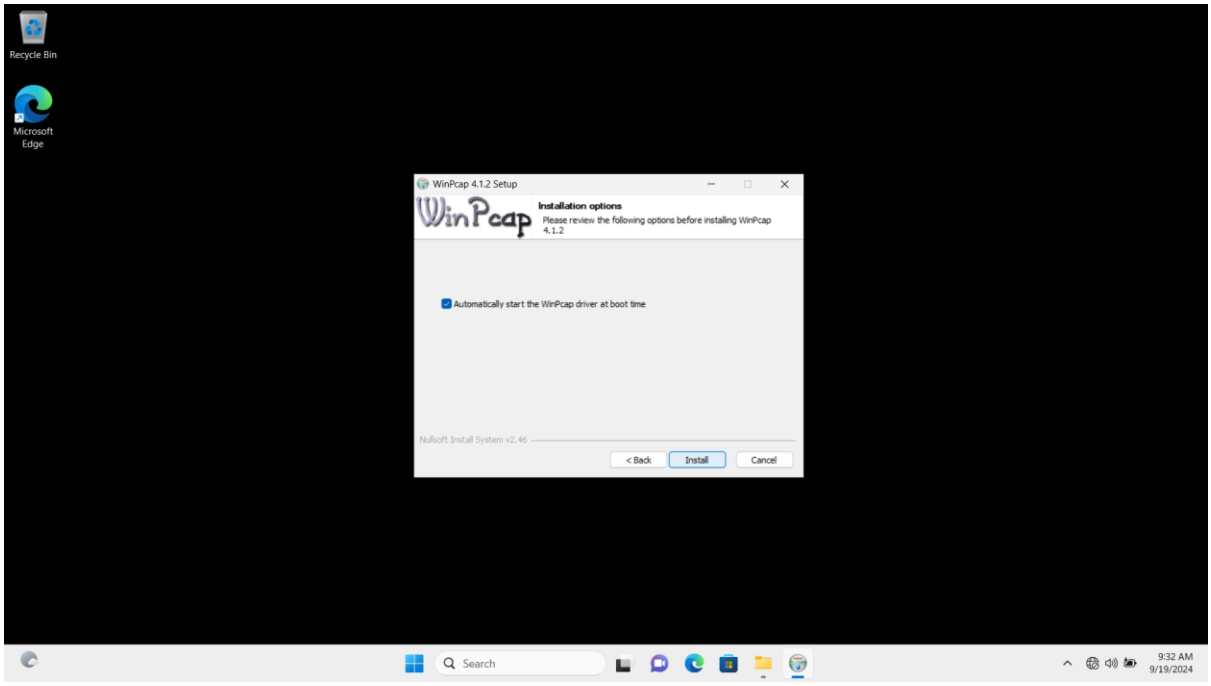
1. Install WinPcap

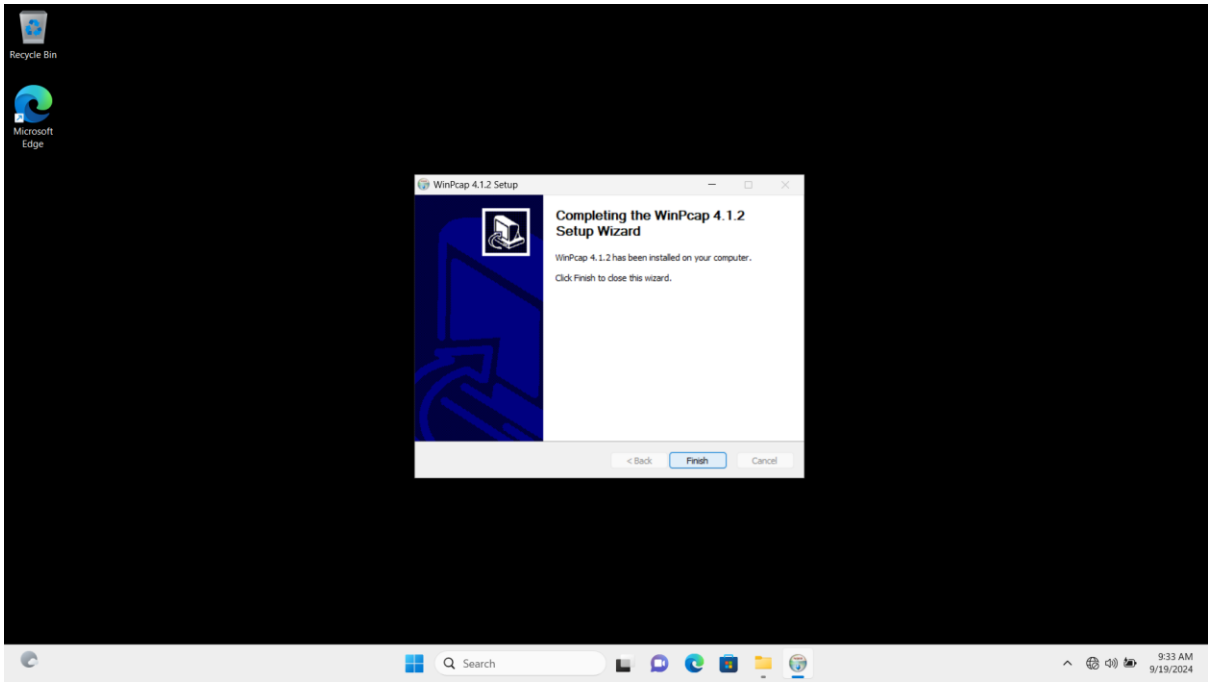
http://www.winpcap.org/install/bin/WinPcap_4_1_2.exe




Recycle Bin
Microsoft Edge
WinPcap 4.1.2 Setup
Welcome to the WinPcap 4.1.2 Setup Wizard
This Wizard will guide you through the entire WinPcap installation.
For more information or support, please visit the WinPcap home page.
http://www.winpcap.org
< Back
Next >
Cancel
Search
9:32 AM
9/19/2024

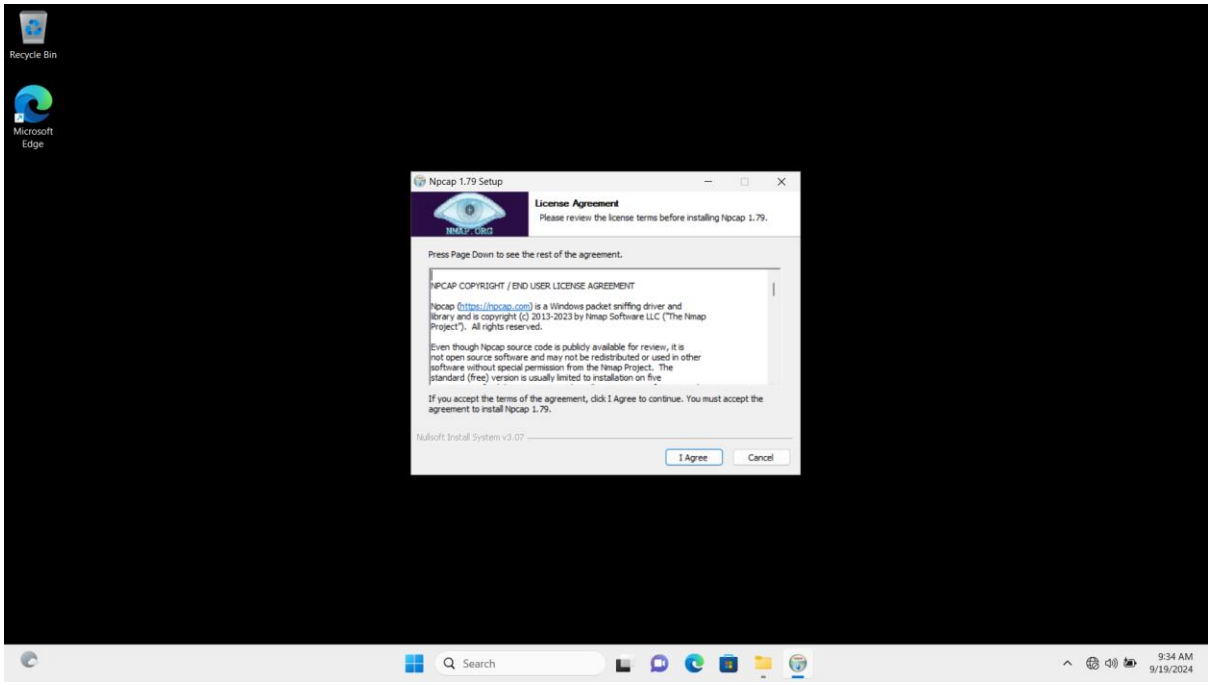

Recycle Bin
Microsoft Edge
WinPcap 4.1.2 Setup
License Agreement
Please review the license terms before installing WinPcap 4.1.2.
Press Page Down to see the rest of the agreement.
Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 - 2010 CACE Technologies, Davis (California).
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install WinPcap 4.1.2.
Nullsoft Install System v2.46
< Back
I Agree
Cancel
Search
9:32 AM
9/19/2024

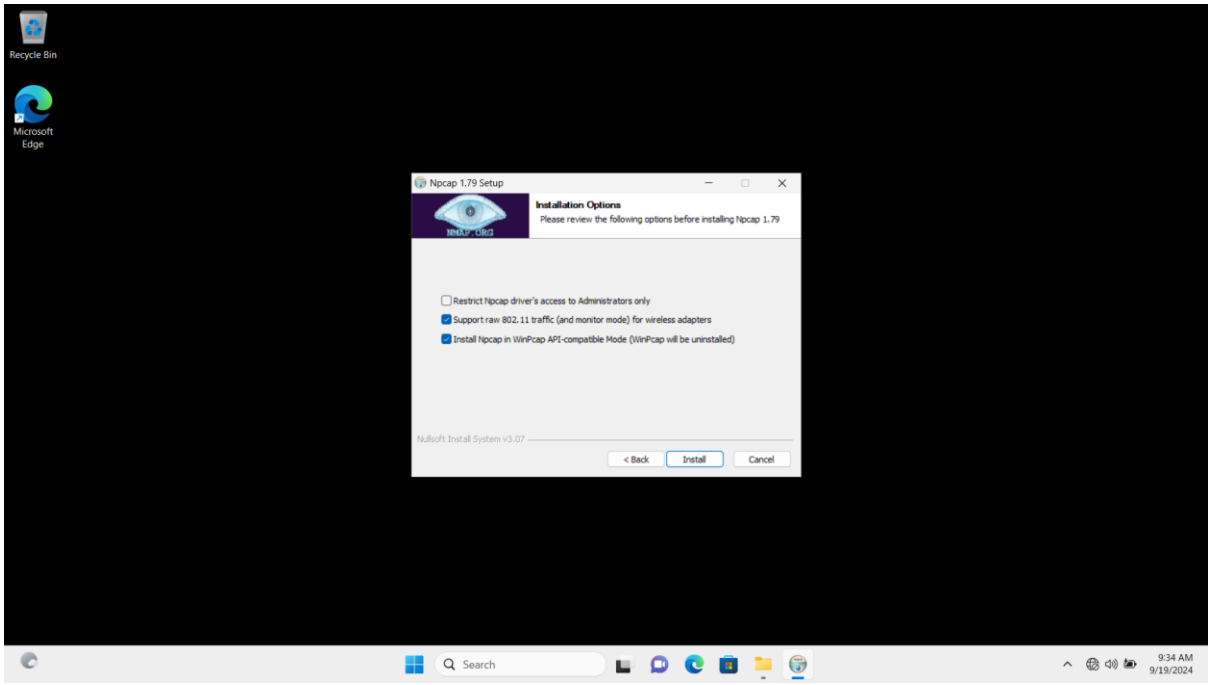

Recycle Bin
Microsoft Edge
WinPcap 4.1.2 Setup
Installation options
Please review the following options before installing WinPcap 4.1.2
Automatically start the WinPcap driver at boot time
Nullsoft Install System v2.46
< Back
Install
Cancel
Search
9:32 AM
9/19/2024

