



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.....	4
Task 1.1 Create a PowerShell script to set up and integrate a second domain controller.....	4
Task 1.2 Create a PowerShell script to automate user creation in Active Directory.....	12
Task/Mahi 2: Deploying Print Management Solution via Group Policy Object	17
Task/Mahi 3: Implementing & Managing Multi-Factor Authentication (MFA) for Network Access	29
Task 3.1 Set up the MFA platform on a server and automate the deployment of MFA to the client machines	29
Task 3.2 Troubleshooting the MFA configurations on a client machine and MFA Admin App	32
Task/Mahi 4: Manage the remote access via VPN.....	43
Task 4.1 Set up and configure a member server of the domain to act as a VPN server.....	43
Task 4.2 Set up a secure VPN connection	57
Task 4.3 Allow file sharing for a shared folder.....	61
Task 4.4 Test the VPN connectivity to verify the setup and configuration.....	65
Task/Mahi 5: Implementing Server Backup.....	68
Task 5.1 Create a complete backup policy using PowerShell Scripts to automate the backup process	69
Task 5.2 Configure Windows backup using the PowerShell Script	72
Task/Mahi 6: Implementing and Managing Intrusion Detection System(IDS)	83
Task 6.1: IDS Deployment and Configuration	83
Task 6.2: Integration, Testing, and Documentation.....	92
Task/Mahi 7: Update Existing Network Diagram.....	101

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

The screenshot shows a Windows PowerShell ISE window with a script named `InstallSecondaryDomainController.ps1`. The script contains the following code:

```
1 #Set Time zone
2 Set-TimeZone -Name "New Zealand Standard Time"
3
4
5 #Change Computer Name
6 $serverName = "SDC"
7 Rename-Computer -NewName $serverName -Restart
8
9
10 #Set a static IP address in the same subnet of the primary domain controller.
11 #Get-NetworkAdapter
12 $interfaceIndex = 7
13 $ipAddress = "192.168.100.4"
14 $defaultGateway = "192.168.100.1"
15 $dnsServerAddresses = ("192.168.100.1")
16
17 New-NetIPAddress -InterfaceIndex $interfaceIndex -IPAddress $ipAddress -PrefixLength 24 -DefaultGateway $defaultGateway
18 #Set DNS for the static IPv4
19 Set-DnsClientServerAddress -InterfaceIndex $interfaceIndex -ServerAddresses $dnsServerAddresses
20
21
22 #Prepare credential information
23 $user = "spark\administrator"
24 $password = ConvertTo-SecureString -AsPlainText 'Aspire2' -Force
25 $credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $user, $password
26
27 #Join to the domain
28
29 $domainName = "techco.co.nz"
30 $domainNetbiosName = "TECHCO"
31
32 $credential = Get-Credential .
```

Below the script, a PowerShell command is run:

```
PS C:\Users\Administrator> Get-NetAdapter
```

Name	InterfaceDescription	ifIndex	Status	MacAddress	LinkSpeed
Ethernet 2	Microsoft Hyper-V Network Adapter #2	7	Up	00-15-50-42-50-37	10 Gbps

Then, the time zone is set:

```
PS C:\Users\Administrator> #Set Time zone
Set-TimeZone -Name "New Zealand Standard Time"
```

Finally, the script runs again:

```
PS C:\Users\Administrator>
```

2. Set static IP address

The screenshot shows a Windows PowerShell ISE window with the title bar "Administrator: Windows PowerShell ISE". The code in the editor is as follows:

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Run Selection (F8) Run Script (F5) Stop Script (Shift+F5) Save All
InstallSecondaryDomainController.ps1* | Line 109 Col 25 | 100% 9:48 AM 9/13/2024
7 $serverName = "SDC"
8 Rename-Computer -NewName $serverName -Restart
9
10
11 #Set a static IP address in the same subnet of the primary domain controller.
12 $ipAddress = "192.168.1.3"
13 $interfaceIndex = 6
14 $dnsServerAddresses = ("192.168.1.1")
15 $defaultGateway = "192.168.1.1"
16
17 New-NetIPAddress -InterfaceIndex $interfaceIndex -IPAddress $ipAddress -PrefixLength 24 -DefaultGateway $defaultGateway
18 #Set DNS for the static IPv4
19 $dnsClientServerAddress = -InterfaceIndex $interfaceIndex -ServerAddresses $dnsServerAddresses
20
21
22 #Prepare credential information
23 $user = "spark\administrator"
24 $password = ConvertTo-SecureString -AsPlainText 'Aspire2' -Force
25 $credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $user, $password
26
27 #Join to the domain
28
29
30 $ipAddress : 192.168.1.3
31 InterfaceIndex : 6
32 InterfaceAlias : Ethernet 2
33 AddressFamily : IPv4
34 Type : Unicast
35 PrefixLength : 24
36 PrefixOrigin : Manual
37 SuffixOrigin : Manual
38 AddressState : Invalid
39 ValidLifetime : Infinite (([TimeSpan]::MaxValue))
40 PreferredLifetime : Infinite (([TimeSpan]::MaxValue))
41 SkipDnsSource : False
42 PolicyStore : ActiveStore
43
44 $ipAddress : 192.168.1.3
45 InterfaceIndex : 6
46 InterfaceAlias : Ethernet 2
47 AddressFamily : IPv4
48 Type : Unicast
49 PrefixLength : 24
50 PrefixOrigin : Manual
51 SuffixOrigin : Manual
52 AddressState : Invalid
53 ValidLifetime : Infinite (([TimeSpan]::MaxValue))
54 PreferredLifetime : Infinite (([TimeSpan]::MaxValue))
55 SkipDnsSource : False
56 PolicyStore : PersistentStore
57
58 PS C:\windows\system32>
59 Completed
60 Type here to search | Ln 109 Col 25 | 100% 9:48 AM 9/13/2024
```

3. Join the domain techco.co.nz

The screenshot shows a Windows PowerShell ISE window with the title bar "Administrator: Windows PowerShell ISE". The code in the editor is as follows:

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Run Selection (F8) Run Script (F5) Stop Script (Shift+F5) Save All
InstallSecondaryDomainController.ps1* | Line 58 Col 1 | 100% 9:48 AM 9/13/2024
19 #Set DNS for the static IPv4
20 $dnsClientServerAddress = -InterfaceIndex $interfaceIndex -ServerAddresses $dnsServerAddresses
21
22
23 #Prepare credential information
24 $user = "spark\administrator"
25 $password = ConvertTo-SecureString -AsPlainText 'Aspire2' -Force
26 $credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $user, $password
27
28 #Join to the domain
29
30 $domainName = "techco.co.nz"
31 $domainNetbiosName = "TECHCO"
32
33 $credential = Get-Credential "$domainNetbiosName\administrator"
34 Add-Computer -domainname $domainName -Credential $credential -Restart
35
36 #Restart-Computer
37
38
39 #Install Roles and Feature of Active Directory
40 Install-WindowsFeature -Name "AD-Domain-Services" -IncludeManagementTools
41
42 $ipAddress : 192.168.100.3
43 InterfaceIndex : 6
44 InterfaceAlias : Ethernet 2
45 AddressFamily : IPv4
46 Type : Unicast
47 PrefixLength : 24
48 PrefixOrigin : Manual
49 SuffixOrigin : Manual
50 AddressState : Invalid
51 ValidLifetime : Infinite (([TimeSpan]::MaxValue))
52 PreferredLifetime : Infinite (([TimeSpan]::MaxValue))
53 SkipDnsSource : False
54 PolicyStore : PersistentStore
55
56 PS C:\windows\system32> #join to the domain
57 $domainName = "techco.co.nz"
58 $domainNetbiosName = "TECHCO"
59
60 $credential = Get-Credential "$domainNetbiosName\administrator"
61 Add-Computer -domainname $domainName -Credential $credential -Restart
62
63 Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger.
```

A credential dialog box titled "Windows PowerShell credential request" is overlaid on the window, prompting for a user name (TECHCO\administrator) and password (*****).

Server Manager

Server Manager > Local Server

PROPERTIES For SDC

Computer name	SDC	Last installed updates	Never
Domain	techco.co.nz	Windows Update	Download updates only, using Windows Update
		Last checked for updates	Never
Microsoft Defender Firewall	Domain: On	Microsoft Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC +12:00) Auckland, Wellington
Ethernet	192.168.1.3, IPv6 enabled	Product ID	Not activated
Operating system version	Microsoft Windows Server 2022 Standard Evaluation	Processors	12th Gen Intel(R) Core(TM) i3-1215U
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	4 GB
		Total disk space	48.89 GB

EVENTS
All events | 60 total

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

The screenshot shows the Windows PowerShell ISE interface. A script named `InstallSecondaryDomainController.ps1` is open in the editor. The script performs several tasks:

- Joins the domain.
- Installs the Active Directory Domain Services role and management tools.
- Promotes the server as a secondary domain controller.
- Creates a new local administrator account (`$User`) and sets its password (`$Pword`).
- Creates a credential object (`$Credential`) for the new administrator account.
- Installs AD DS on the server.

The status bar at the bottom indicates "Start Installation..." and "24%". The bottom right corner shows the date and time as "12/09/2024 10:20 am".

The screenshot shows the Windows PowerShell ISE interface after the script has completed. The status bar at the bottom indicates "Completed". The bottom right corner shows the date and time as "12/09/2024 10:20 am".

The output window displays the results of the command `Install-WindowsFeature -Name "AD-Domain-Services" -IncludeManagementTools`, showing the success of the feature installation.

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	[Active Directory Domain Services, Group P...]

5. Promote the server as a secondary domain controller

The screenshot shows a Windows PowerShell ISE window with the following content:

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
InstallSecondaryDomainController.ps1 X
37
38
39 #Install Rols and Feature of Active Directory
40 Install-WindowsFeature -Name "AD-Domain-Services" -IncludeManagementTools
41
42
43 #Promote the server as a secondary domain controller
44 $User = "spark\administrator"
45 $Pword = ConvertTo-SecureString -AsPlainText "Aspire2" -Force
46 $Credential = New-Object System.Management.Automation.PSCredential -ArgumentList $User, $Pword
47
48 $domainName = "techco.co.nz"
49 $domainNetbiosName = "TECHCO"
50 $Credential = Get-Credential $domainNetbiosName\administrator
51
52 Install-ADDSDomainController -InstallDns -DomainName $domainName -Credential $Credential -SafeModeAdministratorPassword $Pword
53
54
55
56
57
58
59 # windows PowerShell script for AD DS Deployment
60
```

Below the code, the PowerShell window displays the progress of the command:

```
Install-ADDSDomainController.
Determining replication source DC.
Install-ADDSDomainController.
Determining replication source DC.

Validating environment and user input.
Verifying prerequisites for domain controller operation...
```

At the bottom of the window, there is a warning message:

```
WARNING: Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
```

For more information about this setting, see Knowledge Base article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).

Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger.

10:21 am 12/09/2024

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

Properties for PDC

Active Directory Users and Computers

Name	Type	DC Type	Site	Description
PDC	Computer	GC	Default-First-Site	
SDC	Computer	GC	Default-First-Site	

Events

Server Name	ID	Severity	Source	Time
PDC	8198	Error	Microsoft-Windows-Security-SPP	9/11/2024 12:33:49 PM
PDC	1014	Error	Microsoft-Windows-Security-SPP	9/11/2024 12:33:49 PM
PDC	8200	Error	Microsoft-Windows-Security-SPP	9/11/2024 12:33:49 PM
PDC	1046	Error	Microsoft-Windows-DHCP-Server	9/11/2024 12:33:48 PM
PDC	1059	Error	Microsoft-Windows-DHCP-Server	9/11/2024 12:33:48 PM
PDC	1059	Error	Microsoft-Windows-DHCP-Server	9/11/2024 12:33:48 PM

Properties for PDC

Active Directory Users and Computers

Name	Type	Description
DHCP Admins	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 Adm...	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 ...
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 Adm...	Security Group...	Designated administrato...
user1	User	

Server Manager

Server Manager ▾ Local Server

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	192.168.1.3, IPv6 en
Operating system version	Microsoft Windows
Hardware information	Microsoft Corporat

EVENTS

All events | 89 total

Filter	Server Name	ID	Severity	Source	Time	
	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

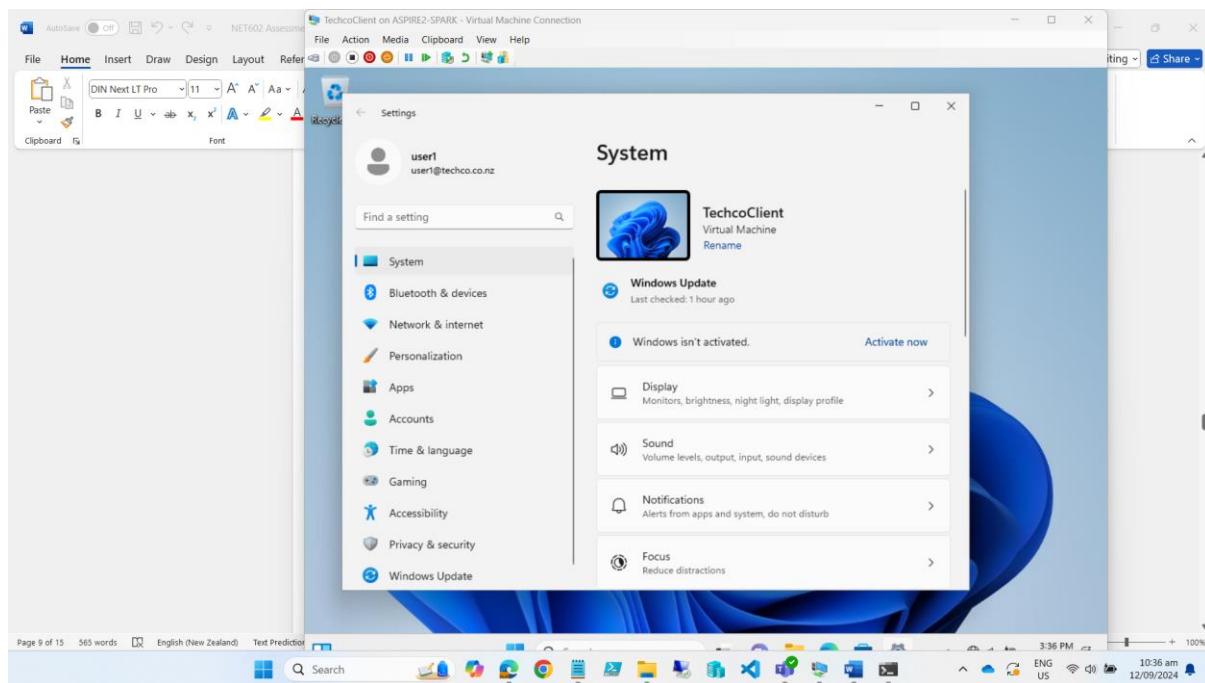
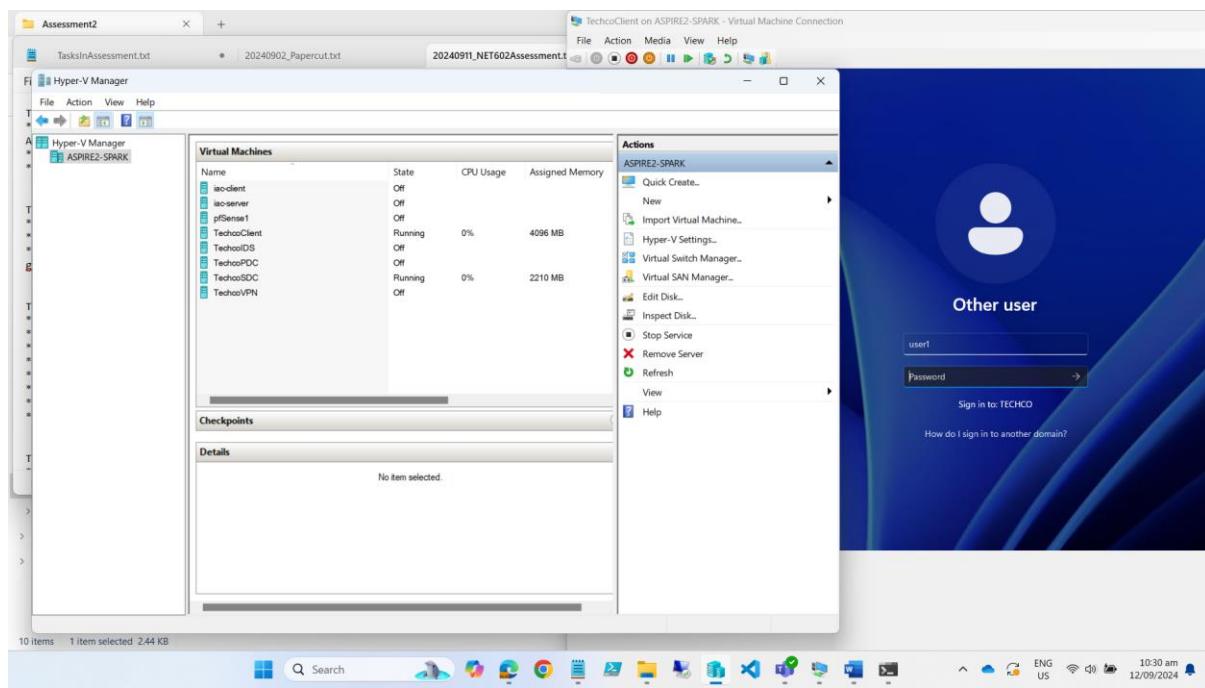
File Action View Help

TASKS

Name	Type	Description
DHCP Admins	Security Group...	Members who have ad...
DHCP Users	Security Group...	Members who have vie...
Builtin	Security Group...	Builtin security gro...
Computers	Security Group...	Computers in the do...
Domain Controllers	Security Group...	Domain controllers in...
ForeignSecurityPrincipals	Security Group...	Foreign security princ...
Managed Service Accounts	Security Group...	Managed service accou...
Users	User	User account in the do...

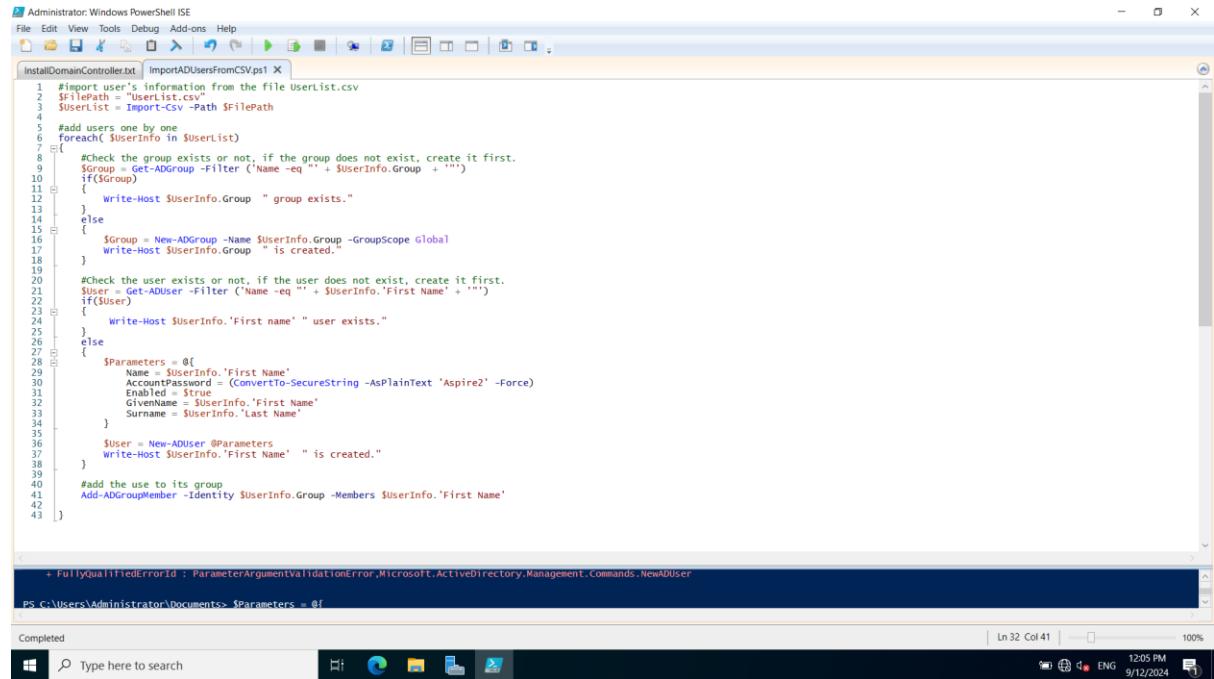
10:27 am 12/09/2024

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



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Import-Module ActiveDirectory
Import-Module PSReadLine
Import-Module -Name UserList.csv

#Import user's information from the file UserList.csv
$filePath = "UserList.csv"
$userList = Import-Csv -Path $filePath

#Add users one by one
foreach($userInfo in $userList)
{
    #Check the group exists or not, if the group does not exist, create it first.
    $group = Get-ADGroup -Filter ('Name -eq "' + $userInfo.Group + '"')
    if(!$group)
    {
        write-host "$userInfo.Group " group exists."
    }
    else
    {
        $group = New-ADGroup -Name $userInfo.Group -GroupScope Global
        write-host "$userInfo.Group " is created."
    }

    #Check the user exists or not, if the user does not exist, create it first.
    $user = Get-ADUser -Filter ('Name -eq "' + $userInfo.'First Name' + '"')
    if(!$user)
    {
        write-host "$userInfo.'First Name' " user exists."
    }
    else
    {
        $parameters = @{
            FirstName = $userInfo.'First Name'
            AccountPassword = (ConvertTo-SecureString -AsPlainText 'Aspire2' -Force)
            Enabled = $true
            GivenName = $userInfo.'First Name'
            Surname = $userInfo.'Last Name'
        }

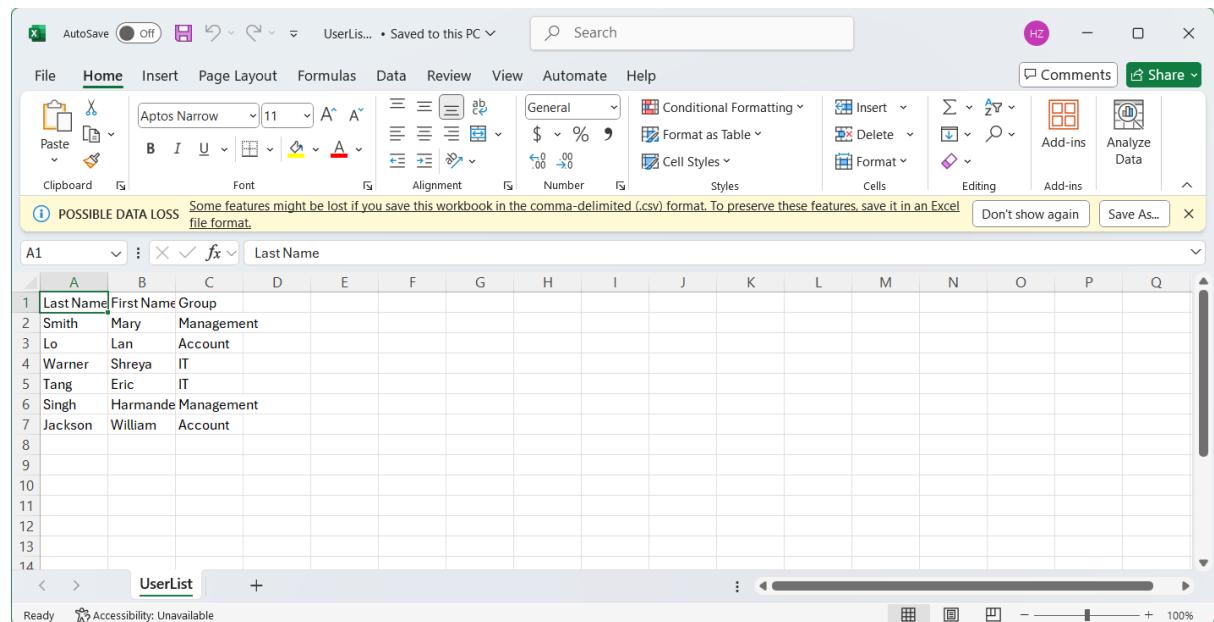
        $user = New-ADUser @parameters
        write-host "$userInfo.'First Name' " is created."
    }

    #Add the user to its group
    Add-ADGroupMember -Identity $userInfo.Group -Members $userInfo.'First Name'
}

```

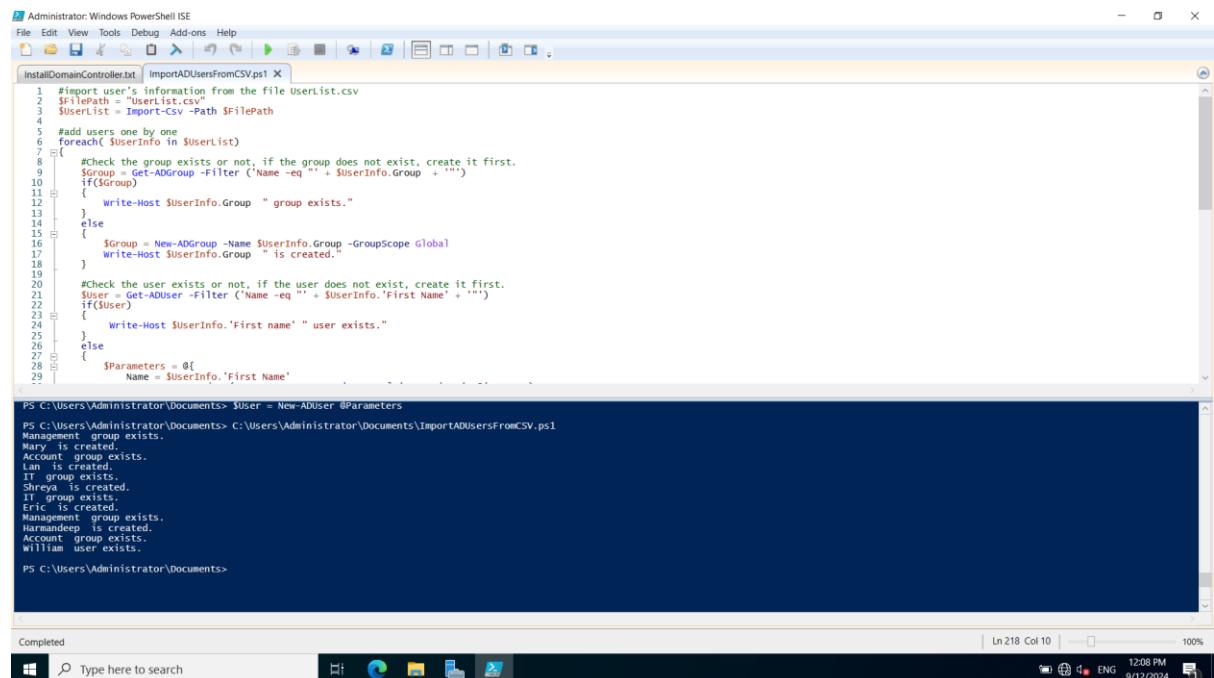
The screenshot shows the Windows PowerShell ISE interface. The code is contained in a file named 'InstallDomainController.ps1'. The code reads a CSV file 'UserList.csv' and iterates through each user entry. For each user, it checks if the user already exists. If not, it creates a new user account with the specified first name and a password of 'Aspire2'. It also checks if the user is part of a specific group ('Management' or 'IT') and adds the user to that group if it exists. A warning message is displayed at the bottom of the PowerShell window: '+ FullyQualifiedErrorId : ParameterArgumentValidationError,Microsoft.ActiveDirectory.Management.Commands.NewADUser'.

2. Users in userList.csv file



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Last Name	First Name	Group													
2	Smith	Mary	Management													
3	Lo	Lan	Account													
4	Warner	Shreya	IT													
5	Tang	Eric	IT													
6	Singh	Harmeande	Management													
7	Jackson	William	Account													
8																
9																
10																
11																
12																
13																
14																

3. Run the PowerShell script

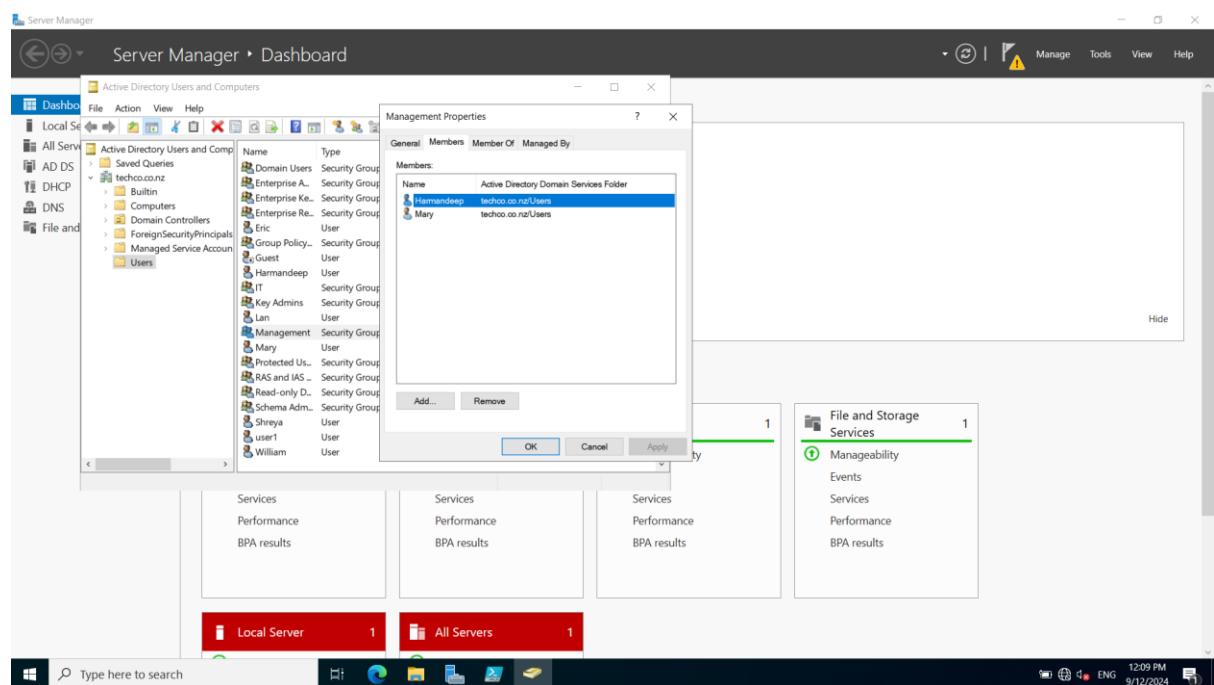


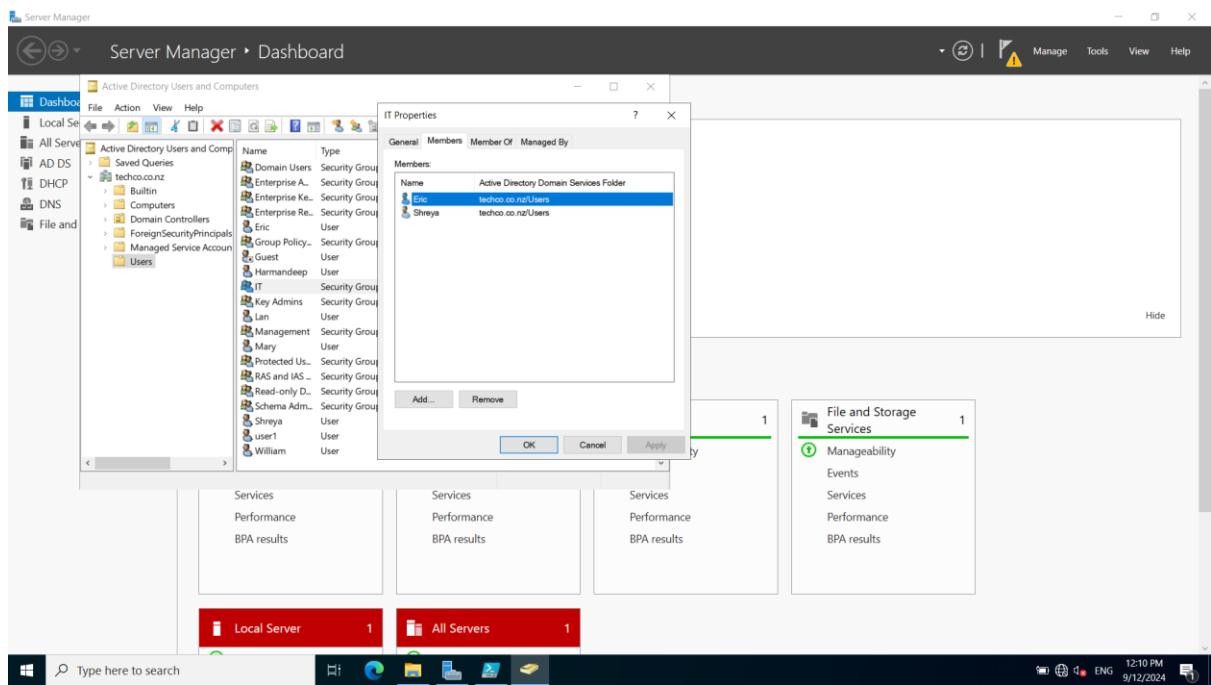
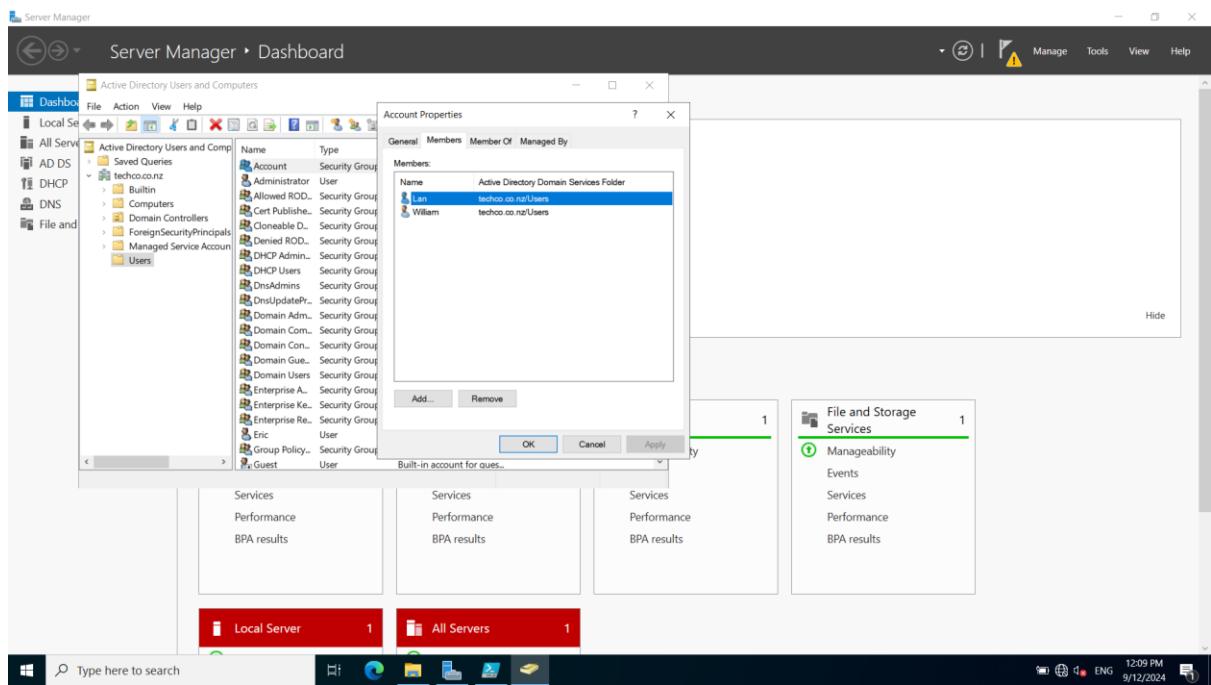
```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
ImportADUsersFromCSV.ps1
1 #Import user's information from the file UserList.csv
2 $FilePath = "UserList.csv"
3 $UserList = Import-Csv -Path $FilePath
4
5 #Add users one by one
6 foreach($userInfo in $UserList)
7 {
8     #Check the group exists or not, if the group does not exist, create it first.
9     $Group = Get-ADGroup -Filter ("Name -eq '" + $userInfo.Group + "'")
10    if($Group)
11    {
12        Write-Host $userInfo.Group " group exists."
13    }
14    else
15    {
16        $Group = New-ADGroup -Name $userInfo.Group -GroupScope Global
17        Write-Host $userInfo.Group " is created."
18    }
19
20    #Check the user exists or not, if the user does not exist, create it first.
21    $User = Get-ADUser -Filter ("Name -eq '" + $userInfo.'First Name' + "'")
22    if($User)
23    {
24        Write-Host $userInfo.'First name' " user exists."
25    }
26    else
27    {
28        $Parameters = @{
29            Name = $userInfo.'First Name'
30
PS C:\Users\Administrator\Documents> $User = New-ADUser @Parameters
PS C:\Users\Administrator\Documents> C:\Users\Administrator\Documents\ImportADUsersFromCSV.ps1
Management group exists.
Mary is created.
Account group exists.
Lan is created.
IT group exists.
Shreya is created.
IT group exists.
Eric is created.
Management group exists.
Harmandeep is created.
Account group exists.
William user exists.

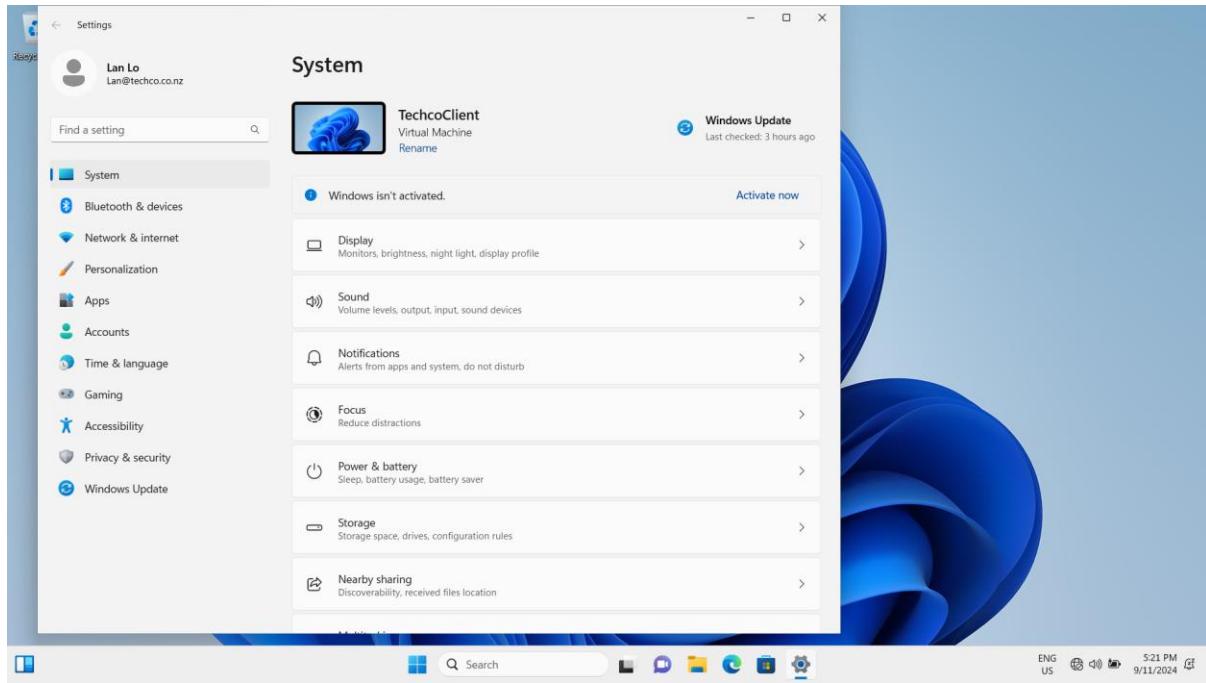
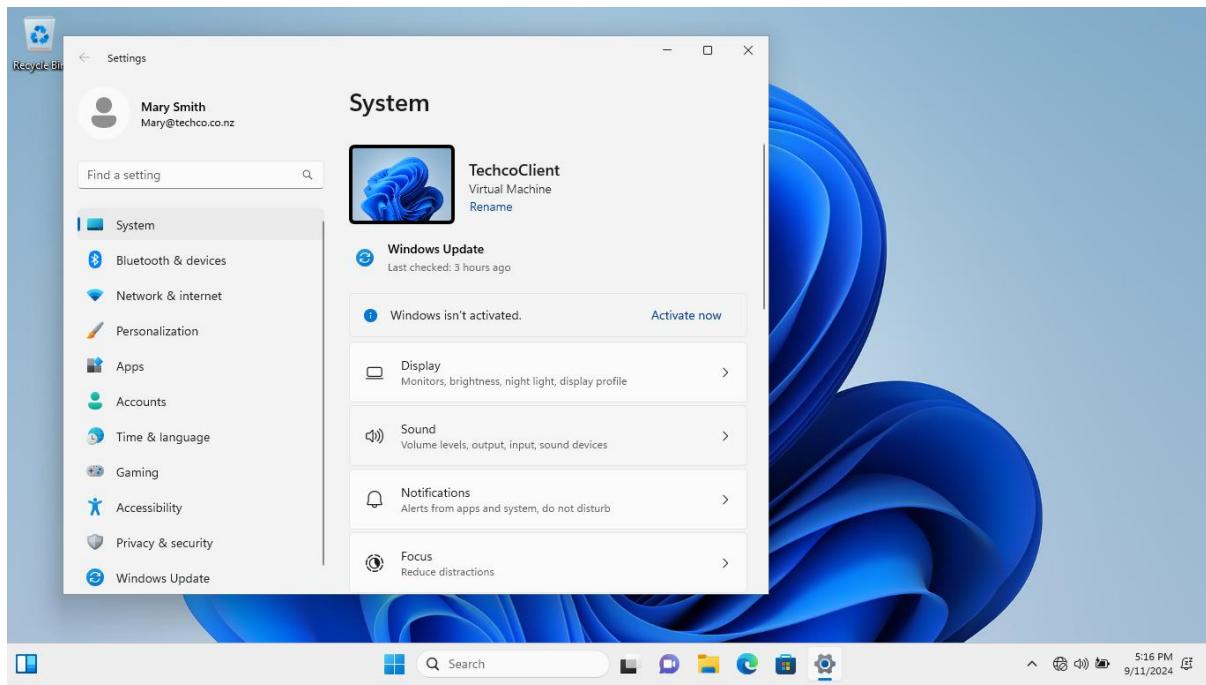
PS C:\Users\Administrator\Documents>

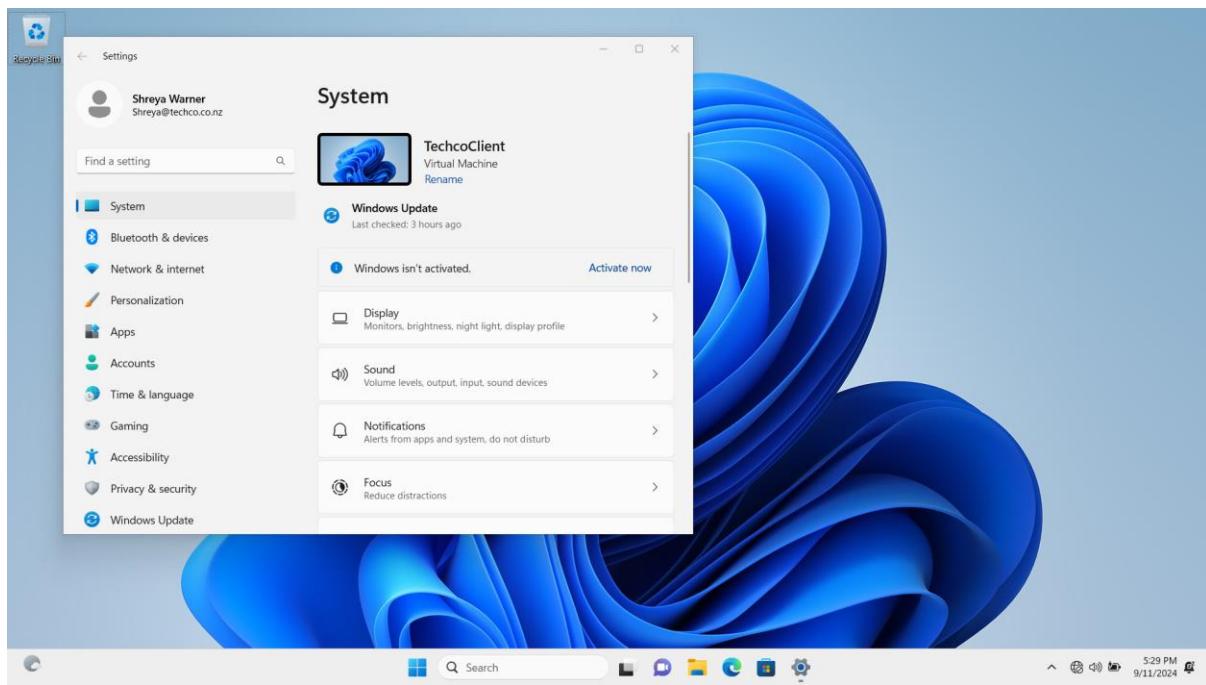
```