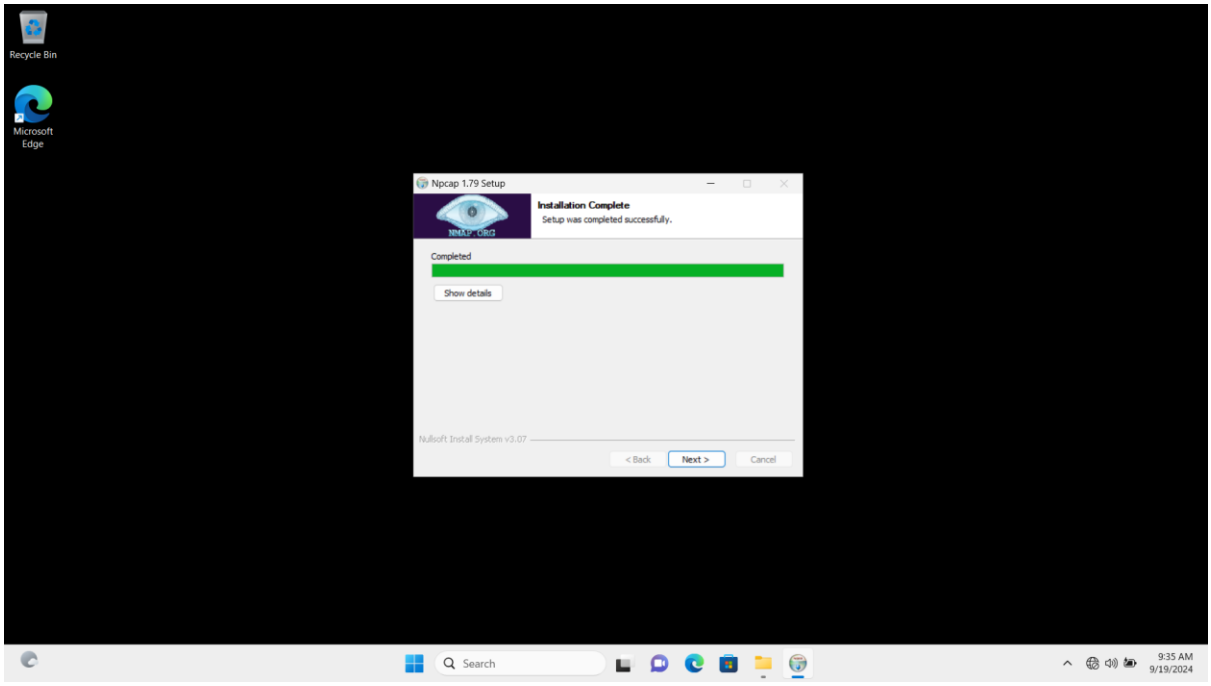

Recycle Bin
Microsoft Edge
WinPcap 4.1.2 Setup
Completing the WinPcap 4.1.2 Setup Wizard
WinPcap 4.1.2 has been installed on your computer.
Click Finish to close this wizard.
< Back
Finish
Cancel
Search
9:33 AM
9/19/2024