4. Test users created to login on the client machine





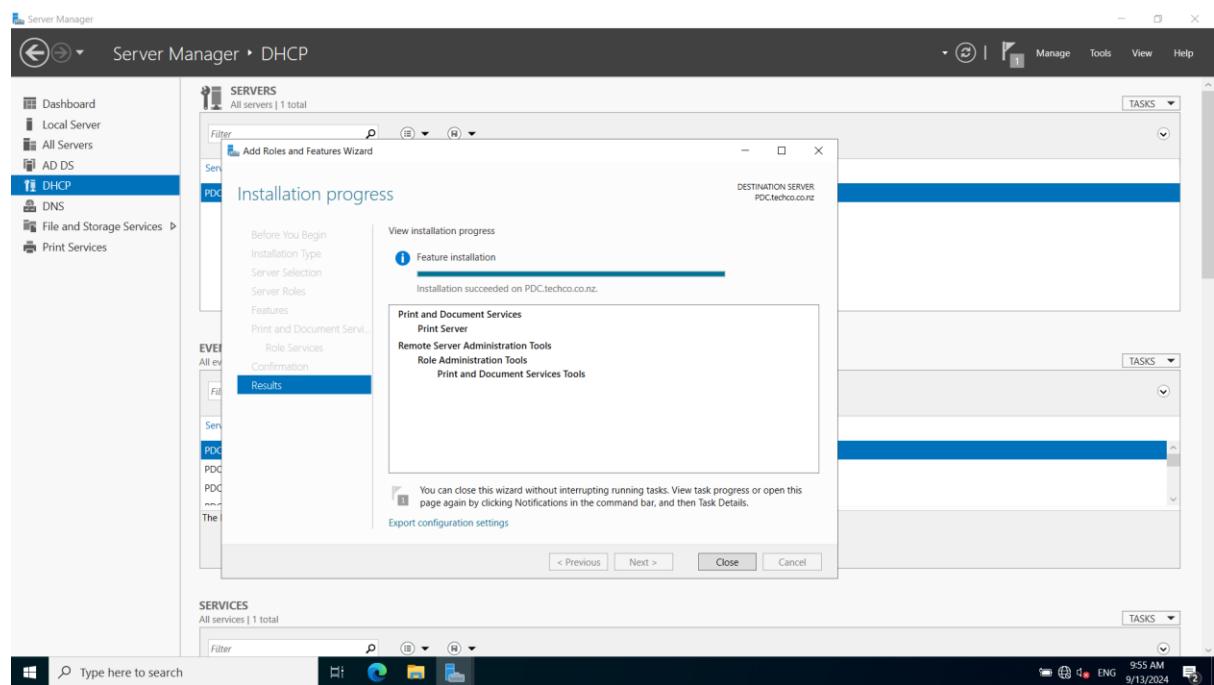
Task/Mahi 2: Deploying Print Management Solution via Group Policy Object

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

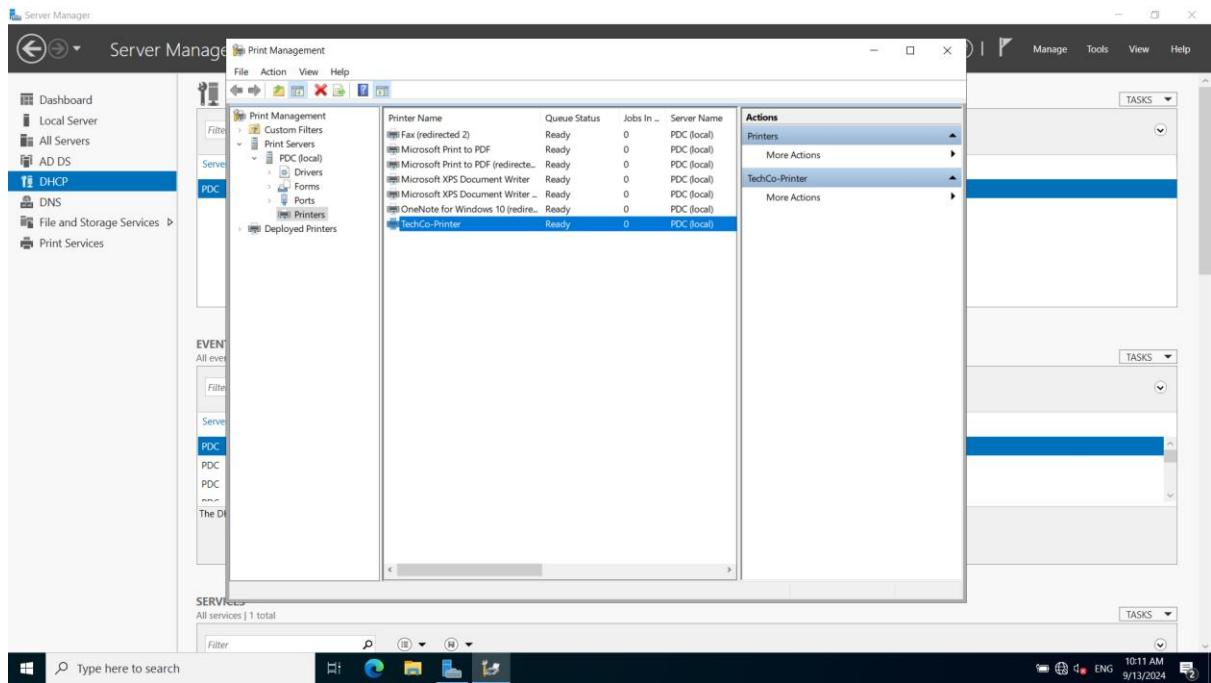
2.1 Install Printer service role on DC



2.2 Install Lexmark printer driver on DC

Download Lexmark Printer Drivers from

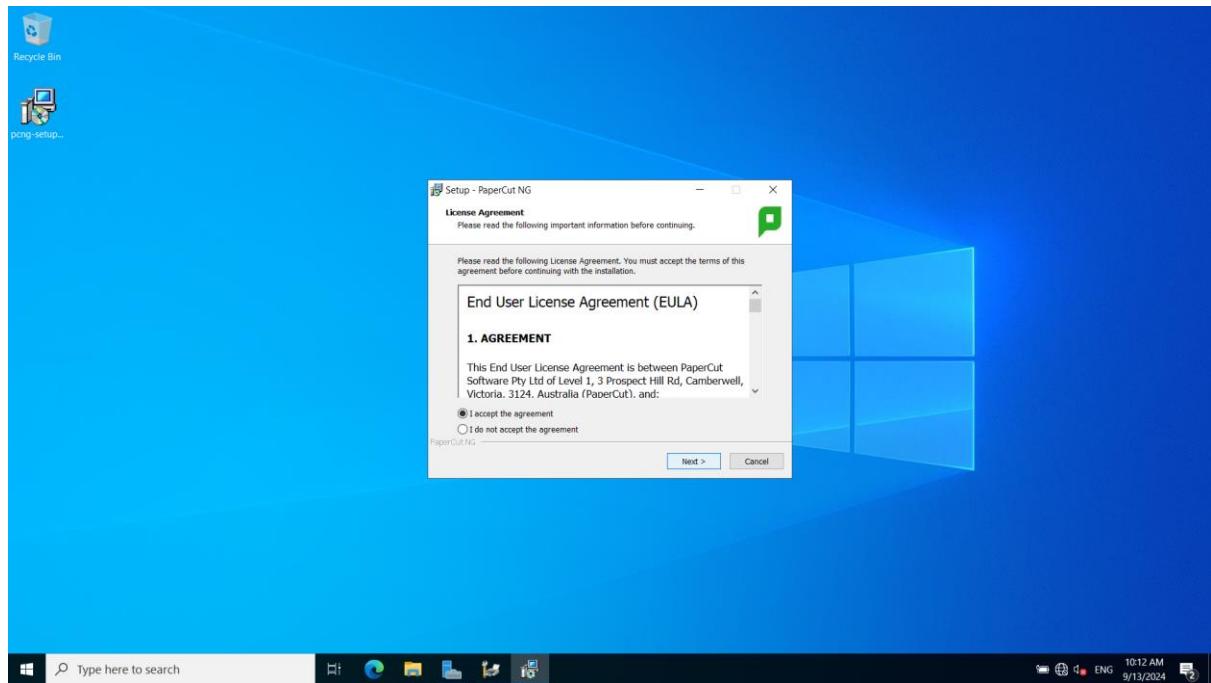
https://downloads.lexmark.com/downloads/drivers/Lexmark_Universal_v2_UD1_Installation_Package_02092023.exe

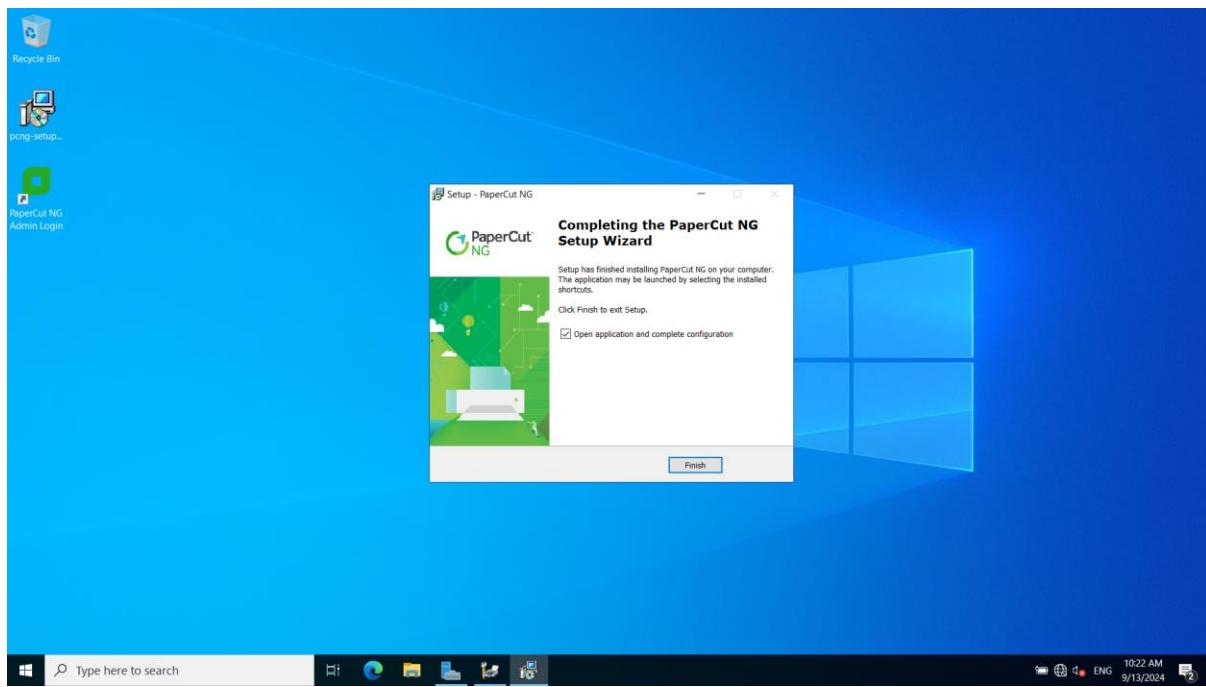
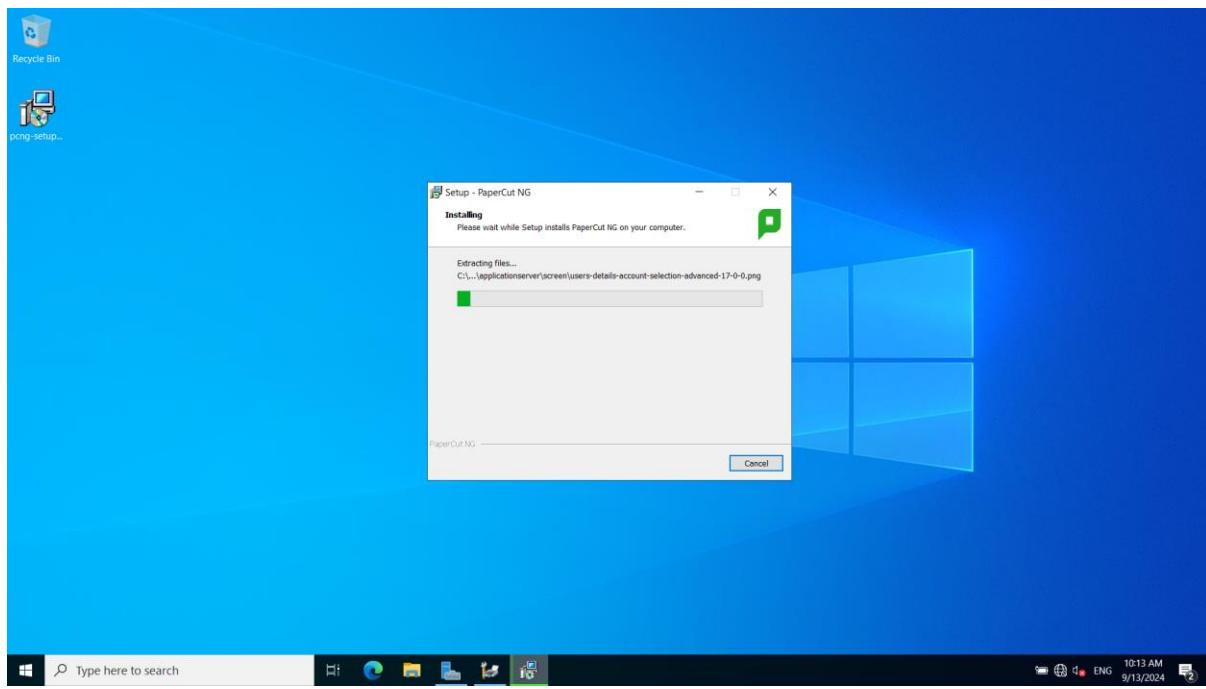


2.3 Download Papercut software.

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

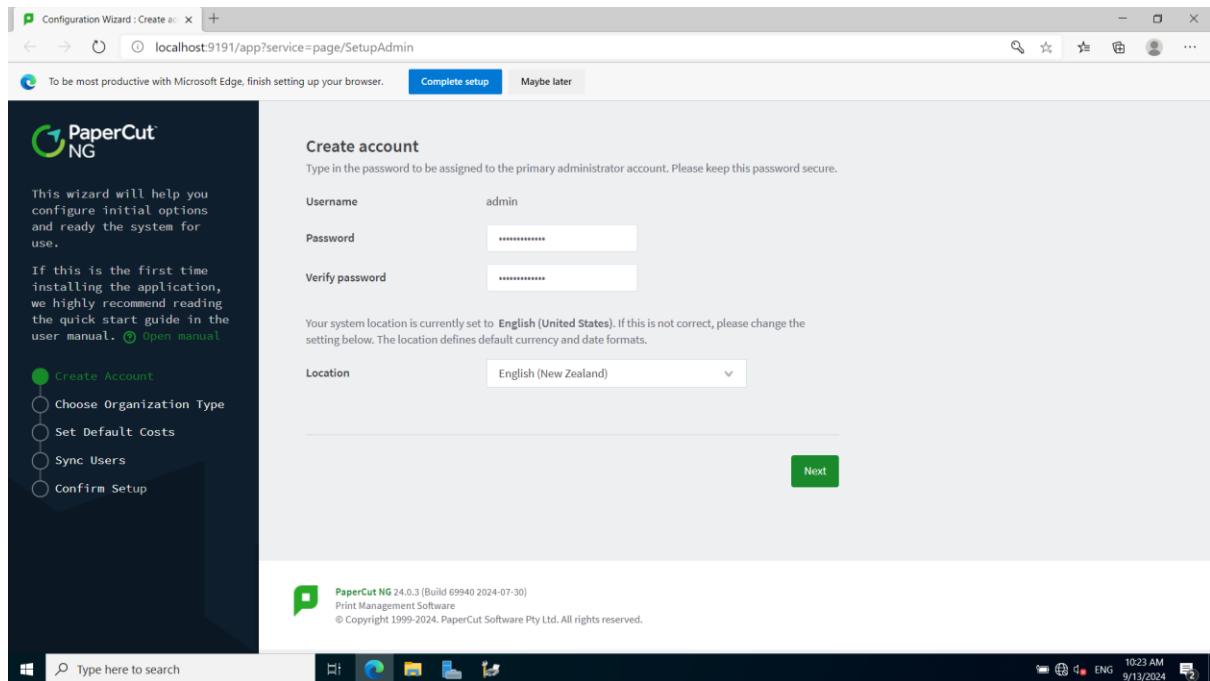
2.4 Install Papercut software on DC. (Admin/Spark@Aspire2)



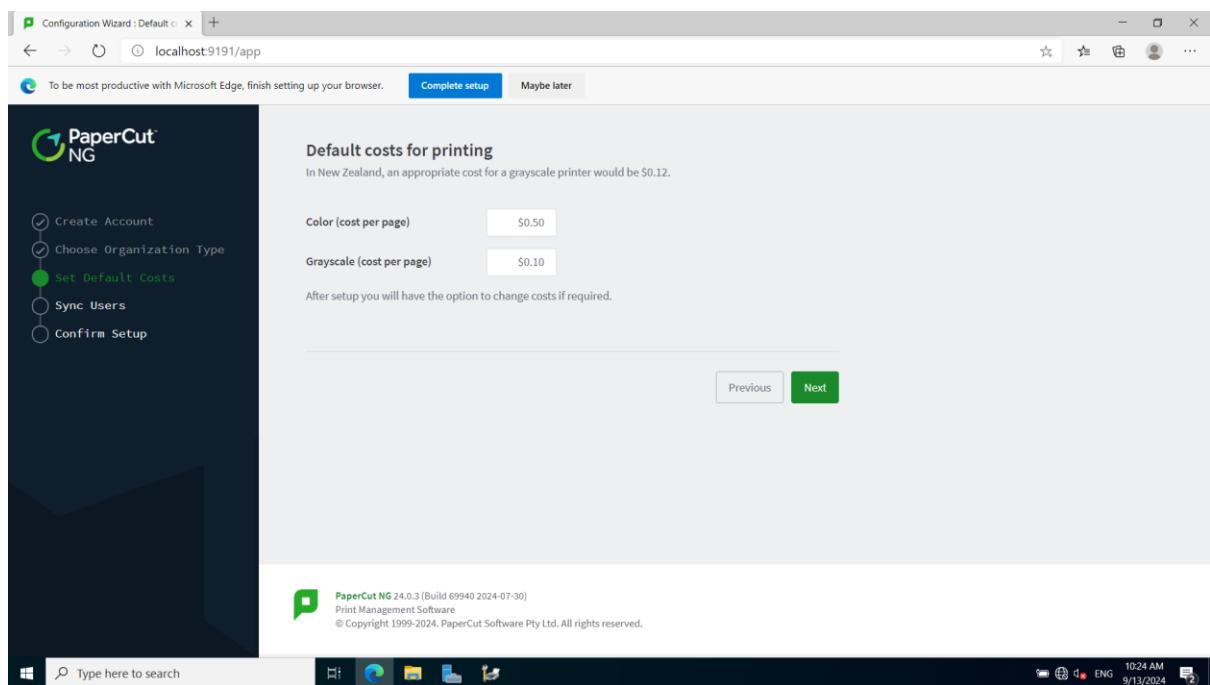


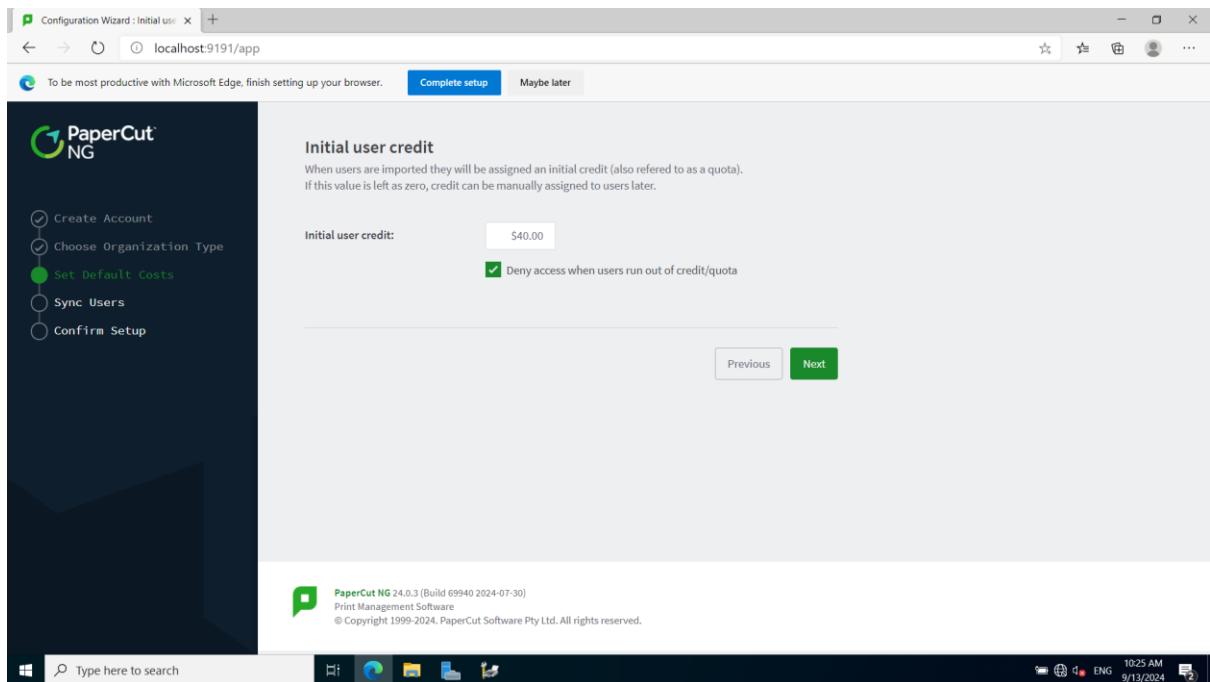
3. Configure PaperCut

3.1 Login to Admin portal.

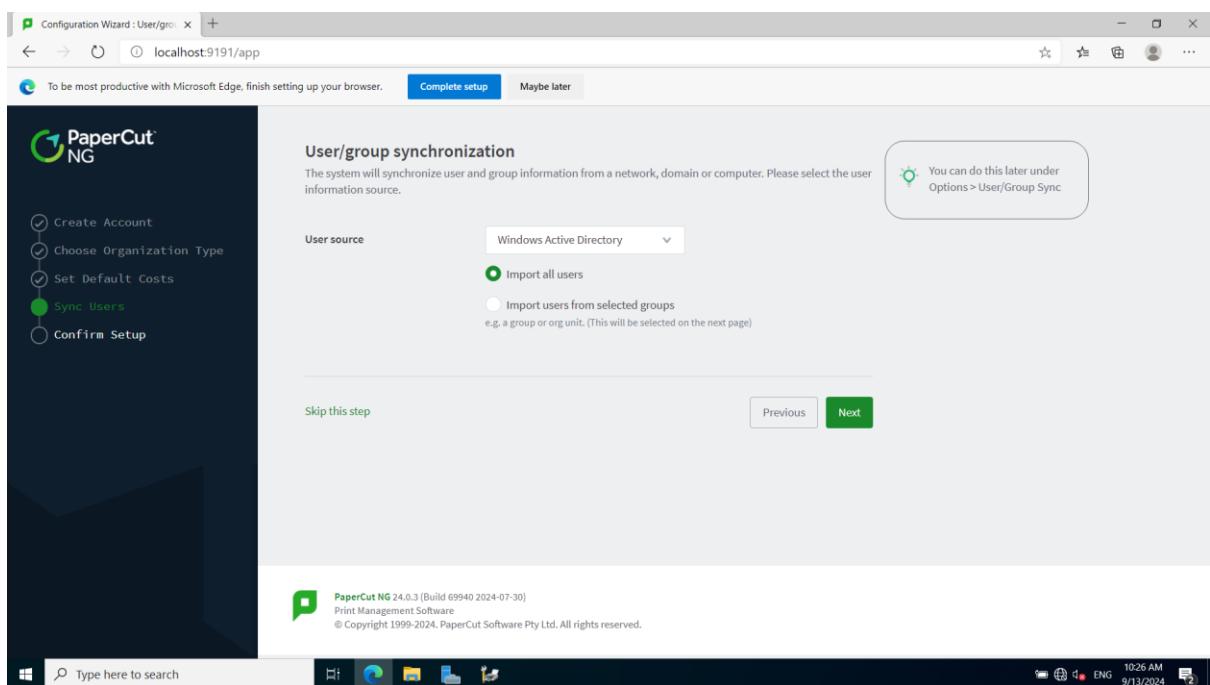


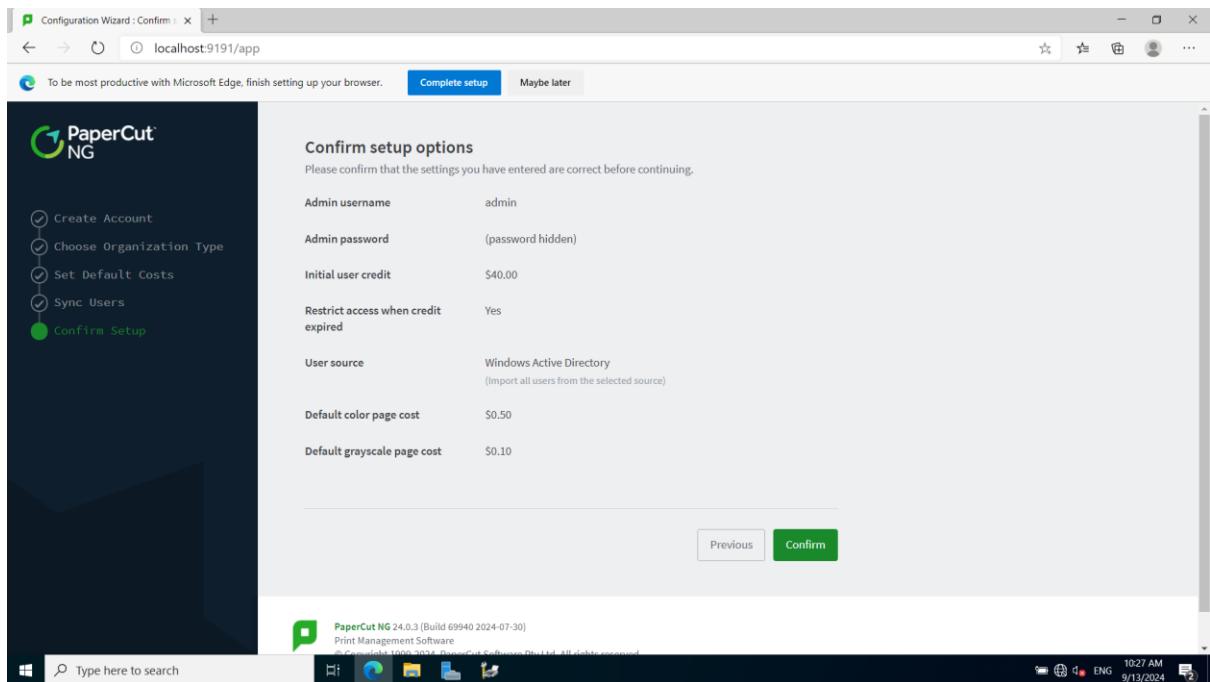
3.2 Set printing price





3.3 Sync users with AD





The screenshot shows the 'Papercut NG : Users : User List' window in Microsoft Edge. The title bar says 'Papercut NG : Users : User List' and the address bar shows 'localhost:9191/app?service=page/UserList'. A message at the top says 'To be most productive with Microsoft Edge, finish setting up your browser.' with 'Complete setup' and 'Maybe later' buttons. The left sidebar has a 'Users' section expanded, showing 'Groups', 'Accounts', 'Printers', 'Devices', 'Enable Printing', 'Reports', 'Cards', 'Options', 'Logs', 'About', and 'Help'. The main content area is titled 'User List' and shows a table of users:

USERNAME	FULL NAME	BALANCE	RESTRICTED	PAGES	JOBJS
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

To the right of the table is a green 'Actions (4)' button with options: 'Bulk user actions ...', 'Export/Print', 'User printing - summary (last 30 days)', and 'Batch import - Standard users'. At the bottom are 'Export/Print' buttons and a Windows taskbar.

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

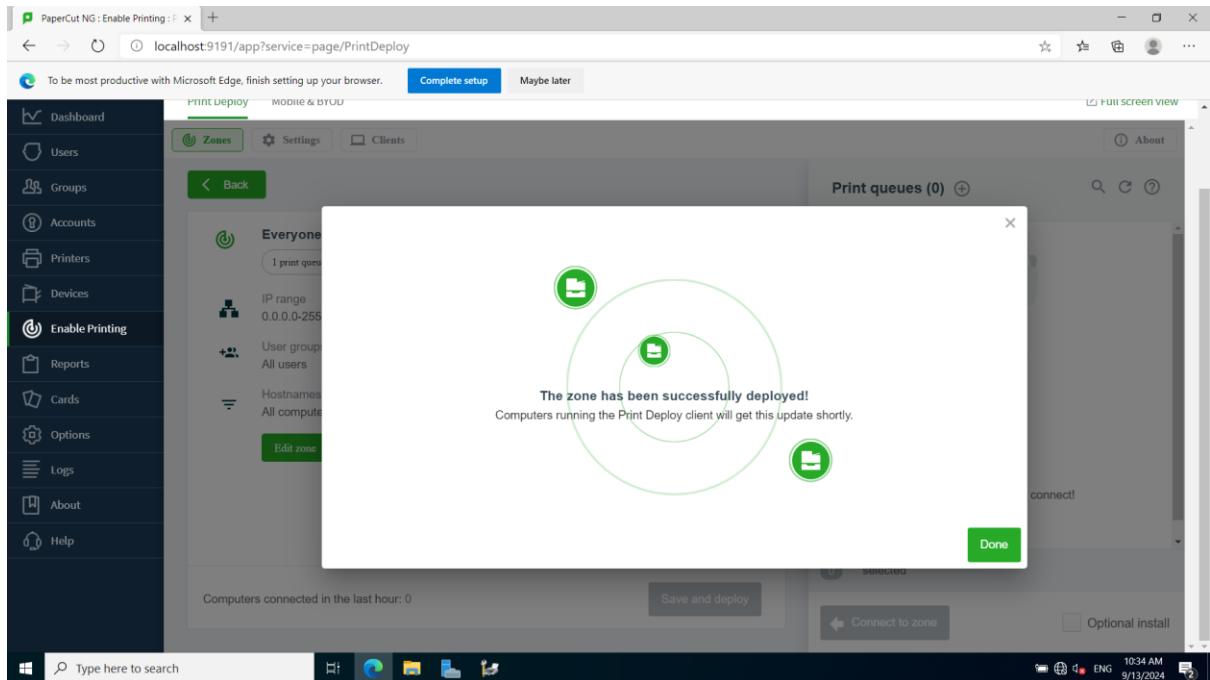
The screenshot shows the PaperCut NG Print Deploy interface. The main navigation bar at the top includes links for 'Enable Printing' (which is currently selected), 'Print Deploy', 'Mobile & BYOD', 'Complete setup' (button), and 'Maybe later'. On the far right, there's a user icon for 'admin' and a 'Full screen view' link. The left sidebar has a tree structure with 'Enable Printing' expanded, showing 'Print Deploy' as the active tab, along with other options like 'Reports', 'Cards', 'Options', and 'Logs'. Below the sidebar is a search bar with placeholder text 'Type here to search' and a set of system icons. The main content area is titled 'Print Deploy' and shows the 'Your zones' section. It lists a single zone named 'Everyone' with '0 print queues' and '0 clients connected'. To the right, a large panel titled 'Print queues' displays a list with one item: 'TechCo-Printer'. Below this panel, there's a section titled 'Import print queues by cloning printer drivers' with a list of reasons for using this method, a 'Download cloner tool for Windows' button, and a 'Download for macOS' link. The bottom right corner of the window shows the system tray with icons for battery, signal, and date/time (10:29 AM, 9/13/2024).

This screenshot is nearly identical to the previous one, showing the same interface and data. The main difference is the system tray at the bottom right, which now shows the date and time as 10:31 AM on 9/13/2024.

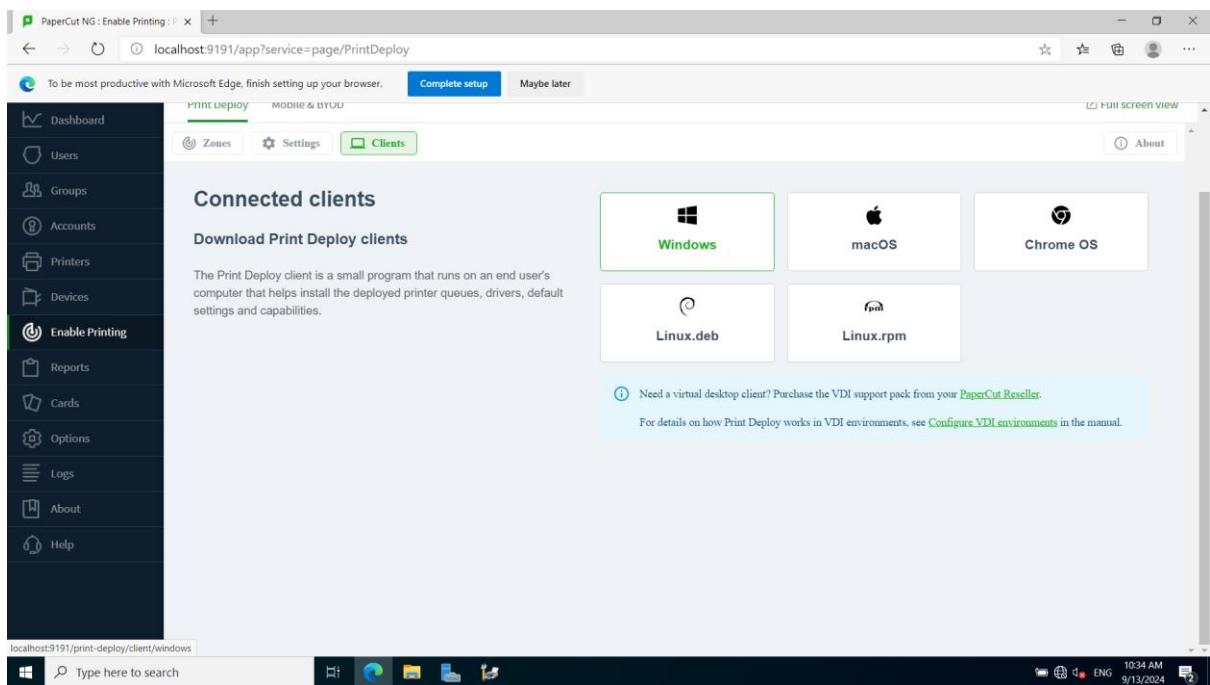
5. Add printer to Zone.

The screenshot shows the PaperCut NG : Enable Printing web interface. The left sidebar includes options like Dashboard, Users, Groups, Accounts, Printers, Devices, Enable Printing, Reports, Cards, Options, Logs, About, and Help. The main navigation bar has tabs for PRINT DEPLOY, MOBILE & BYOD, and ZONES (which is selected). A 'Complete setup' button is at the top right. The central area shows a 'Print queues (1)' section with a list containing 'TechCo-Printer'. Below it is a 'Print queues (0)' section with a message 'There are no queues to connect!'. A sidebar on the left under 'Everyone' shows '0 print queues' and lists 'IP range 0.0.0-255.255.255.255', 'User groups All users', and 'Hostnames All computers'. A green 'Edit zone' button is at the bottom. At the bottom of the screen, there's a Windows taskbar with icons for File Explorer, Edge, File History, Task View, Taskbar settings, and Start.

This screenshot shows the same PaperCut interface after some changes. The 'Print queues (1)' section now shows 'TechCo-Printer' with a checkmark. The 'Print queues (0)' section still says 'There are no queues to connect!' with a cartoon character icon. The sidebar under 'Everyone' now shows '1 print queue'. The rest of the interface and the Windows taskbar at the bottom remain the same.

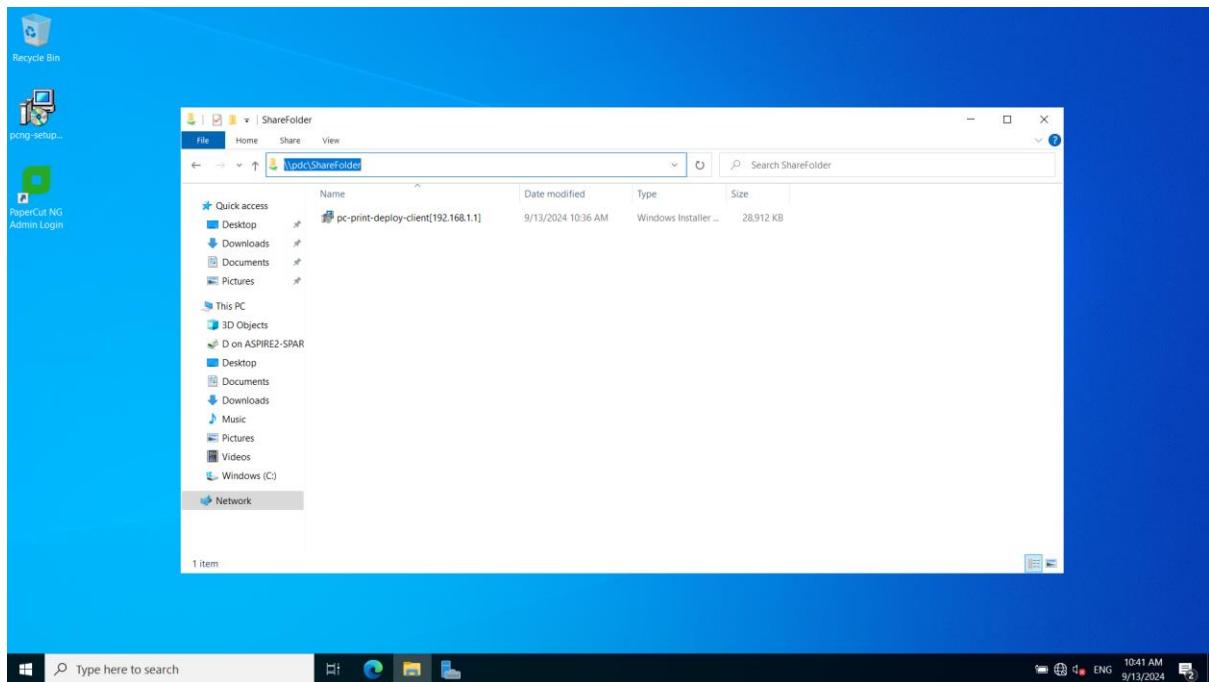
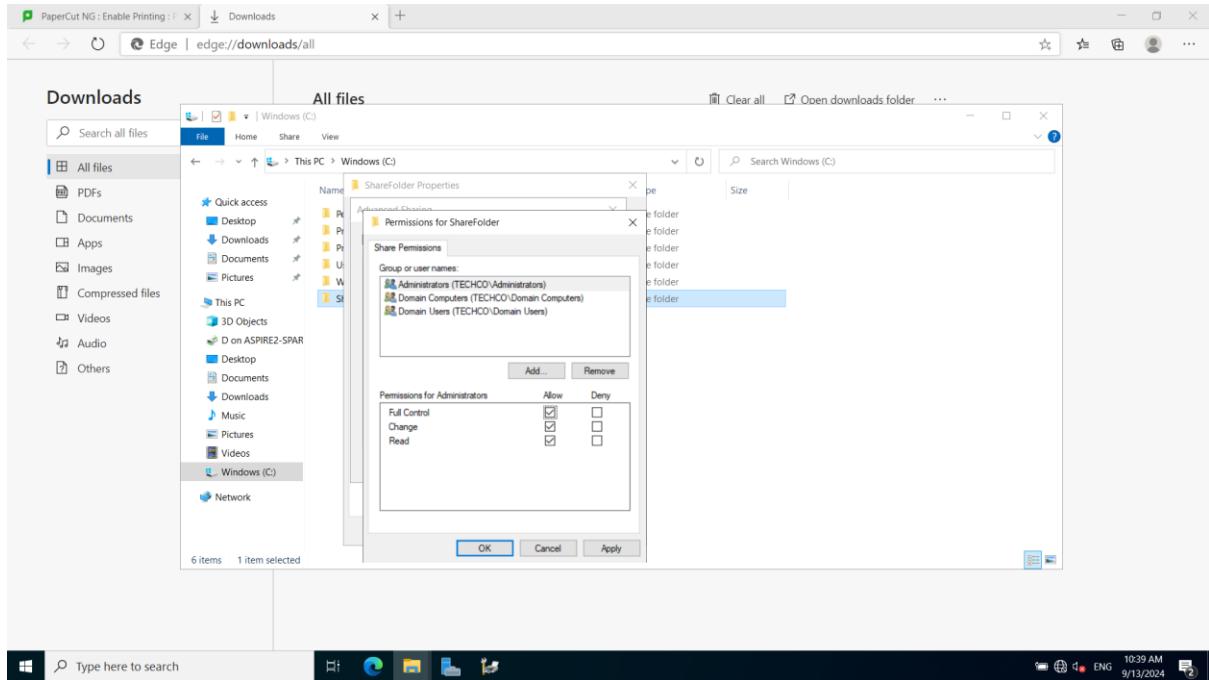


6. Generate a client software in "Zone->Client->Windows"

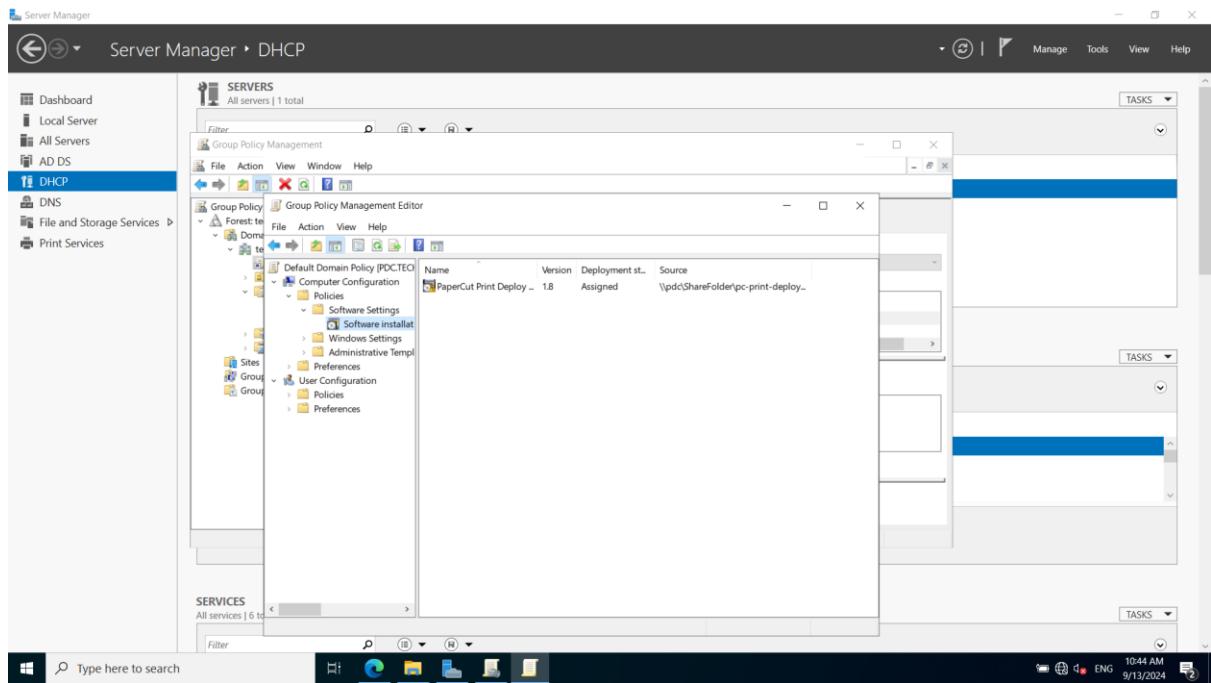


7. Create a Papercut Group Policy to deploy the client software to the client machine.

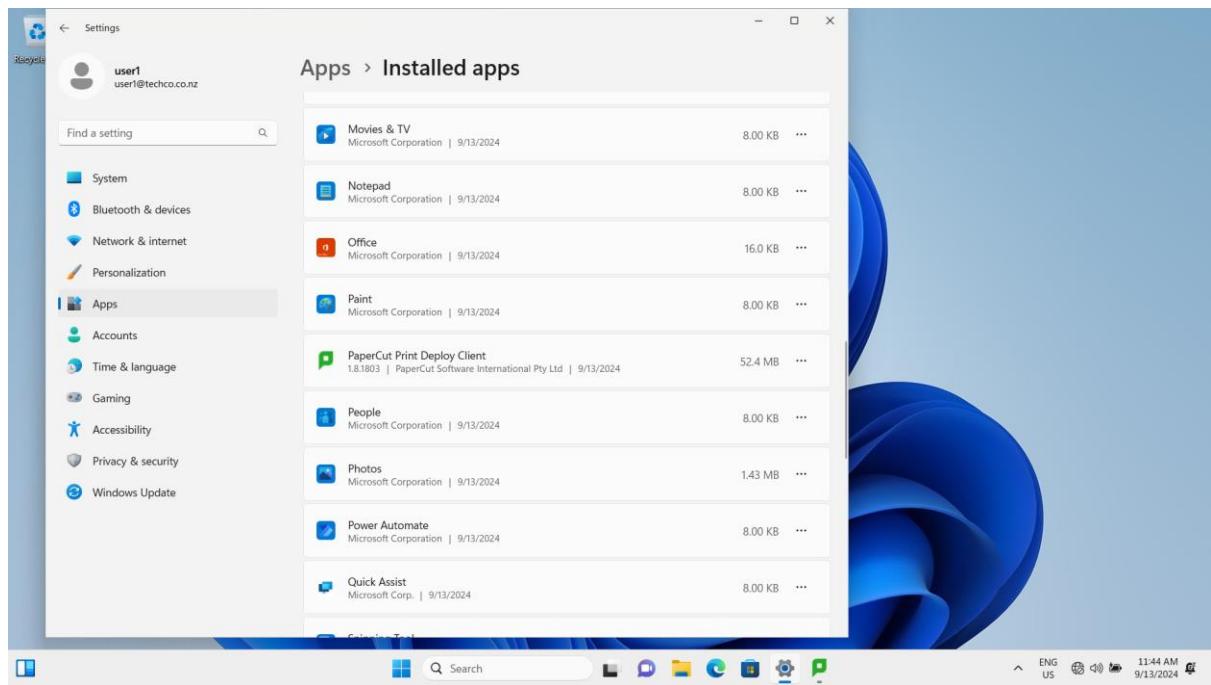
- Set up shared folder (Administrators, Domain Computers, Domain Users)

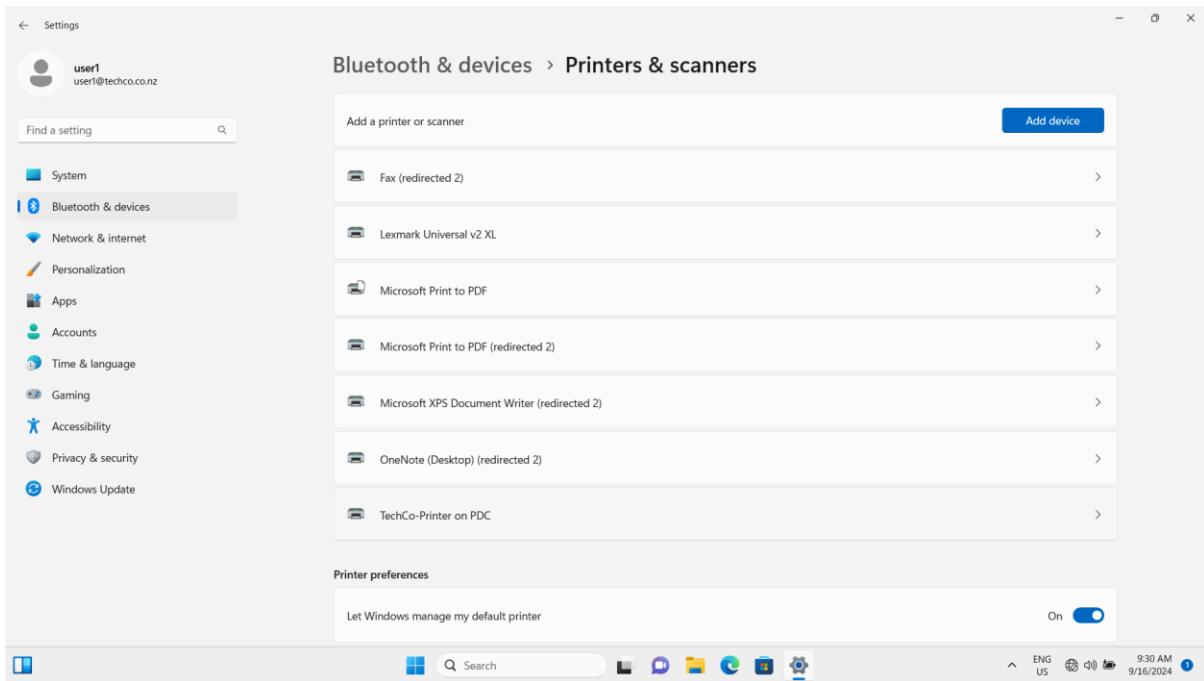
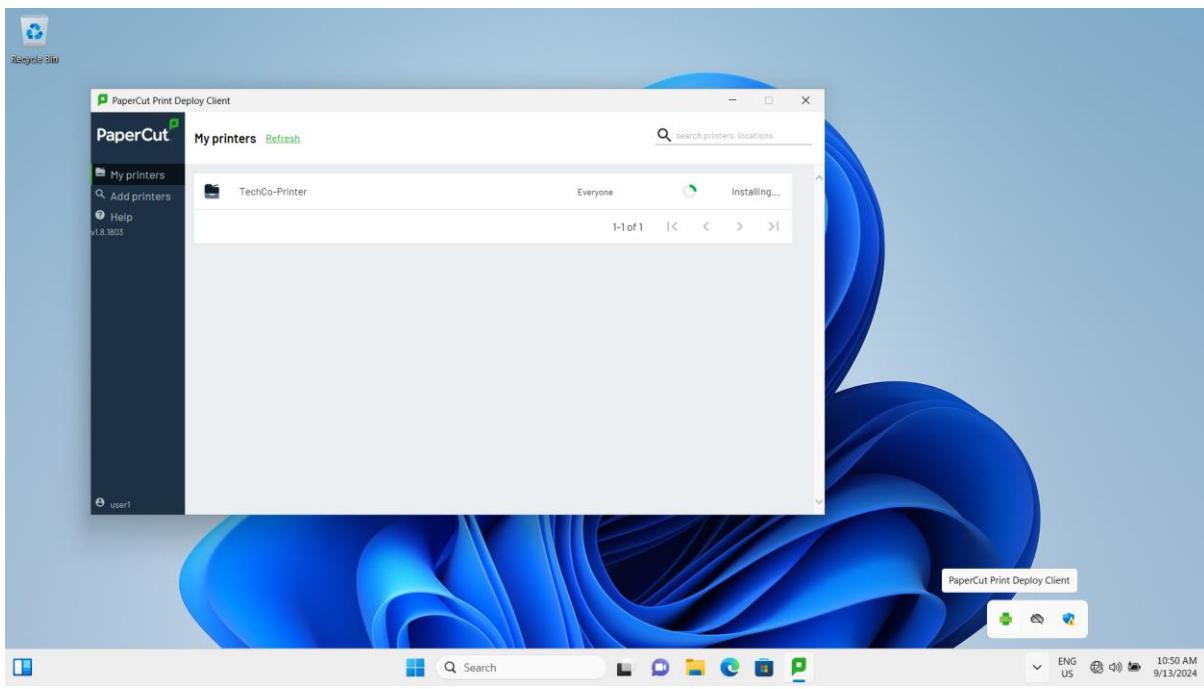


- Deploy client version of Papercut to client machine using GPO.