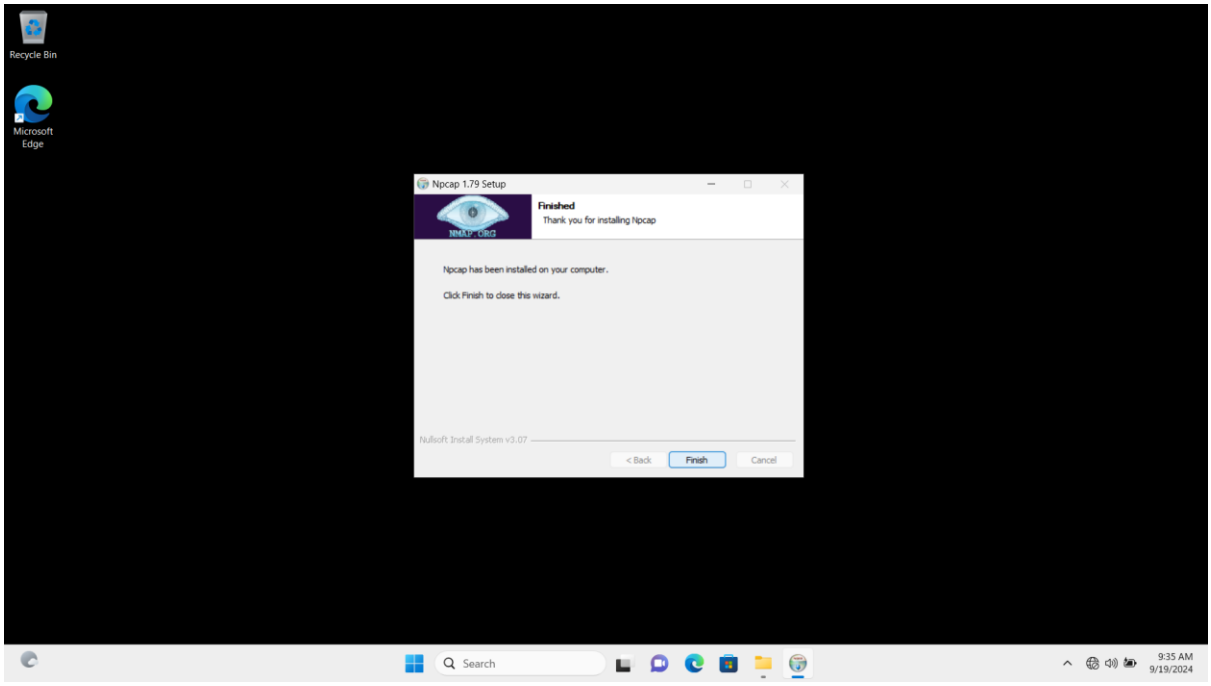
2. Install Npcap

https://npcap.com/dist/npcap-1.79.exe



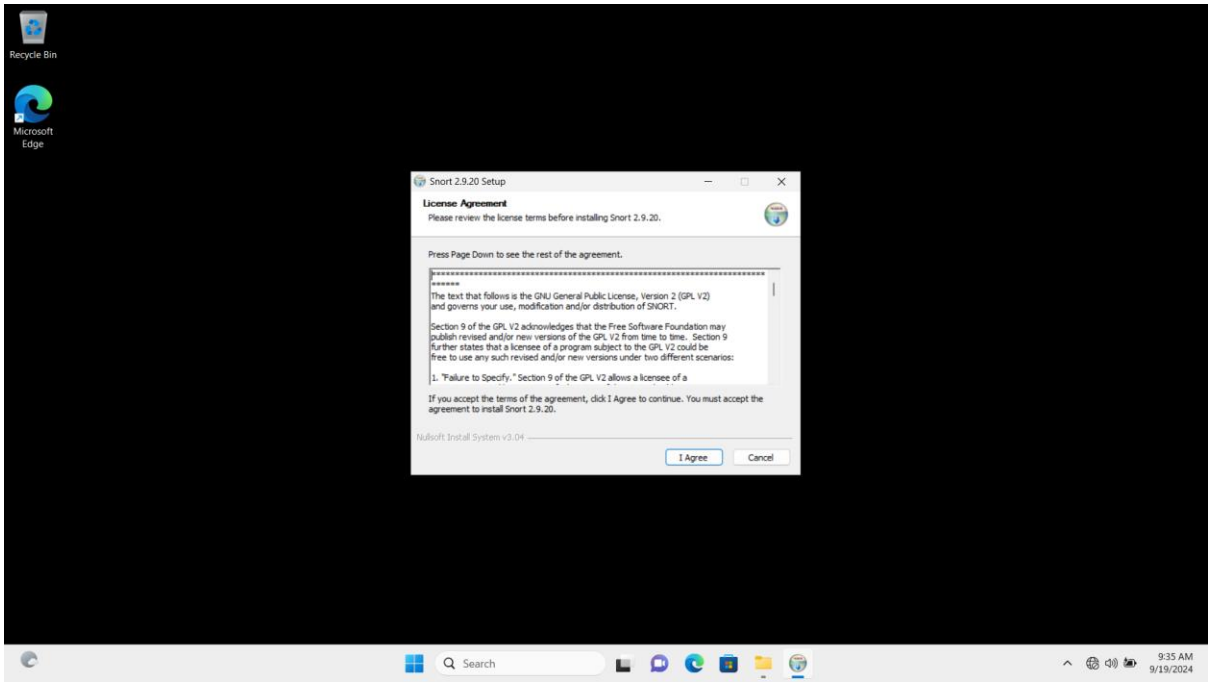


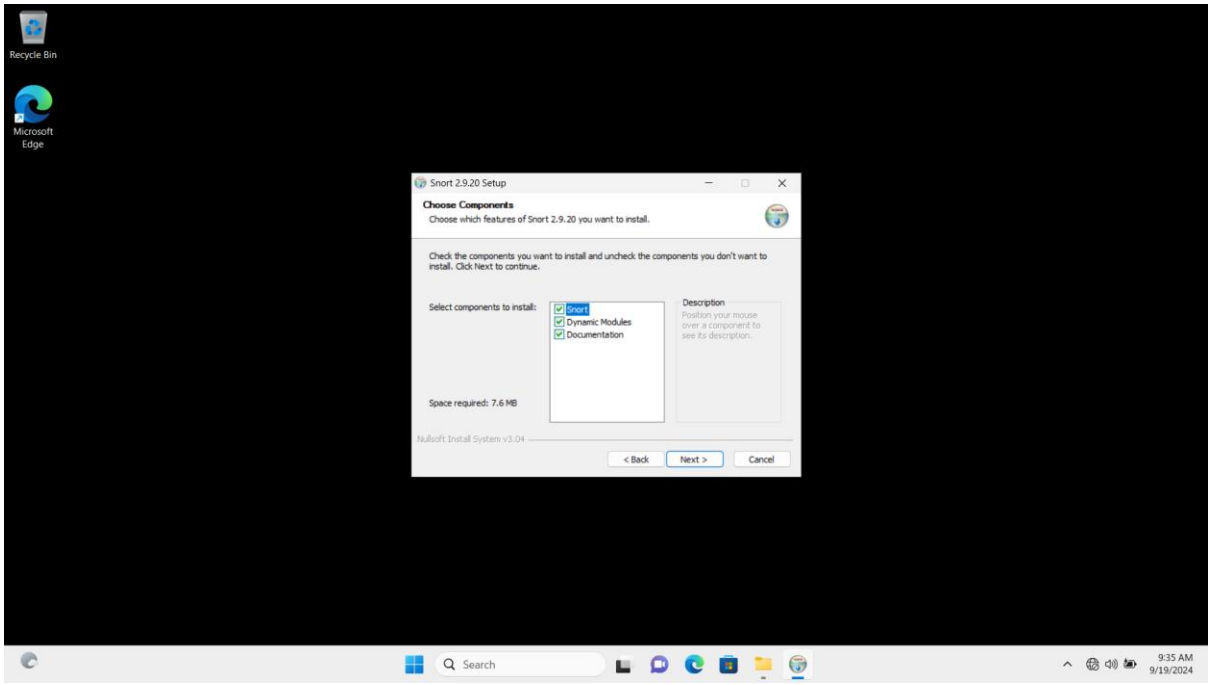

Recycle Bin
Microsoft Edge
Npcap 1.79 Setup
Installation Complete
Setup was completed successfully.
Completed
Show details
Nullsoft Install System v3.07
< Back
Next >
Cancel
Search
9:35 AM
9/19/2024

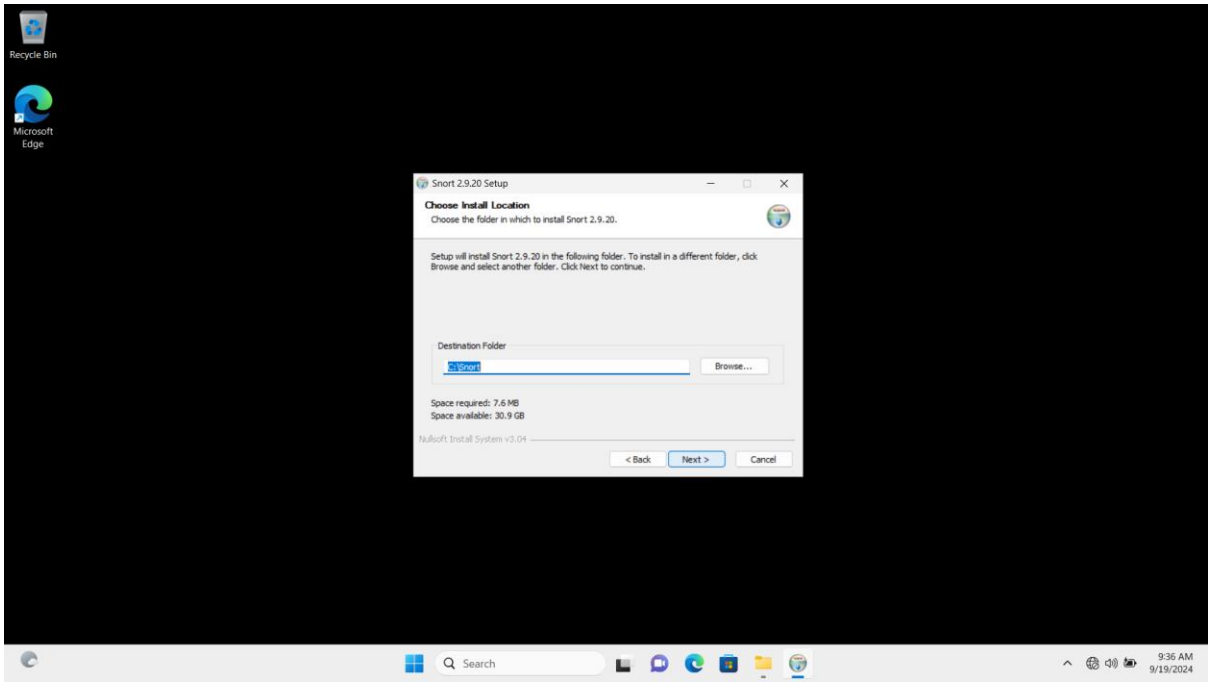

Recycle Bin
Microsoft Edge
Npcap 1.79 Setup
Finished
Thank you for installing Npcap
Npcap has been installed on your computer.
Click Finish to close this wizard.
Nullsoft Install System v3.07
< Back
Finish
Cancel
Search
9:35 AM
9/19/2024

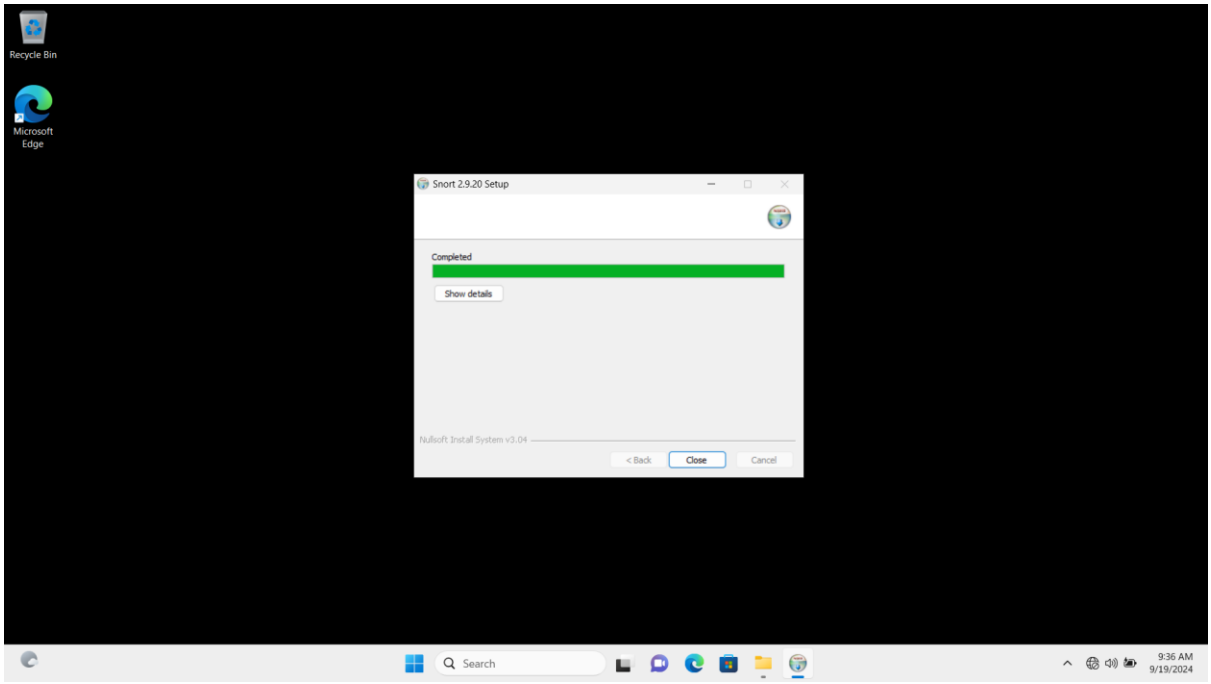
3. Install Snort

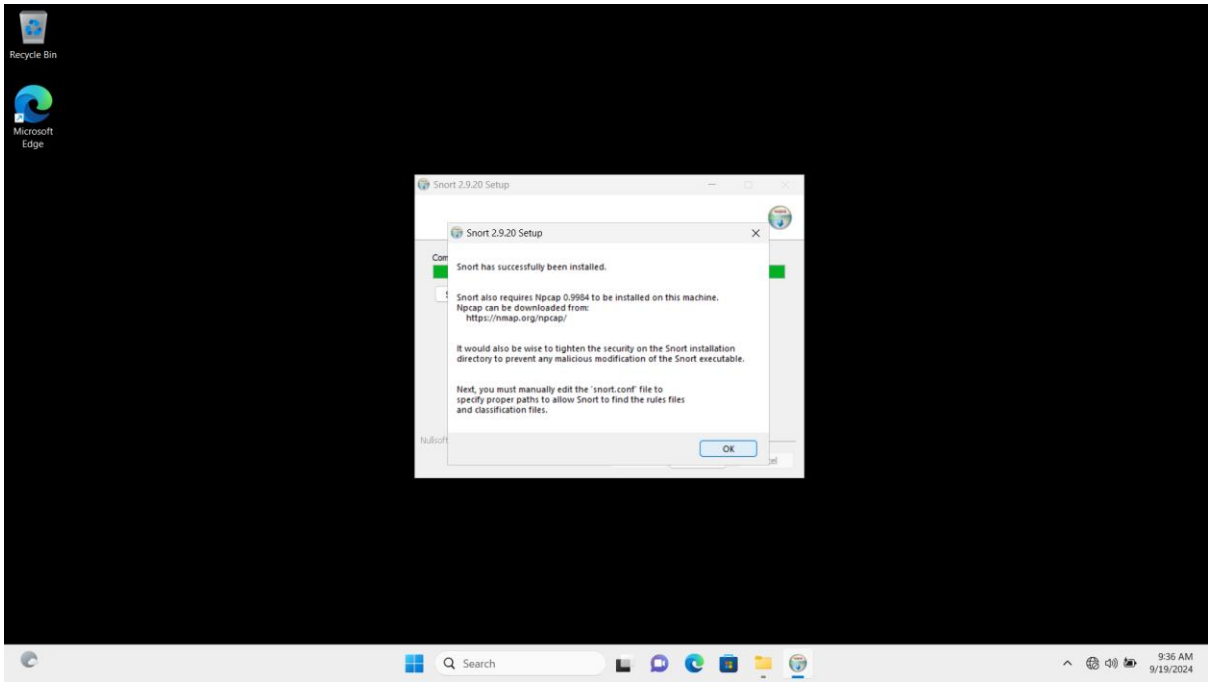
https://www.snort.org/downloads/snort/Snort_2_9_20_Installer.x64.exe