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



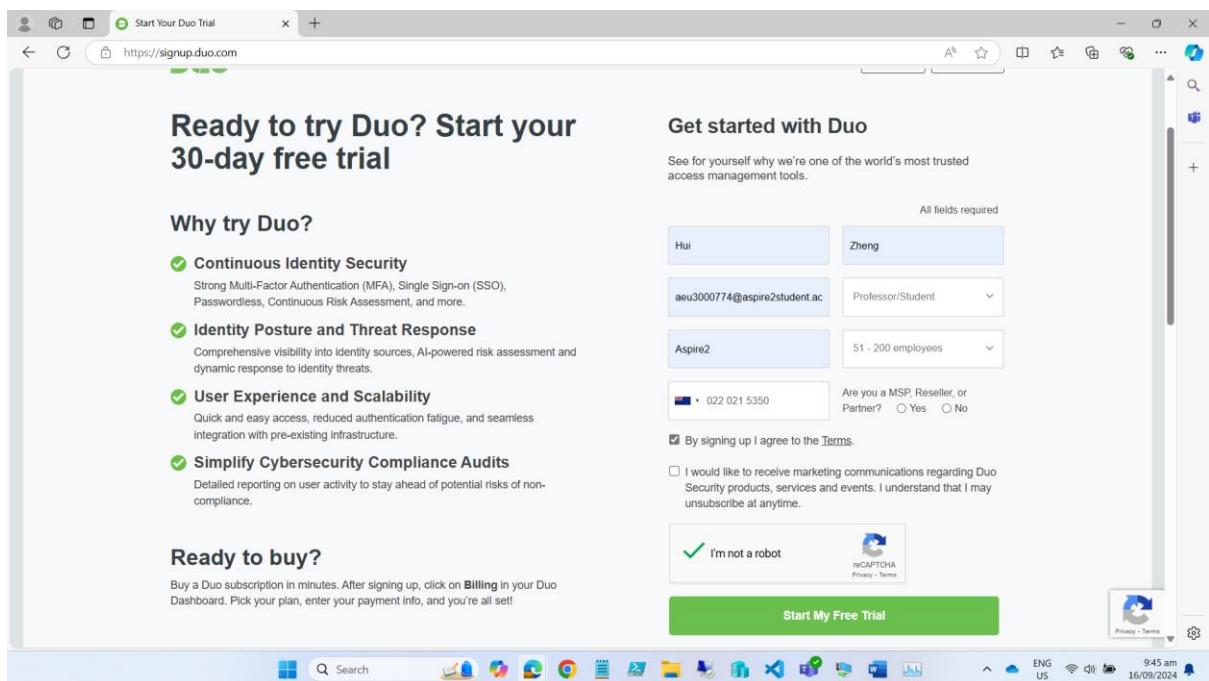


Task/Mahi 3: Implementing & Managing Multi-Factor Authentication (MFA) for Network Access

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

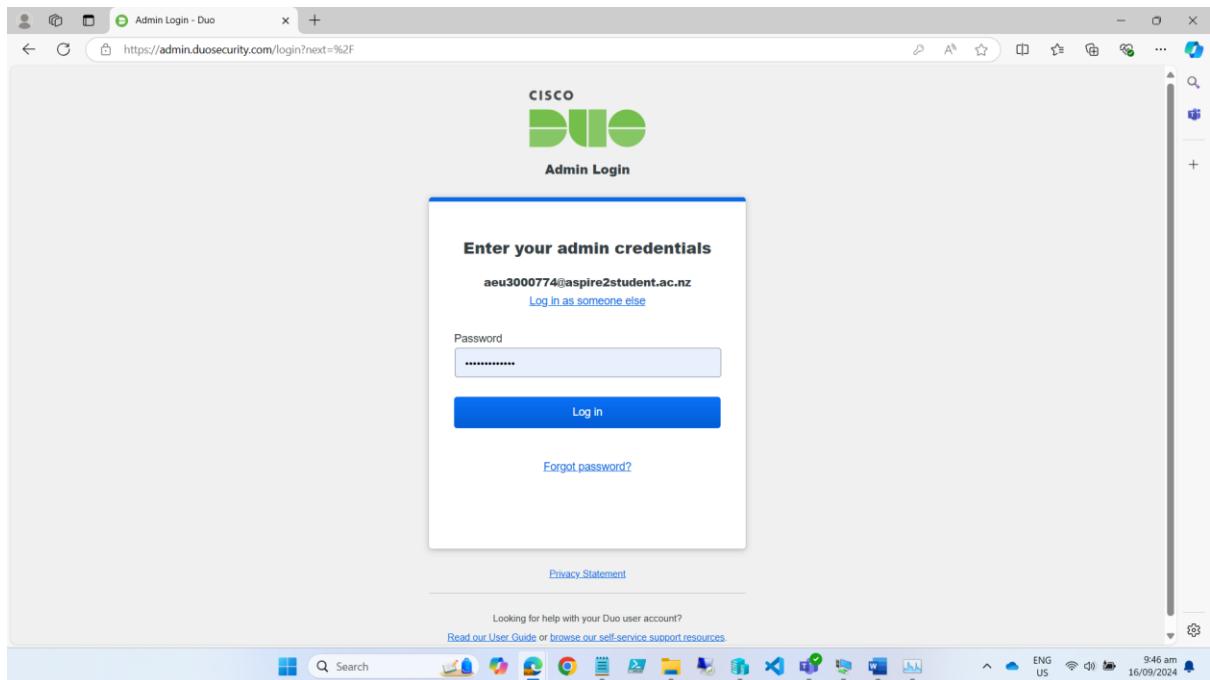


The screenshot shows a Microsoft Edge browser window with the URL <https://signup.duo.com>. The page is titled "Ready to try Duo? Start your 30-day free trial". On the left, there's a section titled "Why try Duo?" listing four benefits with green checkmarks:

- Continuous Identity Security**: Strong Multi-Factor Authentication (MFA), Single Sign-on (SSO), Passwordless, Continuous Risk Assessment, and more.
- Identity Posture and Threat Response**: Comprehensive visibility into identity sources, AI-powered risk assessment and dynamic response to identity threats.
- User Experience and Scalability**: Quick and easy access, reduced authentication fatigue, and seamless integration with pre-existing infrastructure.
- Simplify Cybersecurity Compliance Audits**: Detailed reporting on user activity to stay ahead of potential risks of non-compliance.

On the right, there's a "Get started with Duo" section with fields for first name (Hui), last name (Zheng), email (aue3000774@aspire2student.ac), and organization (Aspire2). It also includes dropdowns for "Professor/Student" and "51 - 200 employees". Below these are checkboxes for "Are you a MSP, Reseller, or Partner?" (Yes/No) and "By signing up I agree to the [Terms](#)". There's also a checkbox for marketing communications and a reCAPTCHA field. At the bottom is a large green button labeled "Start My Free Trial". The taskbar at the bottom shows various pinned icons like File Explorer, Task View, and Microsoft Edge.

2. Log in to Admin Console



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

The screenshot shows two side-by-side browser windows. Both windows are for the URL <https://admin-285fc7c7.duosecurity.com/users/DUT1U49SGCHXOHLUCUQ>.

Left Window (Initial User Creation):

- Header:** techco\user1 - Users - Aspire2 - https://admin-285fc7c7.duosecurity.com/users/DUT1U49SGCHXOHLUCUQ
- Left Sidebar (Users):** Add User, Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, Groups, Endpoints, 2FA Devices, Administrators, Trusted Endpoints.
- Right Content:**
 - Success Message:** User added successfully. [Add another.](#)
 - User Details:** Username: techco\user1, Full name: Spark Zheng, Email: aeu3000774@aspire2student.ac.nz, Status: Active.
 - Note:** This user has not enrolled yet. See our [enrollment documentation](#) to learn more about enrolling users.
 - Actions:** Logs, Send Enrollment Email, Send to Trash.

Right Window (Adding Username Aliases):

- Header:** techco\user1 - Users - Aspire2 - https://admin-285fc7c7.duosecurity.com/users/DUT1U49SGCHXOHLUCUQ
- Left Sidebar (Users):** Add User, Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, Groups, Endpoints, 2FA Devices, Administrators, Trusted Endpoints.
- Right Content:**
 - Username:** techco\user1
 - Username aliases:** + Add a username alias
 - Username alias 1: techco.co.nz\user1
 - Username alias 2: user1
 - Note:** Users can have up to 8 aliases. Optionally, you may choose to reserve using an alias number for a specific alias (e.g., Username alias 1 should only be used for Employee ID).
 - Full name:** Spark Zheng
 - Status:** Active
 - Actions:** Logs, Send Duo Push, Send to Trash.

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

The screenshot shows the Duo Applications interface. On the left, there's a sidebar with options like Dashboard, Device Insight, Policies, and Applications (which is currently selected). Under Applications, there are sub-options: Protect an Application and Authentication Proxy. The main content area is titled "Microsoft RDP". It displays three fields with their respective values and copy buttons:

- Integration key: DIO5SEIFSKJSOPUR6FM
- Secret key: bdNS18FAuPITDCCgsz59N25IA5SfwEynPqCLb5cg
- API hostname: api-285fc7c7.duosecurity.com

Below these fields is a "Policy" section with a "Group policies" button.

Integration key: DIO5SEIFSKJSOPUR6FM

Secret key: bdNS18FAuPITDCCgsz59N25IA5SfwEynPqCLb5cg

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

Server Manager

Server Manager • Dashboard

WELCOME TO SERVER MANAGER

Group Policy Management Editor

Default Domain Policy [DC.TECHICO.CO.NZ] Policy

Duo Service Settings

Select an item to view its description.

Setting State Comment

- Duo Service: Enable Smart Cards Not configured No
- Duo Service: Fail Open if Unable to Contact Duo Not configured No
- Duo Service: Duo API Hostname Not configured No
- Duo Service: HTTP Proxy Hostname Not configured No
- Duo Service: HTTP Proxy Port Not configured No
- Duo Service: Duo Integration Key Not configured No
- Duo Service: Log File Max Count Not configured No
- Duo Service: Log File Max Size MB Not configured No
- Duo Service: Duo Secret Key Not configured No
- Duo Service: Specify format of username sent to Duo service Not configured No
- Duo Service: Wrap Smart Cards Not configured No

Print Services 1 Local Server 1 All Servers 1

Type here to search

Duo Service: Duo API Hostname

Duo Service: Duo API Hostname

Previous Setting Next Setting

Not Configured Comment:

Enabled

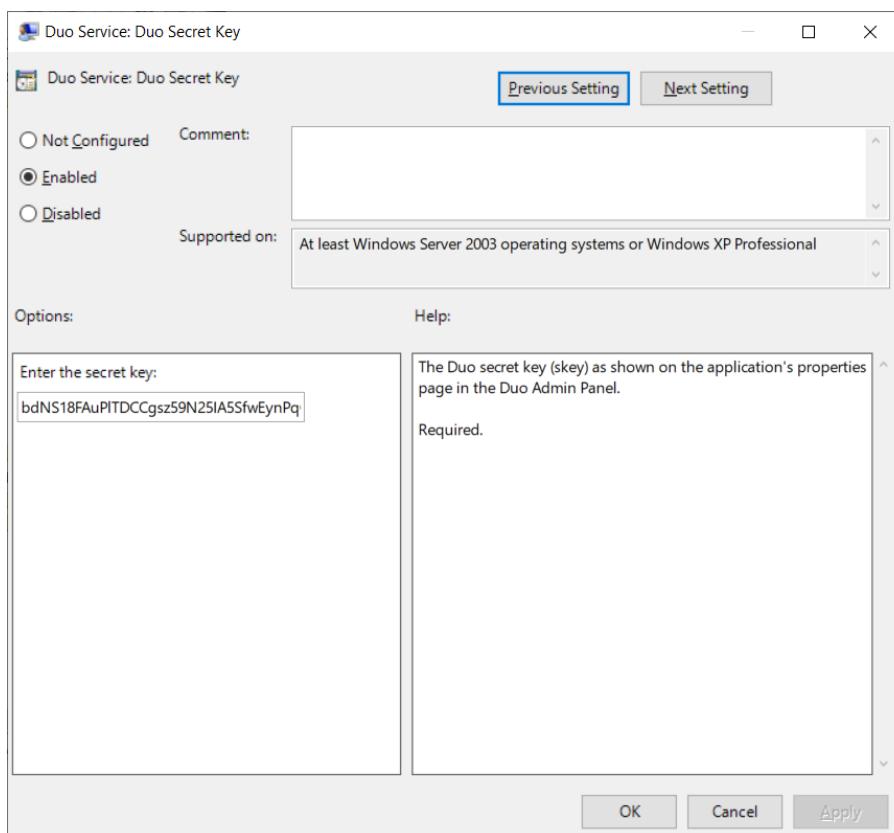
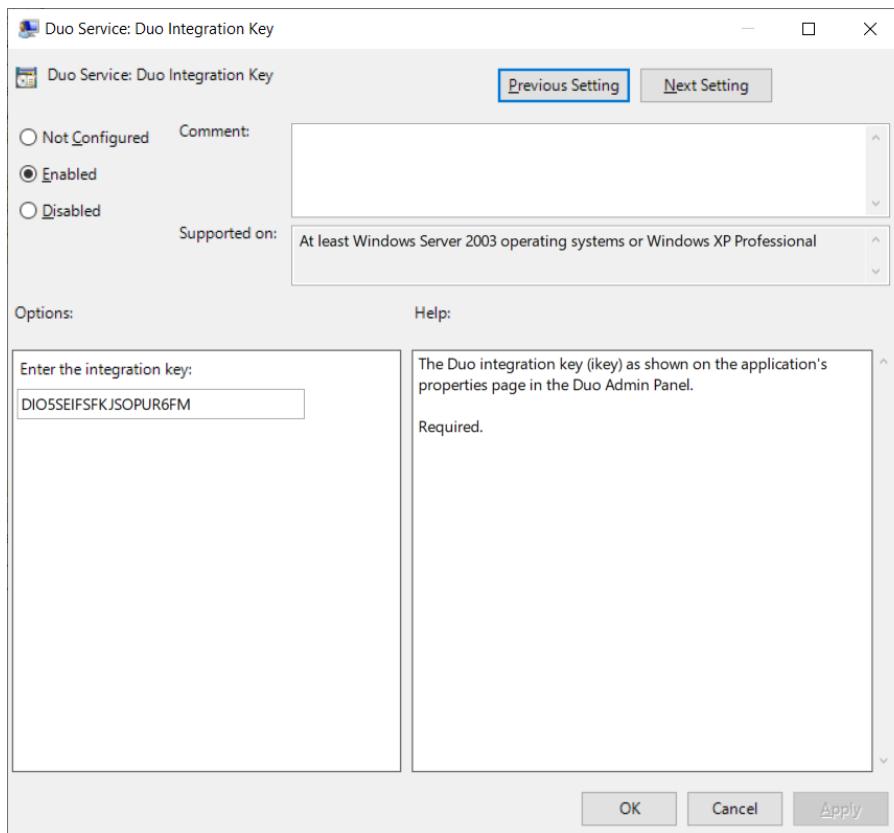
Disabled Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options: Enter the Duo API Hostname: api-285fc7c7.duosecurity.com

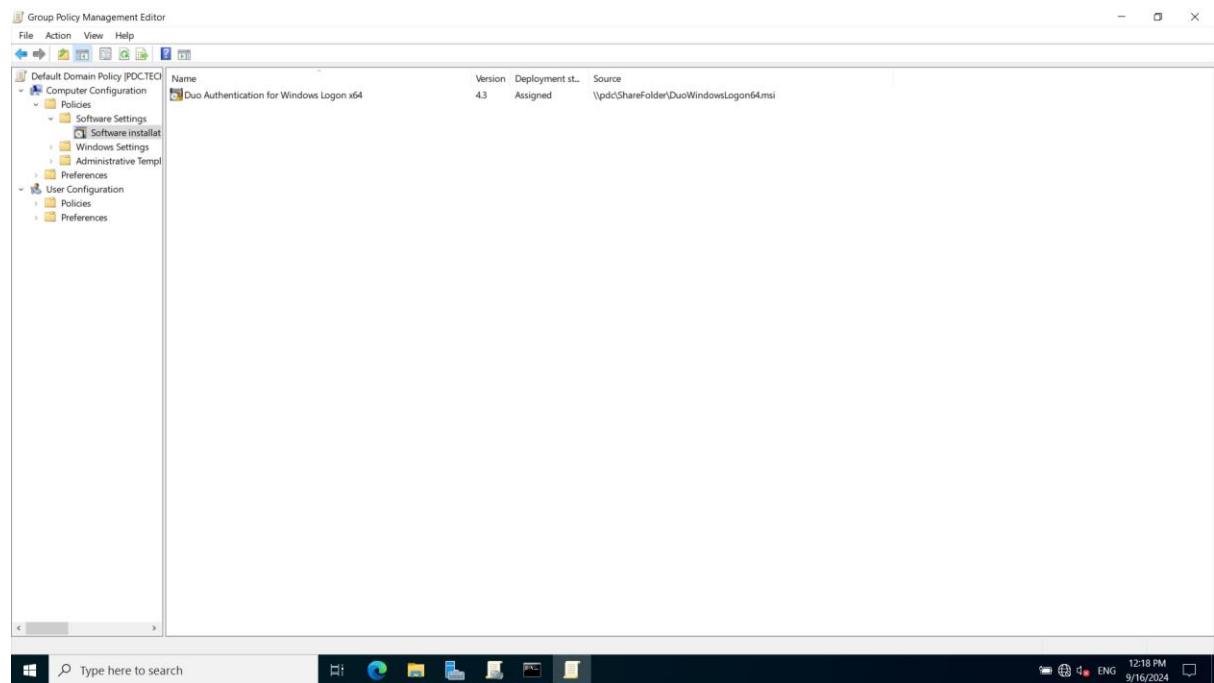
The DNS name of the Duo API host as shown on the application's properties page in the Duo Admin Panel.

Required.

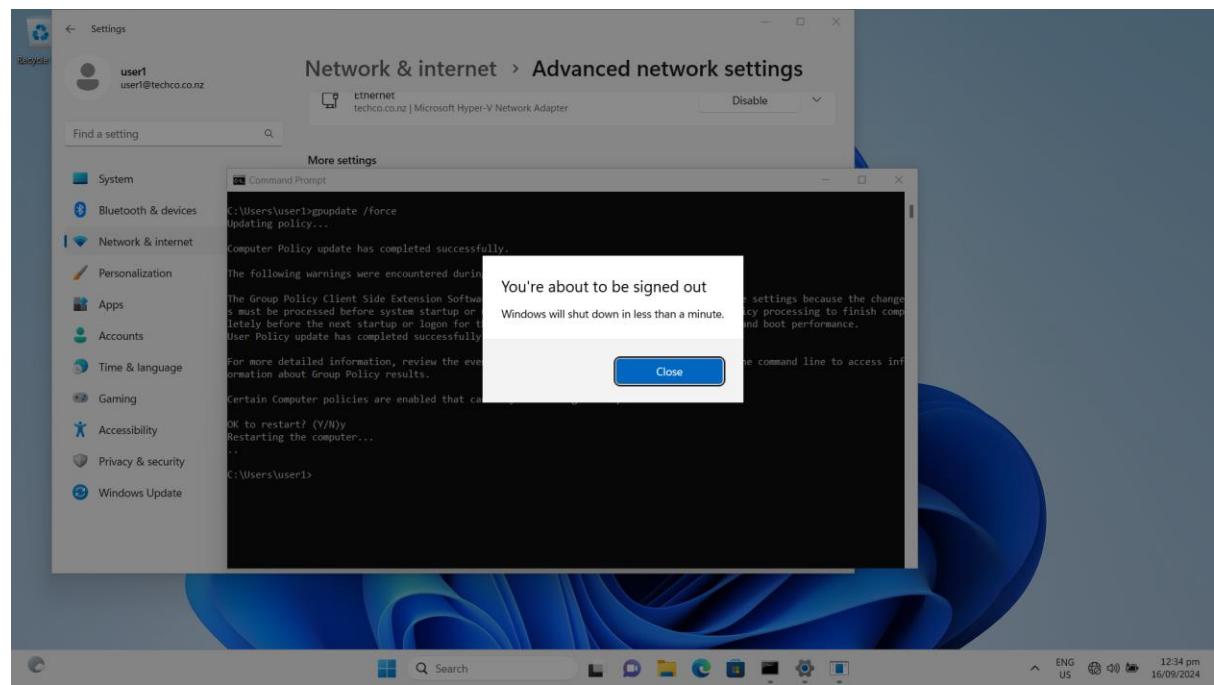
OK Cancel Apply

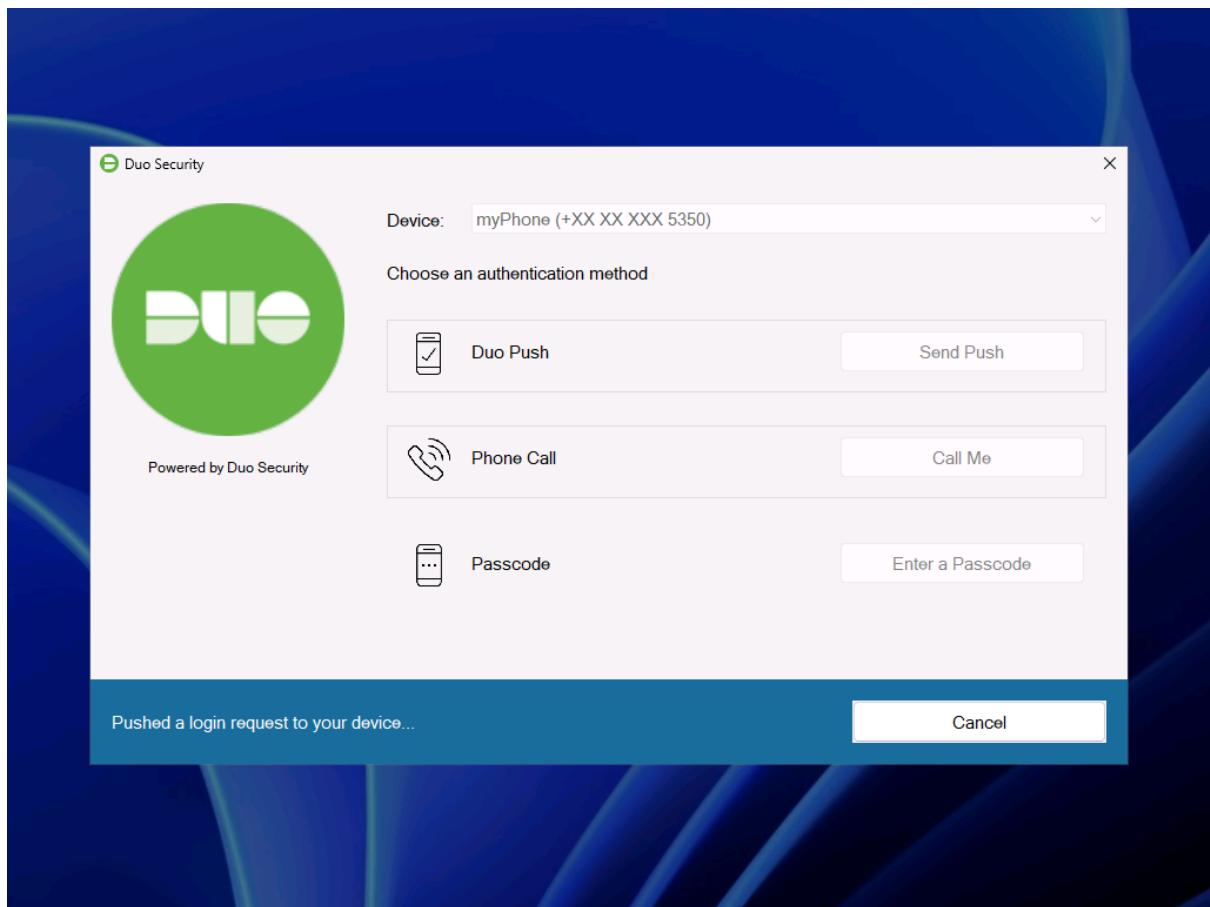


8. Add new Software installation to the GPO policy



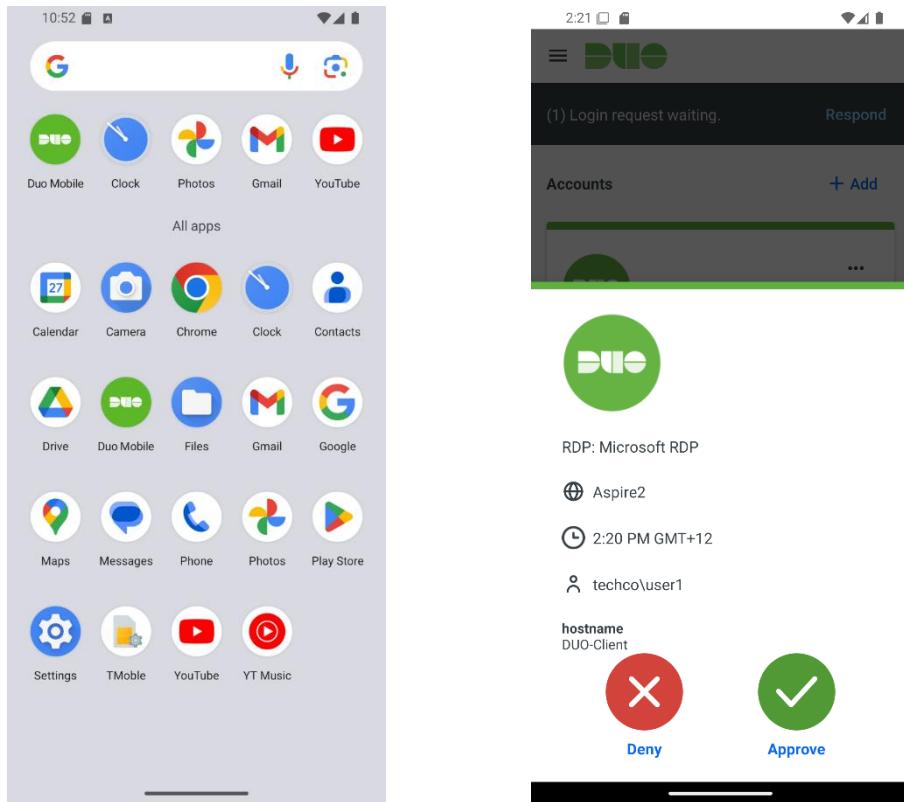
9. Login on Client machine and update group policy



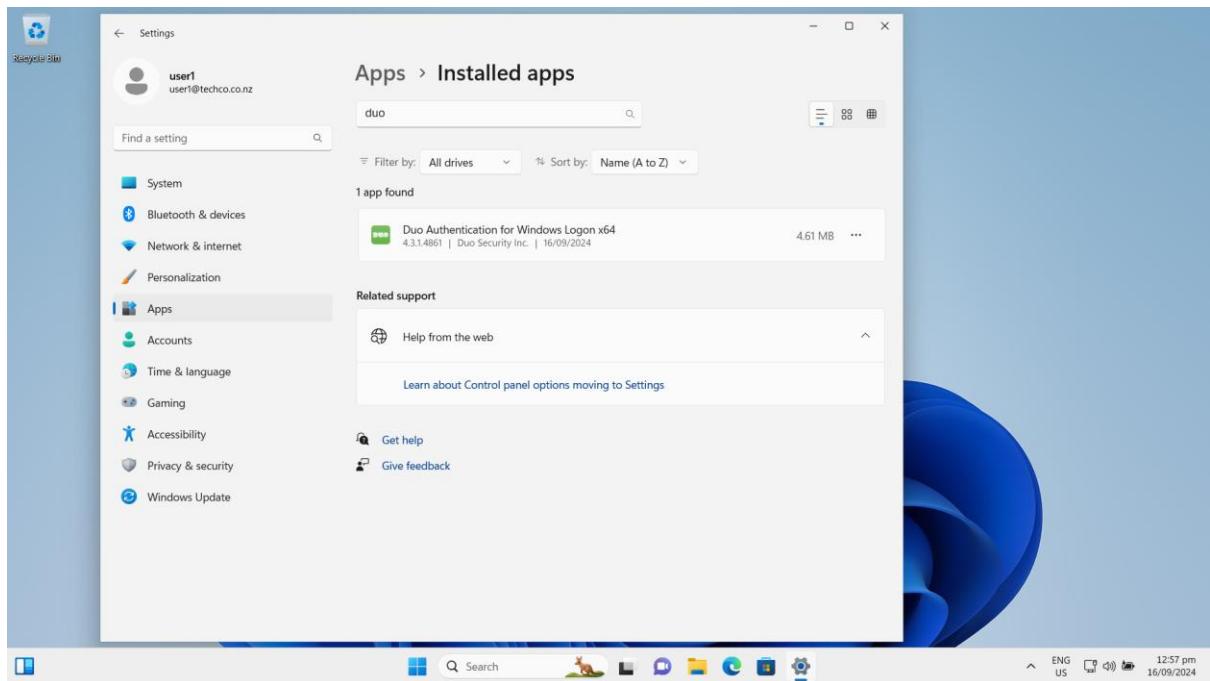
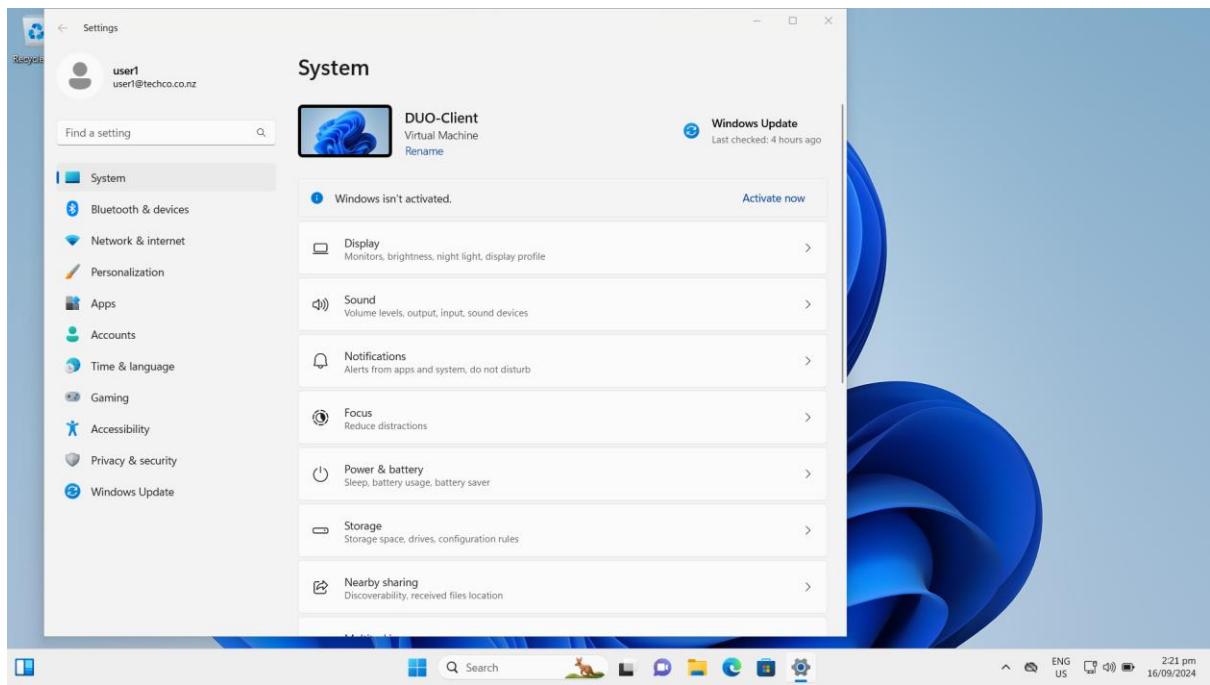


10. Active mobile phone and approve the client login request

- copy and paste active link into Duo Mobile manually:
<https://m-285fc7c7.duosecurity.com/activate/83nFnX6BN7Aj7pBIOMAw>

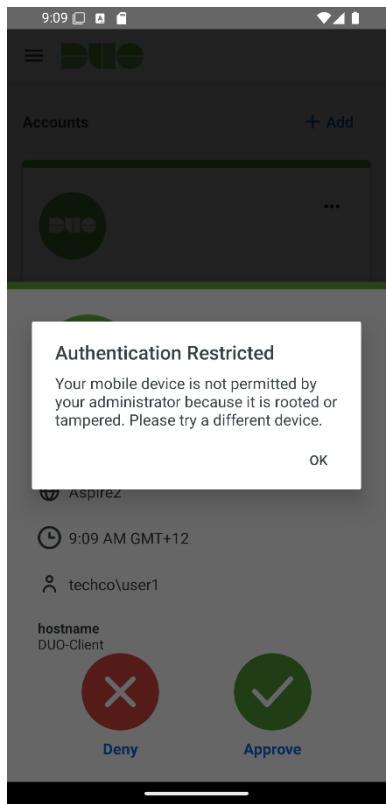


11. Client machine logged in with DUO app installed.

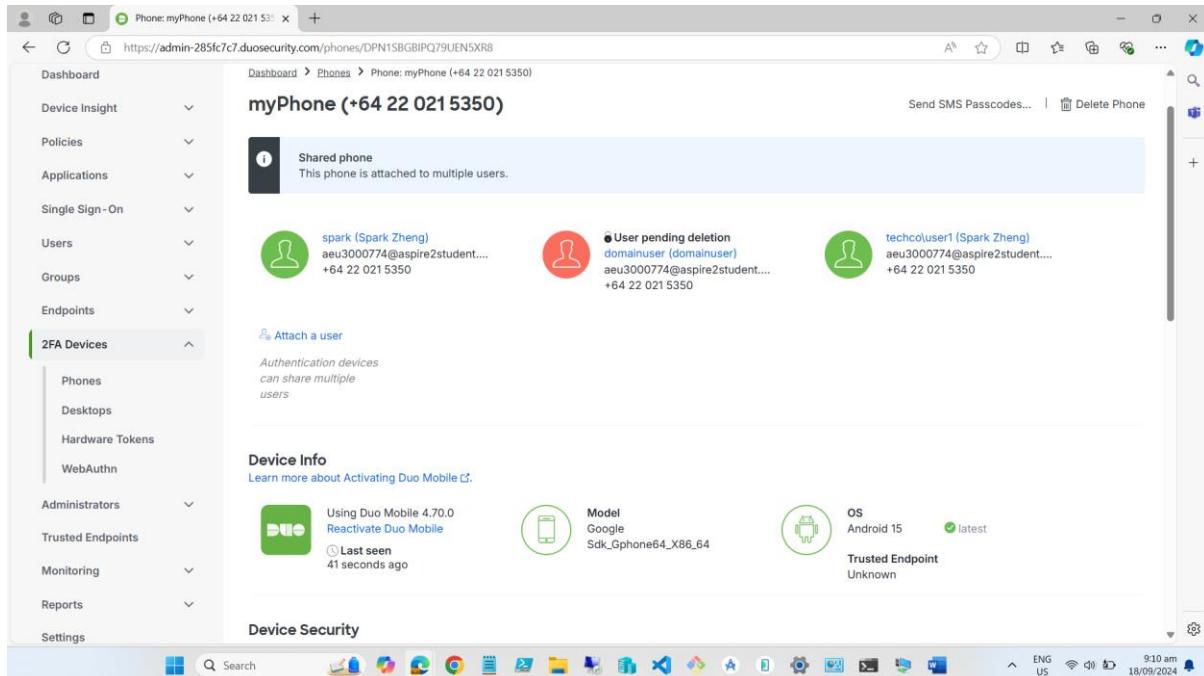


Task 3.2 Troubleshooting the MFA configurations on a client machine and MFA Admin App

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



2. Reactivate the mobile device and send notification email



The screenshot shows the Duo Device Management interface for a phone labeled "myPhone (+64 22 021 5350)". It is identified as a "Shared phone" attached to multiple users:

- spark (Spark Zheng)**: aeu3000774@aspire2student.... +64 22 021 5350
- User pending deletion**: domainuser (domainuser) aeu3000774@aspire2student.... +64 22 021 5350
- techcoluser1 (Spark Zheng)**: aeu3000774@aspire2student.... +64 22 021 5350

Device Info section details:

- Using Duo Mobile 4.70.0
- Reactivate Duo Mobile
- Last seen: 41 seconds ago
- Model: Google Sdk_Gphone64_X86_64
- OS: Android 15
- Trusted Endpoint: Unknown

Activate Duo Mobile form:

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone: myPhone (+64 22 021 5350)

Expiration: 24 hours after generation

Generate Duo Mobile Activation Code

© 2024 Duo Security. All rights reserved. Terms of service

The screenshot shows a Microsoft Edge browser window with the URL https://admin-285fc7c7.duosecurity.com/phones/DPN1S1GBIPQ79UEN5XK8/regen_mobile. The page title is "Activate Duo Mobile". The left sidebar shows navigation options like Dashboard, Device Insight, Policies, Applications, Single Sign-On, Users, Groups, Endpoints, and 2FA Devices. Under 2FA Devices, "Phones" is selected. The main content area shows a "Phone" entry for "myPhone (+64 22 021 5350)". Below it, there's a "Send links via" section with "Email" selected (radio button is blue). An email input field contains "aeu3000774@aspire2student.ac.nz". A "Customize Email" section includes a note about saving the email for next time and a "Revert to default" link. A "Logo" section shows a green circular logo with the word "Duo". The bottom of the screen shows the Windows taskbar with various pinned icons.