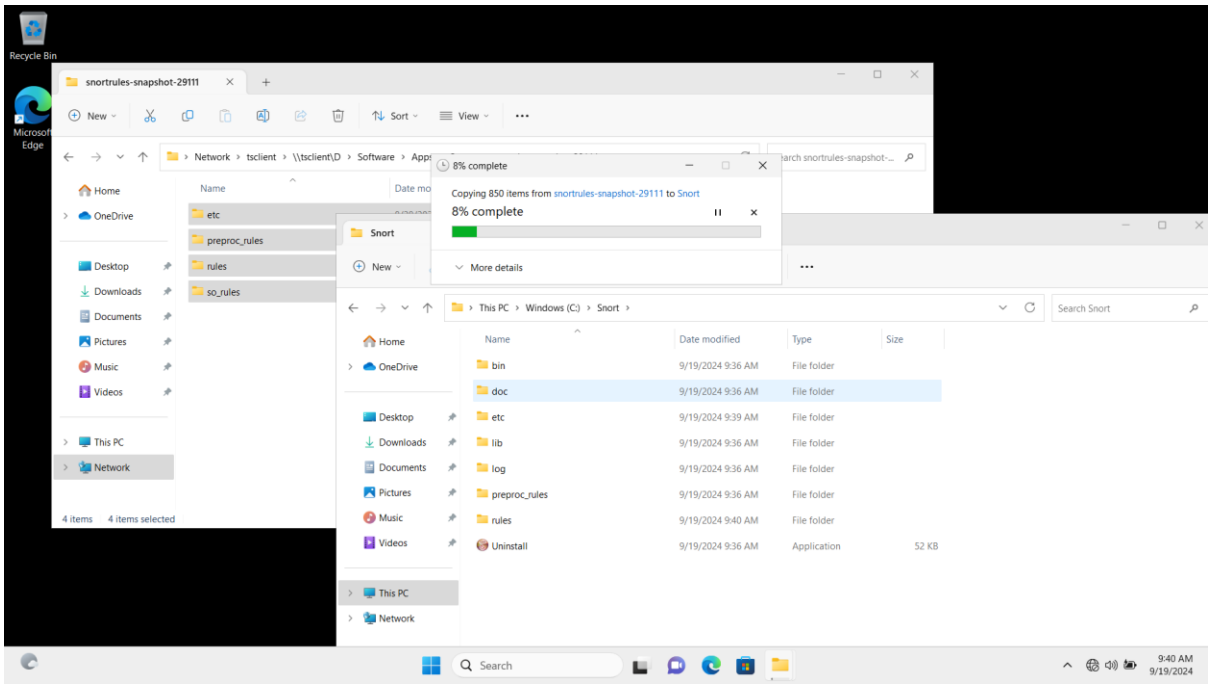

Recycle Bin
Microsoft Edge
Snort 2.9.20 Setup
Choose Install Location
Choose the folder in which to install Snort 2.9.20.
Setup will install Snort 2.9.20 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:\Snort
Browse...
Space required: 7.6 MB
Space available: 30.9 GB
Nullsoft Install System v3.04
< Back
Next >
Cancel
Search
9:36 AM
9/19/2024


Recycle Bin
Microsoft Edge
Snort 2.9.20 Setup
Completed
Show details
Nullsoft Install System v3.04
< Back
Close
Cancel
Search
9:36 AM
9/19/2024



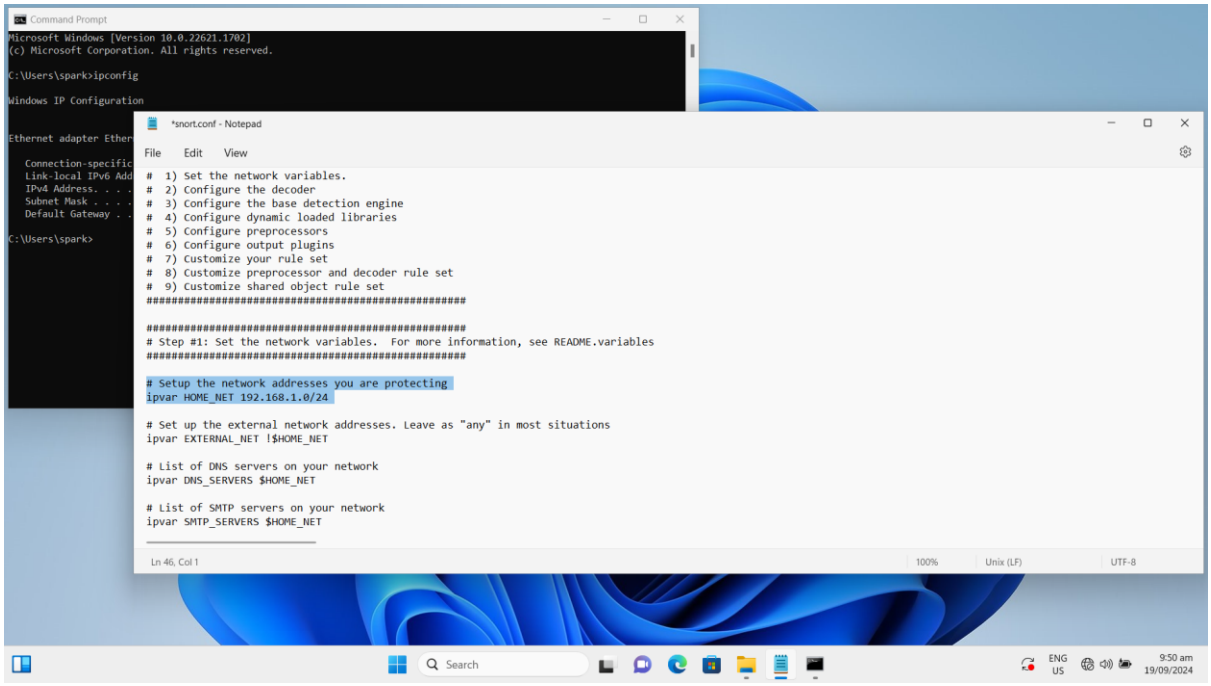
4. Download Snort Rules to local snort folder