The screenshot shows an email titled "Duo Mobile Activation". The body of the email contains the following text:

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

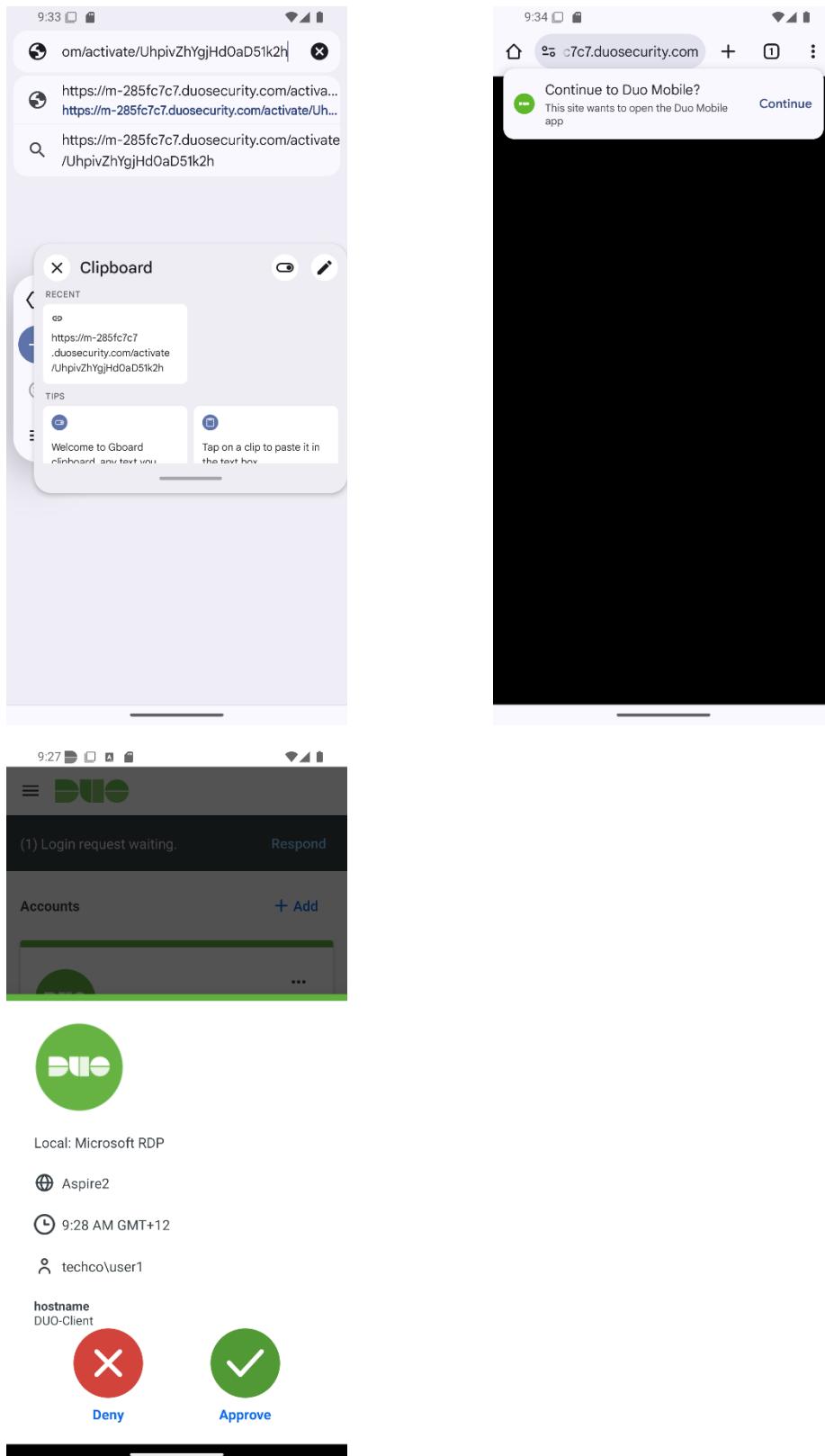
Just tap this link from +64 22 021 5350, or copy and paste it into Duo Mobile manually:

<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:

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

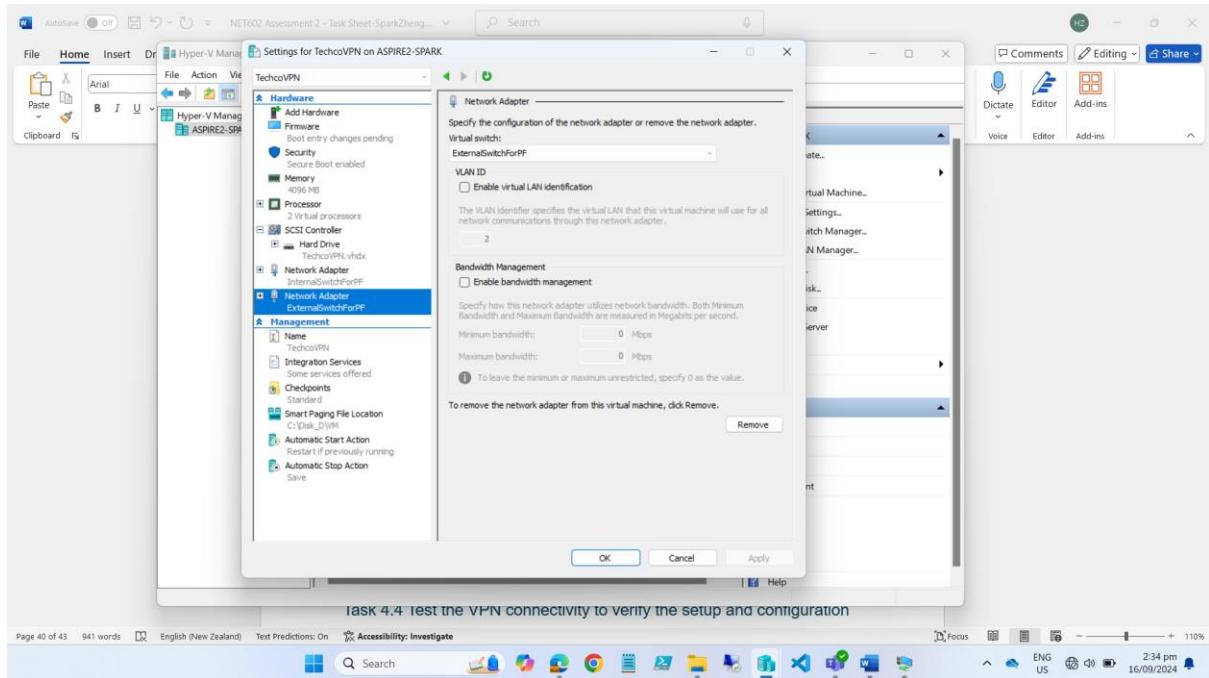
3. Access reactivating link on the mobile device and the issue is resolved.



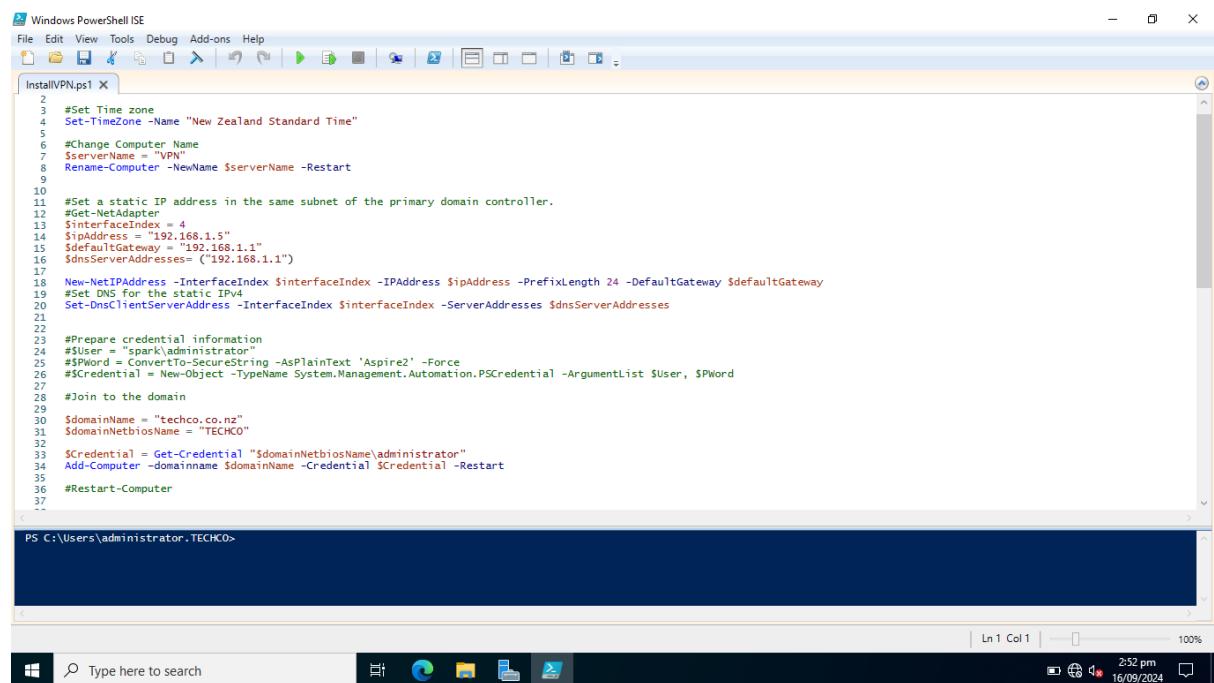
Task/Mahi 4: Manage the remote access via VPN

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



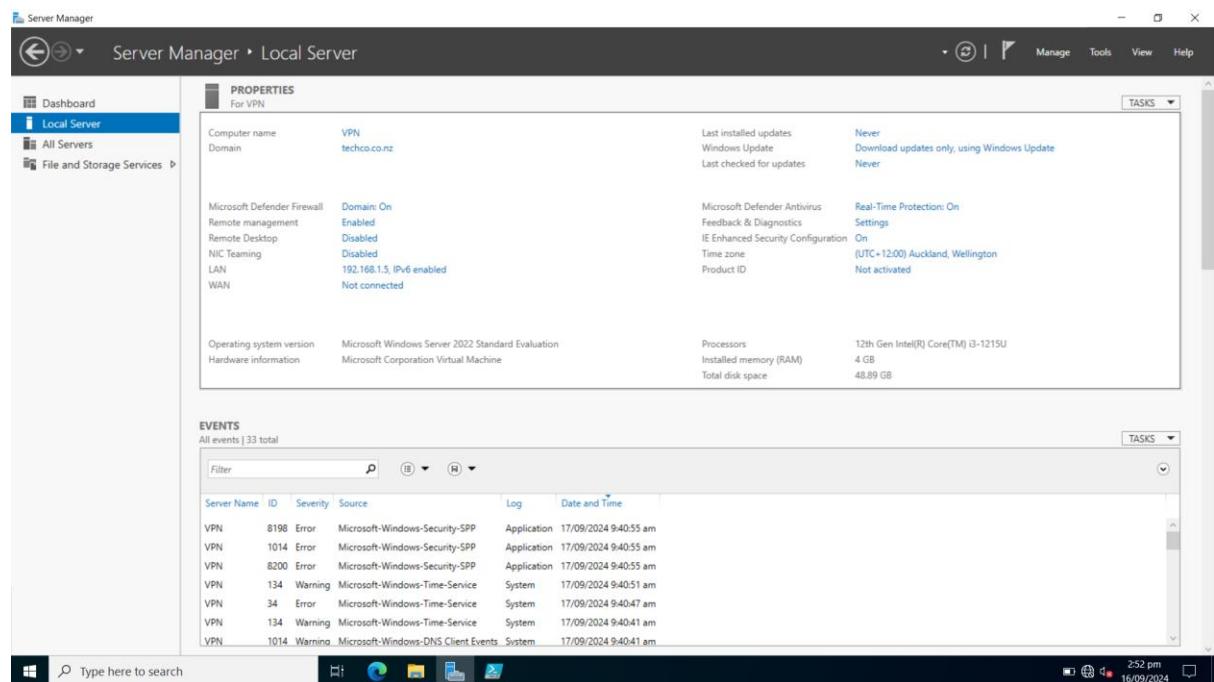
2. Add the new virtual machine to domain "techco.co.nz"



```

Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
InstallVPN.ps1 X
1 #Set Time zone
2 Set-TimeZone -Name "New Zealand Standard Time"
3
4 #Change Computer Name
5 $serverName = "VPN"
6 Rename-Computer -NewName $serverName -Restart
7
8
9
10
11 #Set a static IP address in the same subnet of the primary domain controller.
12 $InterfaceIndex = 4
13 $ipAddress = "192.168.1.5"
14 $defaultGateway = "192.168.1.1"
15 $dnsServerAddresses = ("192.168.1.1")
16
17 New-NetIPAddress -InterfaceIndex $interfaceIndex -IPAddress $ipAddress -PrefixLength 24 -DefaultGateway $defaultGateway
18 #Set DNS for the static IPv4
19 Set-DnsClientServerAddress -InterfaceIndex $interfaceIndex -ServerAddresses $dnsServerAddresses
20
21
22 #Prepare credential information
23 $user = "spark\administrator"
24 $password = ConvertTo-SecureString -AsPlainText 'Aspire2' -Force
25 $credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $user, $password
26
27 #Join to the domain
28
29 $domainName = "techco.co.nz"
30 $domainNetbiosName = "TECHCO"
31
32 $credential = Get-Credential "$domainNetbiosName\administrator"
33 Add-Computer -domainname $domainName -Credential $credential -Restart
34
35
36 #Restart Computer
37
PS C:\Users\administrator.TECHCO>

```



PROPERTIES

For VPN		LAST INSTALLED UPDATES	
Computer name	VPN	Last installed updates	Never
Domain	techco.co.nz	Windows Update	Download updates only, using Windows Update
		Last checked for updates	Never

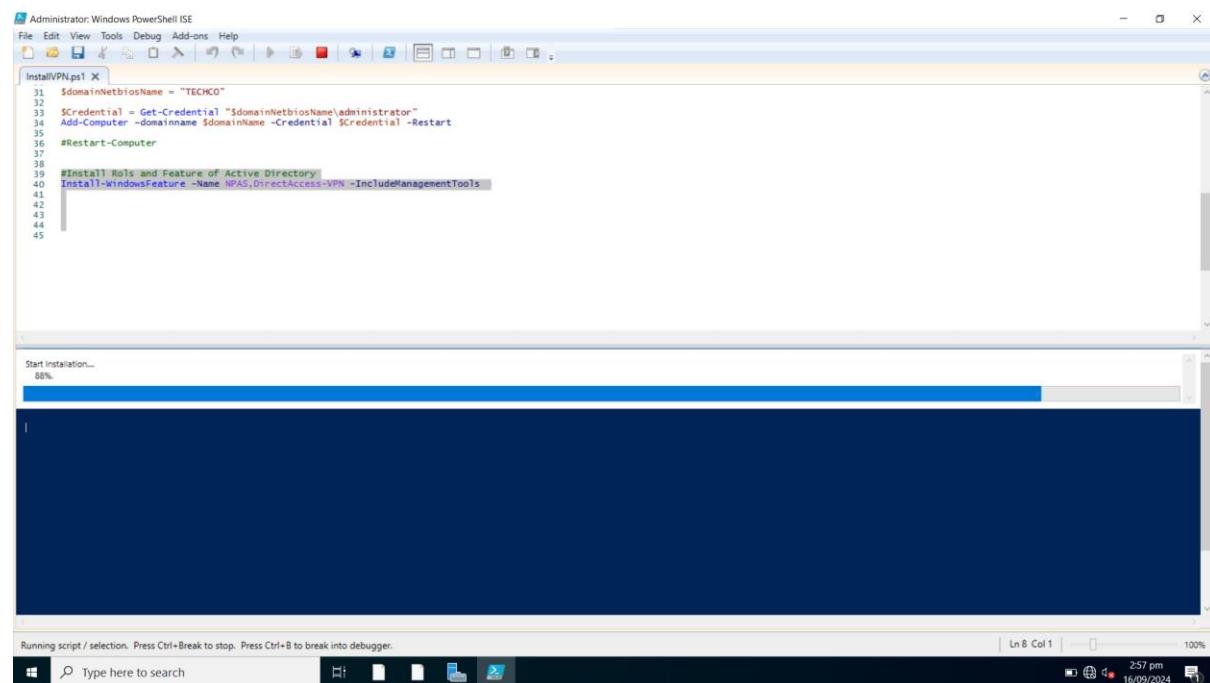
MICROSOFT DEFENDER FIREWALL		MICROSOFT DEFENDER ANTIVIRUS	
Domain	On	Real-Time Protection	On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC+12:00) Auckland, Wellington
LAN	192.168.1.5, IPv6 enabled	Product ID	Not activated
WAN	Not connected		

OPERATING SYSTEM VERSION		PROCESSORS	
Operating system version	Microsoft Windows Server 2022 Standard Evaluation	Processors	12th Gen Intel(R) Core(TM) i3-1215U
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	4 GB
		Total disk space	48.89 GB

EVENTS

All events 33 total						
Server Name	ID	Severity	Source	Log	Date and Time	
VPN	8198	Error	Microsoft-Windows-Security-SPP	Application	17/09/2024 9:40:55 am	
VPN	1014	Error	Microsoft-Windows-Security-SPP	Application	17/09/2024 9:40:55 am	
VPN	8200	Error	Microsoft-Windows-Security-SPP	Application	17/09/2024 9:40:55 am	
VPN	134	Warning	Microsoft-Windows-Time-Service	System	17/09/2024 9:40:51 am	
VPN	34	Error	Microsoft-Windows-Time-Service	System	17/09/2024 9:40:47 am	
VPN	134	Warning	Microsoft-Windows-Time-Service	System	17/09/2024 9:40:41 am	
VPN	1014	Warning	Microsoft-Windows-DNS Client Events	System	17/09/2024 9:40:41 am	

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

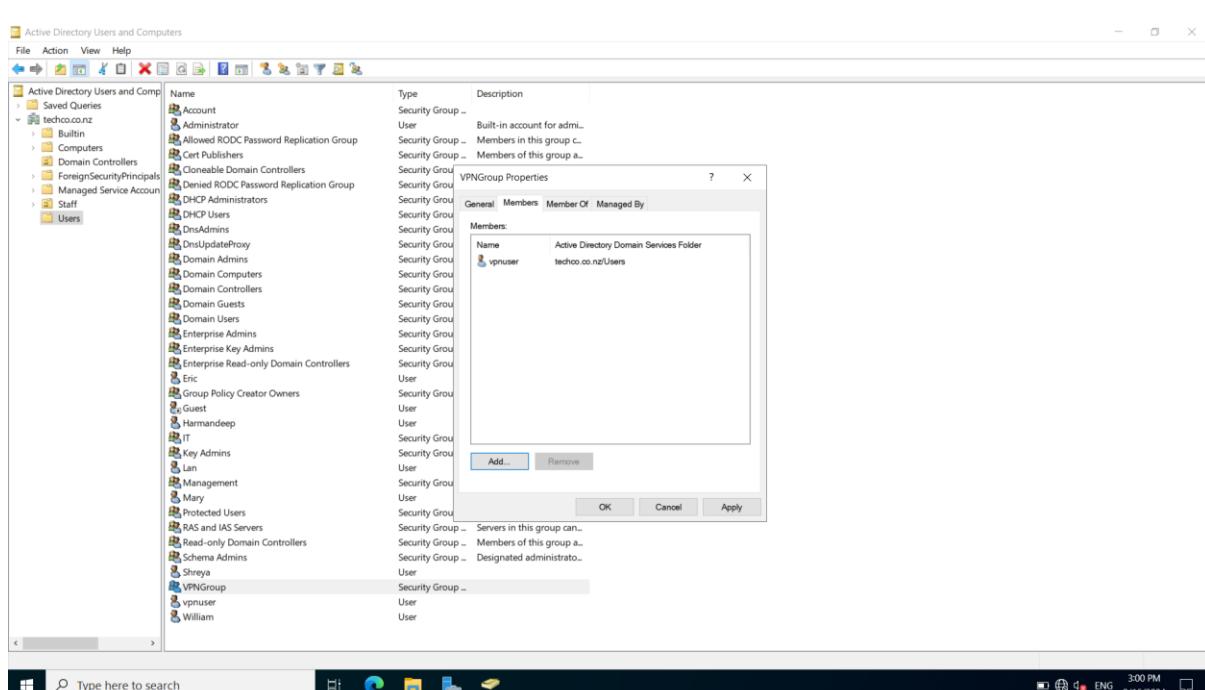
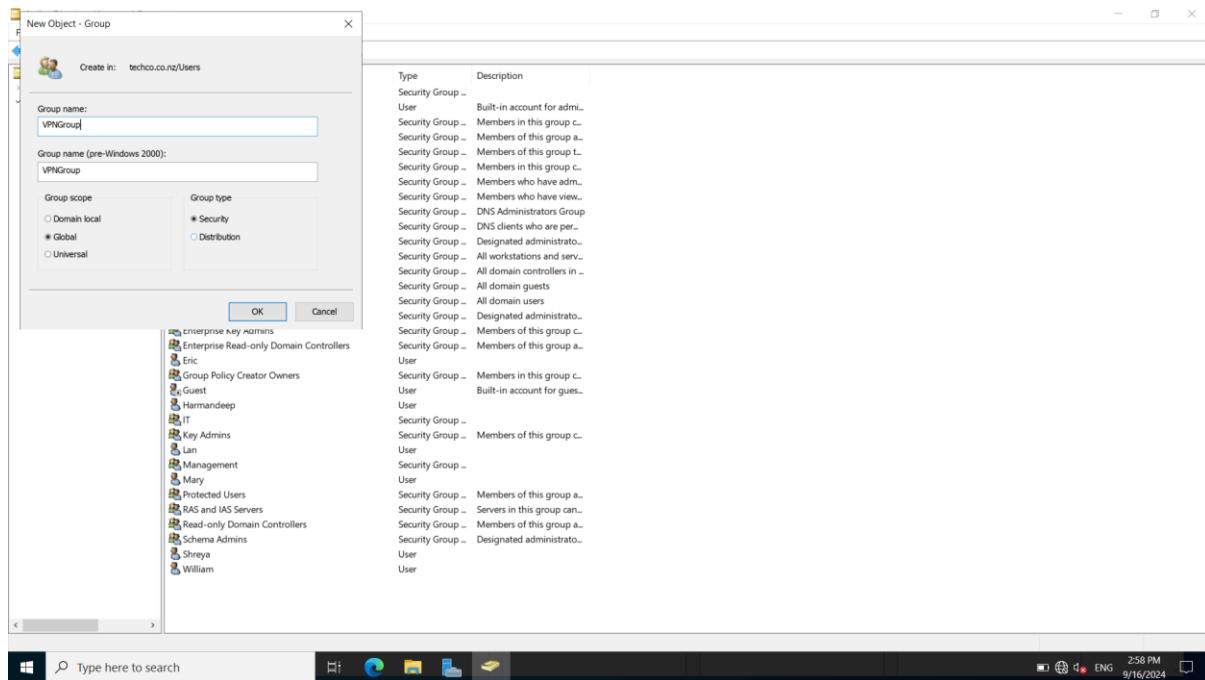


The screenshot shows a Windows PowerShell ISE window titled "Administrator: Windows PowerShell ISE". The script file is named "InstallVPN.ps1". The code in the script is as follows:

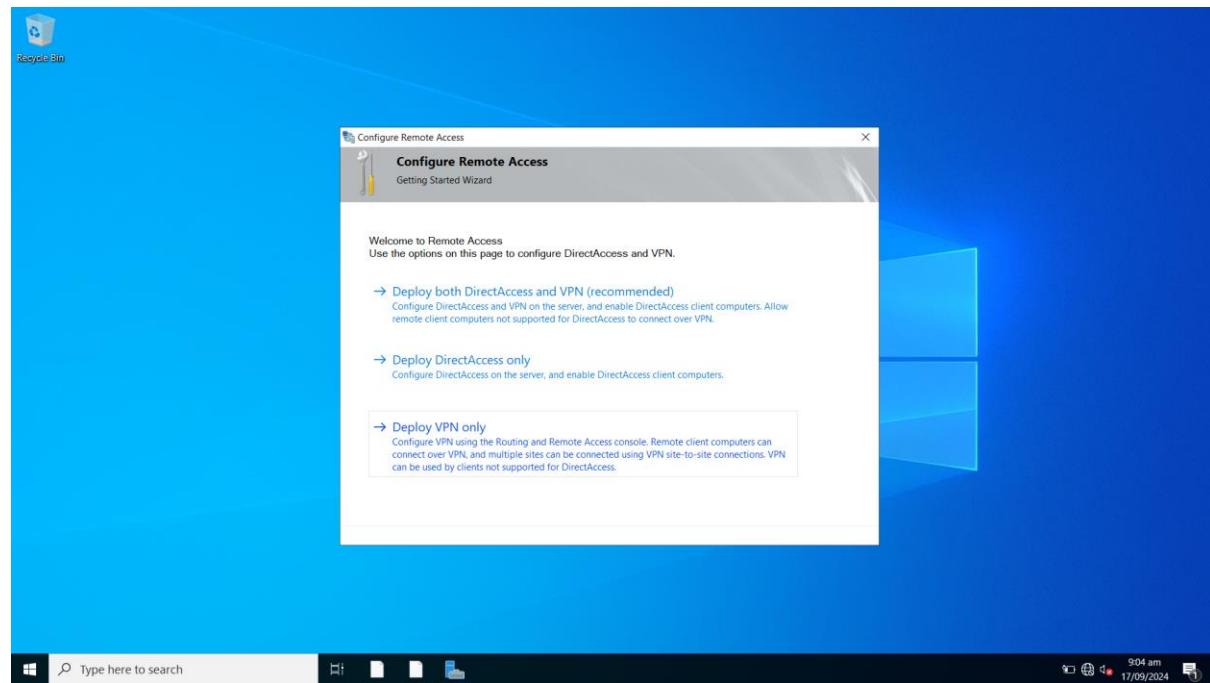
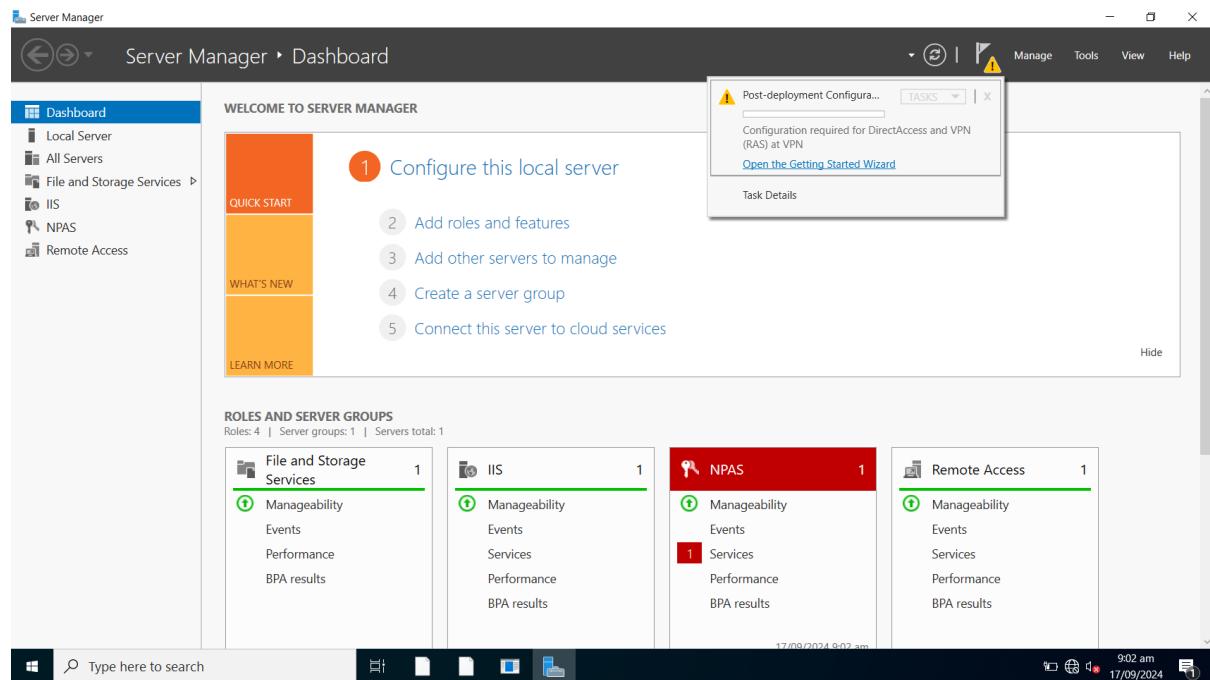
```
31 $domainNetbiosName = "TECHCO"
32 $Credential = Get-Credential "$domainNetbiosName\administrator"
33 Add-Computer -domainname $domainName -Credential $Credential -Restart
34 #Restart-Computer
35
36 #Install Rols and Feature of Active Directory
37 Install-WindowsFeature -Name NPAS,DirectAccess-VPN -IncludeManagementTools
38
39 Start Installation...
40
41
42
43
44
45
```

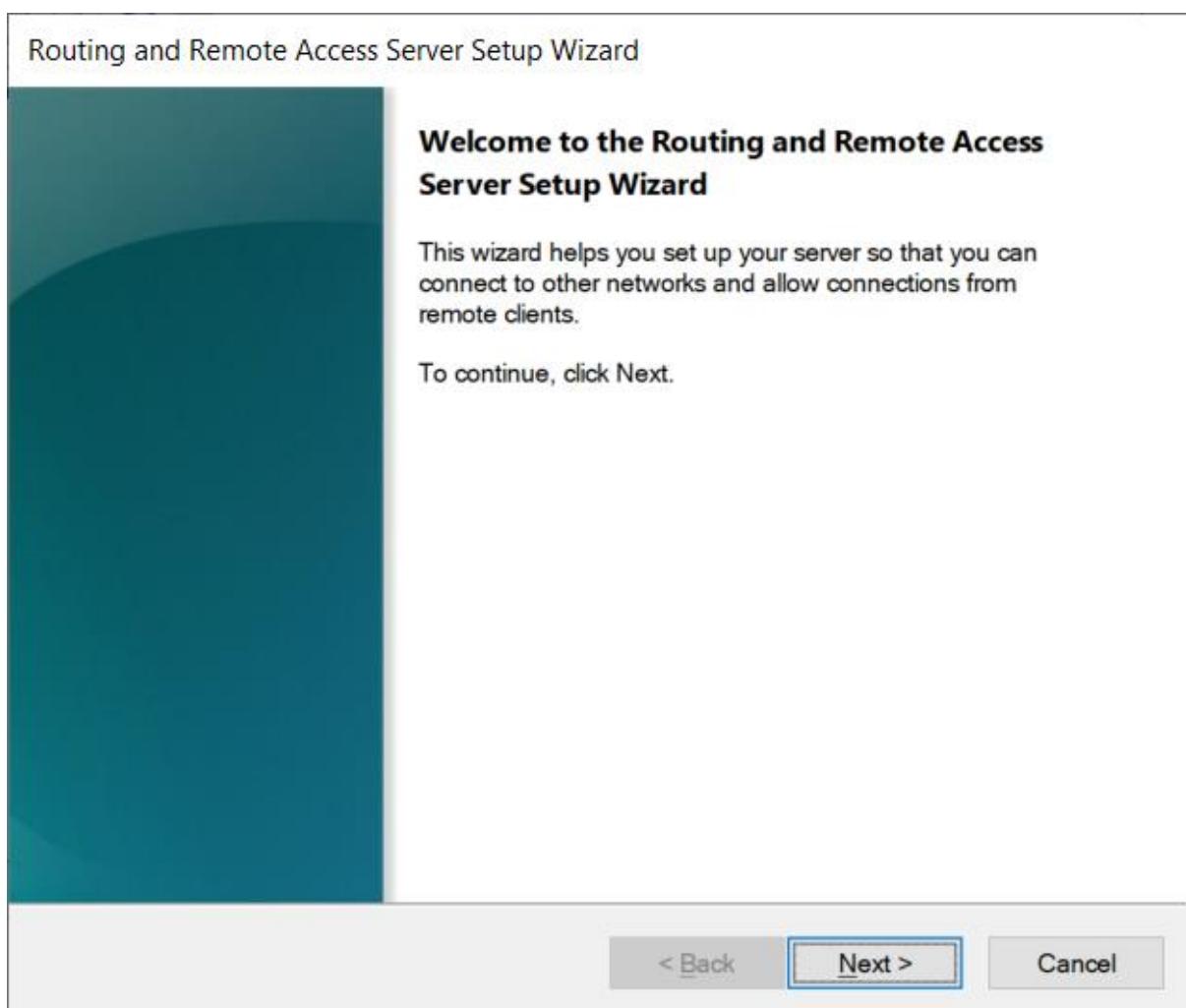
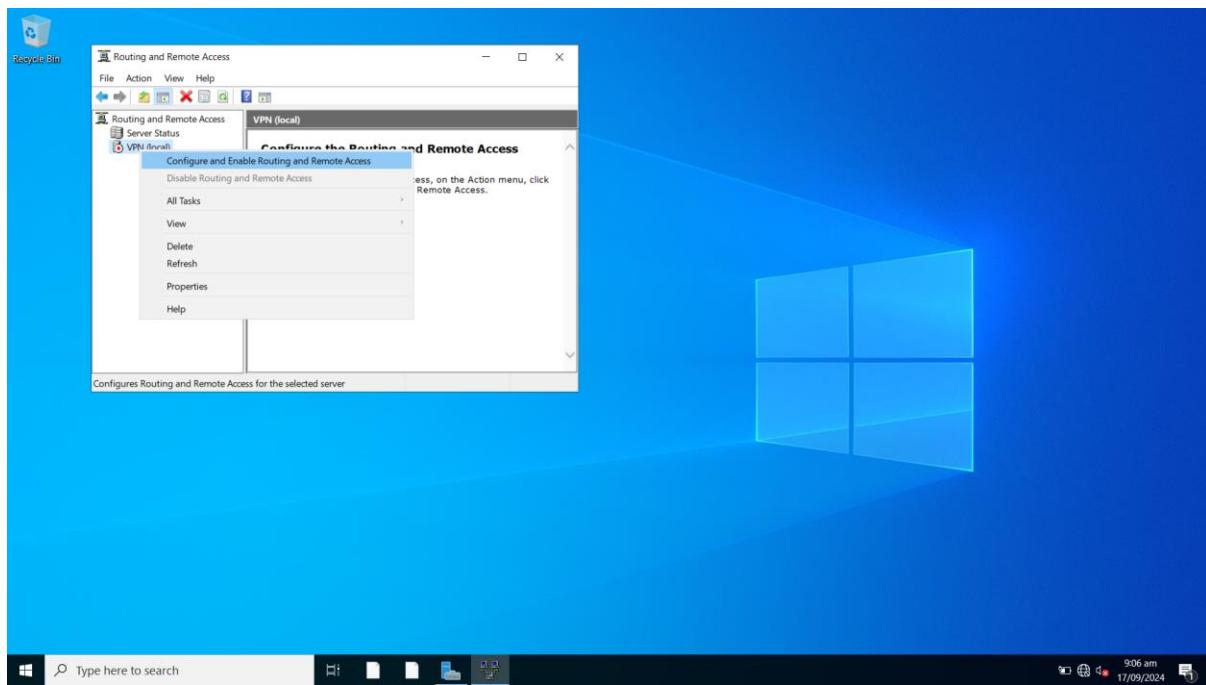
The status bar at the bottom of the window indicates "Start Installation..." and "88%". The bottom right corner shows the date and time as "16/09/2024" and "2:57 pm".

4. Create new VPN group and VPN users

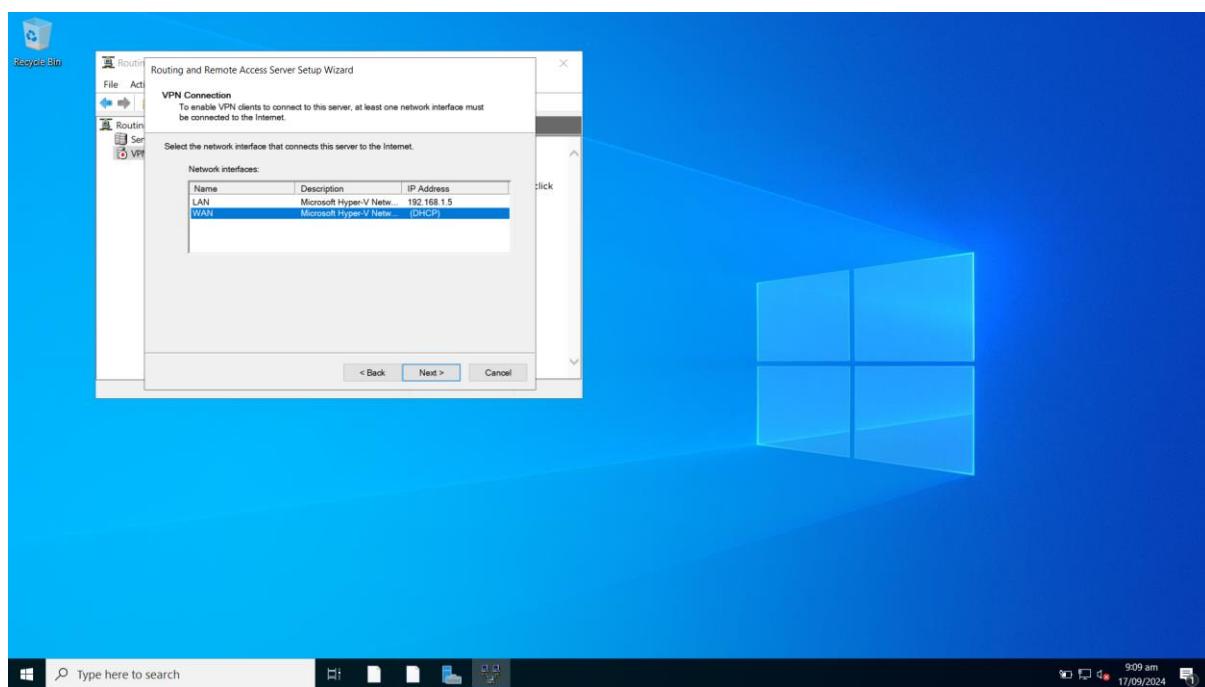
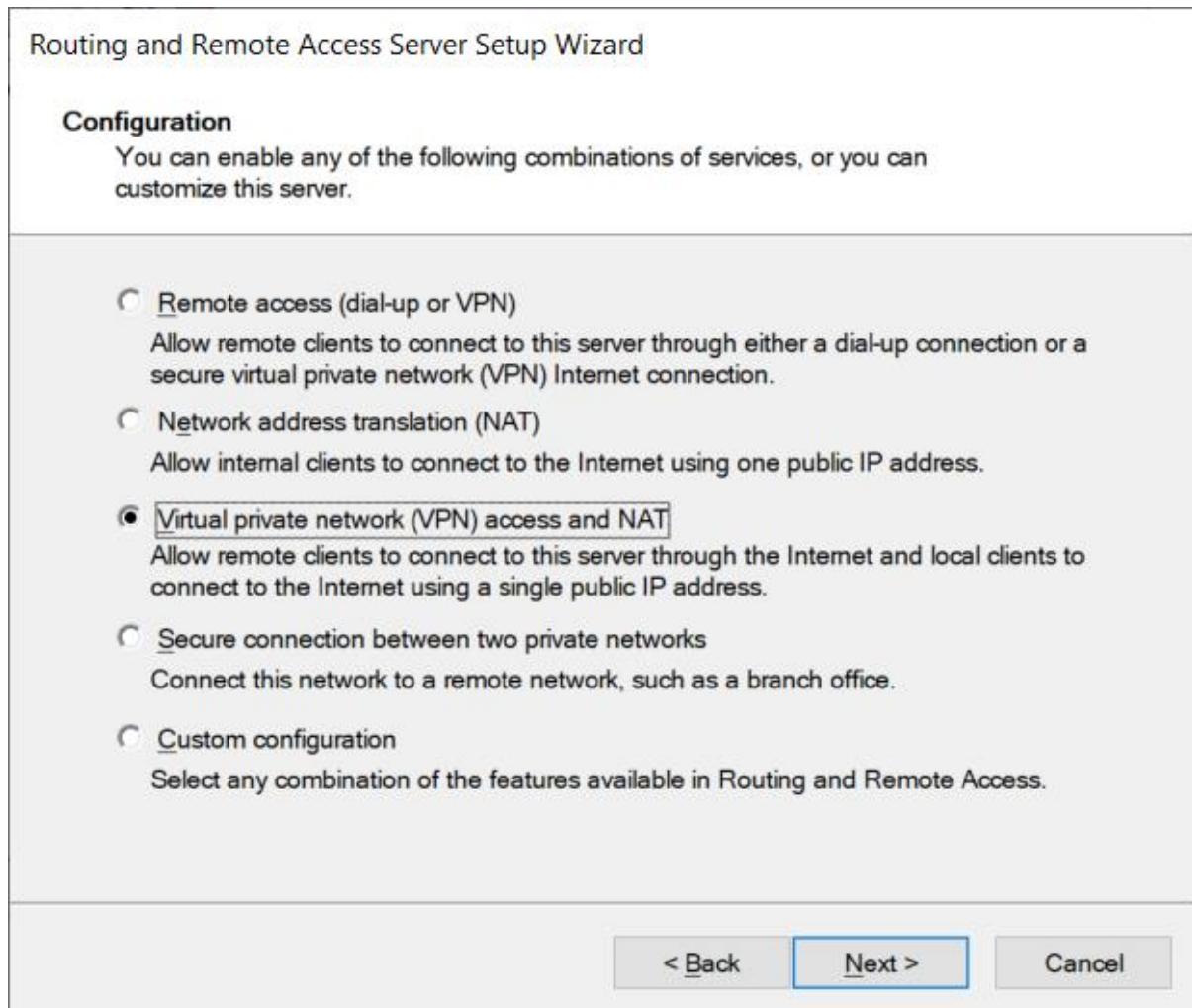


5. Configure DirectAccess and VPN





Choose Virtual Private Network(VPN) access and NAT.



Routing and Remote Access Server Setup Wizard

IP Address Assignment

You can select the method for assigning IP addresses to remote clients.

How do you want IP addresses to be assigned to remote clients?

Automatically

If you use a DHCP server to assign addresses, confirm that it is configured properly.
If you do not use a DHCP server, this server will generate the addresses.

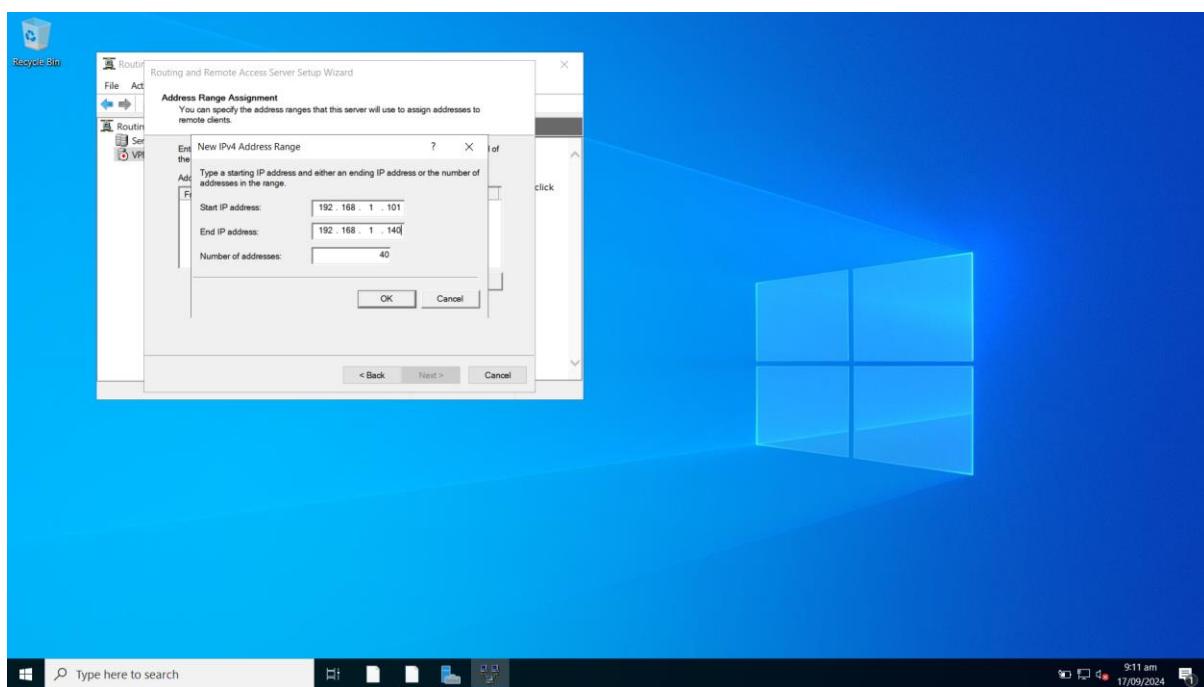
From a specified range of addresses

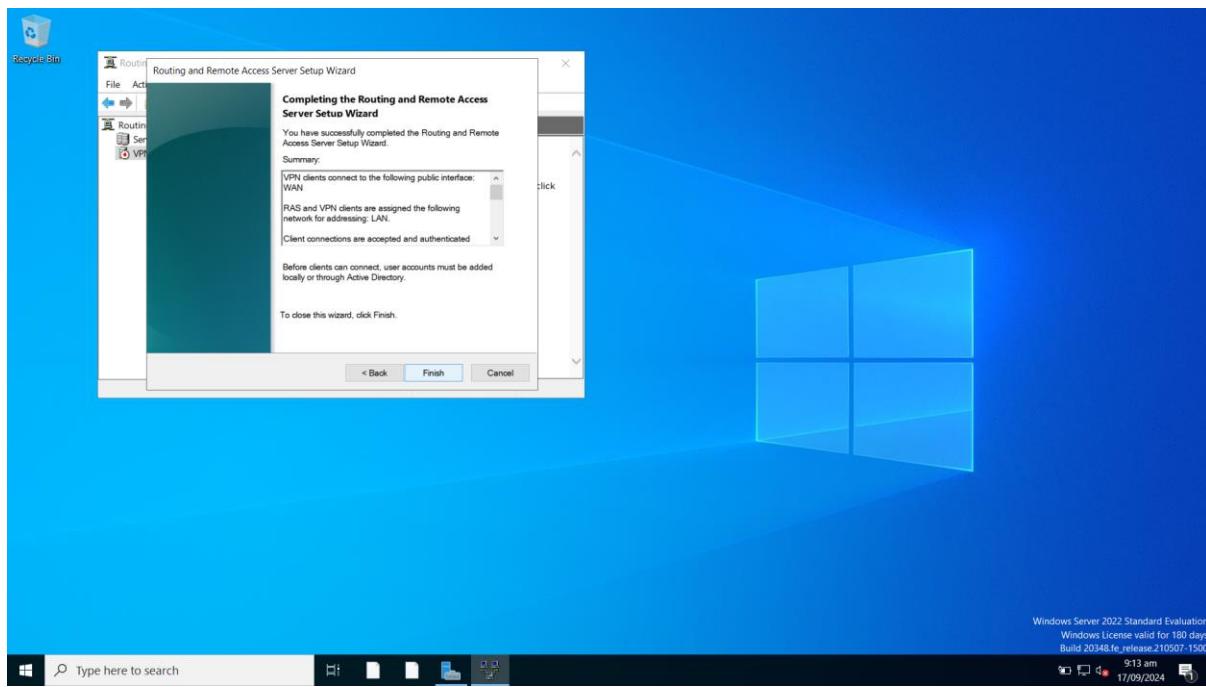
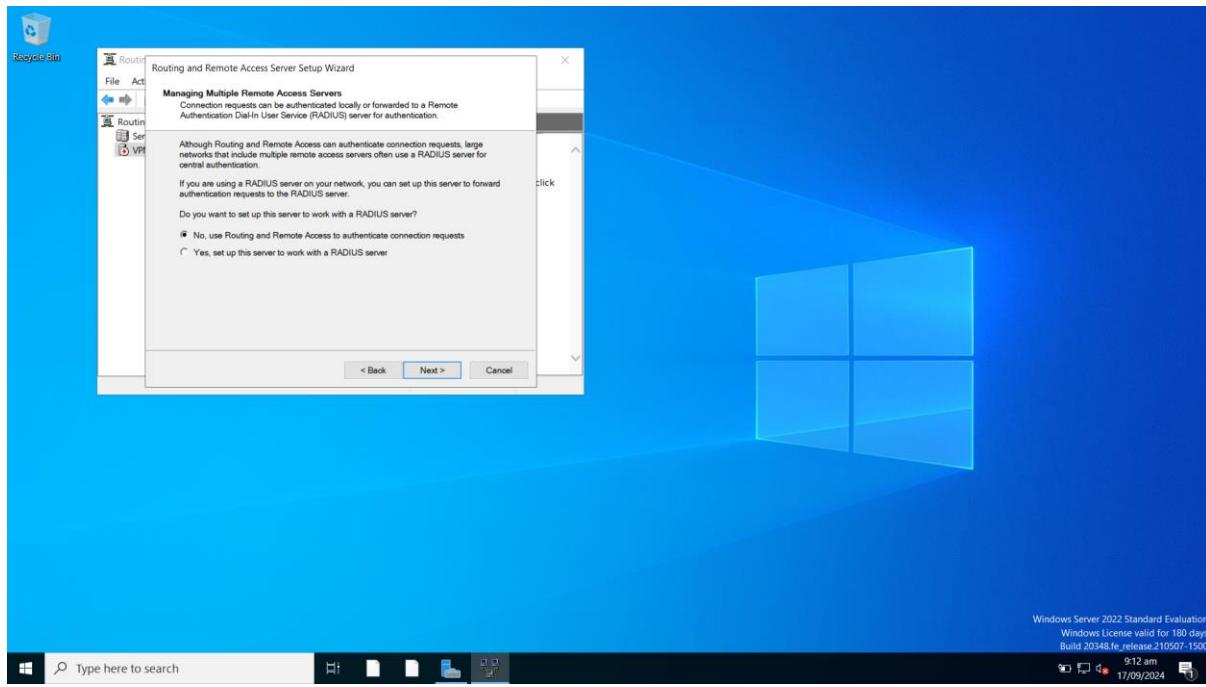
< Back

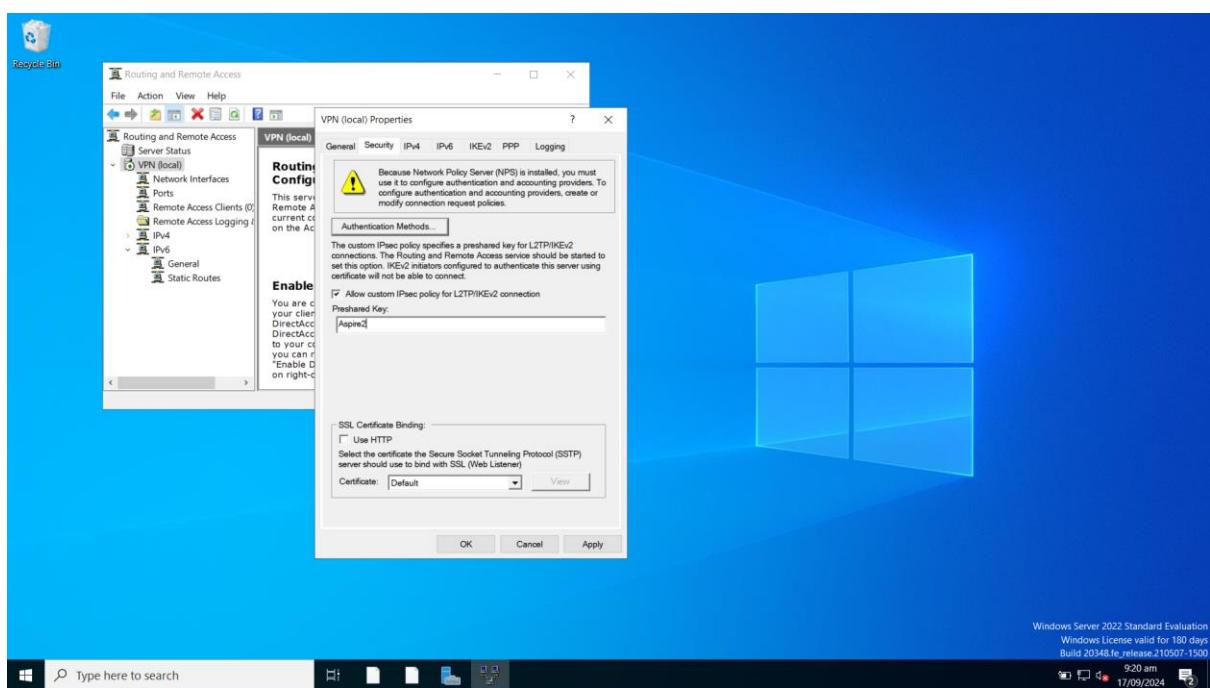
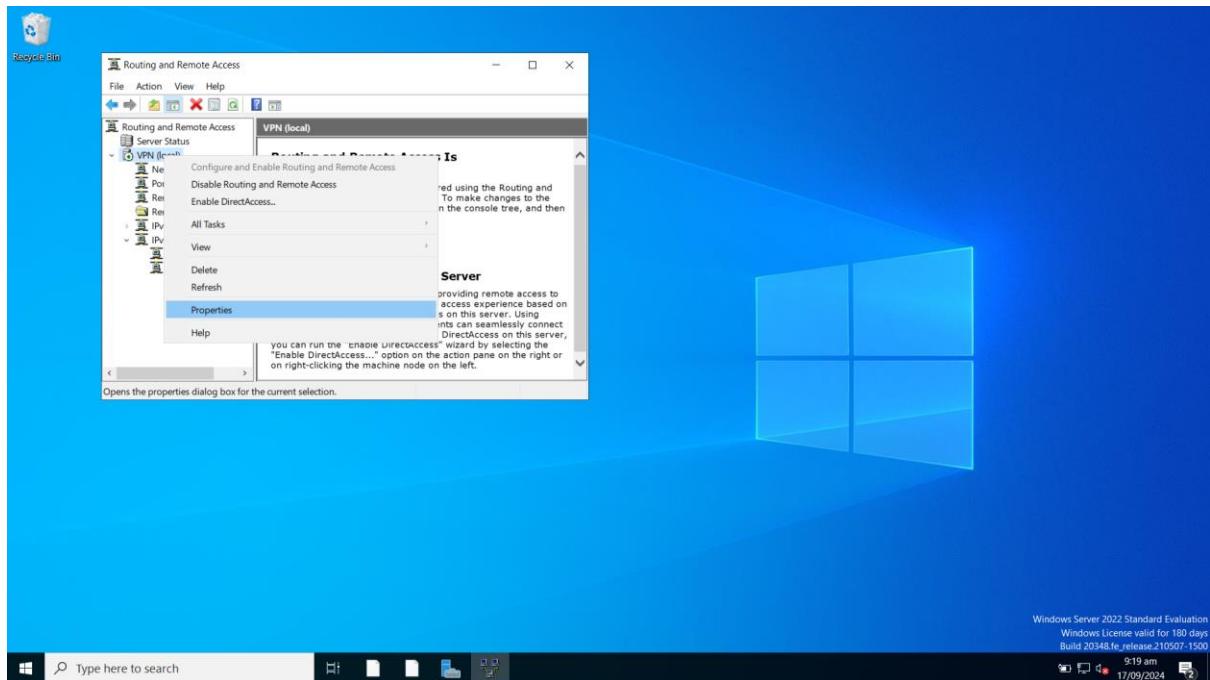
Next >

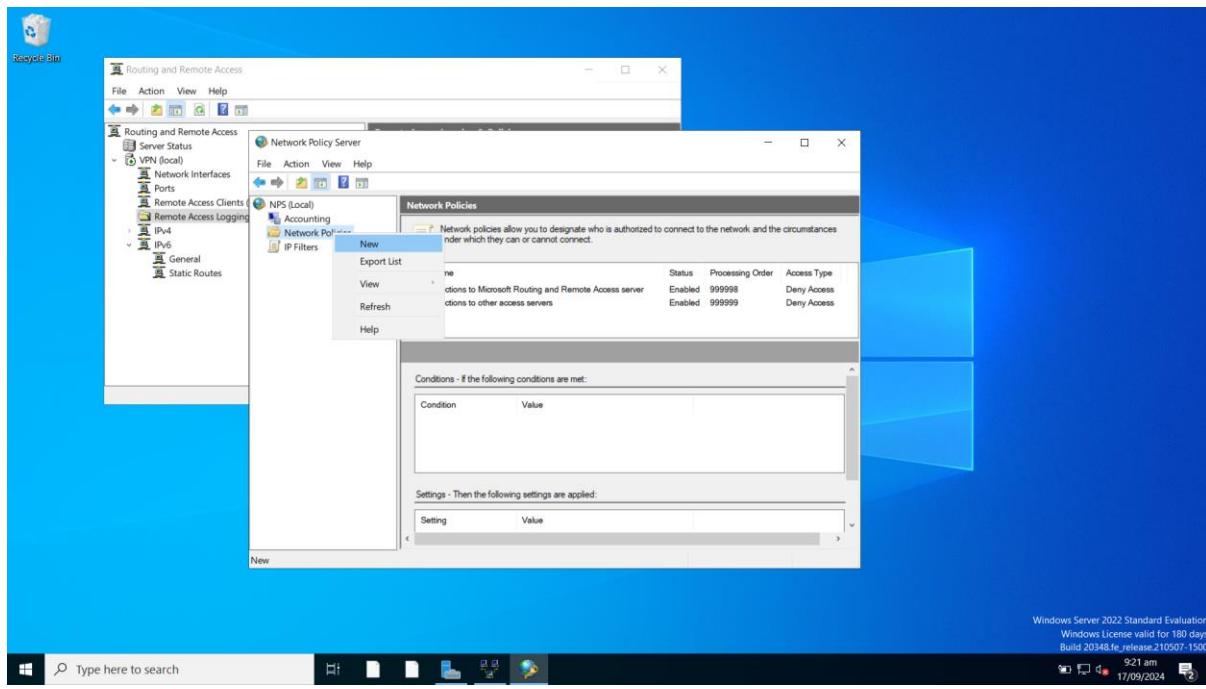
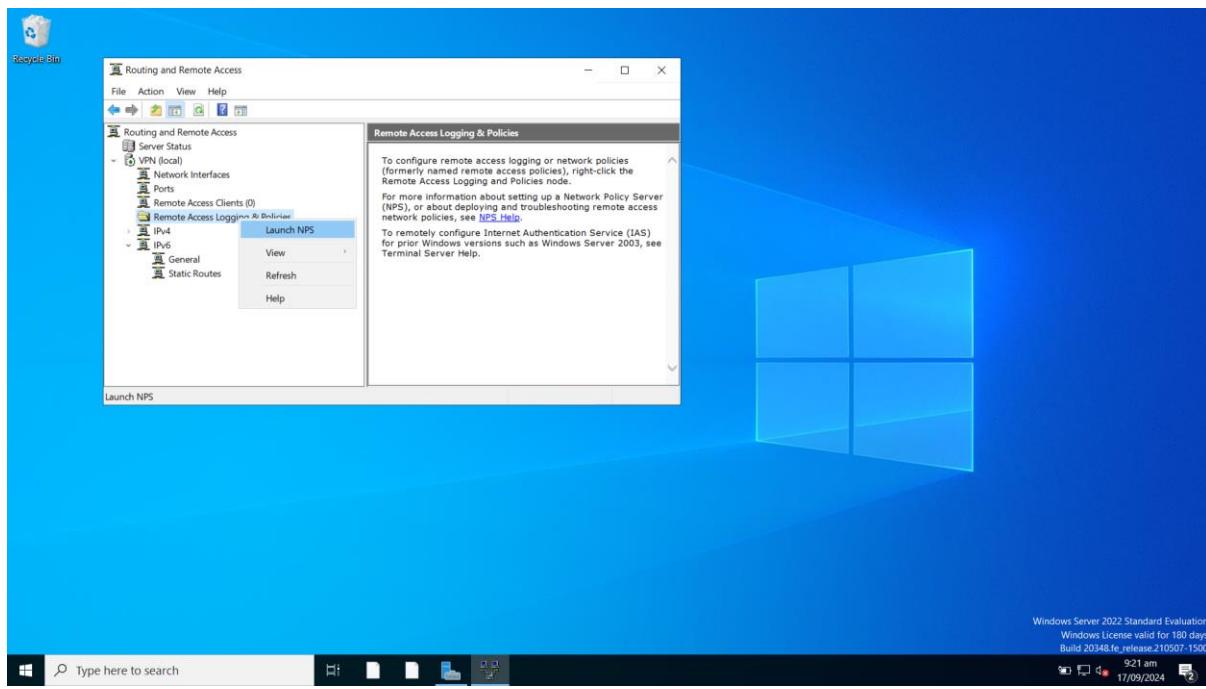
Cancel

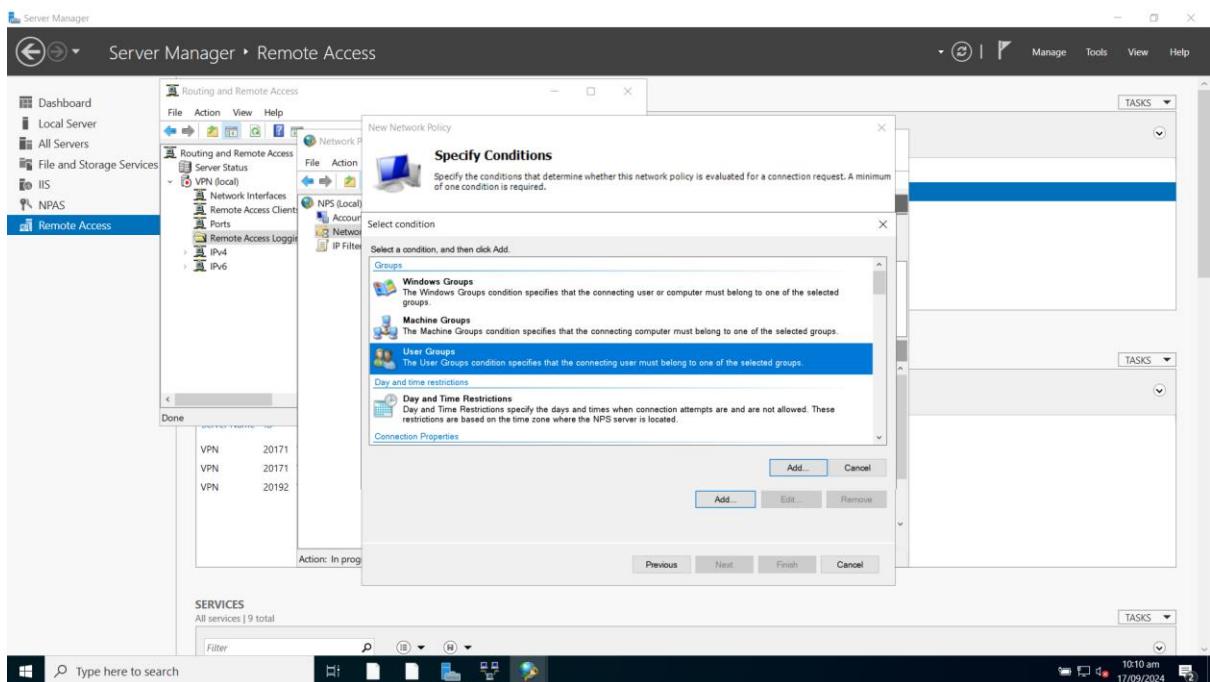
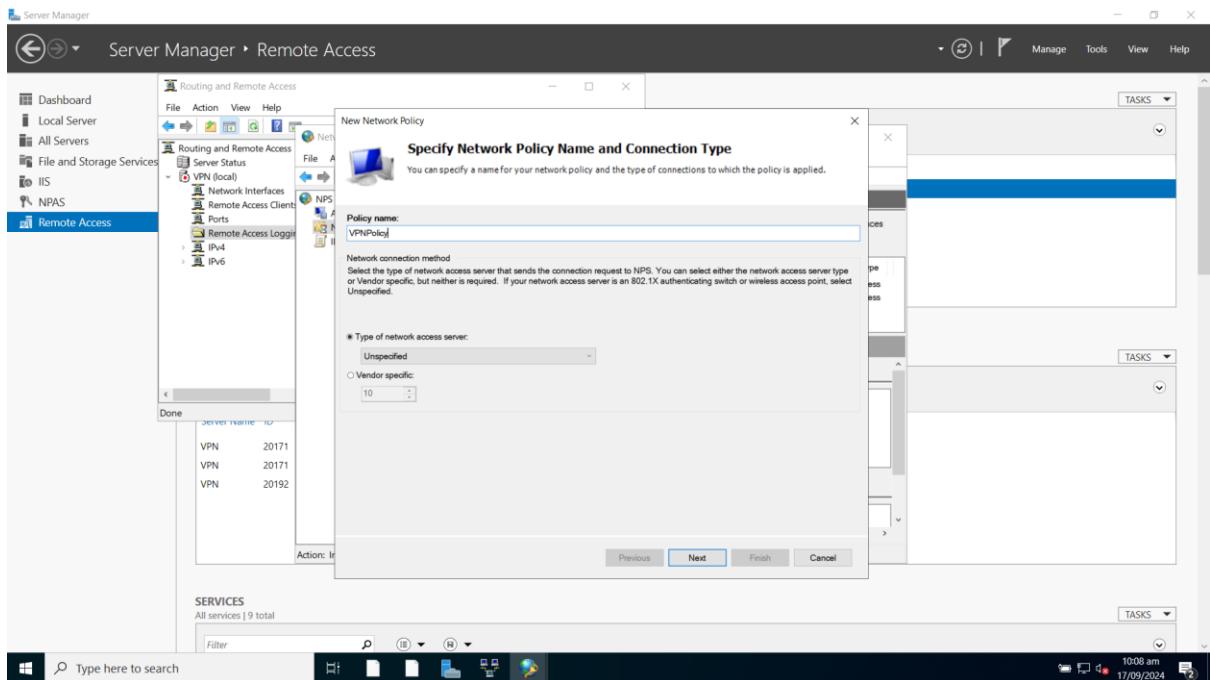
40 IP addresses assigned to VPN users. (192.168.1.101~140/24)

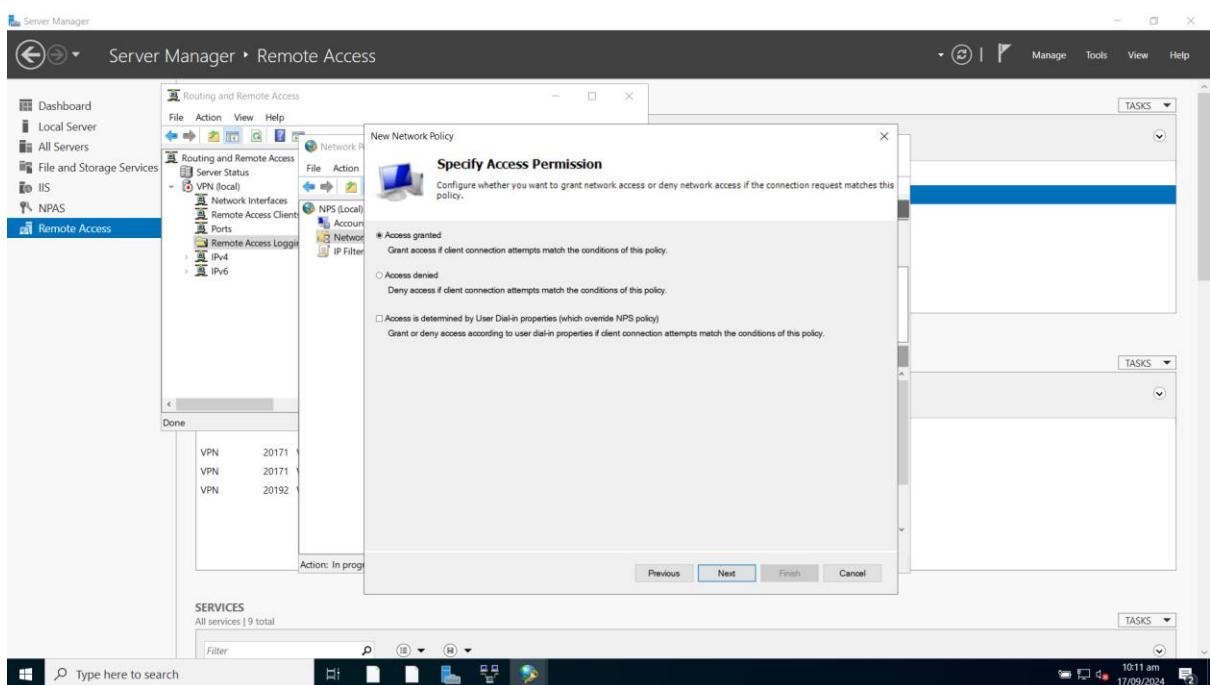
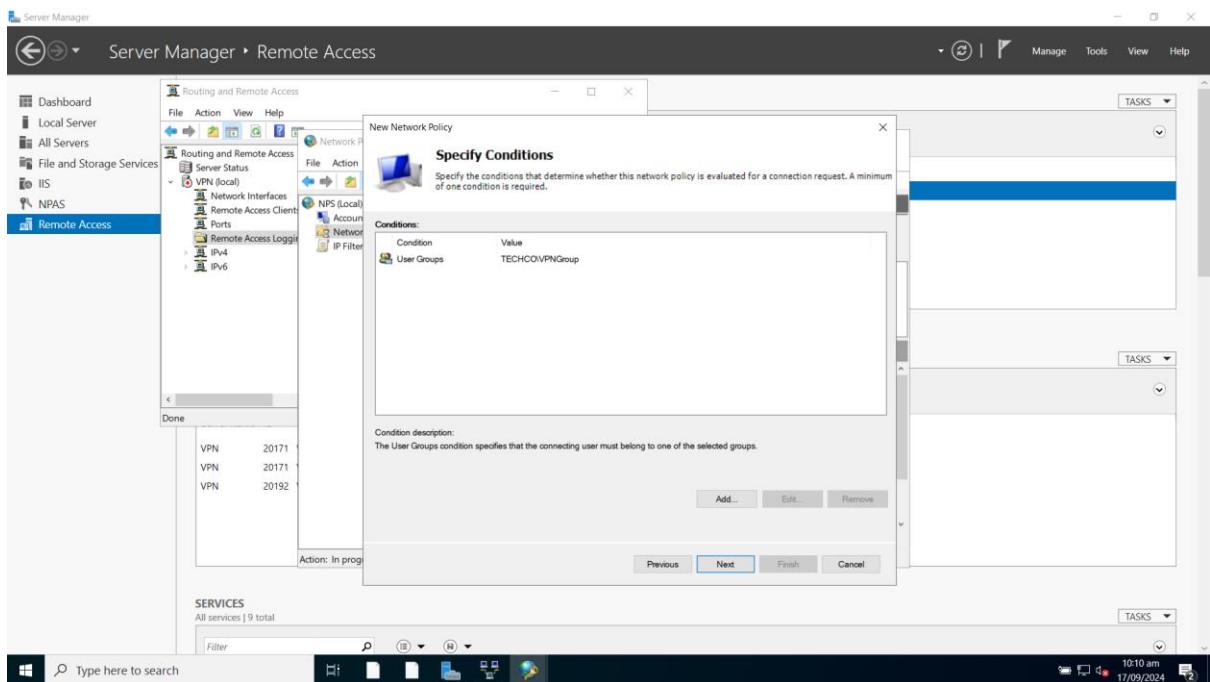


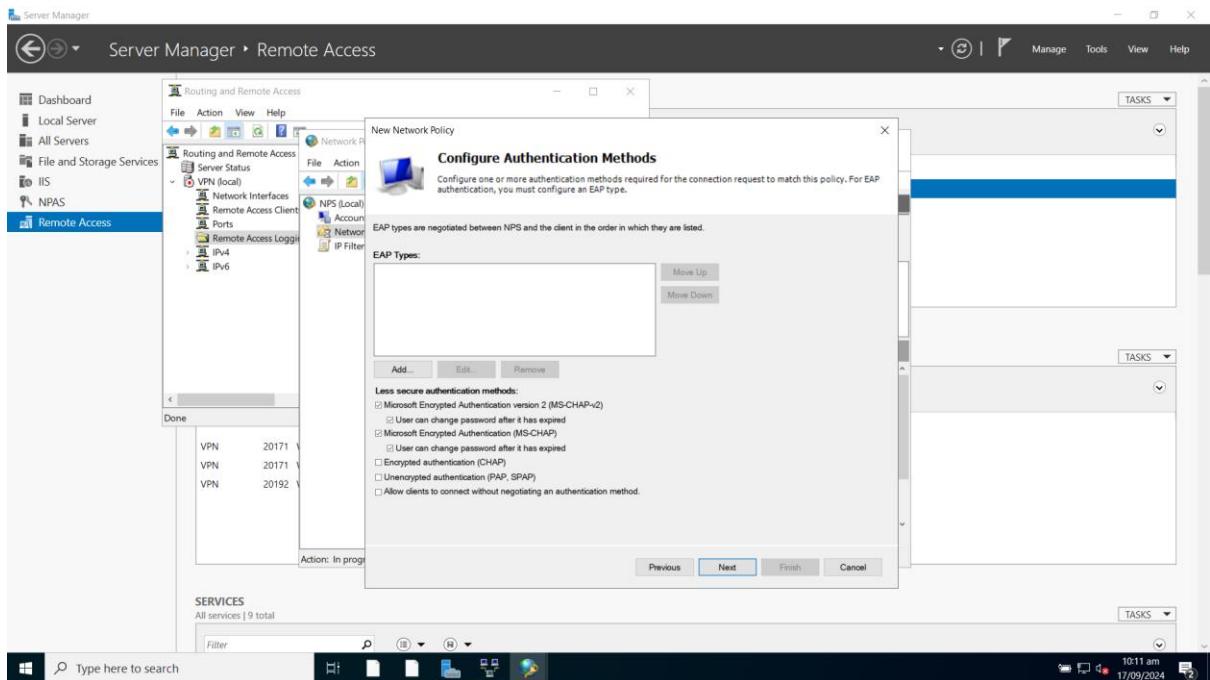




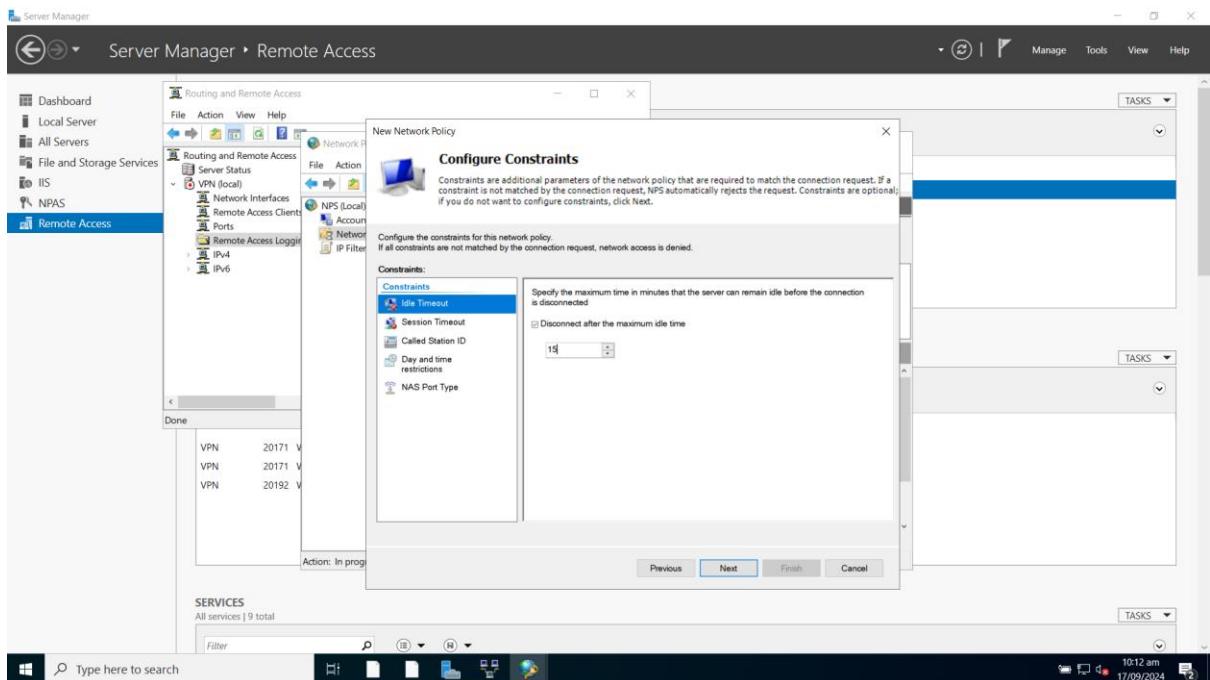


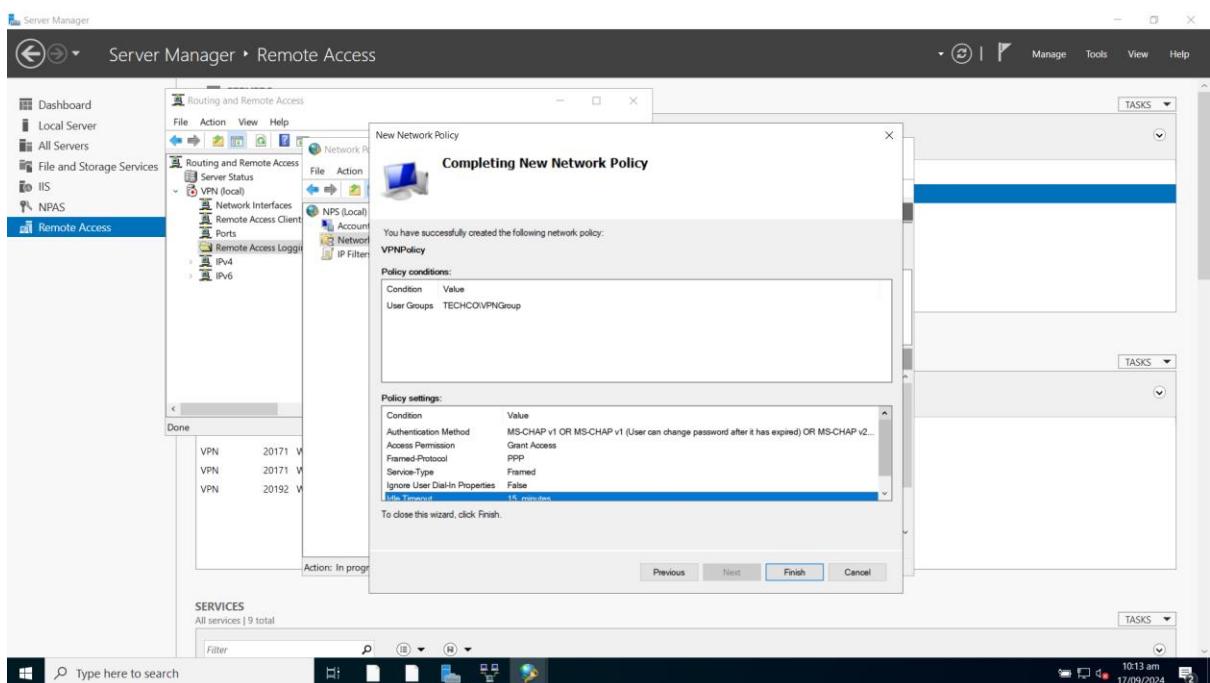
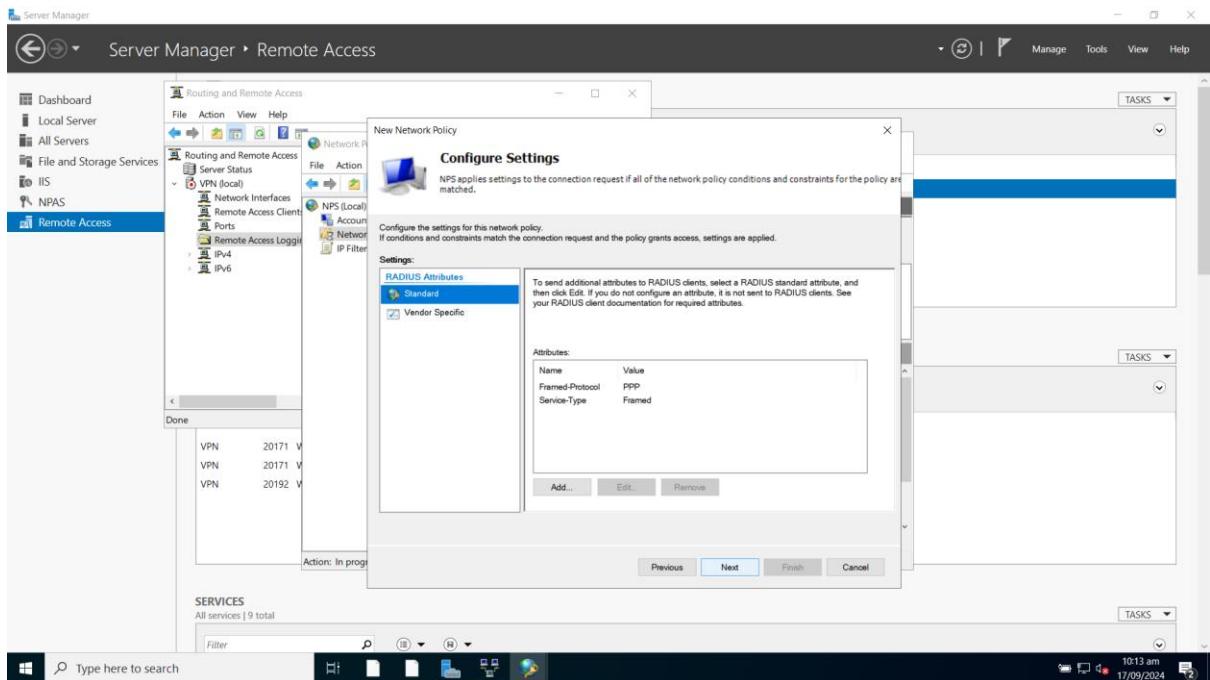


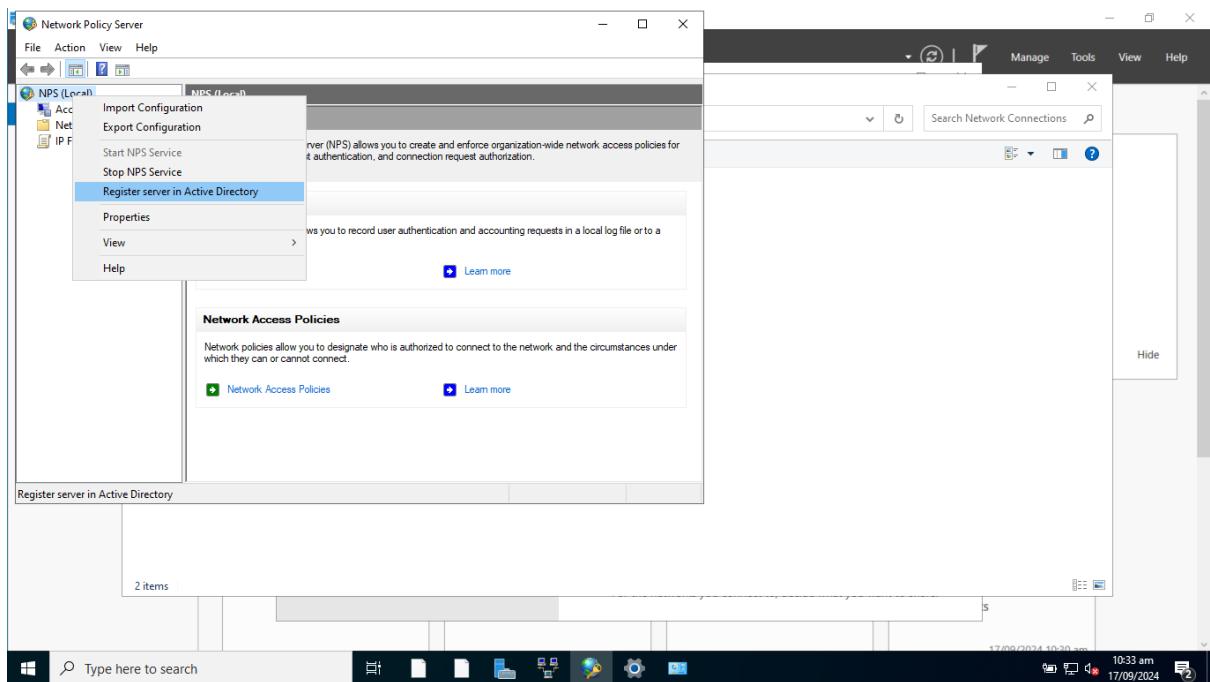




Set the default idle timeout for VPN connections to 15 minutes.





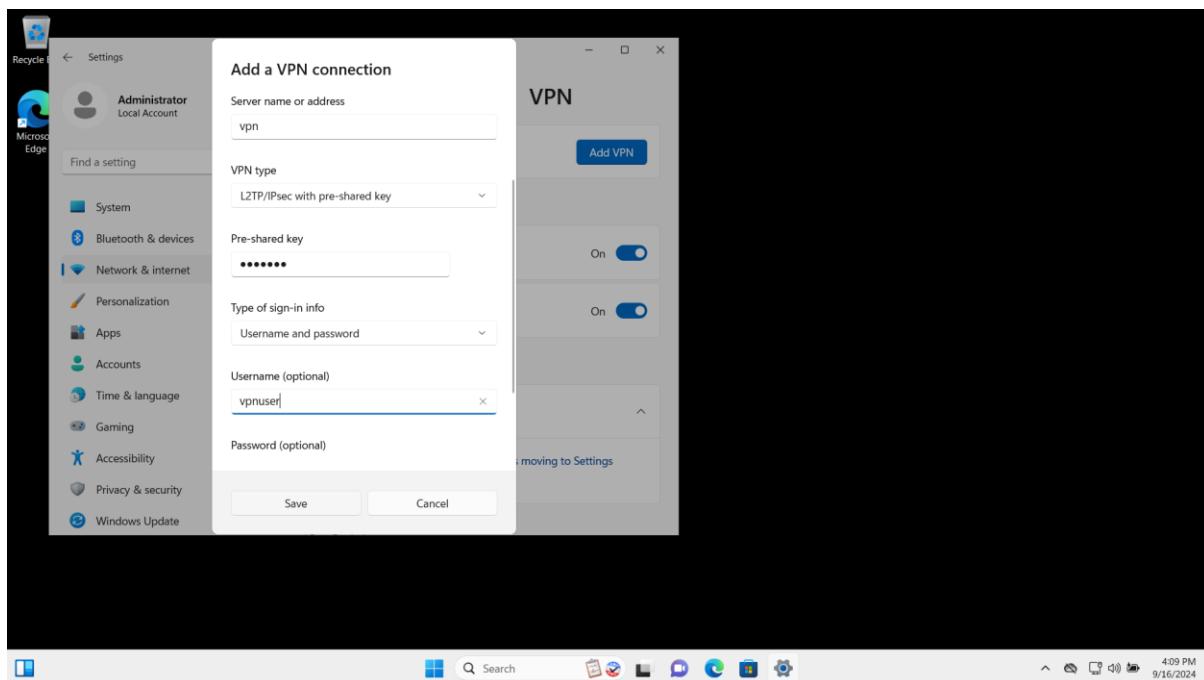
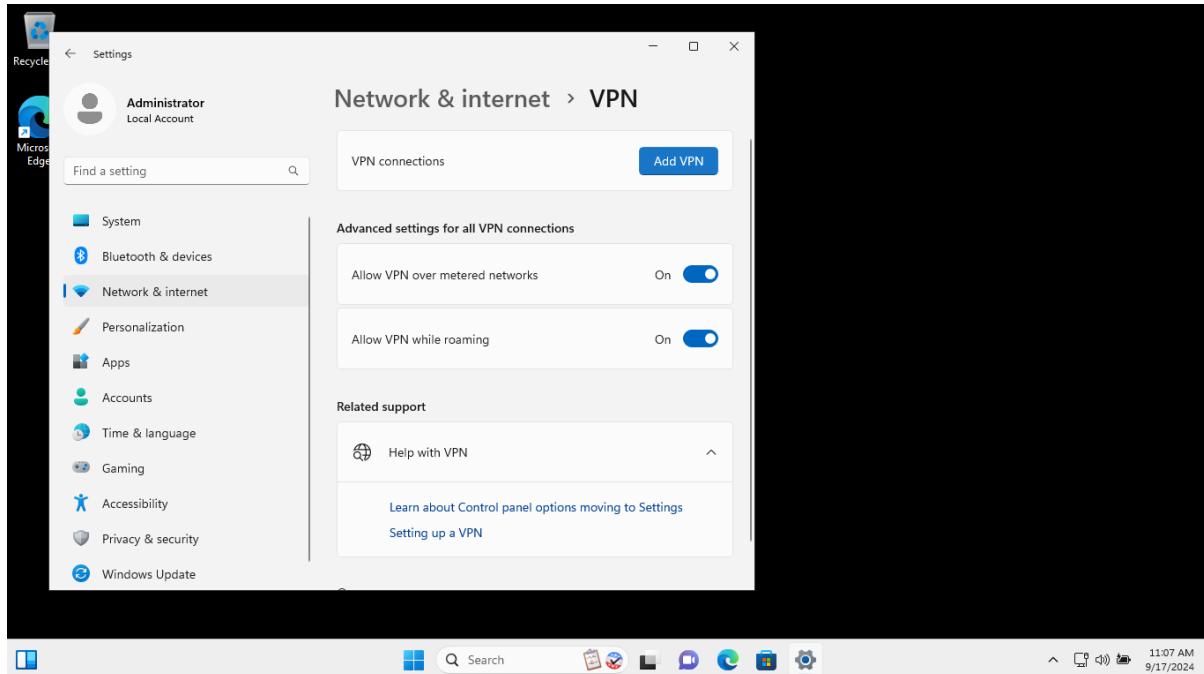


VPN server is ready.