https://www.snort.org/downloads/registered/snortrules-snapshot-29111.tar.gz

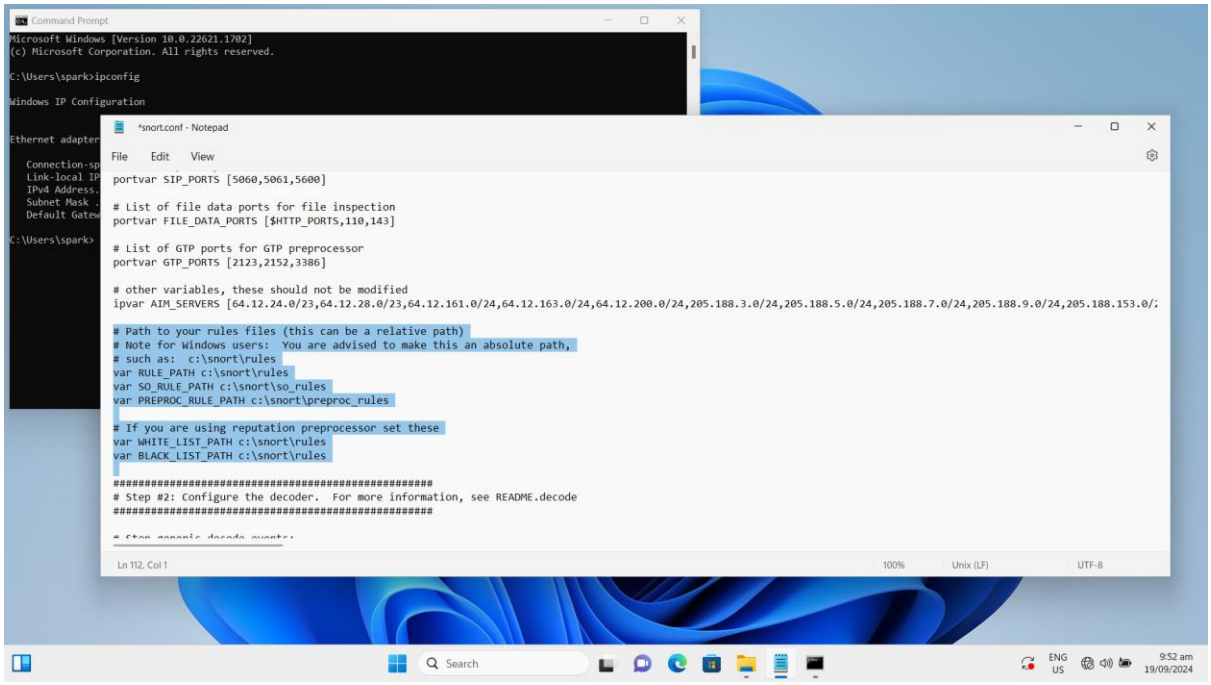


5. Configure Snort

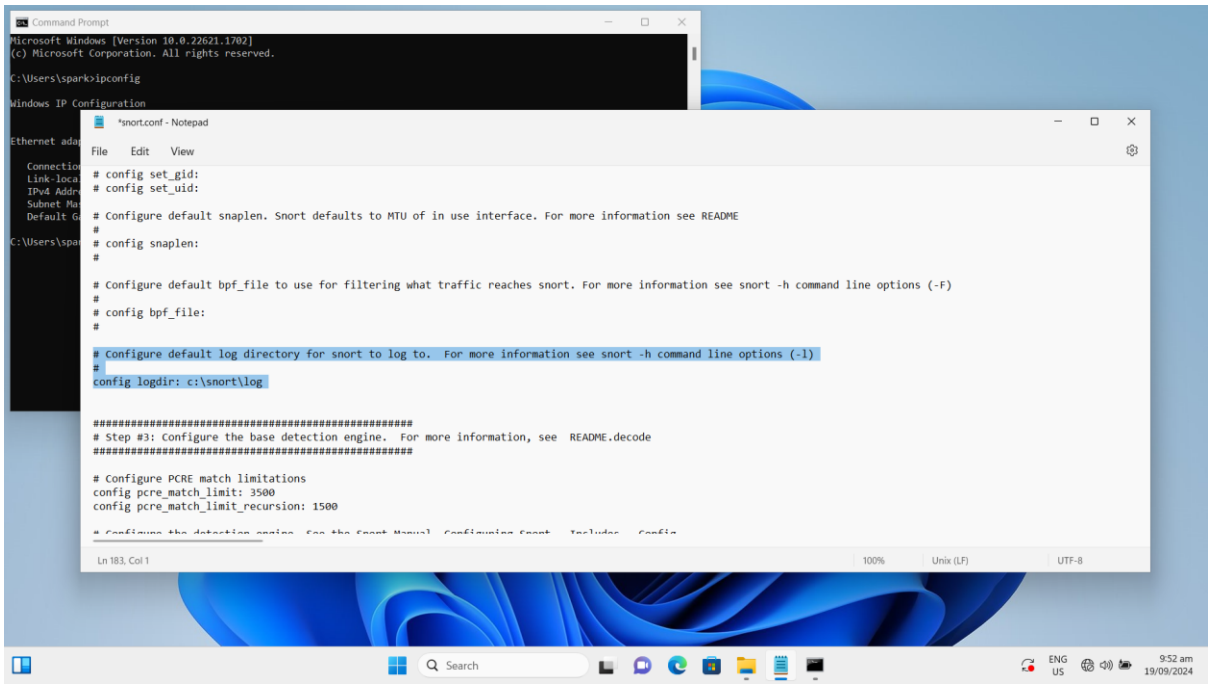
- **Set the network variables**



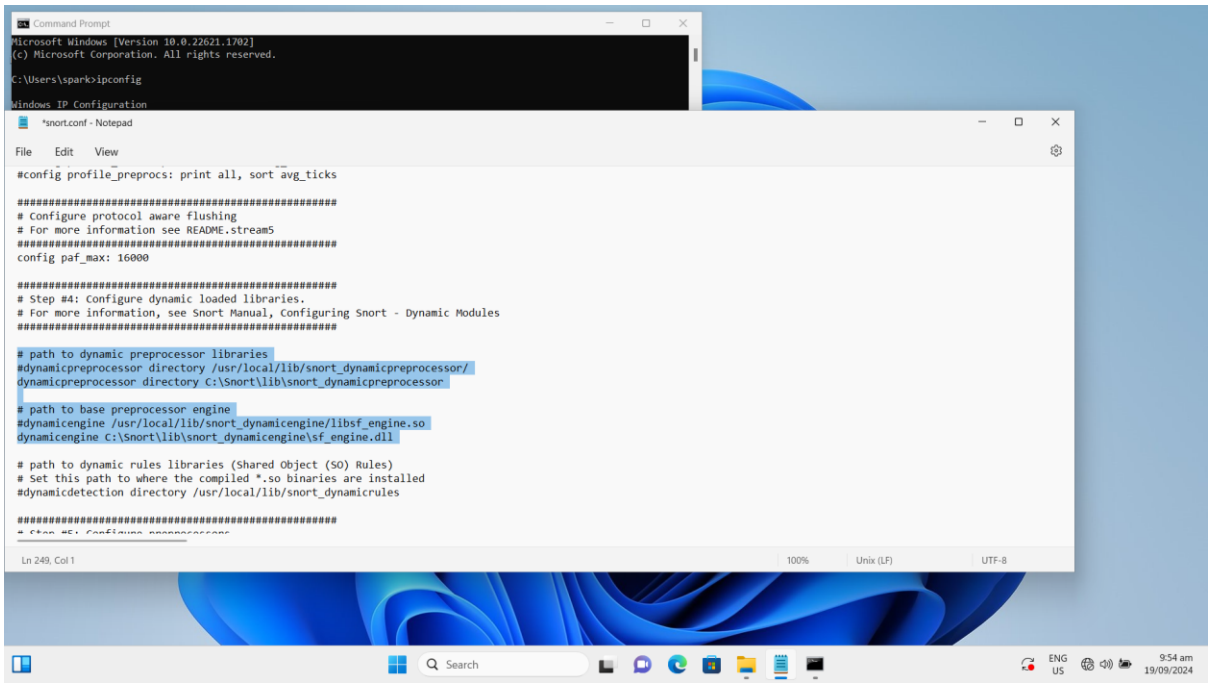
- **Set the path of rules**

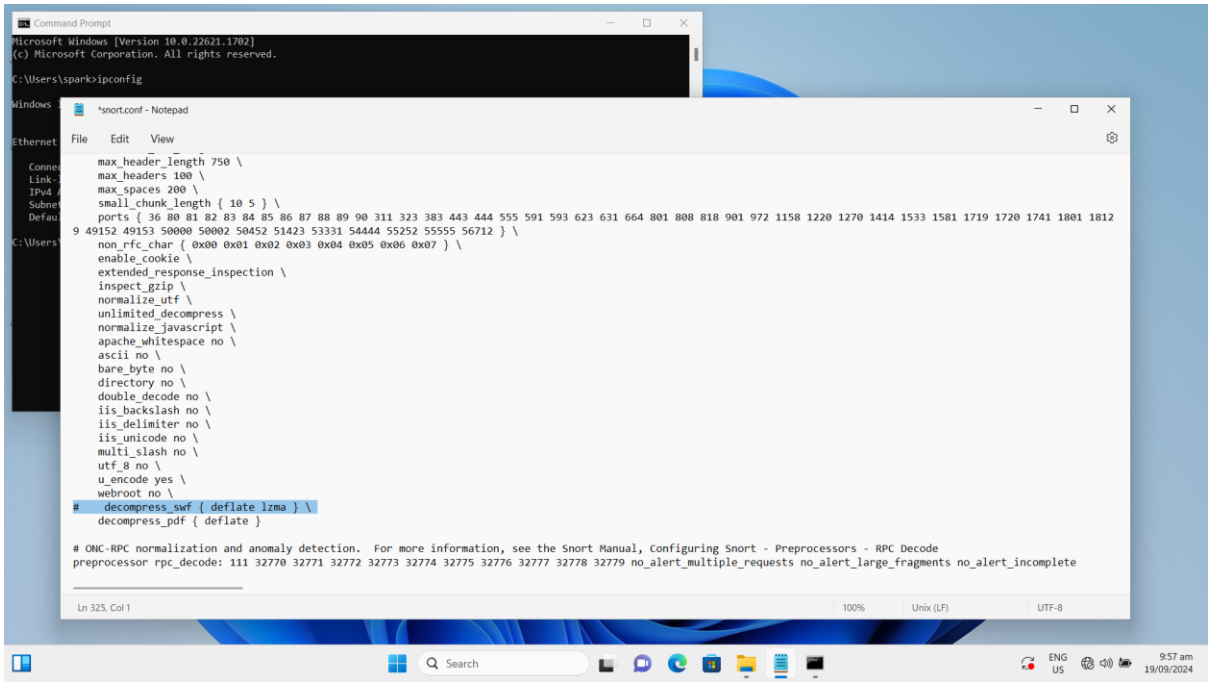


- **Set the path of log file**

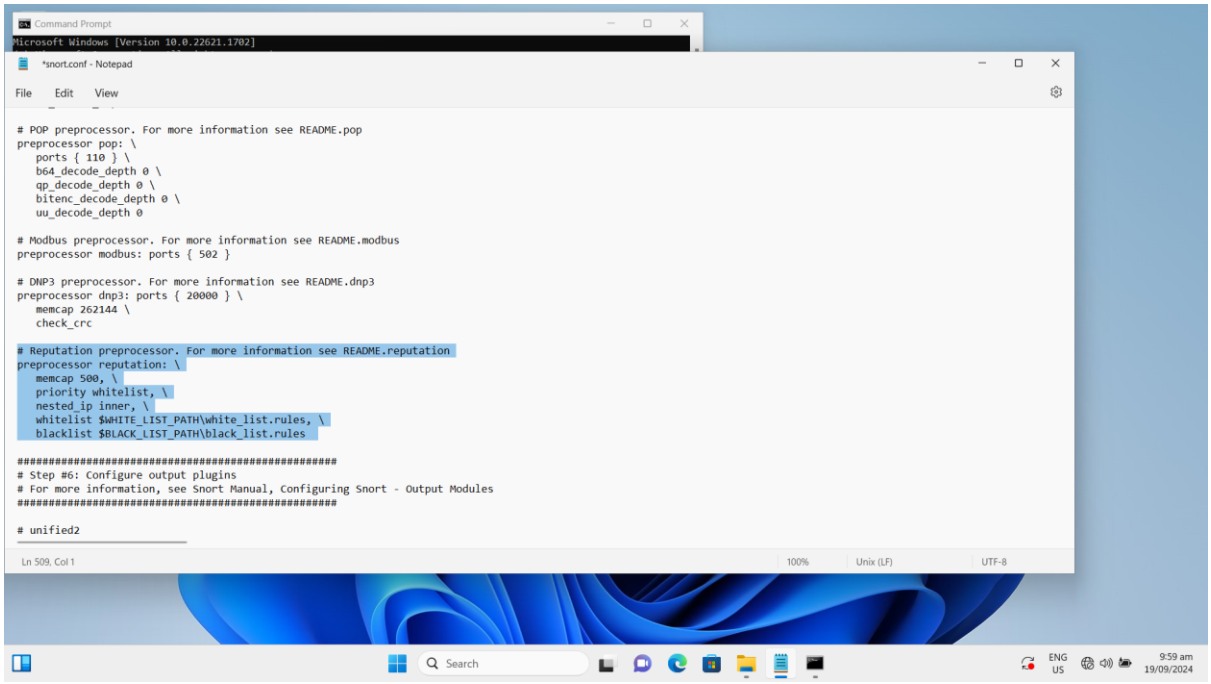


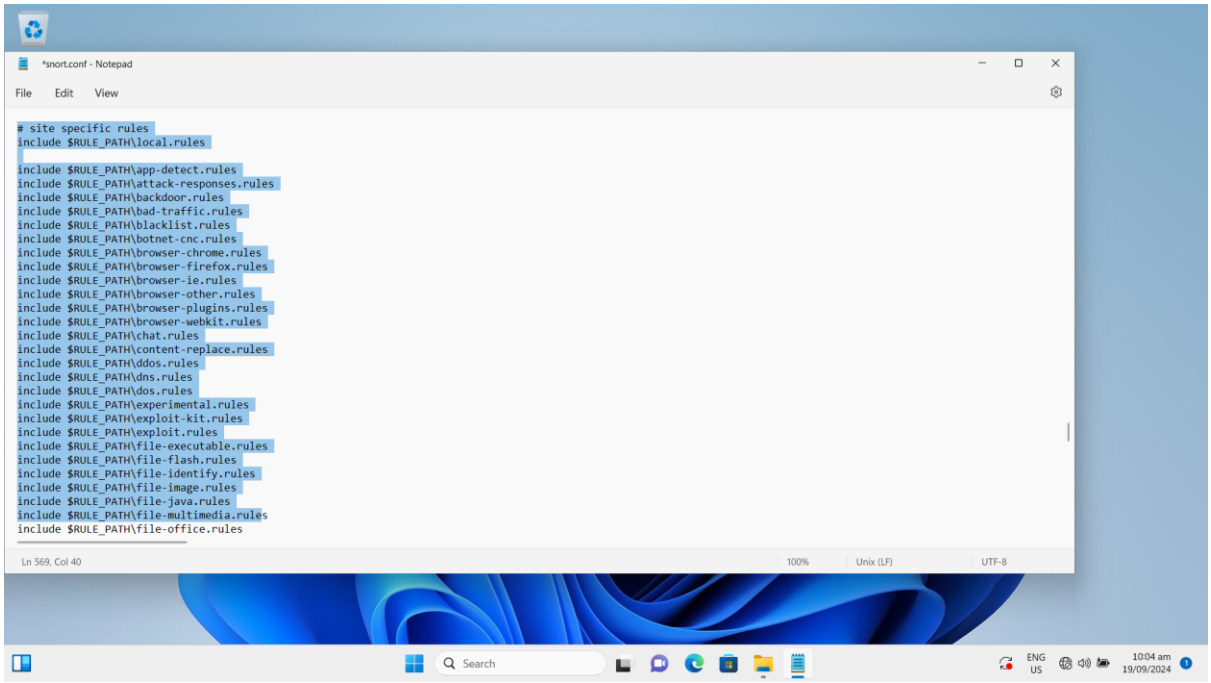
- **Configure dynamic loaded libraries**





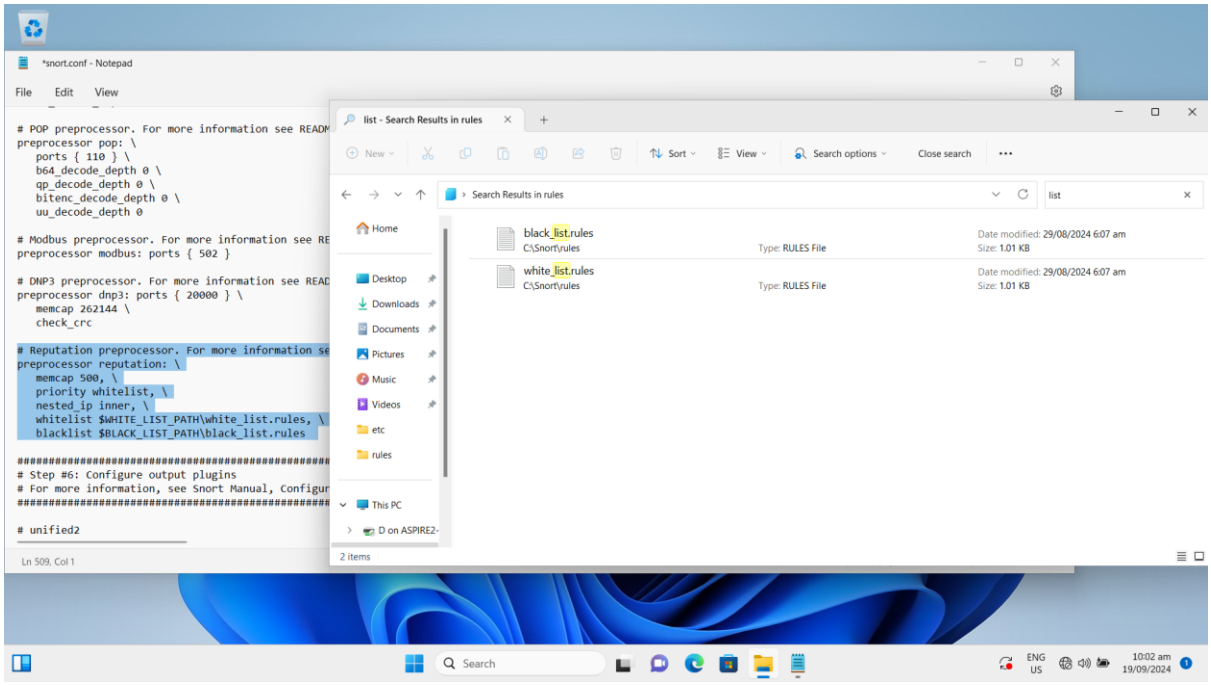
- **Change slash for Windows path**

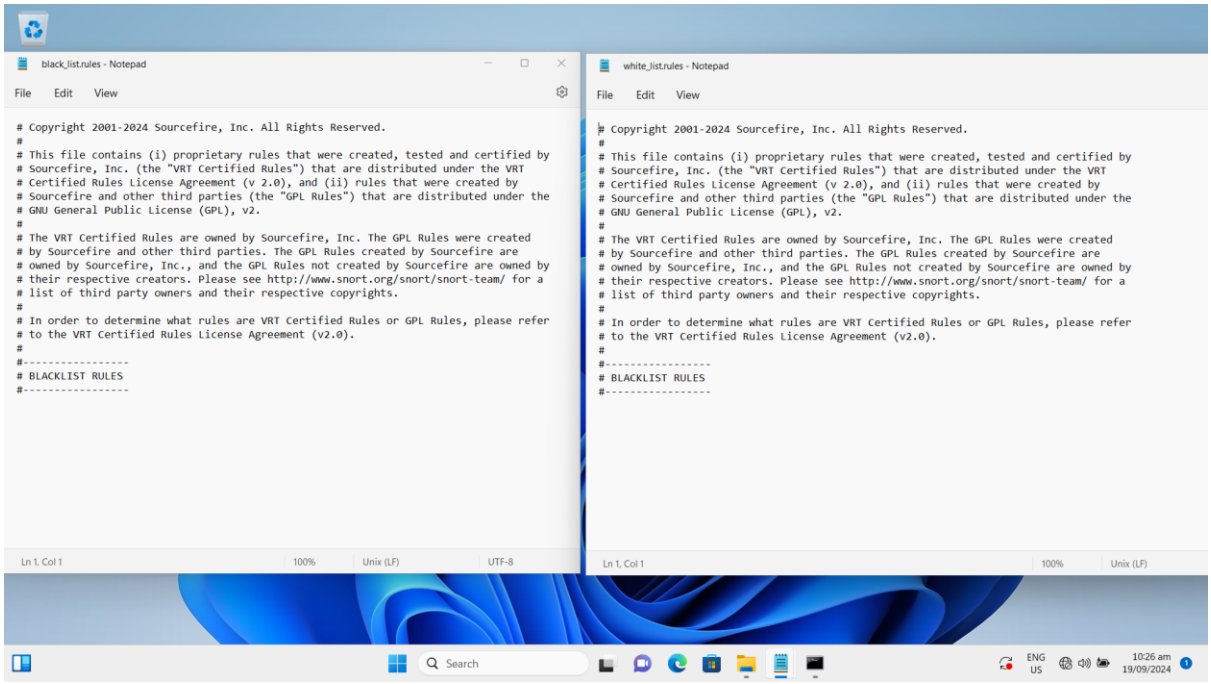



*snort.conf - Notepad
File Edit View
site specific rules
include $RULE_PATH\local.rules
include $RULE_PATH\app-detect.rules
include $RULE_PATH\attack-responses.rules
include $RULE_PATH\backdoor.rules
include $RULE_PATH\bad-traffic.rules
include $RULE_PATH\blacklist.rules
include $RULE_PATH\botnet-cnc.rules
include $RULE_PATH\browser-chrome.rules
include $RULE_PATH\browser-firefox.rules
include $RULE_PATH\browser-ie.rules
include $RULE_PATH\browser-other.rules
include $RULE_PATH\browser-plugins.rules
include $RULE_PATH\browser-webkit.rules
include $RULE_PATH\chat.rules
include $RULE_PATH\content-replace.rules
include $RULE_PATH\ddos.rules
include $RULE_PATH\dns.rules
include $RULE_PATH\dos.rules
include $RULE_PATH\experimental.rules
include $RULE_PATH\exploit-kit.rules
include $RULE_PATH\exploit.rules
include $RULE_PATH\file-executable.rules
include $RULE_PATH\file-flash.rules
include $RULE_PATH\file-identify.rules
include $RULE_PATH\file-image.rules
include $RULE_PATH\file-java.rules
include $RULE_PATH\file-multimedia.rules
include $RULE_PATH\file-office.rules
Ln 569, Col 40
100%
Unix (LF)
UTF-8
Search
ENG
US
10:04 am
19/09/2024

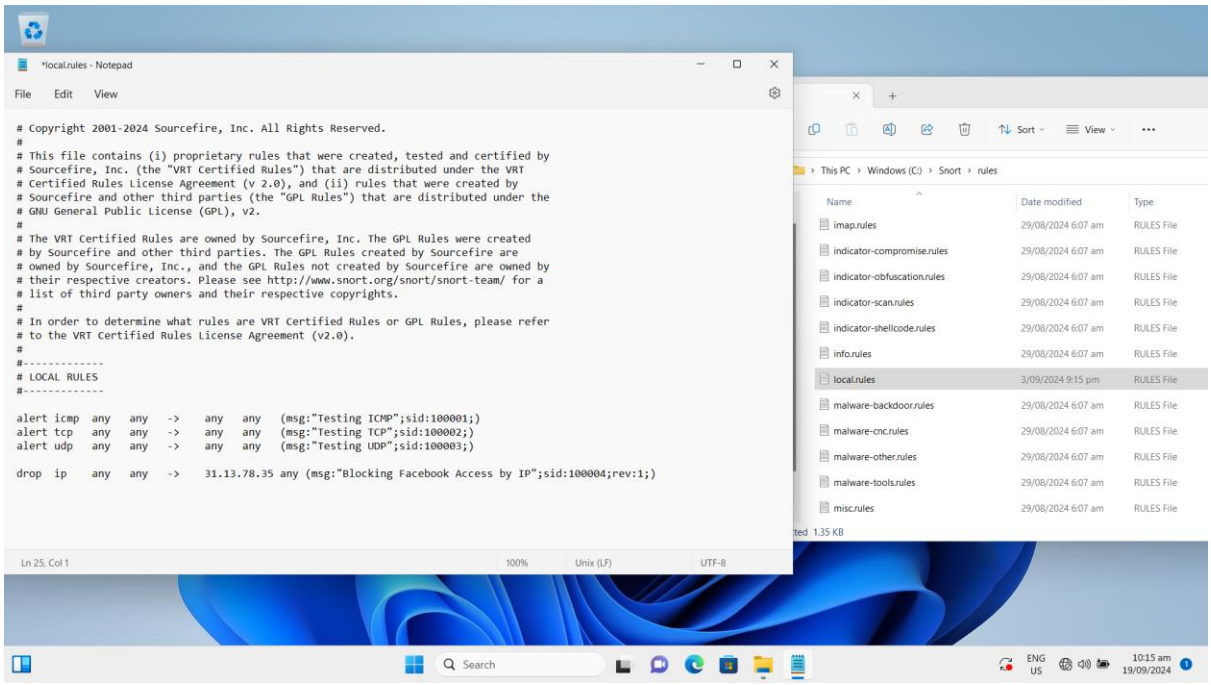
Task 6.2: Integration, Testing, and Documentation