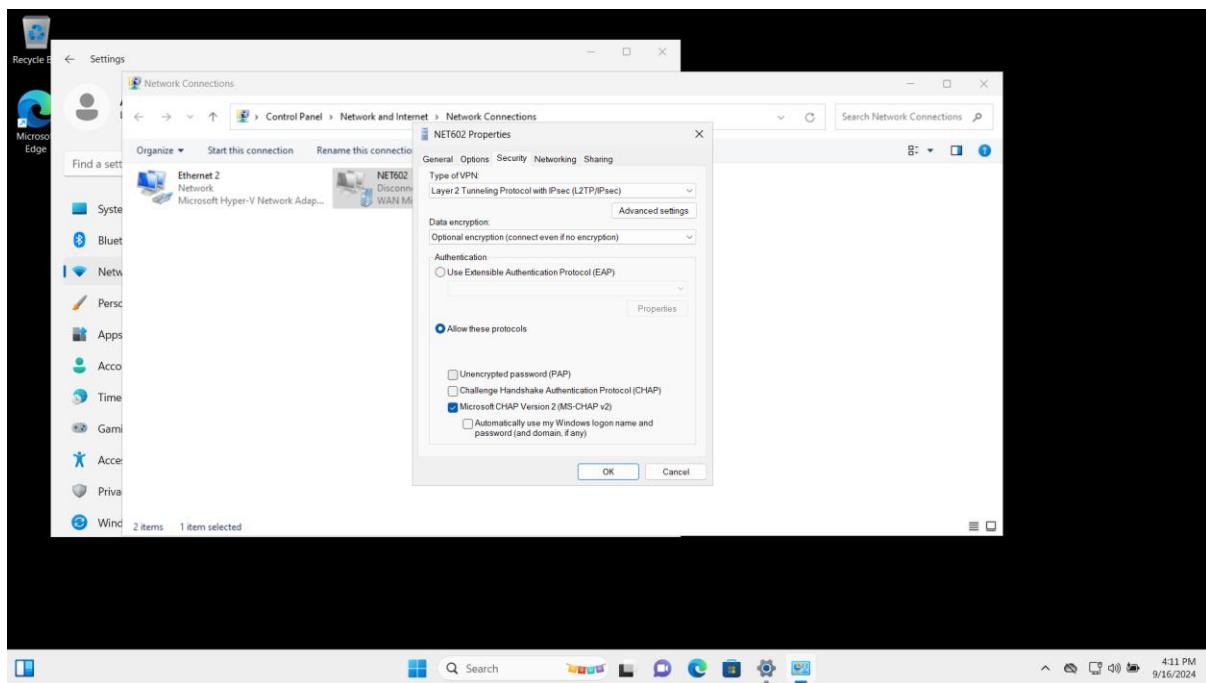
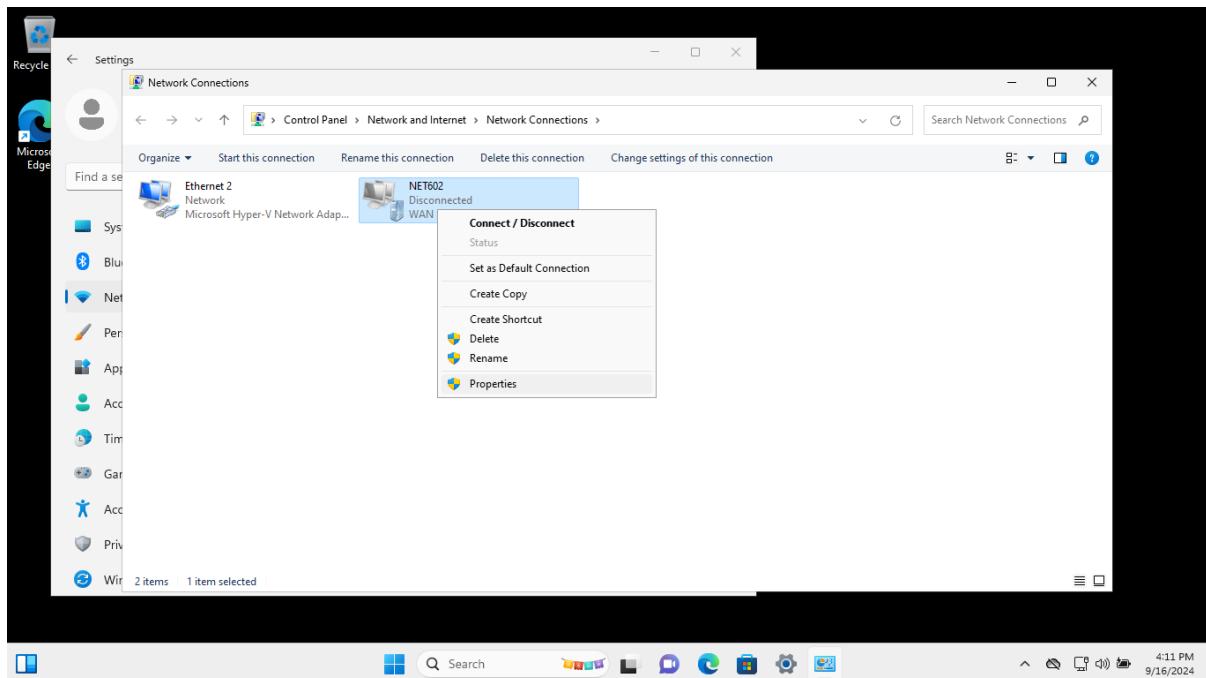
The screenshot shows the 'Remote Access Management Console' window. The left sidebar has 'Dashboard' selected under 'VPN'. The main area is the 'Remote Access Dashboard', which includes sections for 'Server Status' and 'DirectAccess and VPN Client Status'. In 'Server Status', it shows 'Operations Status' for 'VPN.techco.co.nz' with all items checked (VPN, Services, VPN addressing, VPN connectivity). In 'DirectAccess and VPN Client Status', it shows 0 active clients, 0 DirectAccess clients, 0 active VPN clients, and 0 cumulative connections. The taskbar at the bottom shows the date and time as 17/09/2024 10:37 am.

Task 4.2 Set up a secure VPN connection

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

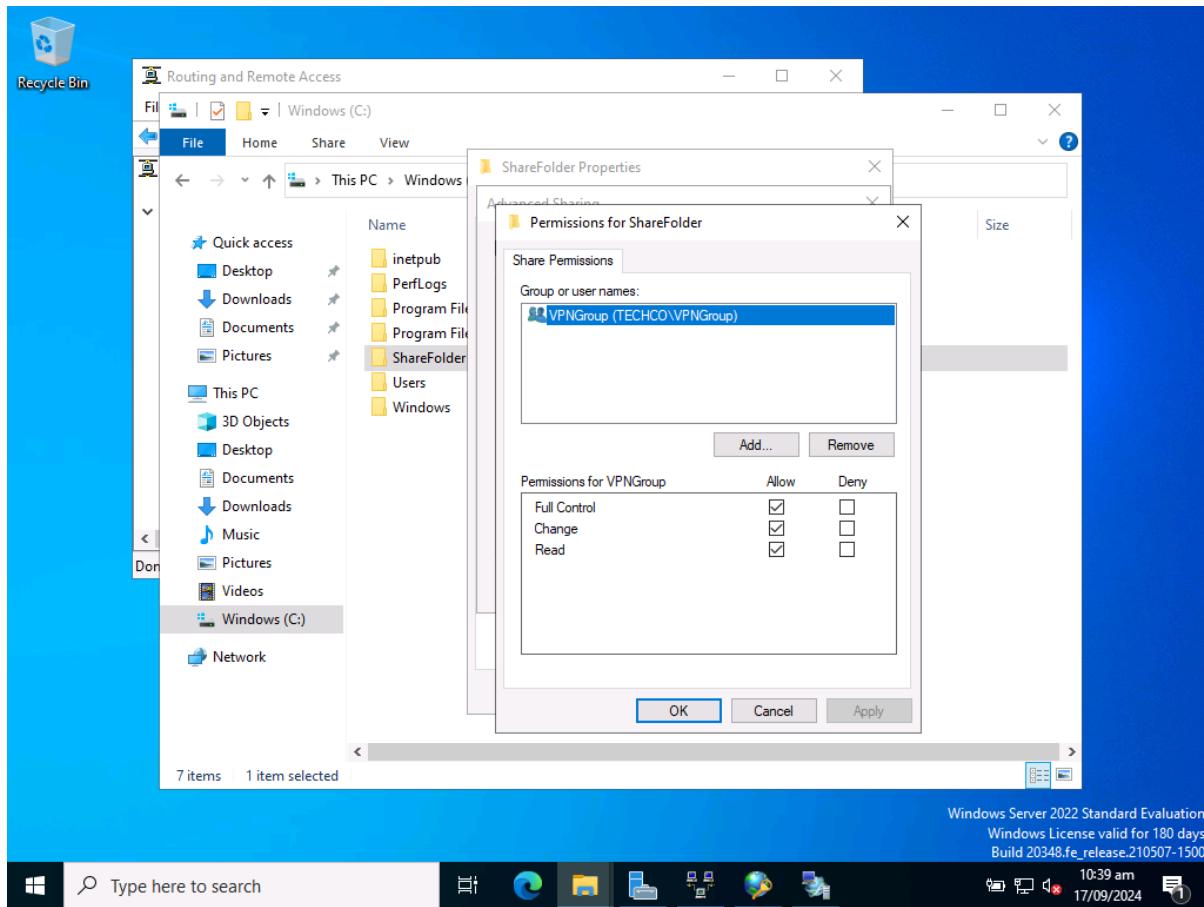


2. Modify the properties of VPN to allow MS CHAP v2.



Task 4.3 Allow file sharing for a shared folder

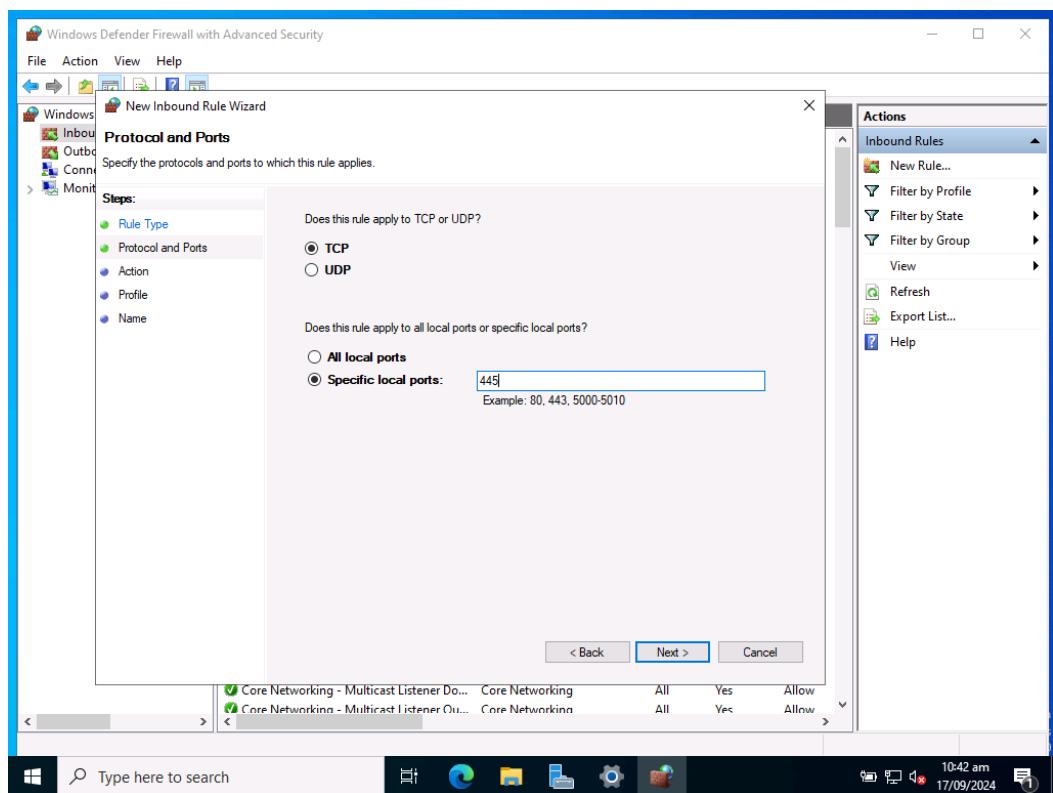
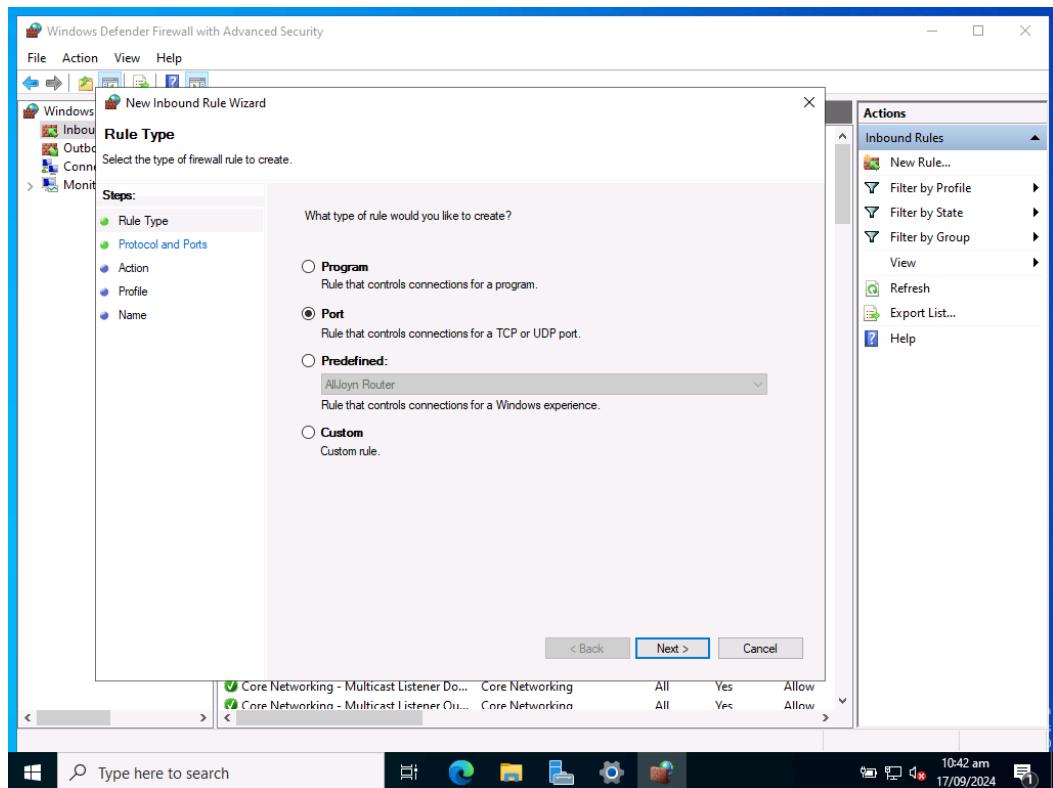
1. Create a shared folder on VPN server

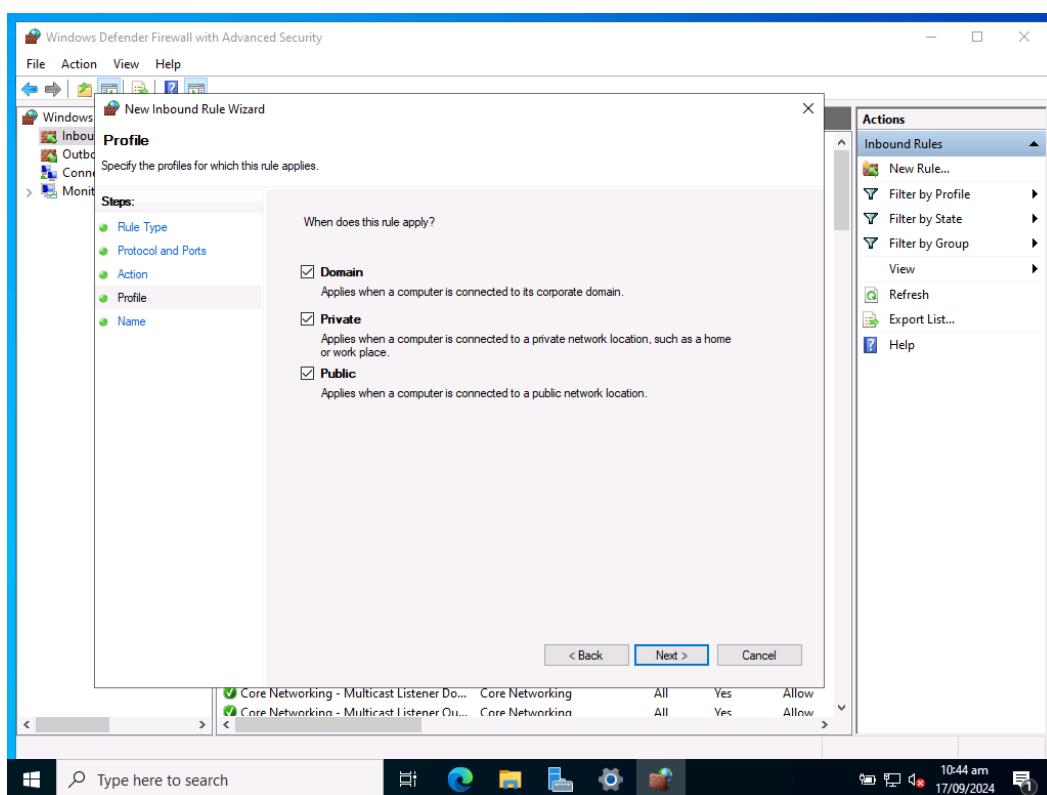
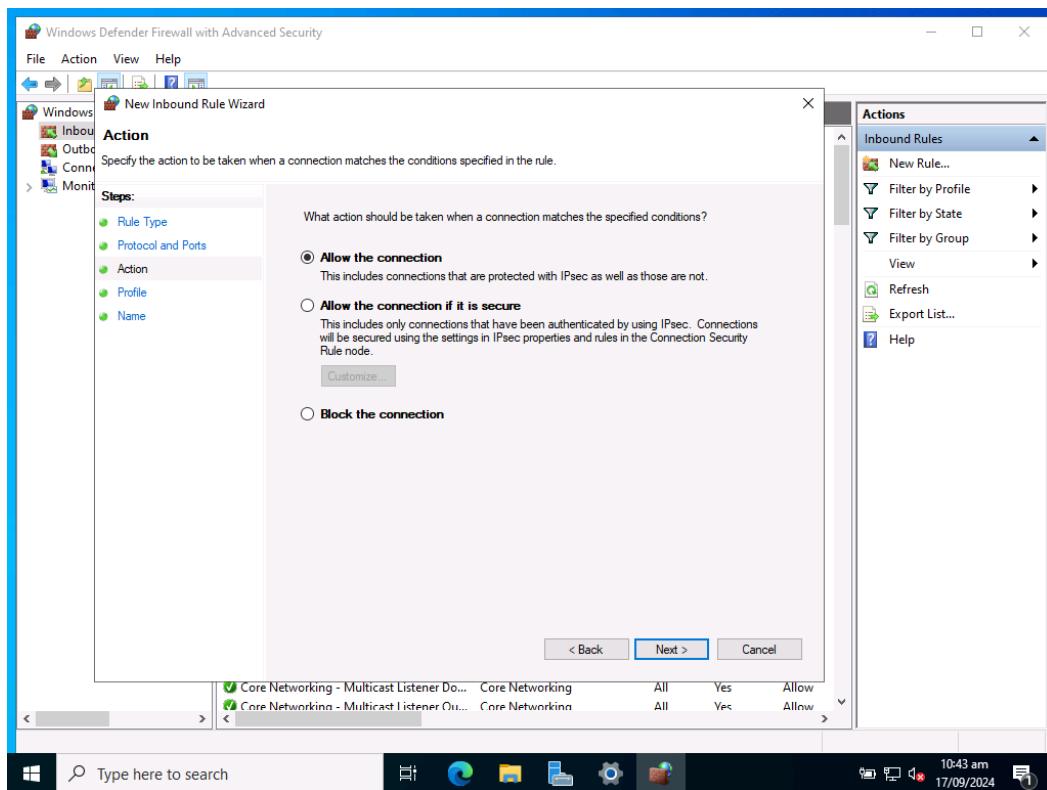


2. Disable all inbound rules which allow port 445 on Windows Firewall settings

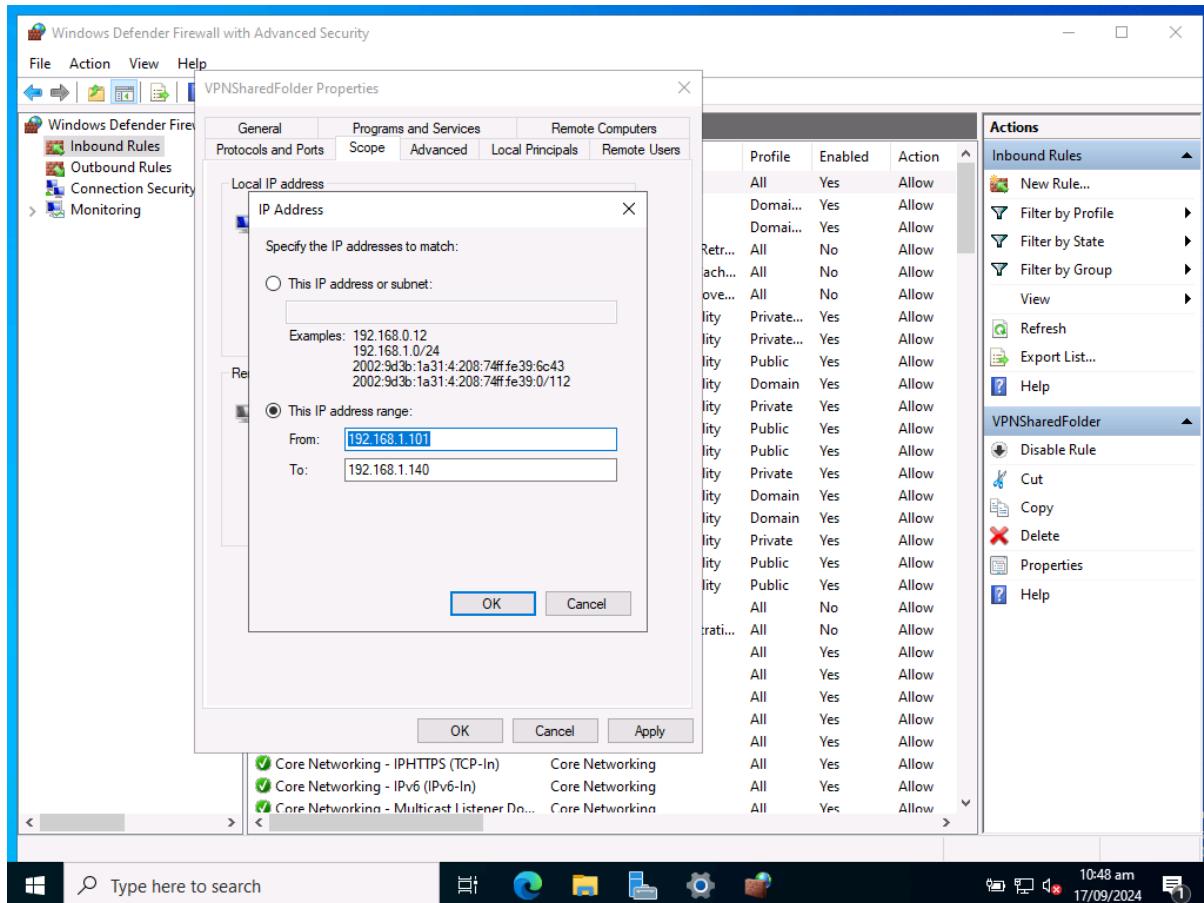
The screenshot shows the Windows Defender Firewall with Advanced Security interface. The 'Inbound Rules' section is selected. A list of rules is displayed, including various network discovery and sharing rules. On the right side, there is a 'Actions' pane with options like 'New Rule...', 'Filter by Profile', 'Filter by State', 'Filter by Group', 'View', 'Refresh', 'Export List...', 'Help', 'Selected Items', 'Enable Rule', 'Cut', 'Copy', and 'Delete'. One specific rule, 'File and Printer Sharing (SMB-QUIC-In)', is highlighted in the list.

3. Create a new inbound rule which allows port 445



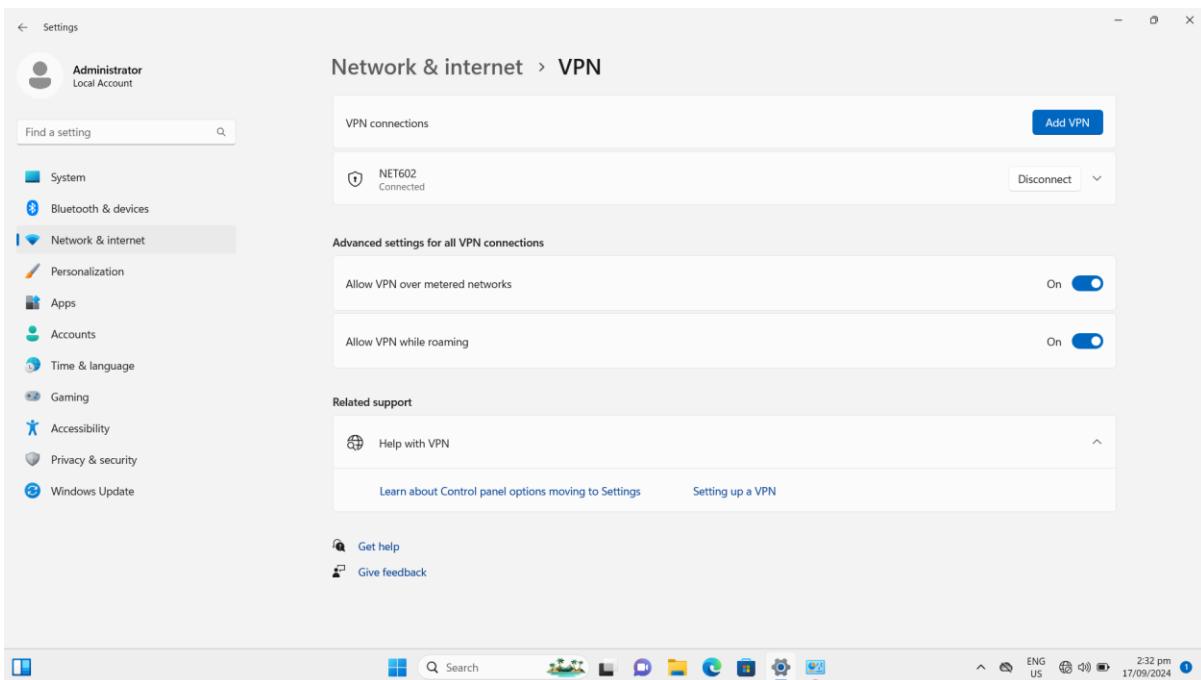
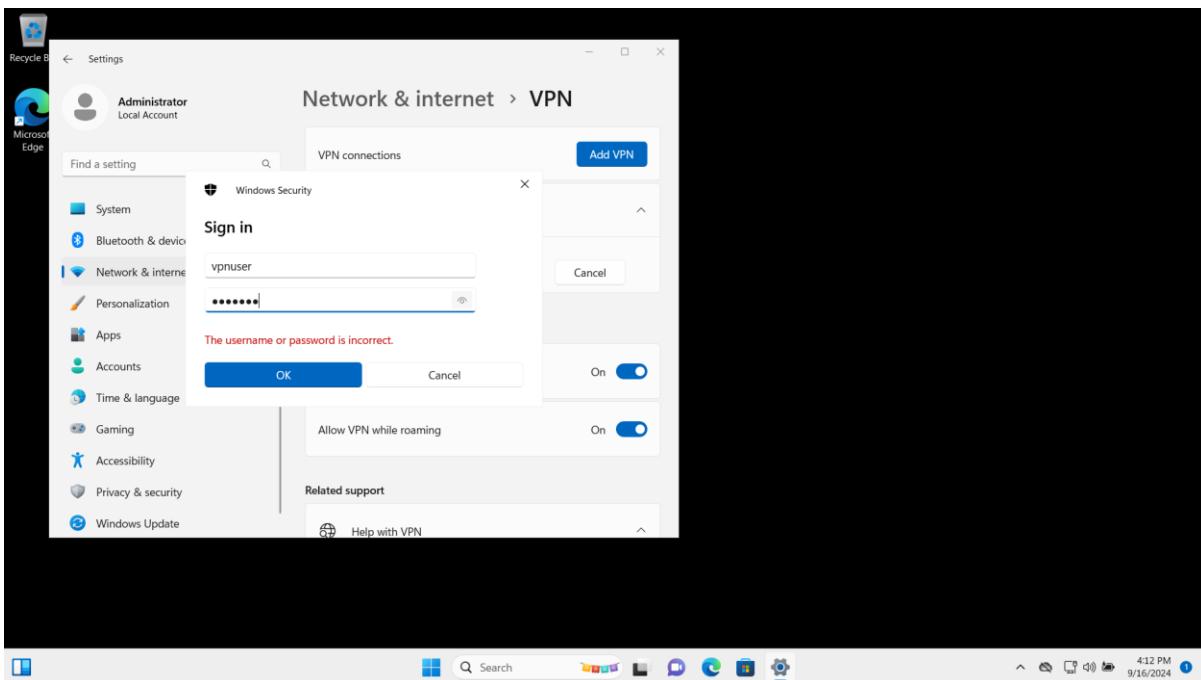


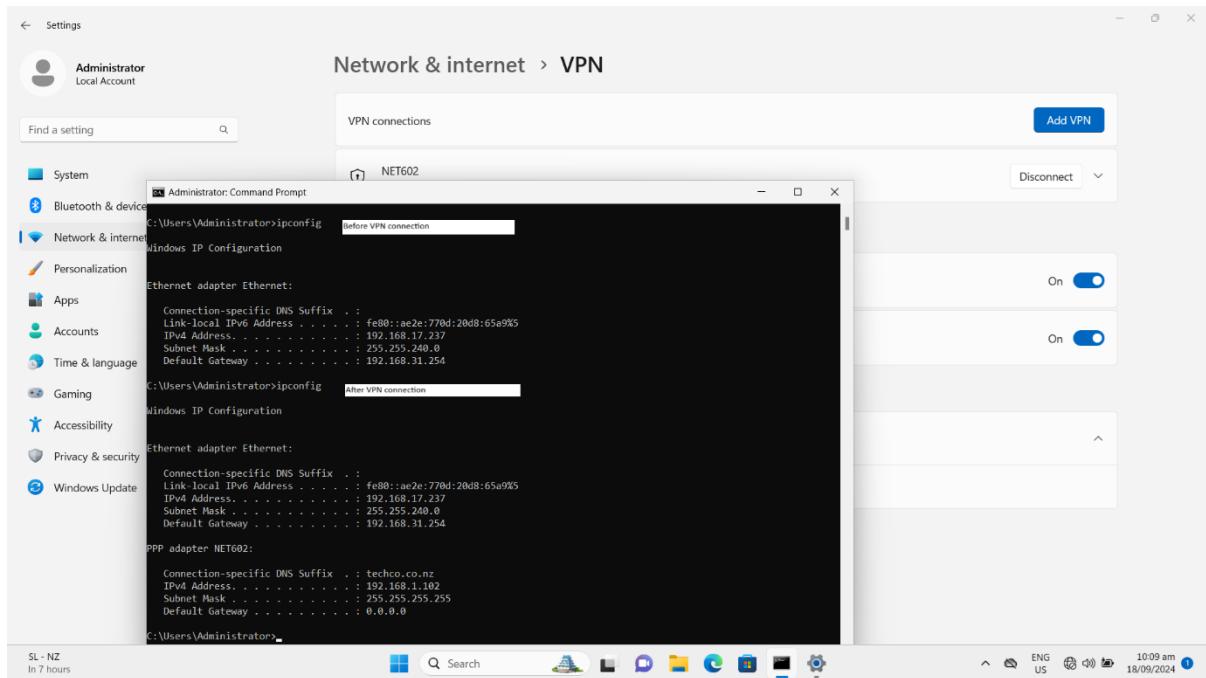
4. Set the inbound rule properties, and set remote IP addresses scope same as VPN settings.



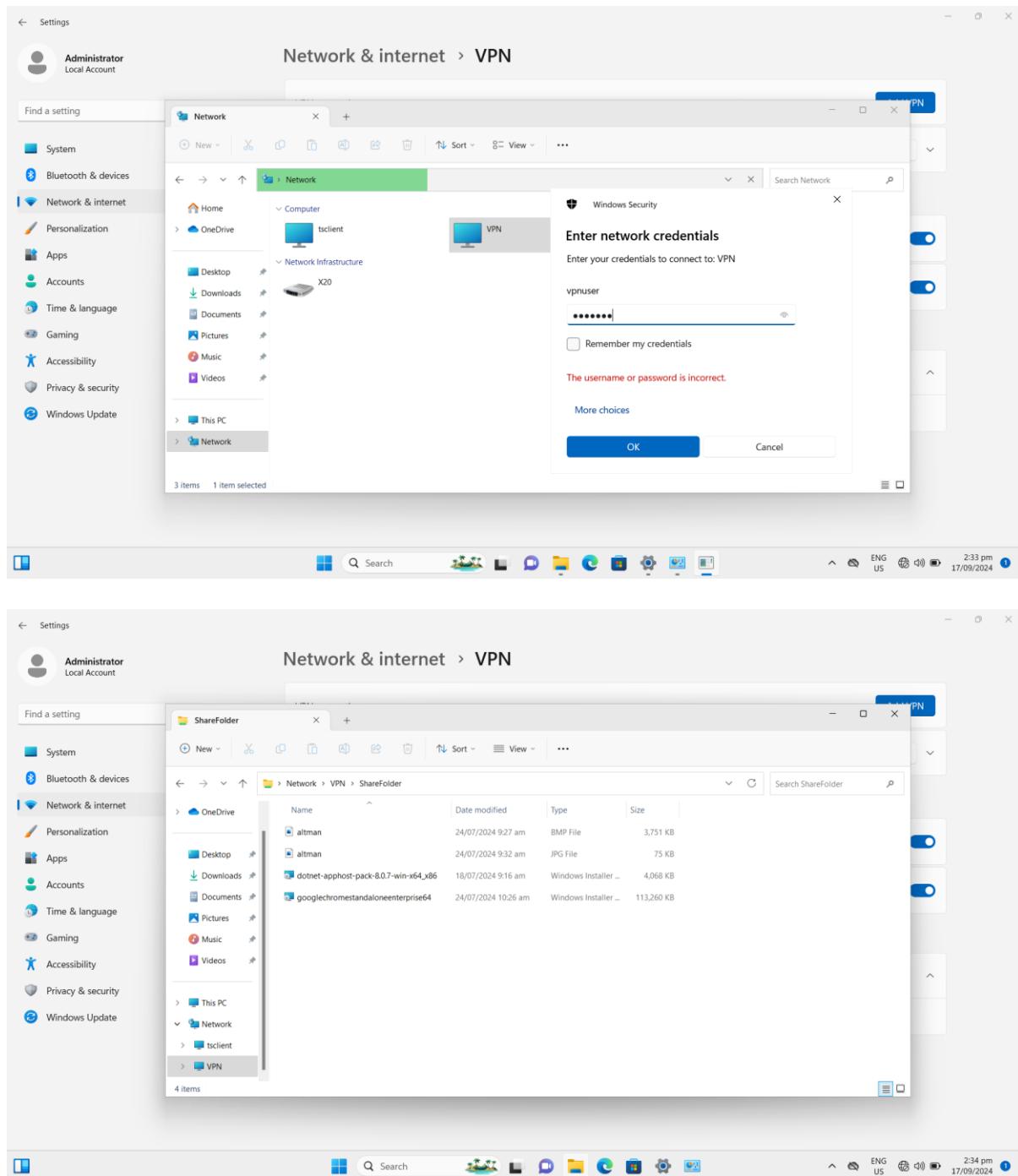
Task 4.4 Test the VPN connectivity to verify the setup and configuration

1. Connect the client machine VPN





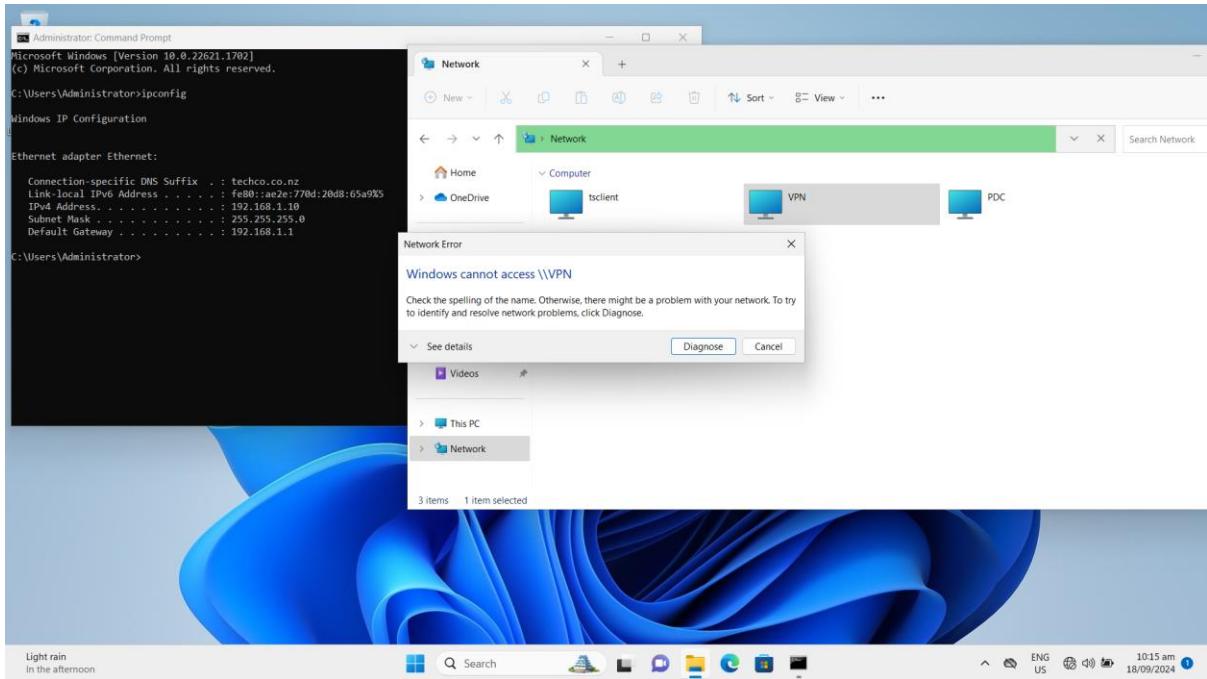
2. The VPN user “vpnuser” can access the shared folder on the VPN server:



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 backedup.

$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

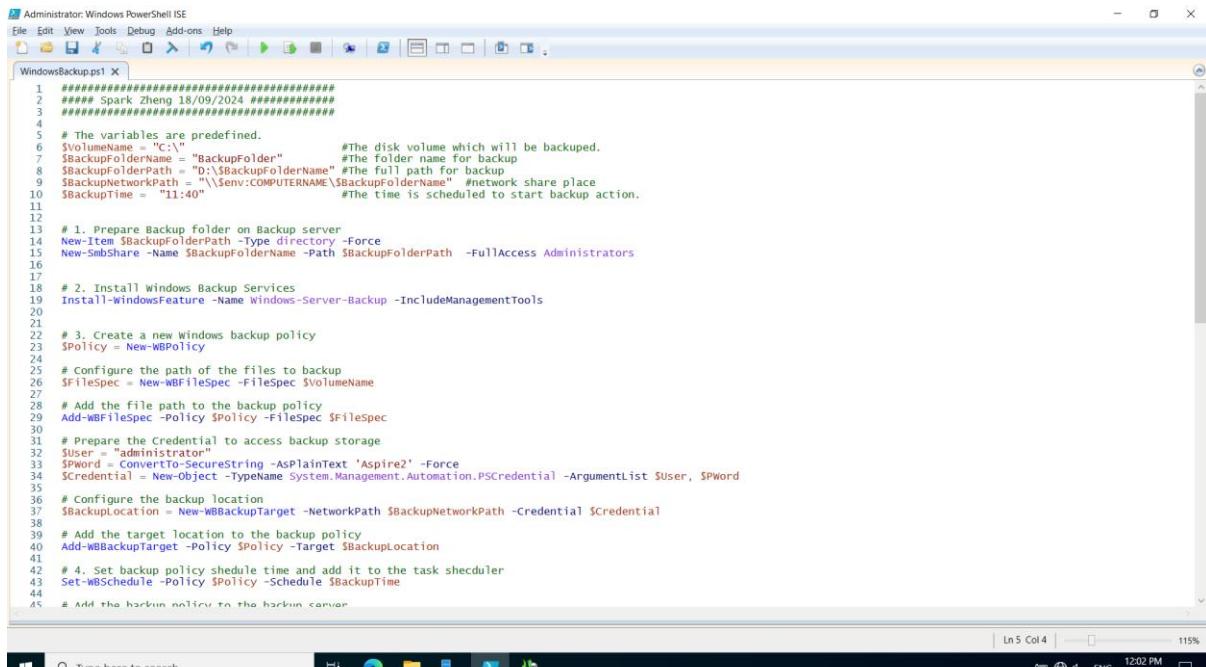
# 4. Set backup policy schedule time and add it to the task scheduler
Set-WBSchedule -Policy $Policy -Schedule $BackupTime

# 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()}}

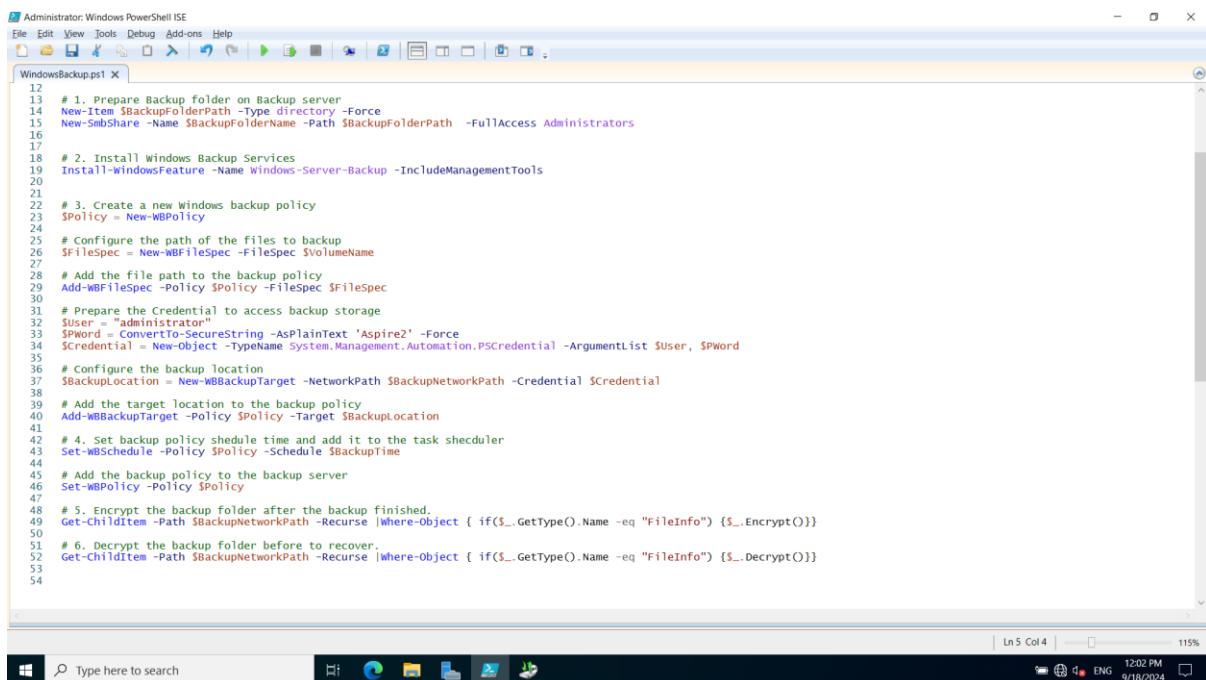
```



```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
WindowsBackup.ps1 X
1 ##### Spark.Zheng 18/09/2024 #####
2
3
4
5 # The variables are predefined.
6 $volumeName = "e:\\" #The disk volume which will be backedup.
7 $backupFolderName = "BackupFolder" #The folder name for backup
8 $backupFolderPath = "D:\$backupFolderName" #The full path for backup
9 $backupNetworkPath = "\\$env:COMPUTERNAME\$backupFolderName" #network share place
10 $backupTime = "11:40" #The time is scheduled to start backup action.
11
12
13 # 1. Prepare Backup folder on Backup server
14 New-Item $backupFolderPath -Type directory -Force
15 New-SmbShare -Name $backupFolderName -Path $backupFolderPath -FullAccess Administrators
16
17
18 # 2. Install Windows Backup Services
19 Install-WindowsFeature -Name Windows-Server-Backup -IncludeManagementTools
20
21
22 # 3. Create a new Windows backup policy
23 $Policy = New-WBPolicy
24
25 # Configure the path of the files to backup
26 $fileSpec = New-WBFileSpec -FileSpec $volumeName
27
28 # Add the file path to the backup policy
29 Add-WBFileSpec -Policy $Policy -FileSpec $fileSpec
30
31 # Prepare the Credential to access backup storage
32 $User = "administrator"
33 $SPWord = ConvertTo-SecureString -AsPlainText 'Aspire2' -Force
34 $Credential = New-Object System.Management.Automation.PSCredential -ArgumentList $User, $SPWord
35
36 # Configure the backup location
37 $backupLocation = New-WBBackupTarget -NetworkPath $backupNetworkPath -Credential $Credential
38
39 # Add the target location to the backup policy
40 Add-WBBackupTarget -Policy $Policy -Target $backupLocation
41
42 # 4. Set backup policy schedule time and add it to the task scheduler
43 Set-WBSchedule -Policy $Policy -Schedule $backupTime
44
45 # Add the backup policy to the backup server
46 Set-WBPolicy -Policy $Policy
47
48 # 5. Encrypt the backup folder after the backup finished.
49 Get-ChildItem -Path $backupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") { $_.Encrypt() } }
50
51 # 6. Decrypt the backup folder before to recover.
52 Get-ChildItem -Path $backupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") { $_.Decrypt() } }
53
54

```



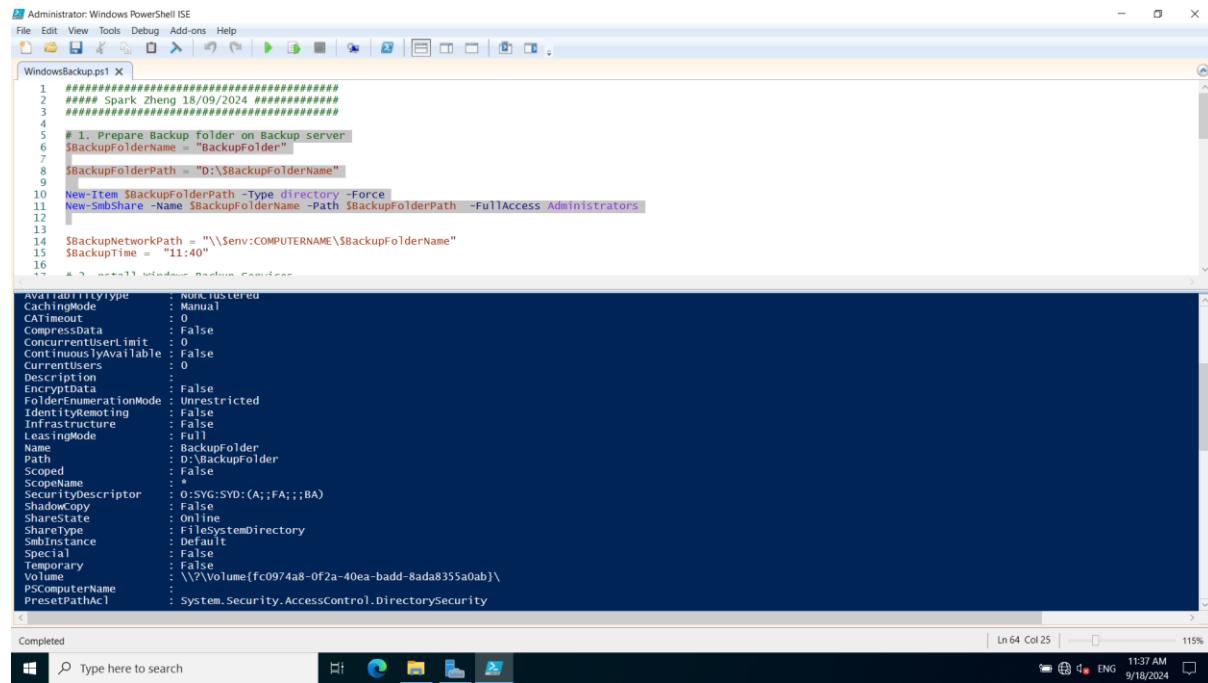
```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
WindowsBackup.ps1 X
12
13 # 1. Prepare Backup folder on Backup server
14 New-Item $backupFolderPath -Type directory -Force
15 New-SmbShare -Name $backupFolderName -Path $backupFolderPath -FullAccess Administrators
16
17
18 # 2. Install Windows Backup Services
19 Install-WindowsFeature -Name Windows-Server-Backup -IncludeManagementTools
20
21
22 # 3. Create a new Windows backup policy
23 $Policy = New-WBPolicy
24
25 # Configure the path of the files to backup
26 $fileSpec = New-WBFileSpec -FileSpec $volumeName
27
28 # Add the file path to the backup policy
29 Add-WBFileSpec -Policy $Policy -FileSpec $fileSpec
30
31 # Prepare the Credential to access backup storage
32 $User = "administrator"
33 $SPWord = ConvertTo-SecureString -AsPlainText 'Aspire2' -Force
34 $Credential = New-Object System.Management.Automation.PSCredential -ArgumentList $User, $SPWord
35
36 # Configure the backup location
37 $backupLocation = New-WBBackupTarget -NetworkPath $backupNetworkPath -Credential $Credential
38
39 # Add the target location to the backup policy
40 Add-WBBackupTarget -Policy $Policy -Target $backupLocation
41
42 # 4. Set backup policy schedule time and add it to the task scheduler
43 Set-WBSchedule -Policy $Policy -Schedule $backupTime
44
45 # Add the backup policy to the backup server
46 Set-WBPolicy -Policy $Policy
47
48 # 5. Encrypt the backup folder after the backup finished.
49 Get-ChildItem -Path $backupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") { $_.Encrypt() } }
50
51 # 6. Decrypt the backup folder before to recover.
52 Get-ChildItem -Path $backupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") { $_.Decrypt() } }
53
54

```

Task 5.2 Configure Windows backup using the PowerShell Script

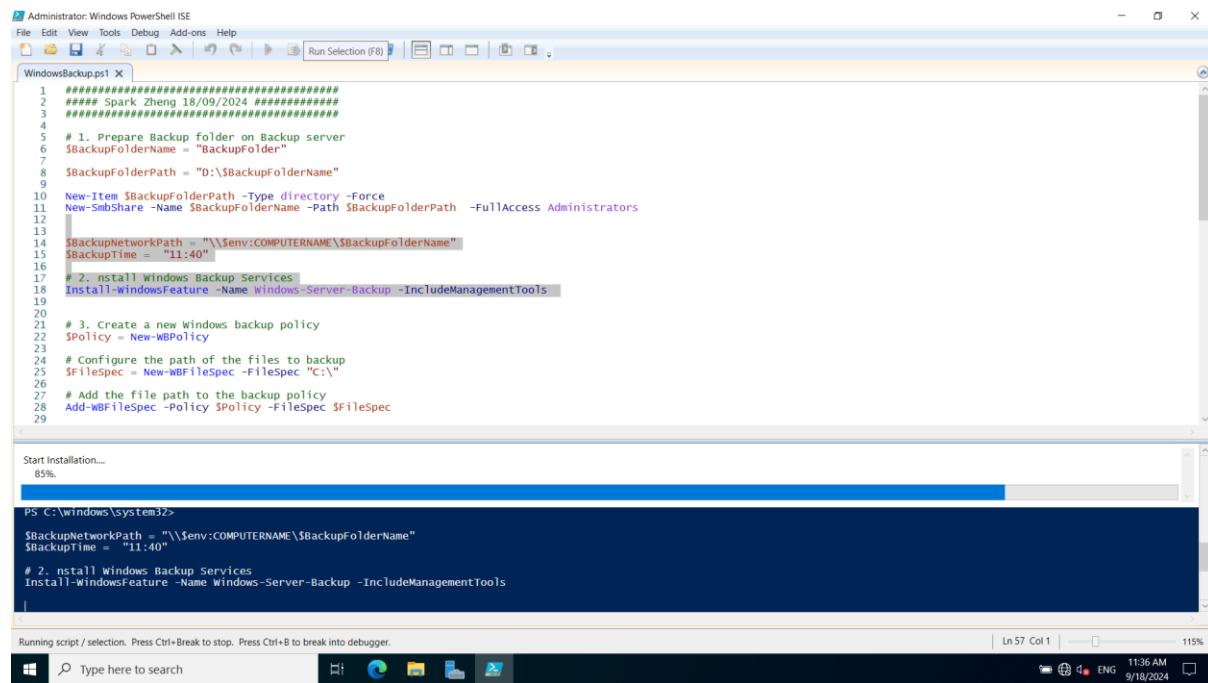
1. Prepare Backup folder on Backup server



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Run Selection (F8) Run All (F5) Stop (Shift+F5) Run Current Line (F11)
WindowsBackup.ps1
1 ###### Spark: Zheng 18/09/2024 ######
2 #####
3 #####
4 # 1. Prepare Backup Folder on Backup server
5 $BackupFolderName = "BackupFolder"
6 $BackupFolderPath = "D:\$BackupFolderName"
7
8 New-Item $BackupFolderPath -Type directory -Force
9 New-SmbShare -Name $BackupFolderName -Path $BackupFolderPath -FullAccess Administrators
10
11 $BackupNetworkPath = "\\$env:COMPUTERNAME\$BackupFolderName"
12 $BackupTime = "11:40"
13
14 # 2. install windows Backup Services
15
16
Completed
Ln 64 Col 25 115%
Type here to search 11:37 AM ENG 9/18/2024
```

The screenshot shows the Windows PowerShell ISE interface. A PowerShell script named 'WindowsBackup.ps1' is open. The script contains code to create a new folder named 'BackupFolder' at the path 'D:\\$BackupFolderName' and to share it under the name '\$BackupFolderName'. It also sets variables for the network path and backup time. The status bar at the bottom indicates the script has completed execution.