1. Add blacklist.rules and whitelist.rules



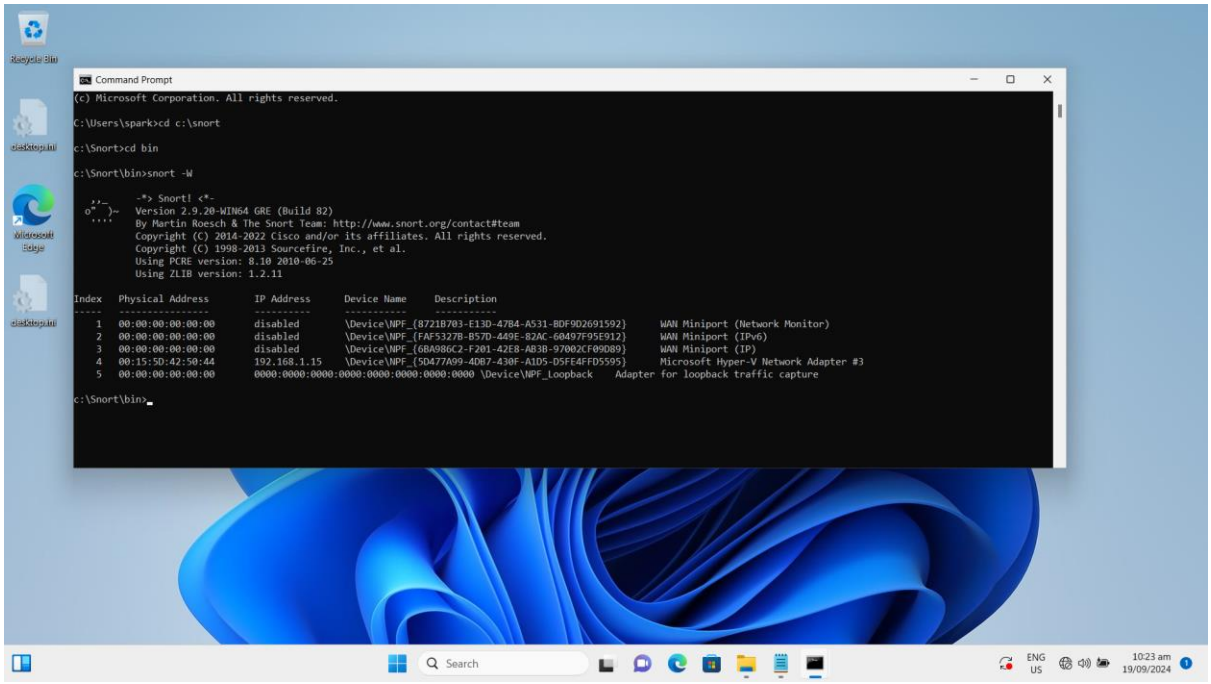


2. Add local.rules



3. Execute snort

- Check interface to work on



- Start Snort on the right interface

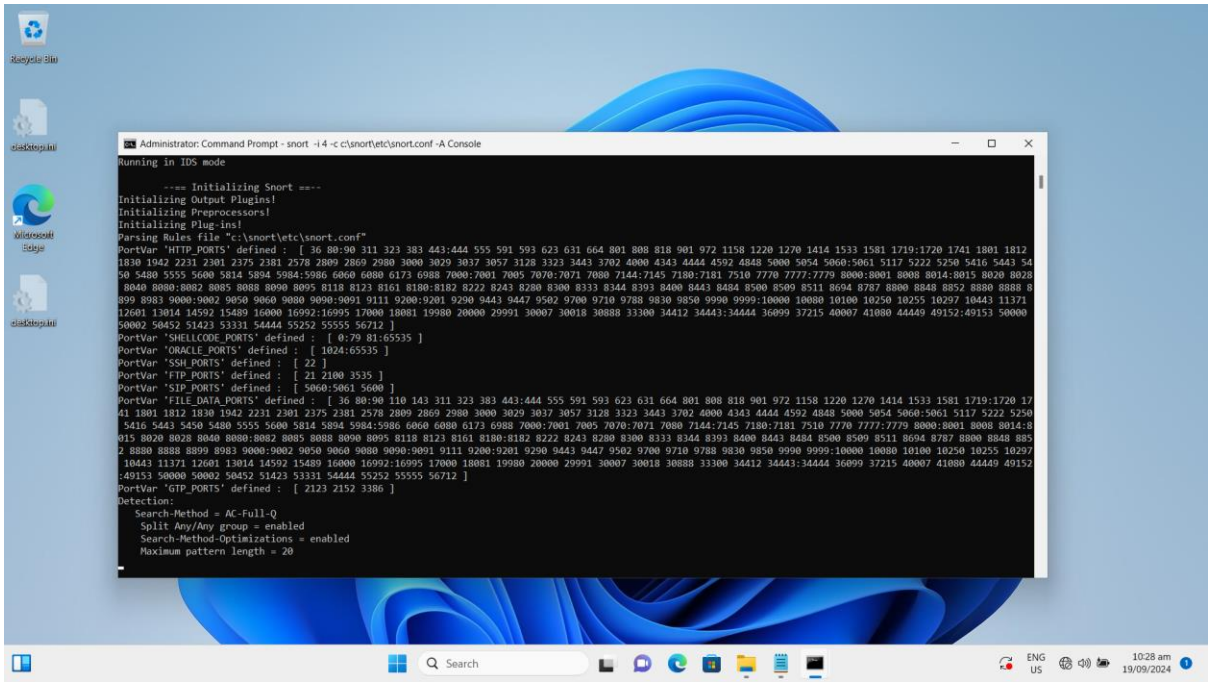
snort -i 4 -c c:\snort\etc\snort.conf -A Console

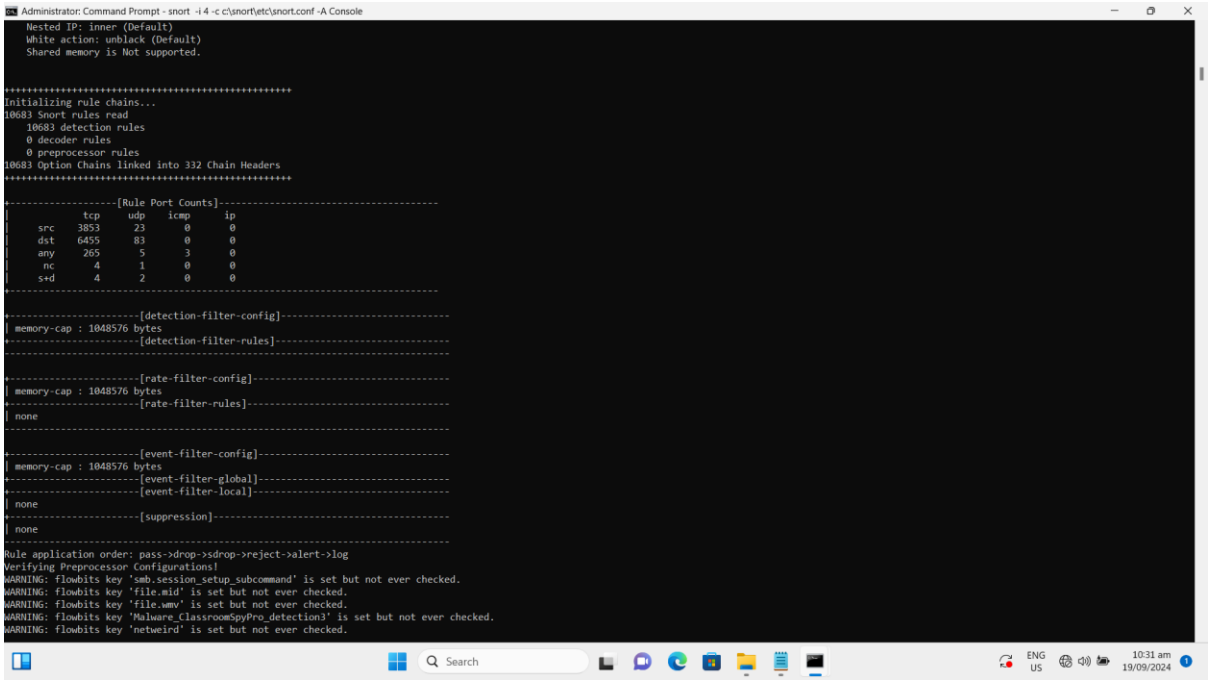
-W Lists available interfaces. (Win32 only)

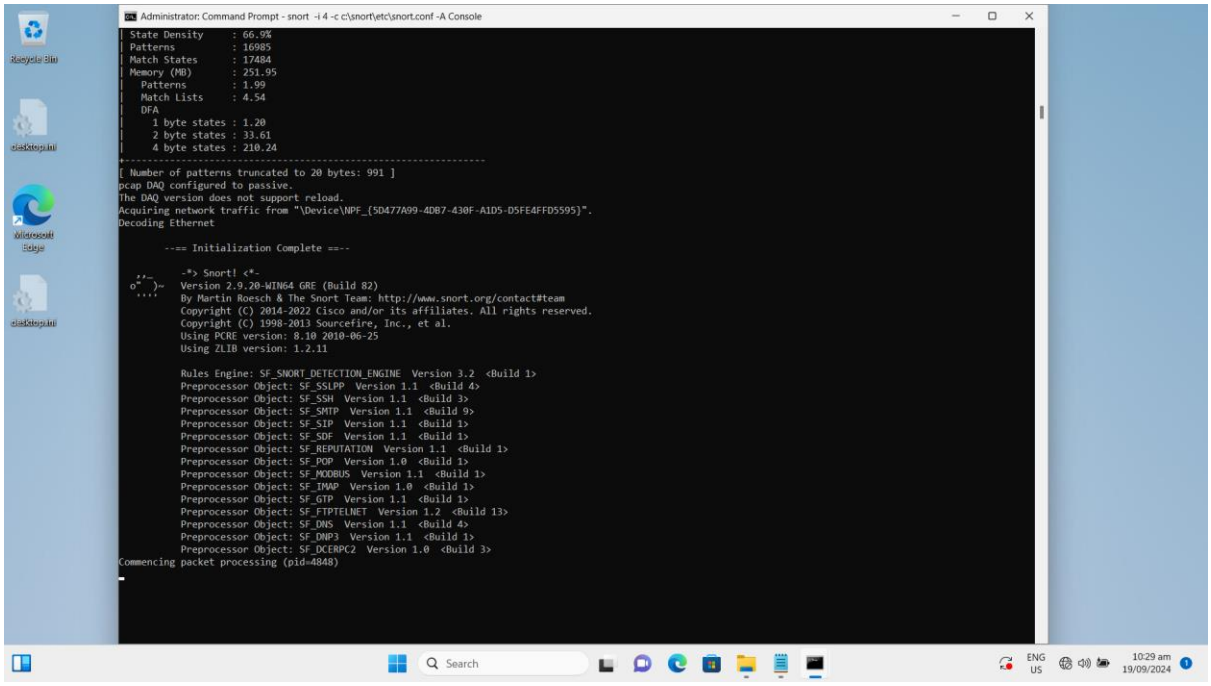
-i <if> Listen on interface <if>

-A Set alert mode: fast, full, console, test or none (alert file alerts only)

-c <rules> Use Rules File <rules>

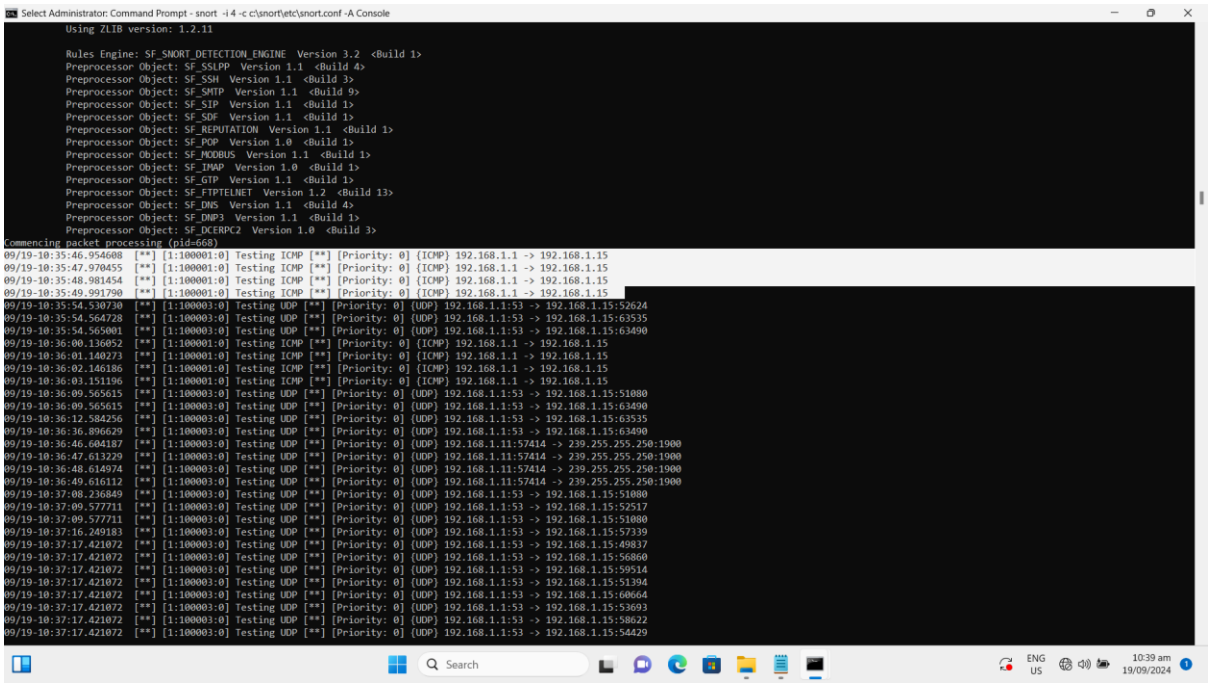



Administrator: Command Prompt - snort -i 4 -c c:\snort\etc\snort.conf -A Console
Nested IP: inner (Default)
White action: unblack (Default)
Shared memory is Not supported.
++
Initializing rule chains...
10683 Snort rules read
10683 detection rules
0 decoder rules
0 preprocessor rules
10683 Option Chains linked into 332 Chain Headers
++
[Rule Port Counts]
tcp udp icmp ip
src 3853 23 0 0
dst 6455 83 0 0
any 265 5 3 0
nc 4 1 0 0
s+d 4 2 0 0
[detection-filter-config]
memory-cap : 1048576 bytes
[detection-filter-rules]
[rate-filter-config]
memory-cap : 1048576 bytes
[rate-filter-rules]
none
[event-filter-config]
memory-cap : 1048576 bytes
[event-filter-global]
[event-filter-local]
none
[suppression]
none
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
WARNING: flowbits key 'smb.session_setup_subcommand' is set but not ever checked.
WARNING: flowbits key 'file.mid' is set but not ever checked.
WARNING: flowbits key 'file.wmv' is set but not ever checked.
WARNING: flowbits key 'Malware_ClassroomSpyPro_detection3' is set but not ever checked.
WARNING: flowbits key 'netweird' is set but not ever checked.
Search
ENG US
10:31 am 19/09/2024

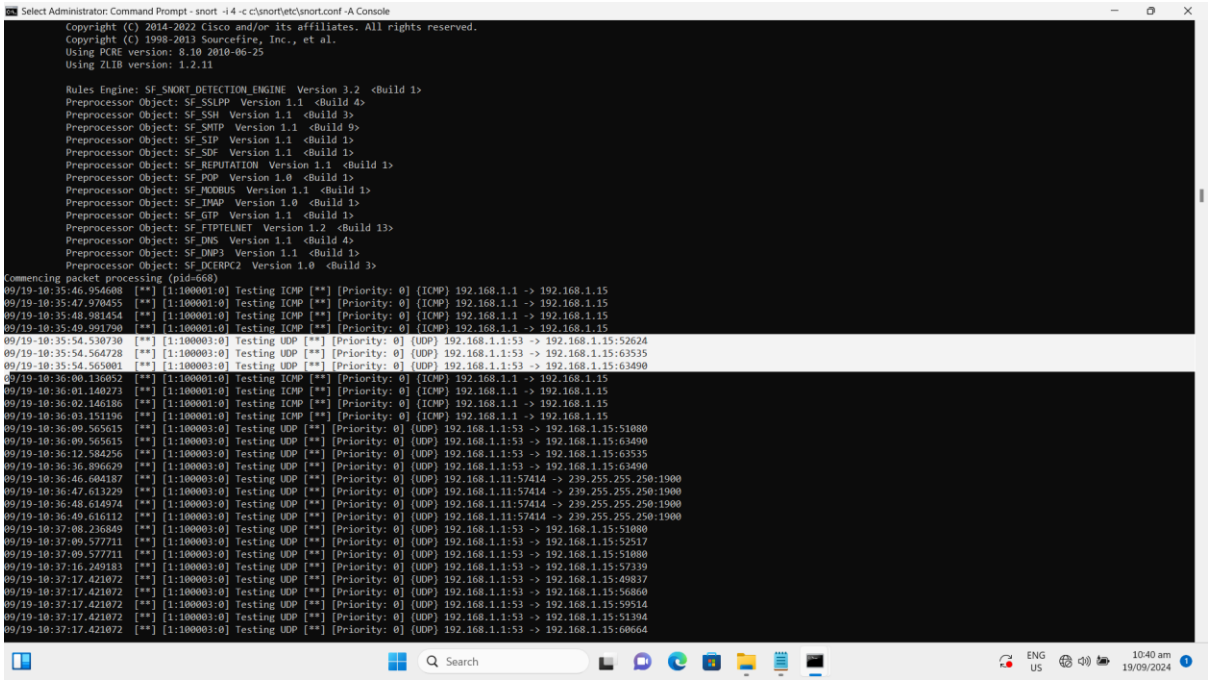

Recycle Bin
desktop.ini
Microsoft Edge
desktop.ini
Administrator: Command Prompt - snort -i 4 -c c:\snort\etc\snort.conf -A Console
State Density : 66.9%
Patterns : 16985
Match States : 17484
Memory (MB) : 251.95
Patterns : 1.99
Match Lists : 4.54
DFA
1 byte states : 1.20
2 byte states : 33.61
4 byte states : 210.24
[Number of patterns truncated to 20 bytes: 991]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{5D477A99-4DB7-430F-A1D5-D5FE4FFD5595}".
Decoding Ethernet
--== Initialization Complete ==--
-*> Snort! <*-
Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Commencing packet processing (pid=4848)
Search
ENG US
10:29 am 19/09/2024

4. Check logs

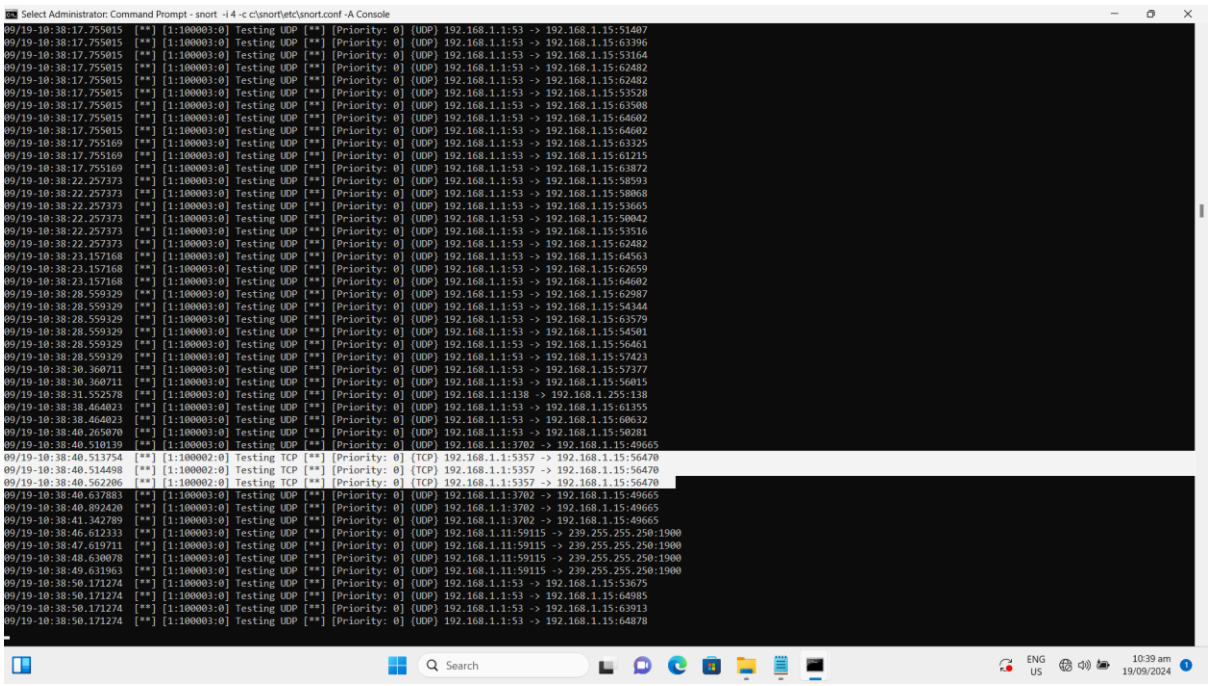
- **ICMP detected.**



- **UDP detected**



- **TCP detected**



Task/Mahi 7: Update Existing Network Diagram

The network infrastructure of TechCo Solutions is enhanced with:

- Secondary Domain Controller
- Centralized printing management
- MFA deployed
- VPN server with traffic encryption
- Encrypted Windows Backup
- IDS server