2. Install Windows Backup Services



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Run Selection (F8) Run All (F5) Stop (Shift+F5) Run Current Line (F11)
WindowsBackup.ps1
1 ###### Spark: Zheng 18/09/2024 ######
2 #####
3 #####
4 # 1. Prepare Backup folder on Backup server
5 $BackupFolderName = "BackupFolder"
6 $BackupFolderPath = "D:\$BackupFolderName"
7
8 New-Item $BackupFolderPath -Type directory -Force
9 New-SmbShare -Name $BackupFolderName -Path $BackupFolderPath -FullAccess Administrators
10
11 $BackupNetworkPath = "\\$env:COMPUTERNAME\$BackupFolderName"
12 $BackupTime = "11:40"
13
14 # 2. install windows Backup Services
15 Install-WindowsFeature -Name Windows-Server-Backup -IncludeManagementTools
16
17
18 # 3. Create a new windows backup policy
19 $Policy = New-WBPolicy
20
21 # Configure the path of the files to backup
22 $FileSpec = New-WBFileSpec -fileSpec "C:\" -includeSubFolders $true
23
24 # Add the file path to the backup policy
25 Add-WBFileSpec -Policy $Policy -fileSpec $FileSpec
26
27
Start Installation...
85%
PS C:\windows\system32>
$BackupNetworkPath = "\\$env:COMPUTERNAME\$BackupFolderName"
$BackupTime = "11:40"
# 2. install Windows Backup Services
Install-WindowsFeature -Name Windows-Server-Backup -IncludeManagementTools
|
Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger.
Ln 57 Col 1 115%
Type here to search 11:36 AM ENG 9/18/2024
```

The screenshot shows the Windows PowerShell ISE interface. A PowerShell script named 'WindowsBackup.ps1' is open. The script performs the same tasks as the previous one but also includes a section to install the 'Windows-Server-Backup' feature using the 'Install-WindowsFeature' cmdlet. The status bar at the bottom indicates the script is running and shows progress. The command prompt shows the path 'C:\windows\system32>' and the variable definitions for the backup network path and time.

3. Create a new Windows backup policy

The screenshot shows a Windows PowerShell ISE window titled "WindowsBackup.ps1". The code in the editor creates a backup policy named \$Policy, which includes specifying the path to backup (\$FileSpec), preparing a credential (\$User, \$SPWord, \$Credential), setting the backup location (\$BackupLocation), adding the target location (\$BackupTarget), and finally setting the schedule (\$BackupTime) and adding it to the task scheduler (\$WBSchedule). A warning message at the bottom of the window states: "WARNING: Backup or recovery of individual files or application data from DVDs or other removable media is not supported. You can only backup or recover full volumes from this media type." The PowerShell prompt at the bottom is PS C:\windows\system32>.

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
WindowsBackup.ps1 | X
22 $Policy = New-WBPolicy
23 # Configure the path of the files to backup
24 $FileSpec = New-WBFileSpec -FileSpec "C:\"
25
26 # Add the file path to the backup policy
27 Add-WBFileSpec -Policy $Policy -FileSpec $FileSpec
28
29 # Prepare the Credential to access backup storage
30 $User = "administrator"
31 $SPWord = ConvertTo-SecureString -AsPlainText 'Aspire2' -Force
32 $Credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $User, $SPWord
33
34 # Configure the backup location
35 $BackupLocation = New-WBBackupTarget -NetworkPath $BackupNetworkPath -Credential $Credential
36
37 # Add the target location to the backup policy
38 Add-WBBackupTarget -Policy $Policy -Target $BackupLocation
39
40 # 4. Set backup policy schedule time and add it to the task scheduler
41 Set-WBSchedule -Policy $Policy -Schedule $BackupTime
42
43 # Add the backup policy to the backup server
44 Set-WBPolicy -Policy $Policy
45
46
```

PS C:\windows\system32>

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

The screenshot shows a Windows PowerShell ISE window titled "WindowsBackup.ps1". The code in the editor is identical to the previous screenshot. The output window shows the command being run: "# 4. Set backup policy schedule time and add it to the task scheduler Set-WBSchedule -Policy \$Policy -Schedule \$BackupTime". Below this, the system log shows the event "Wednesday, September 18, 2024 11:40:00 AM". The PowerShell prompt at the bottom is PS C:\windows\system32>.

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
WindowsBackup.ps1 | X
22 $Policy = New-WBPolicy
23 # Configure the path of the files to backup
24 $FileSpec = New-WBFileSpec -FileSpec "C:\"
25
26 # Add the file path to the backup policy
27 Add-WBFileSpec -Policy $Policy -FileSpec $FileSpec
28
29 # Prepare the Credential to access backup storage
30 $User = "administrator"
31 $SPWord = ConvertTo-SecureString -AsPlainText 'Aspire2' -Force
32 $Credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $User, $SPWord
33
34 # Configure the backup location
35 $BackupLocation = New-WBBackupTarget -NetworkPath $BackupNetworkPath -Credential $Credential
36
37 # Add the target location to the backup policy
38 Add-WBBackupTarget -Policy $Policy -Target $BackupLocation
39
40 # 4. Set backup policy schedule time and add it to the task scheduler
41 Set-WBSchedule -Policy $Policy -Schedule $BackupTime
42
43 # Add the backup policy to the backup server
44 Set-WBPolicy -Policy $Policy
45
46
```

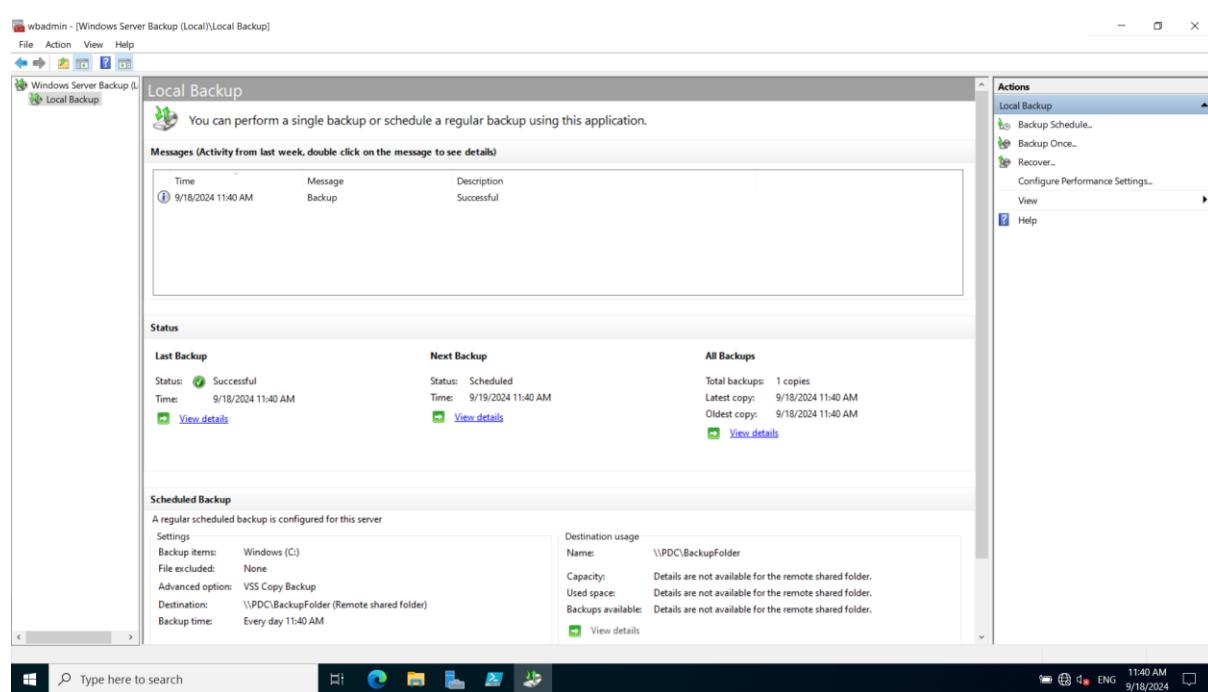
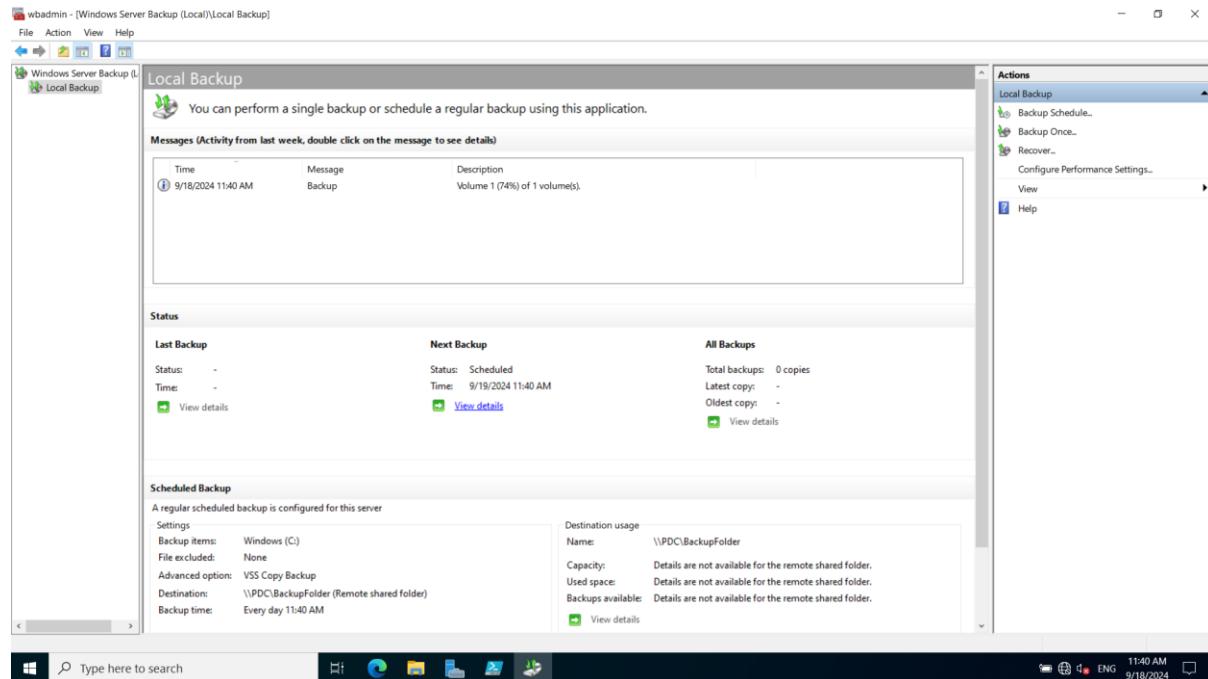
PS C:\windows\system32> # 4. Set backup policy schedule time and add it to the task scheduler
Set-WBSchedule -Policy \$Policy -Schedule \$BackupTime

Wednesday, September 18, 2024 11:40:00 AM

PS C:\windows\system32> # Add the backup policy to the backup server
Set-WBPolicy -Policy \$Policy

PS C:\windows\system32>

5. Check Backup status on Windows Server Backup console



6. Encrypt the backup folder after the backup finished.

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
WindowsBackup.ps1* X
35 # Configure the backup location
36 $BackupLocation = New-WBBackupTarget -NetworkPath $BackupNetworkPath -Credential $Credential
37
38 # Add the target location to the backup policy
39 Add-WBBackupTarget -Policy $Policy -Target $BackupLocation
40
41 # 4. Set backup policy schedule time and add it to the task scheduler
42 Set-WBSchedule -Policy $Policy -Schedule $BackupTime
43
44 # Add the backup policy to the backup server
45 Set-WBPolicy -Policy $Policy
46
47 # 5. Encrypt the backup folder after the backup finished.
48 Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Encrypt()}}
49
50 # 6. Decrypt the backup folder before to recover.
51 Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Decrypt()}}
52
53
# 4. Set backup policy schedule time and add it to the task scheduler
Set-WBSchedule -Policy $Policy -Schedule $BackupTime

Wednesday, September 18, 2024 11:40:00 AM

PS C:\windows\system32> # Add the backup policy to the backup server
Set-WBPolicy -Policy $Policy

PS C:\windows\system32> # 5. Encrypt the backup folder after the backup finished.
Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Encrypt()}}

PS C:\windows\system32>
```

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
WindowsBackup.ps1* X
35 # Configure the backup location
36 $BackupLocation = New-WBBackupTarget -NetworkPath $BackupNetworkPath -Credential $Credential
37
38 # Add the target location to the backup policy
39 Add-WBBackupTarget
40 # 4. Set backup policy
41 Set-WBSchedule -Policy $Policy -Schedule $BackupTime
42
43 # Add the backup policy to the backup server
44 Set-WBPolicy -Policy $Policy
45
46 # 5. Encrypt the backup folder after the backup finished.
47 Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Encrypt()}}
48
49 # 6. Decrypt the backup folder before to recover.
50 Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Decrypt()}}
51
52
# 4. Set backup policy schedule time and add it to the task scheduler
Set-WBSchedule -Policy $Policy -Schedule $BackupTime

Wednesday, September 18, 2024 11:40:00 AM

PS C:\windows\system32> # Add the backup policy to the backup server
Set-WBPolicy -Policy $Policy

PS C:\windows\system32> # Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Encrypt()}}

PS C:\windows\system32>
```

7. Decrypt the backup folder before to recover.

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
WindowsBackup.ps1* | X
35 # Configure the backup location
36 $BackupLocation = New-WBBackupTarget -NetworkPath $BackupNetworkPath -Credential $Credential
37
38 # Add the target location to the backup policy
39 Add-WBBackupTarget -Policy $Policy -Target $BackupLocation
40
41 # 4. Set backup policy schedule time and add it to the task scheduler
42 Set-WBSchedule -Policy $Policy -Schedule $BackupTime
43
44 # Add the backup policy to the backup server
45 Set-WBPolicy -Policy $Policy
46
47 # 5. Encrypt the backup folder after the backup finished.
48 Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Encrypt()}}
49
50 # 6. Decrypt the backup folder before to recover.
51 Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Decrypt()}}
52
53

```

wednesday, September 18, 2024 11:40:00 AM

```

PS C:\windows\system32> # Add the backup policy to the backup server
Set-WBPolicy -Policy $Policy

PS C:\windows\system32> # 5. Encrypt the backup folder after the backup finished.
Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Encrypt()}}

PS C:\windows\system32> # 6. Decrypt the backup folder before to recover.
Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Decrypt()}}

PS C:\windows\system32>

```

Completed

Type here to search

Ln 156 Col 25 | 115% 11:46 AM 9/18/2024

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
WindowsBackup.ps1* | X
35 # Configure the backup location
36 $BackupLocation = New-WBBackupTarget -NetworkPath $BackupNetworkPath -Credential $Credential
37
38 # Add the target location to the backup policy
39 Add-WBBackupTarget -Policy $Policy -Target $BackupLocation
40
41 # 4. Set backup policy schedule time and add it to the task scheduler
42 Set-WBSchedule -Policy $Policy -Schedule $BackupTime
43
44 # Add the backup policy to the backup server
45 Set-WBPolicy -Policy $Policy
46
47 # 5. Encrypt the backup folder after the backup finished.
48 Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Encrypt()}}
49
50 # 6. Decrypt the backup folder before to recover.
51 Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Decrypt()}}
52
53

```

wednesday, September 18, 2024 11:40:00 AM

```

PS C:\windows\system32> # Add the backup policy to the backup server
Set-WBPolicy -Policy $Policy

PS C:\windows\system32> Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Encrypt()}}

PS C:\windows\system32> Get-ChildItem -Path $BackupNetworkPath -Recurse |Where-Object { if($_.GetType().Name -eq "FileInfo") {$_..Decrypt()}}

PS C:\windows\system32>

```

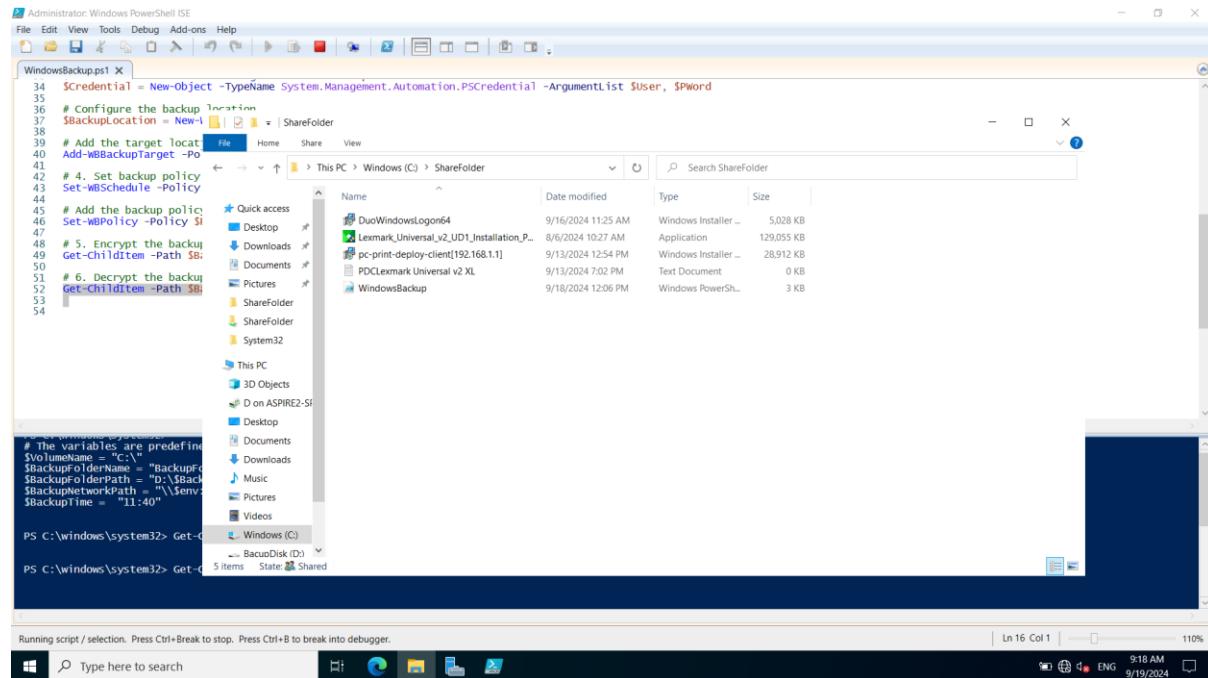
Completed

Type here to search

Ln 156 Col 25 | 115% 11:47 AM 9/18/2024

8. Recover a specified folder from a backup

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



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
WindowsBackup.ps1
34 $Credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $User, $Password
35
36 # Configure the backup location
37 $BackupLocation = New-Item -Path "D:\$env:TEMP\ShareFolder"
38
39 # Add the target location
40 Add-WBBackupTarget -Path $BackupLocation
41
42 # 4. Set backup policy
43 Set-WBSchedule -Policy $Policy
44
45 # Add the backup policy
46 Set-WBPolicy -Policy $Policy
47
48 # 5. Encrypt the backup
49 Get-ChildItem -Path $BackupLocation
50
51 # 6. Decrypt the backup
52 Get-ChildItem -Path $BackupLocation
53
54
```

The variables are predefined:

```
$env:TEMP = "D:\$env:TEMP\ShareFolder"
$BackupFolderPath = "D:\$env:TEMP\ShareFolder"
$BackupNetworkPath = "\\$env:COMPUTERNAME\ShareFolder"
$BackupTime = "11:40"
```

PS C:\windows\system32> Get-ChildItem -Path \$BackupFolderPath

PS C:\windows\system32> Get-ChildItem -Path \$BackupNetworkPath

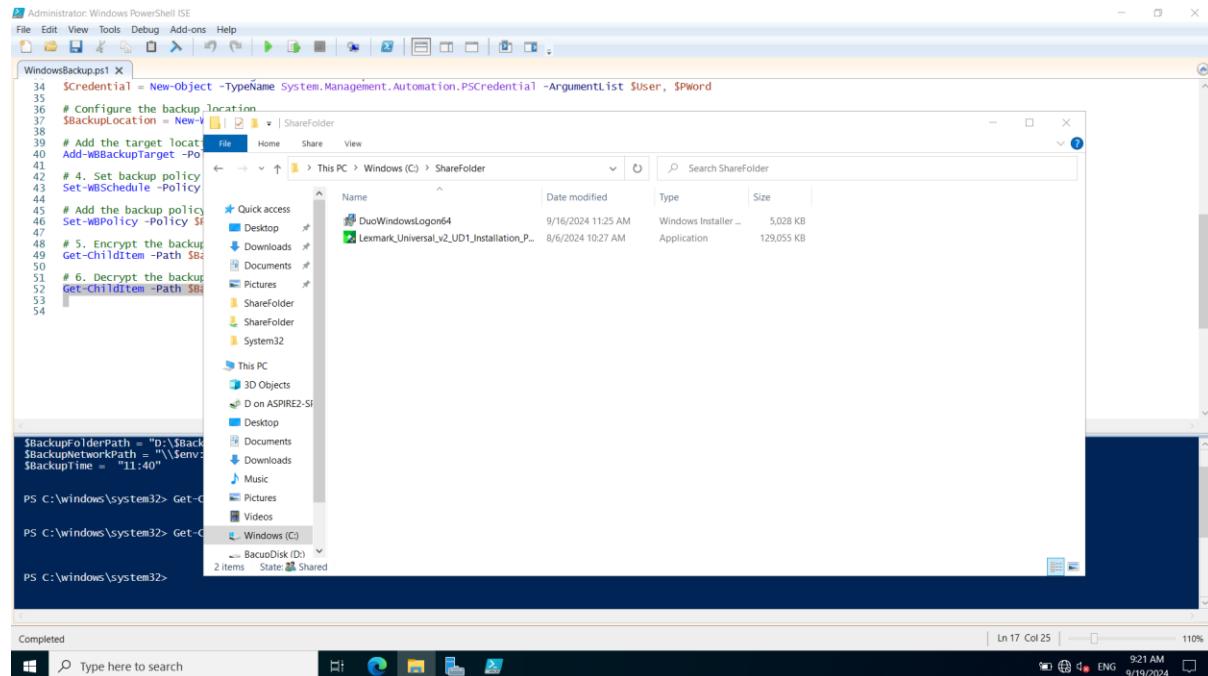
Running script / selection. Press Ctrl+Break to stop. Press Ctrl+B to break into debugger.

Type here to search

Ln 16 Col 1 110%

9:18 AM 9/19/2024

Then 3 files are deleted accidentally:



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
WindowsBackup.ps1
34 $Credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $User, $Password
35
36 # Configure the backup location
37 $BackupLocation = New-Item -Path "D:\$env:TEMP\ShareFolder"
38
39 # Add the target location
40 Add-WBBackupTarget -Path $BackupLocation
41
42 # 4. Set backup policy
43 Set-WBSchedule -Policy $Policy
44
45 # Add the backup policy
46 Set-WBPolicy -Policy $Policy
47
48 # 5. Encrypt the backup
49 Get-ChildItem -Path $BackupLocation
50
51 # 6. Decrypt the backup
52 Get-ChildItem -Path $BackupLocation
53
54
```

\$BackupFolderPath = "D:\\$env:TEMP\ShareFolder"
\$BackupNetworkPath = "\\\$env:COMPUTERNAME\ShareFolder"
\$BackupTime = "11:40"

PS C:\windows\system32> Get-ChildItem -Path \$BackupFolderPath

PS C:\windows\system32> Get-ChildItem -Path \$BackupNetworkPath

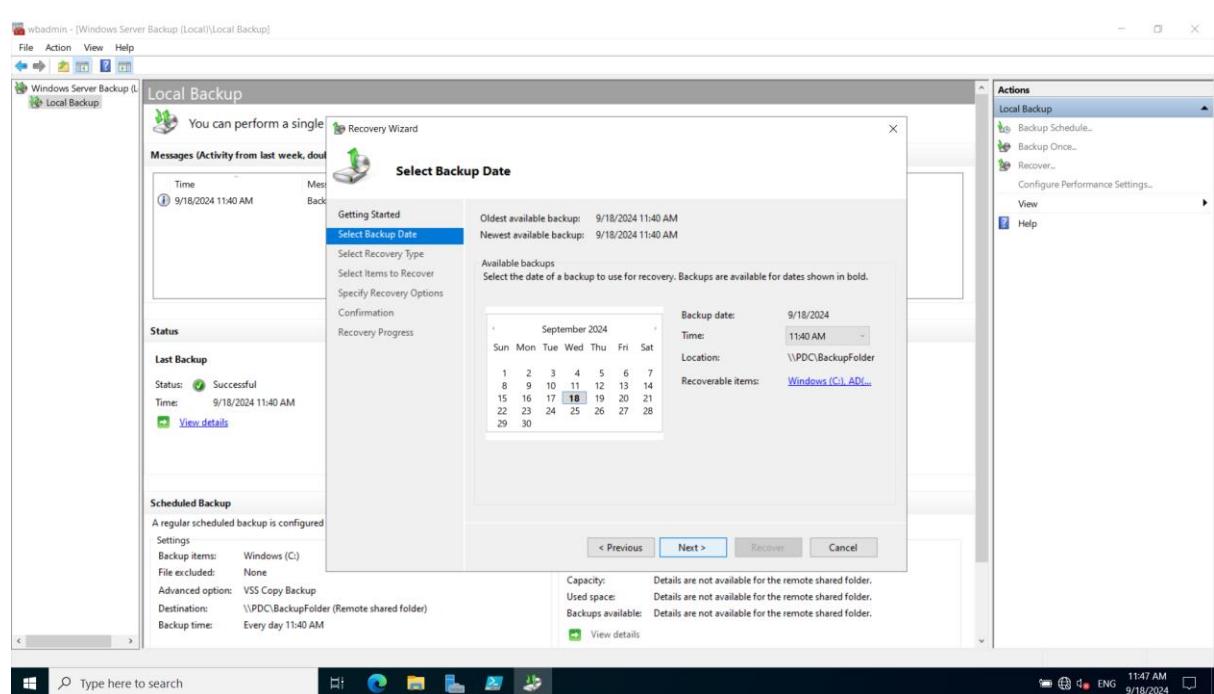
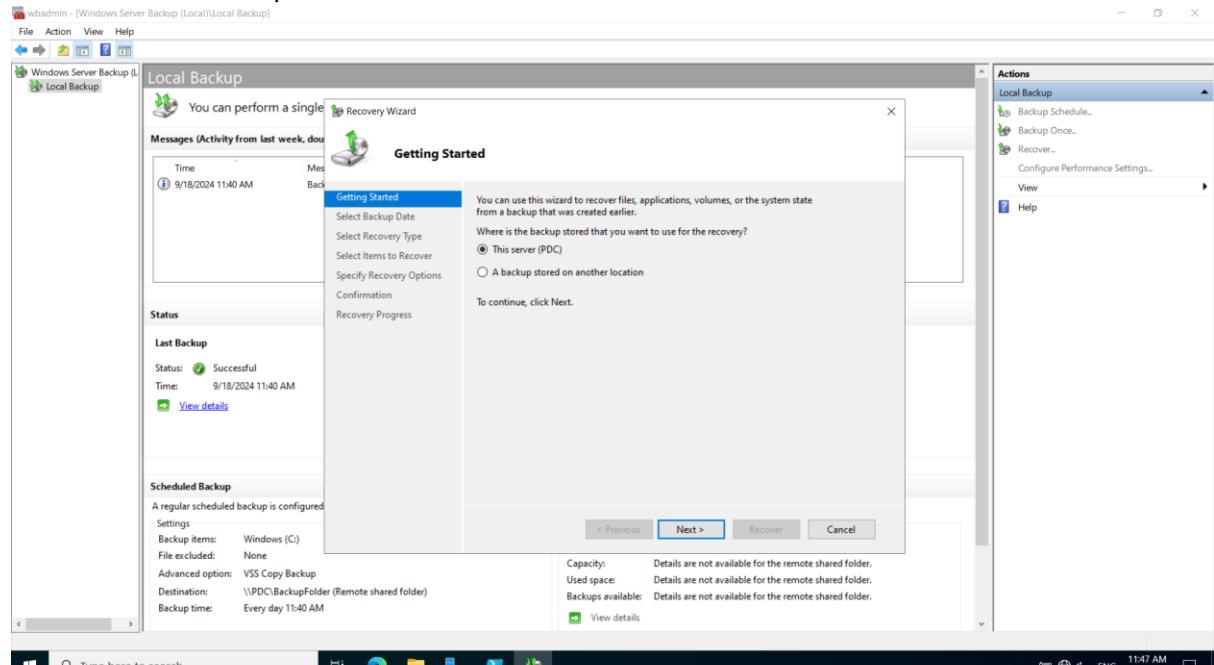
Completed

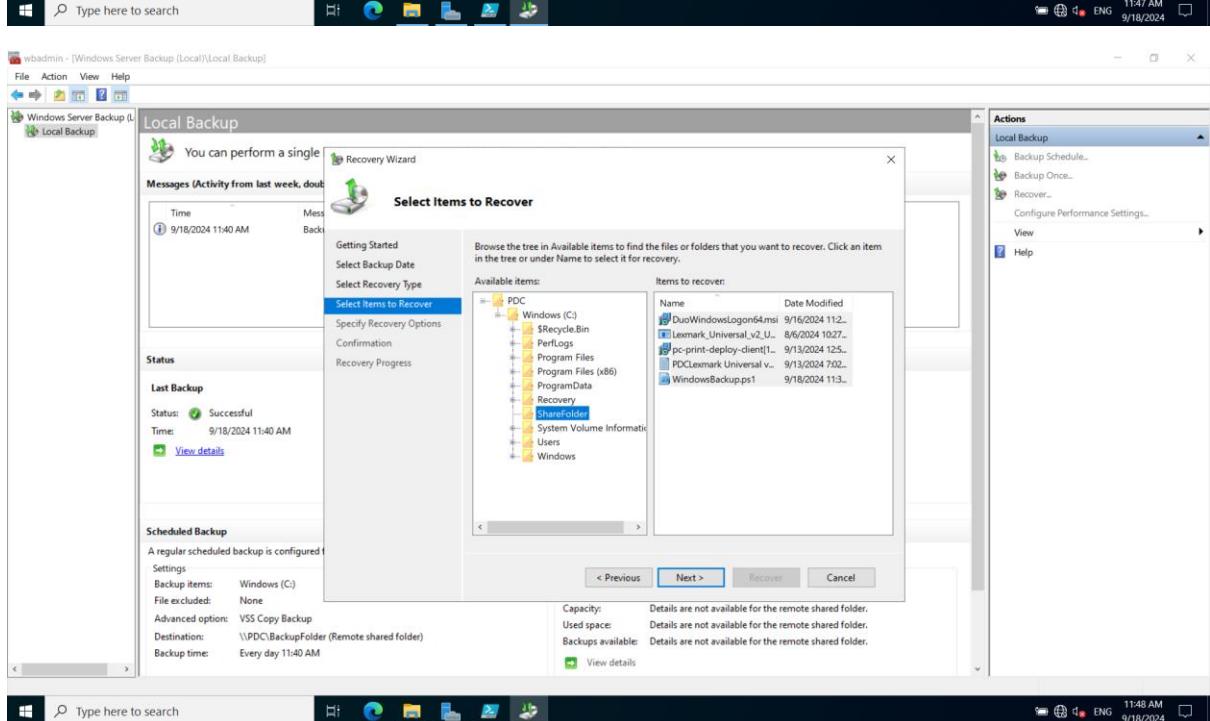
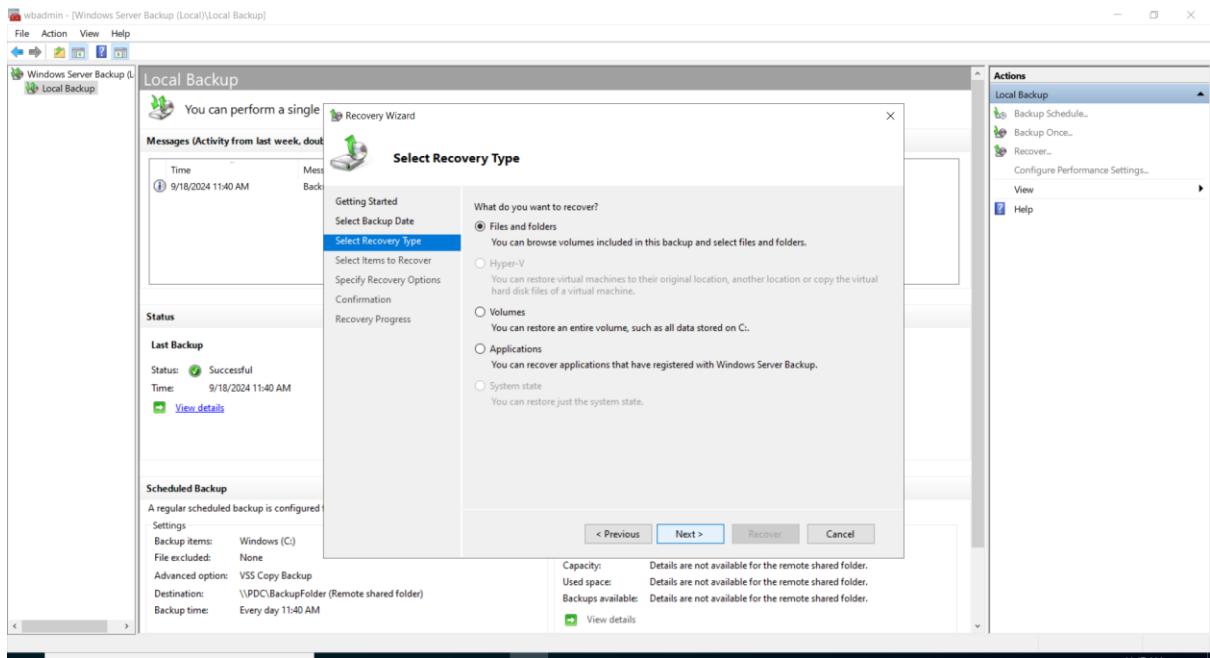
Type here to search

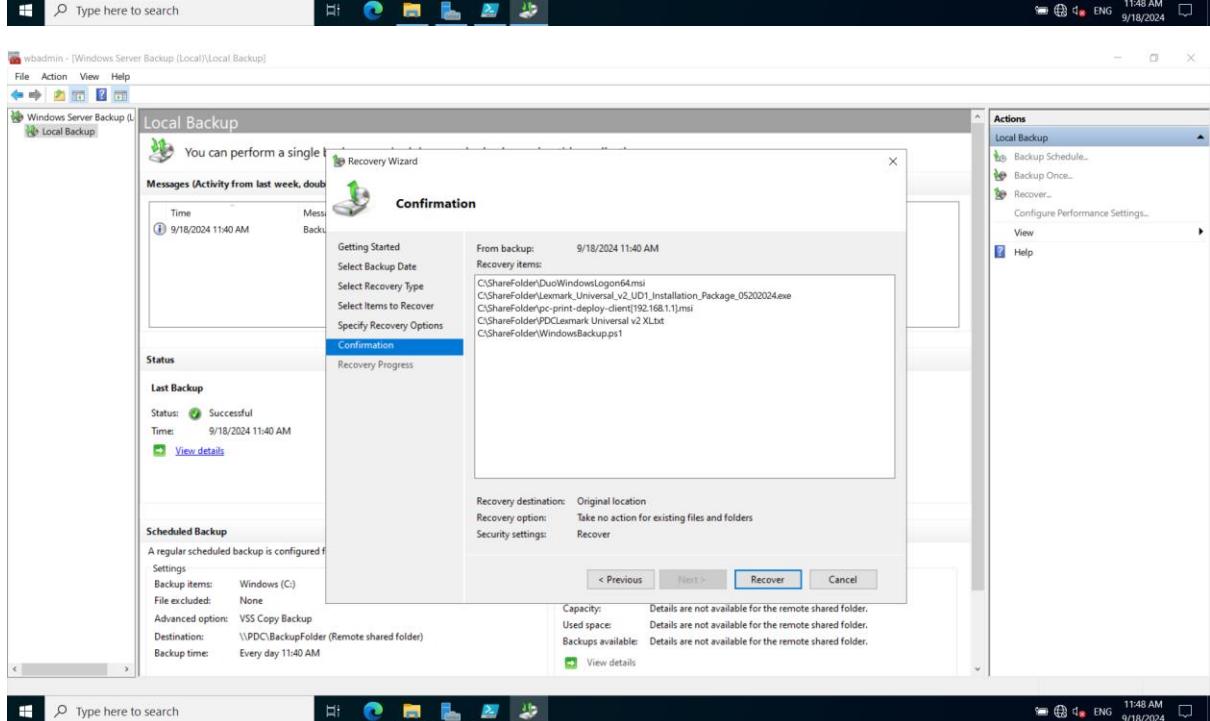
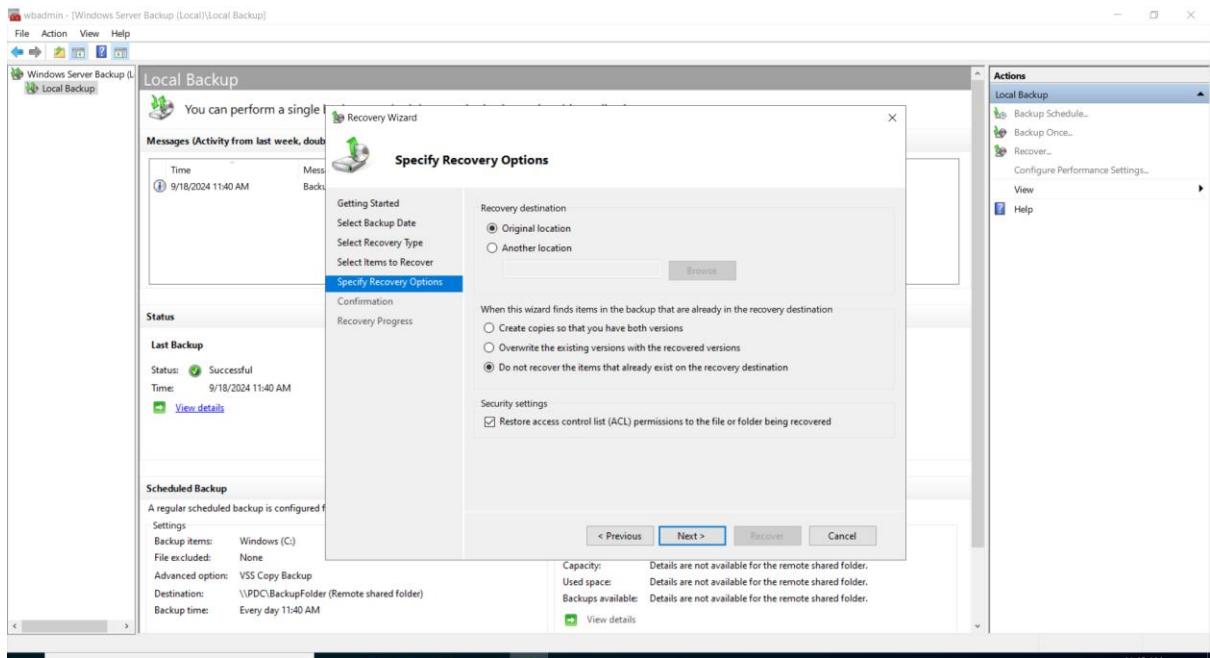
Ln 17 Col 25 110%

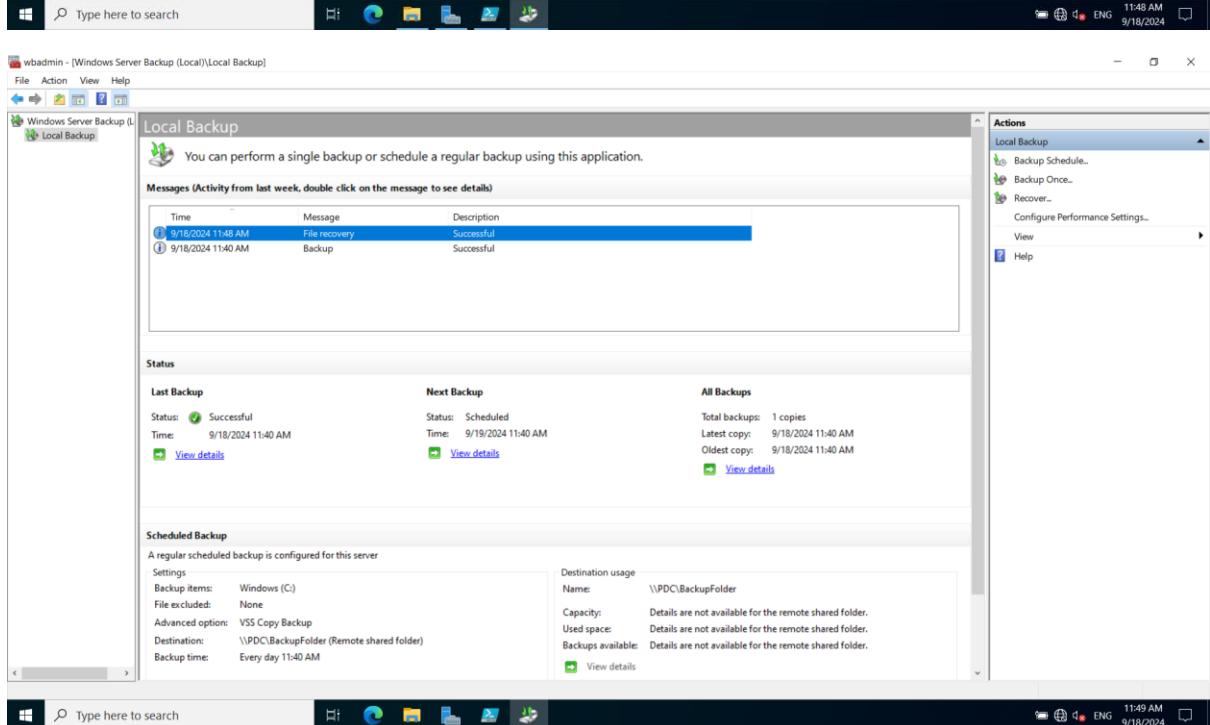
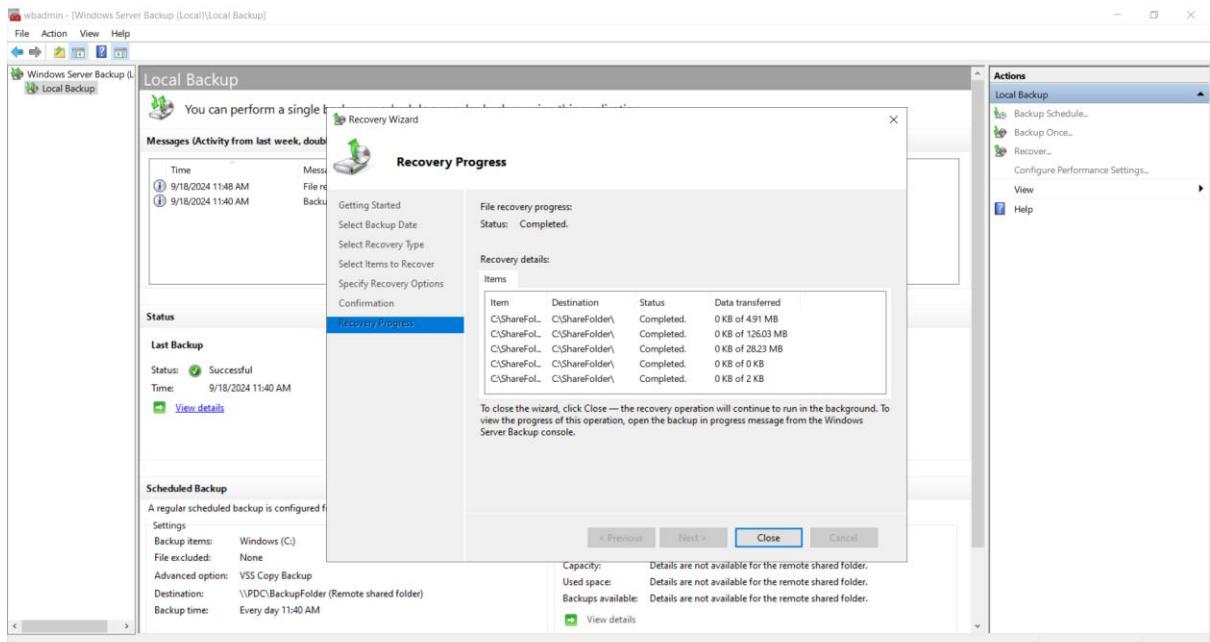
9:18 AM 9/19/2024

Start a new recover process:

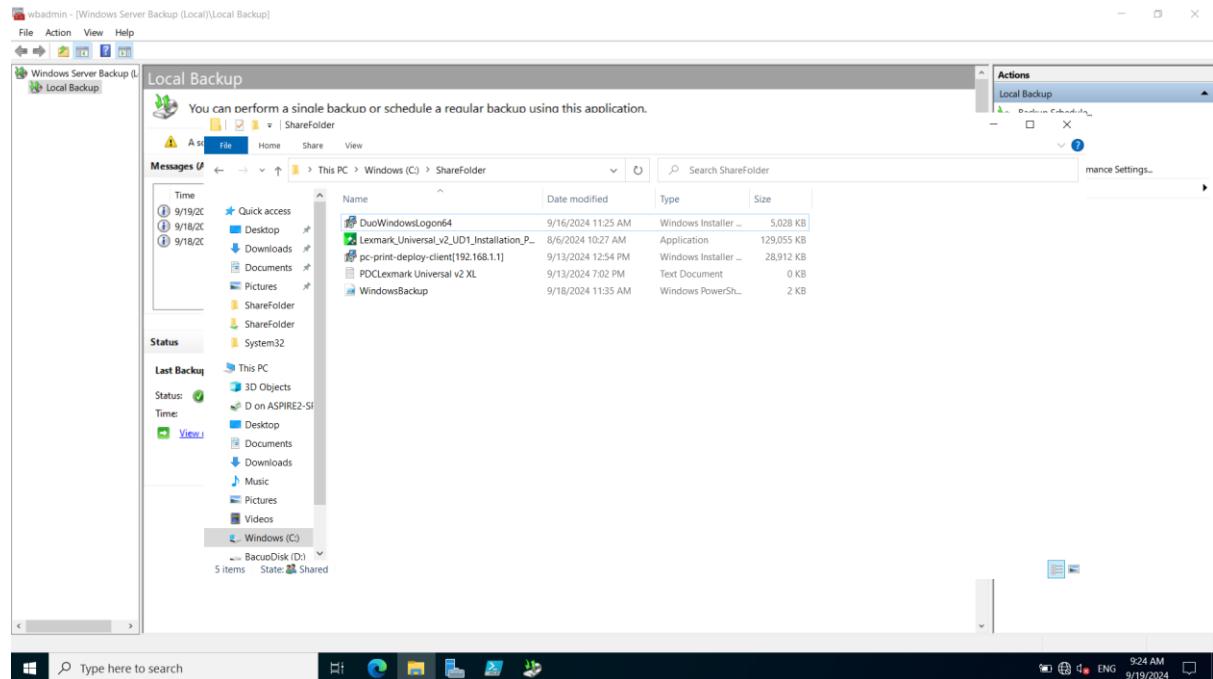








The 3 files deleted accidentally have been recovered to the original place:



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

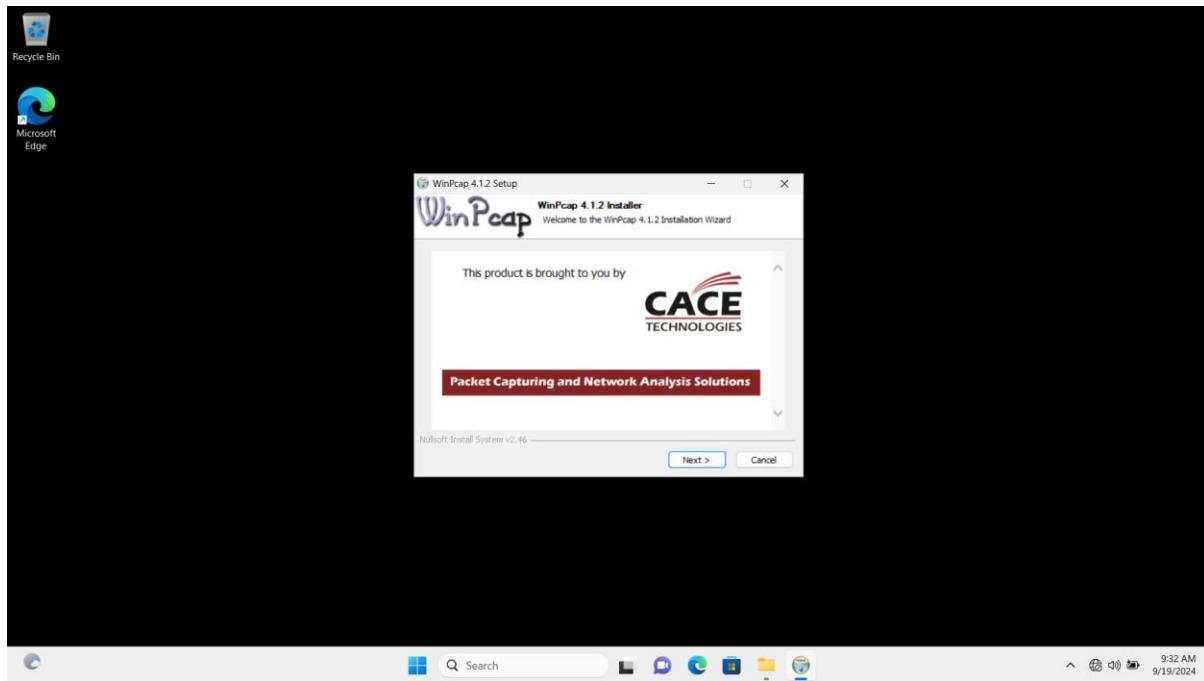
Task 6.1: IDS Deployment and Configuration

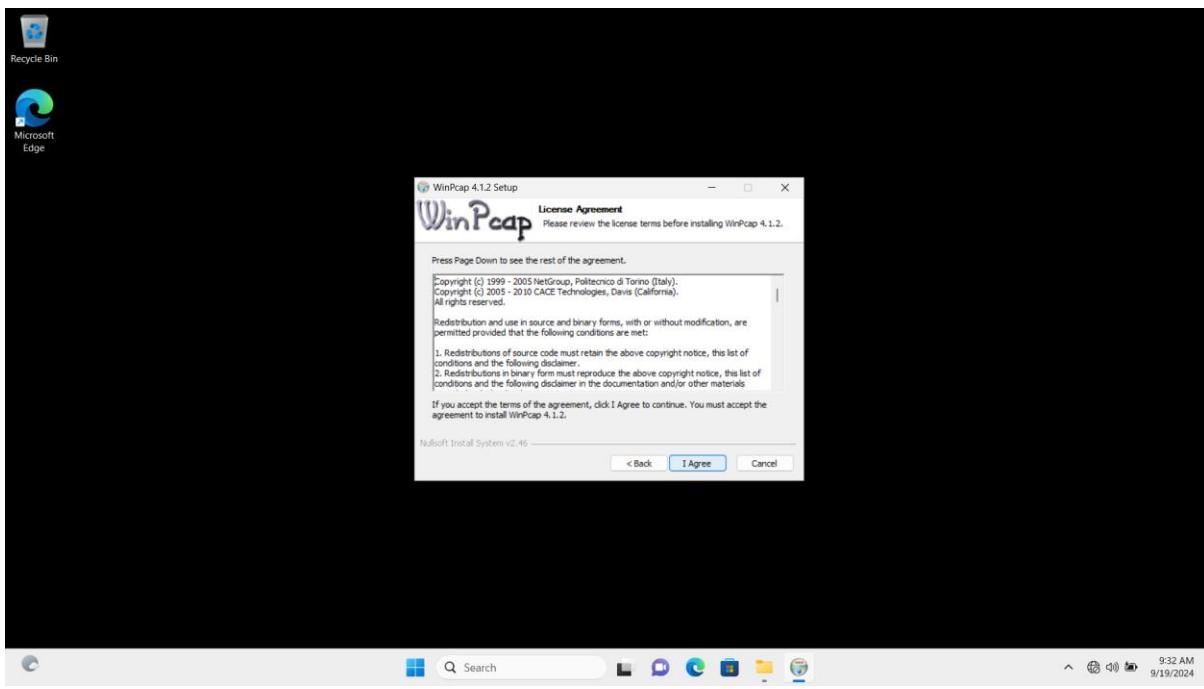
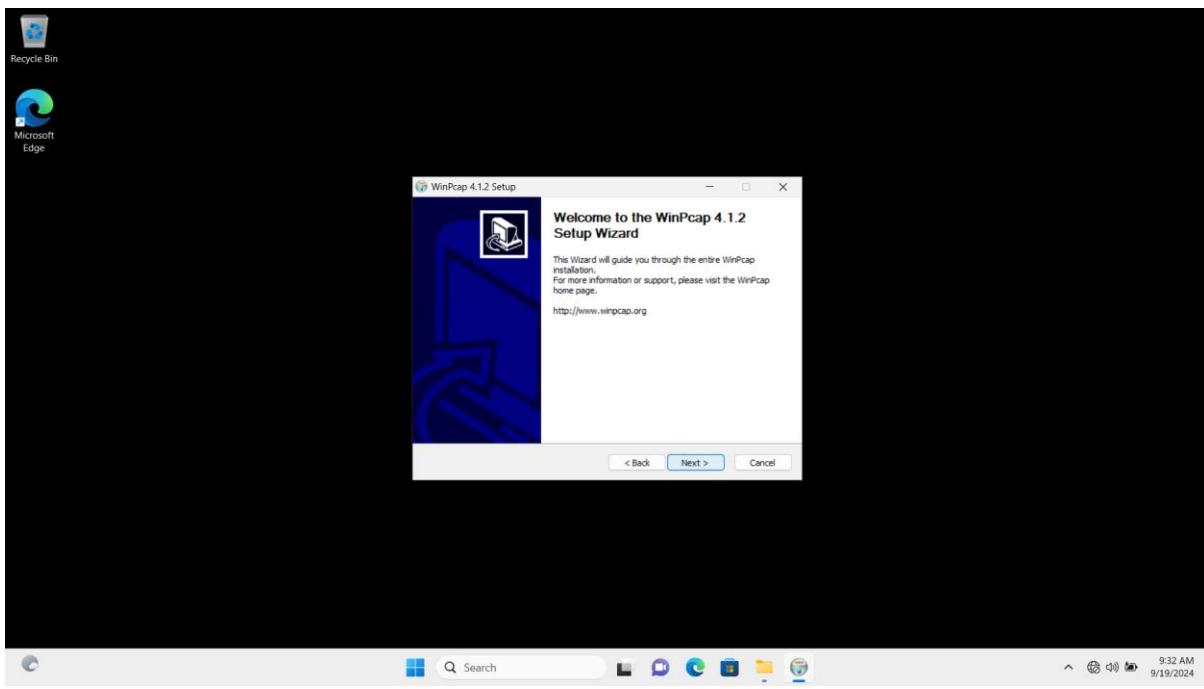
Snort is chosen as IDS solution for TechCo Solutions because it is cost effective, flexibility and strong community support.

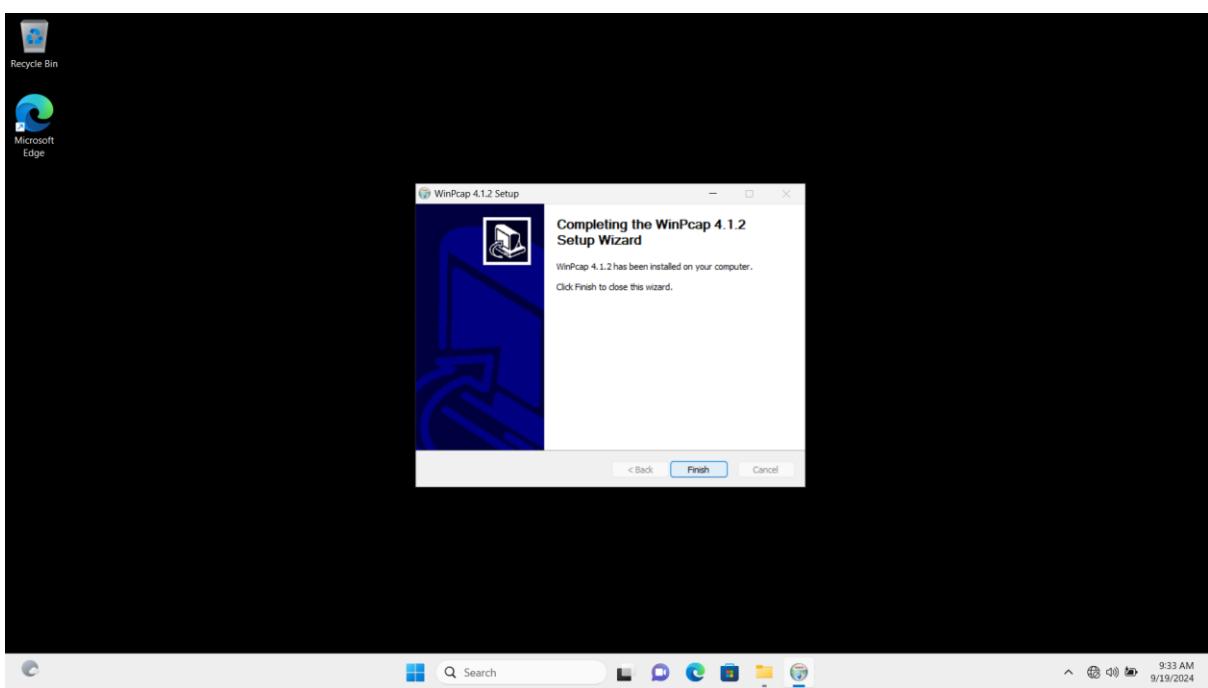
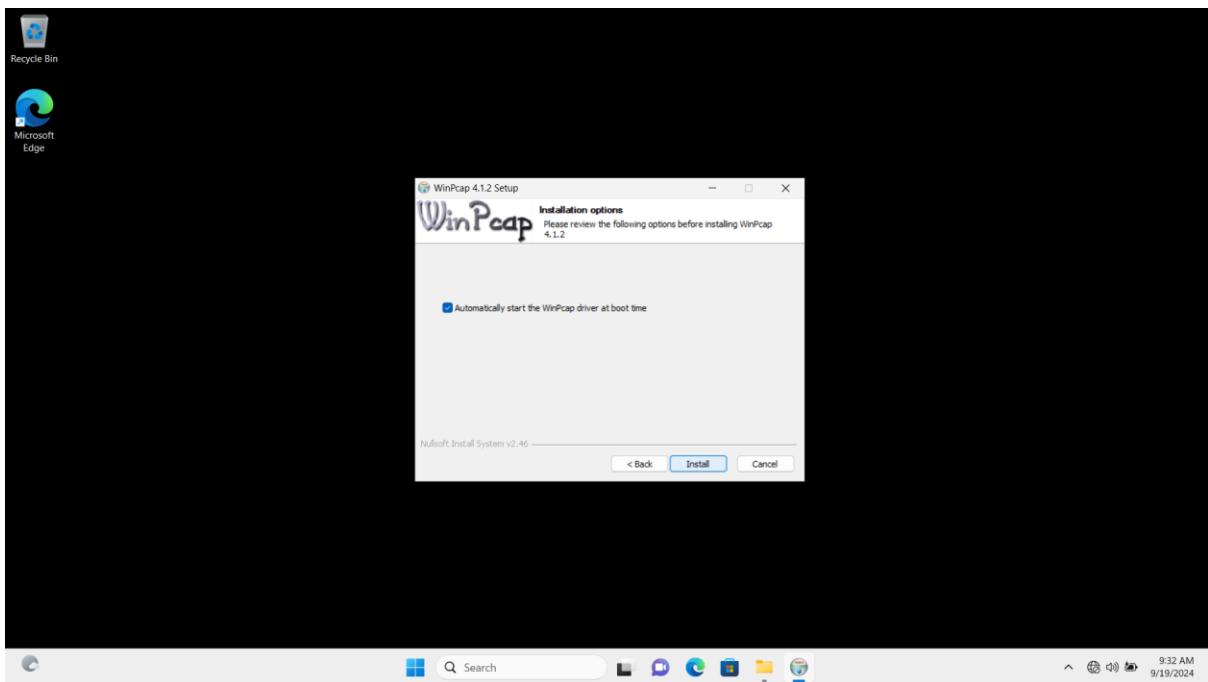
- Low cost. Snort is an open-source software, and it is free and no license fee.
- Ease of use and deployment. Snort has good documentation and strong community support.
- Completed rules sets. Snort provides a lot of detection rules and update rules set regularly.

1. Install WinPcap

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

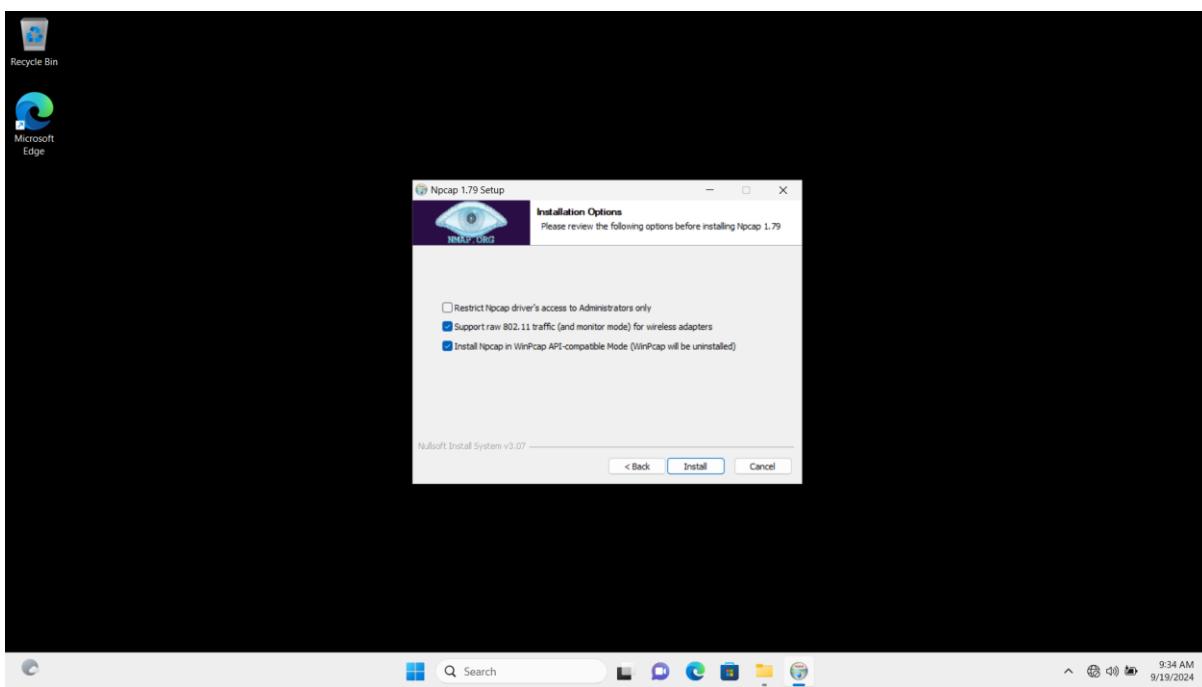
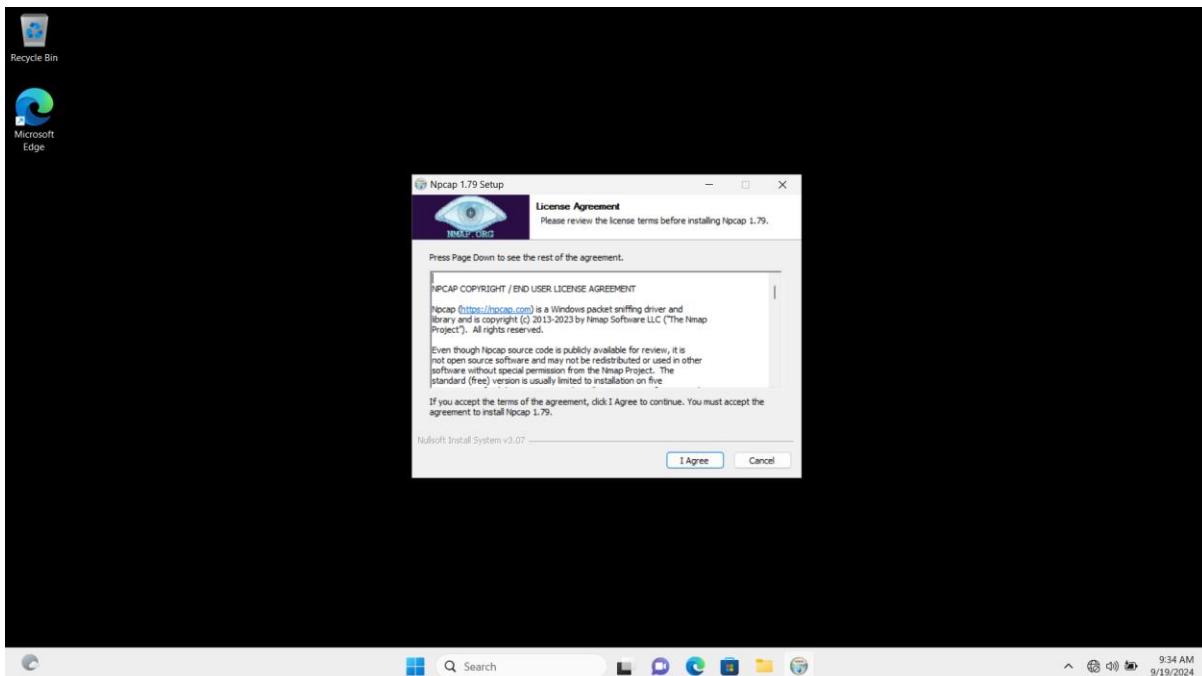


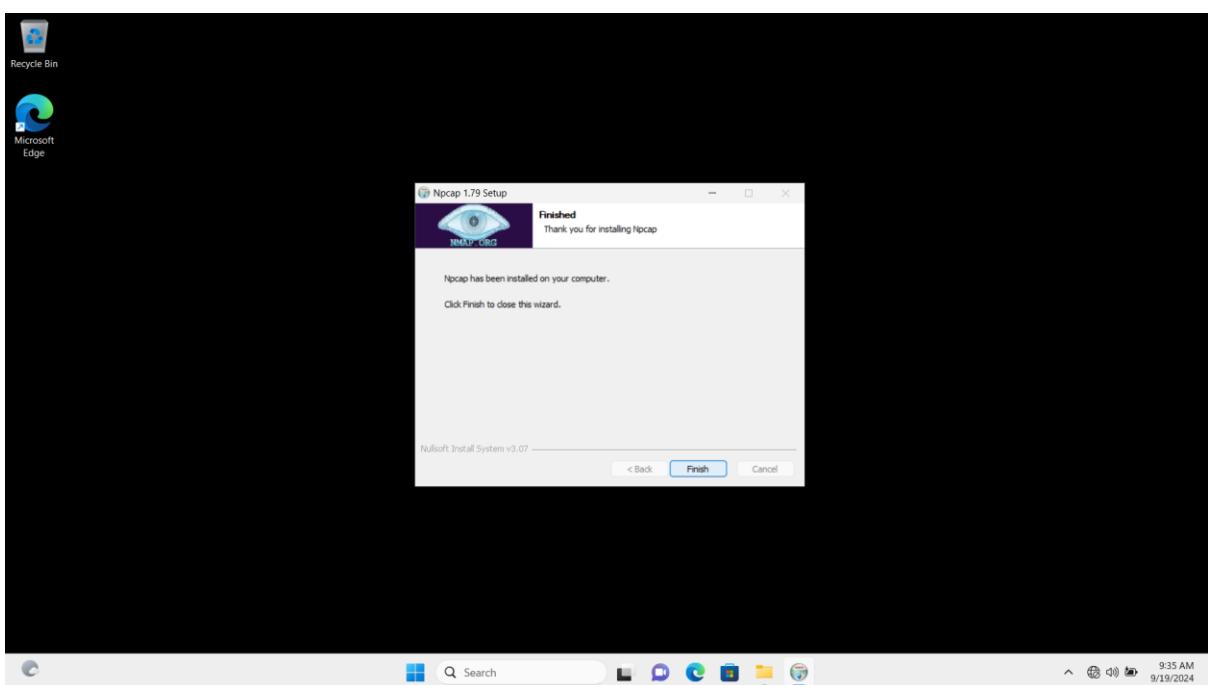
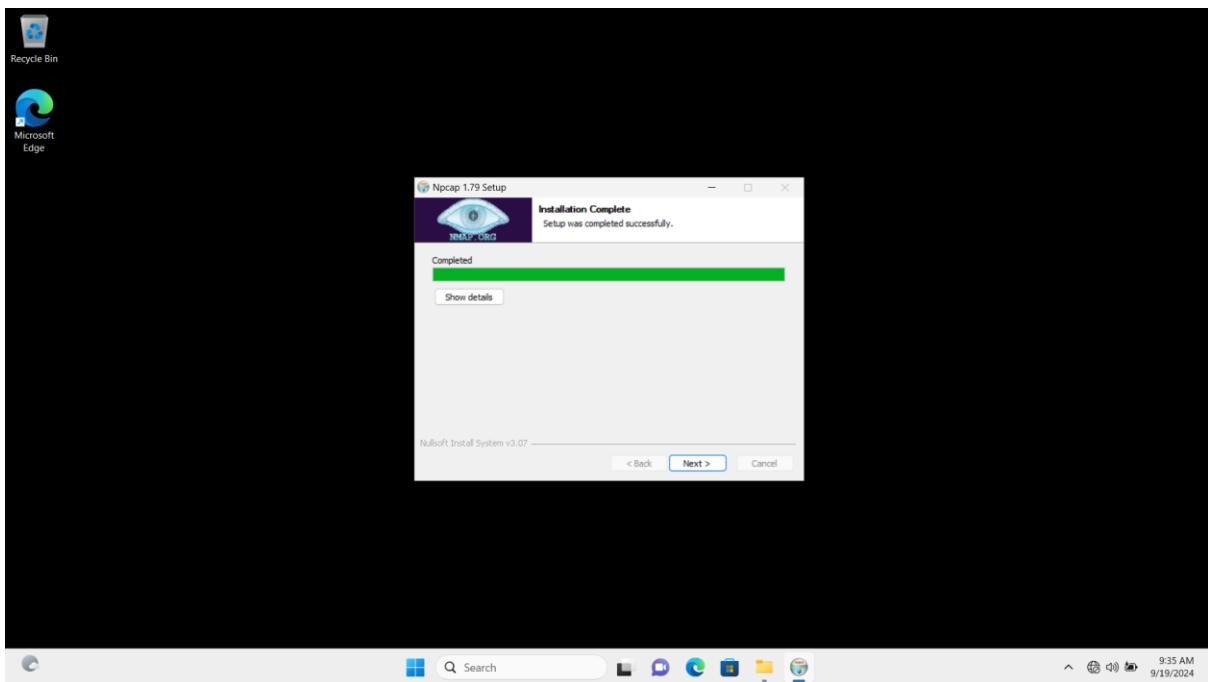




2. Install Npcap

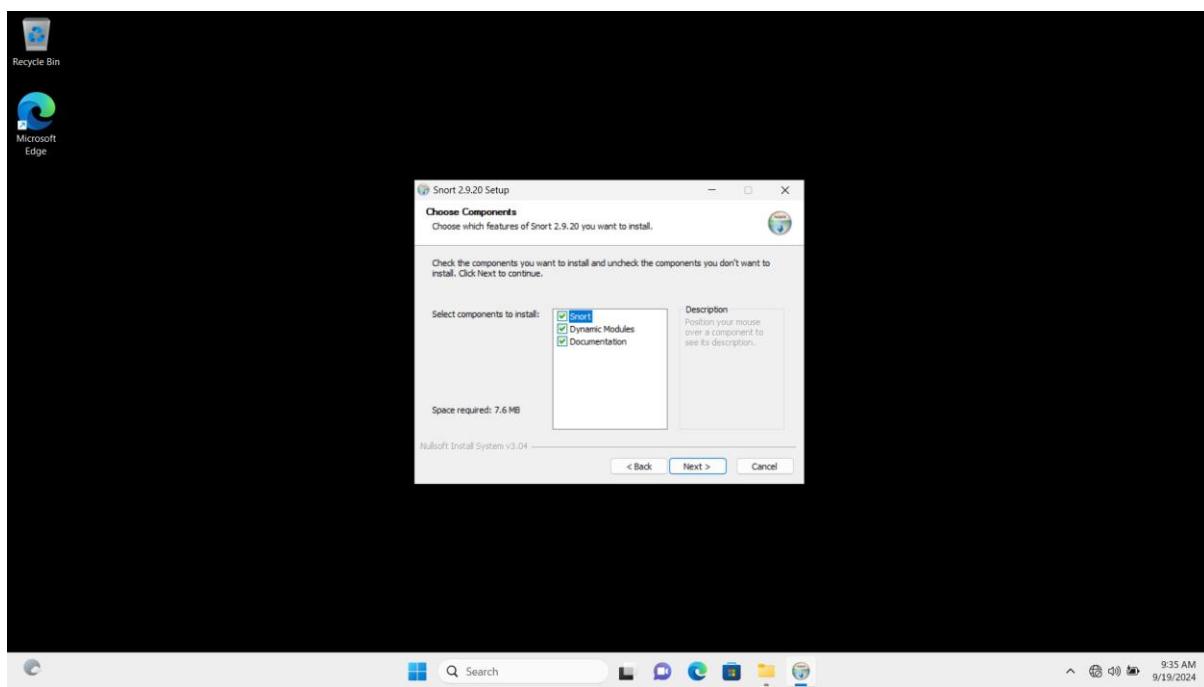
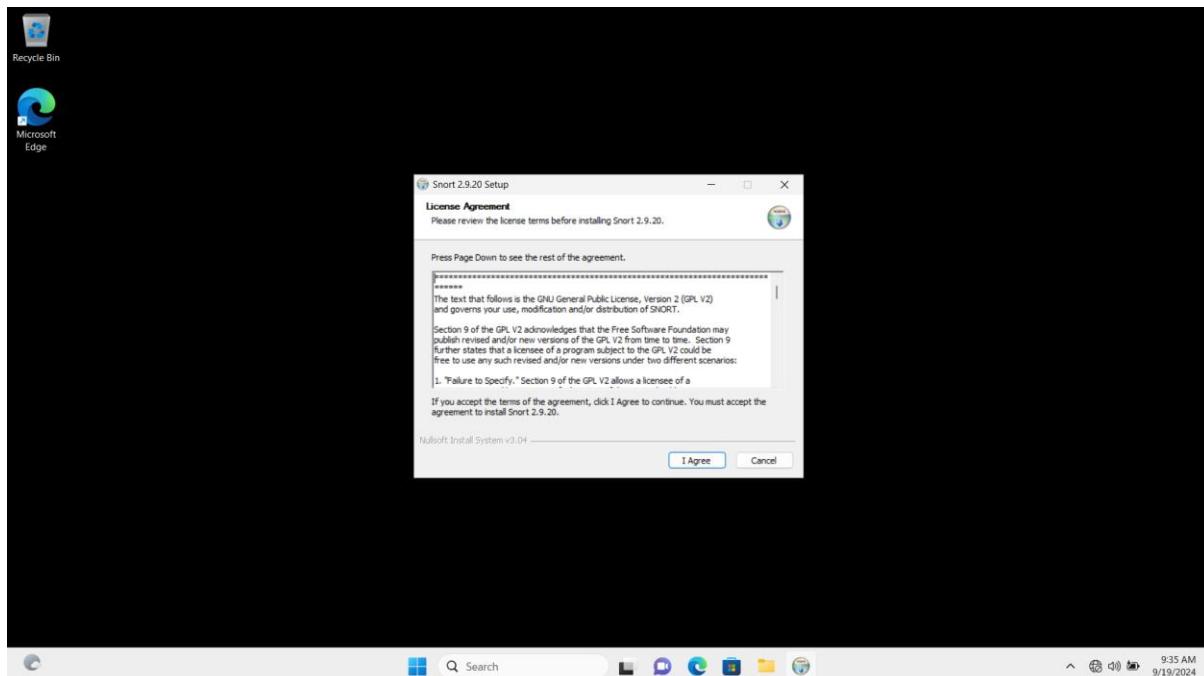
<https://npcap.com/dist/npcap-1.79.exe>

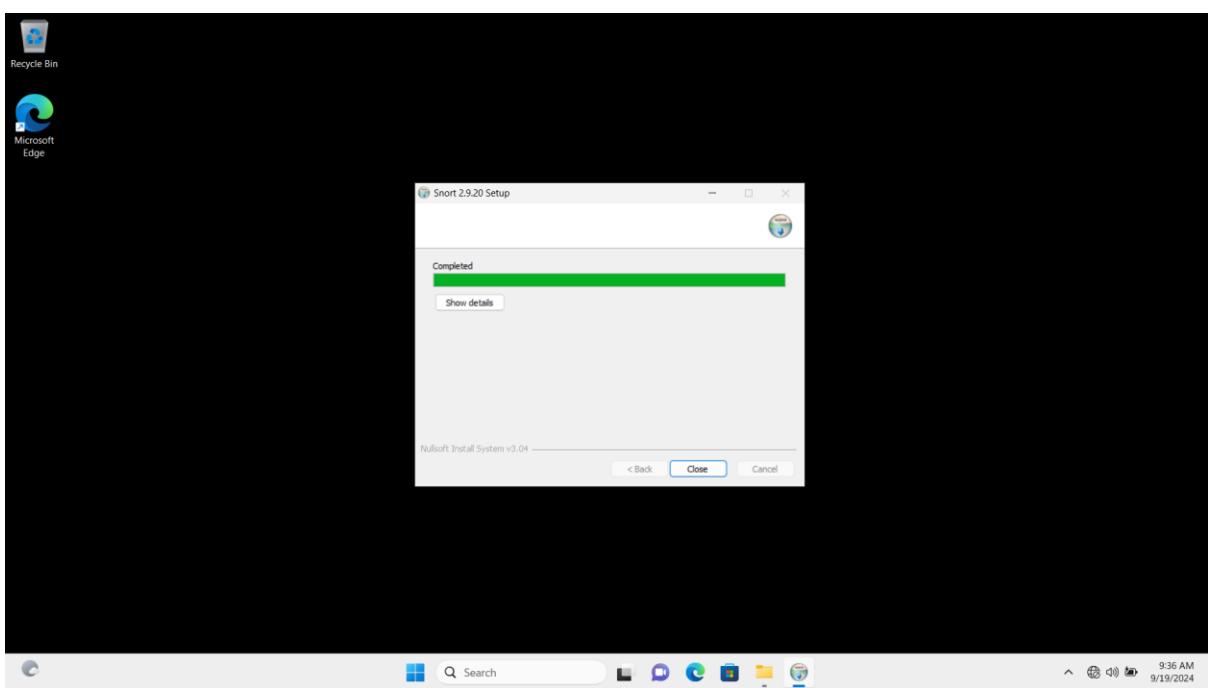
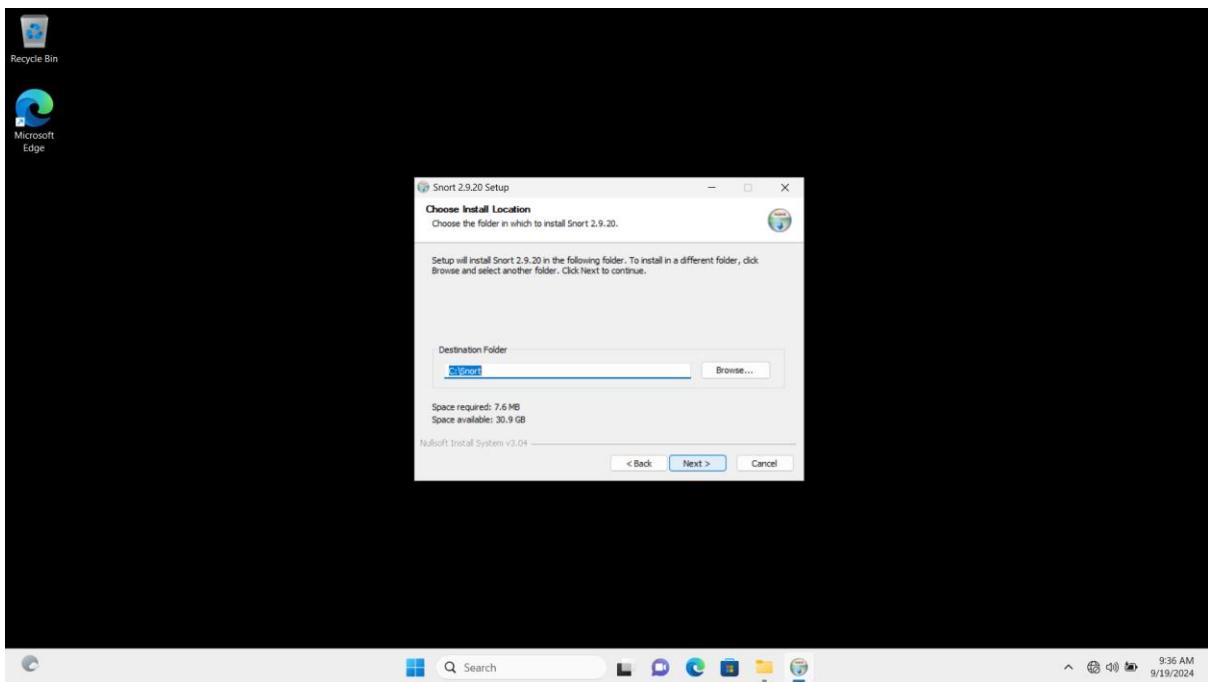


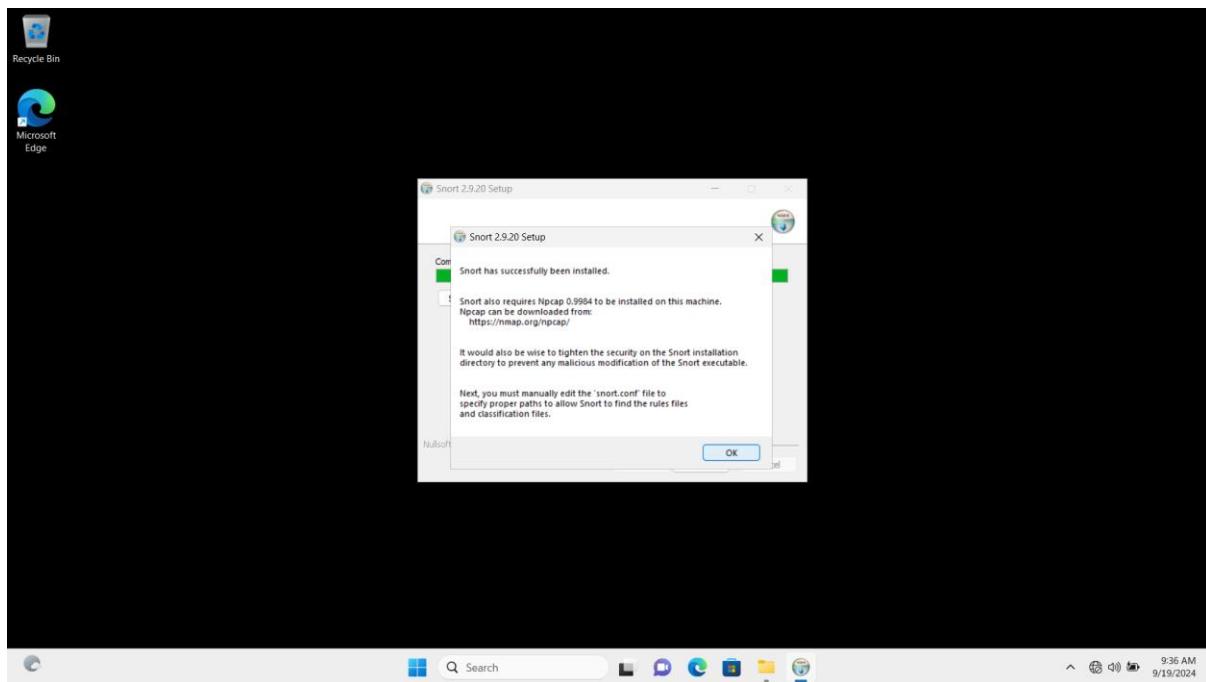


3. Install Snort

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

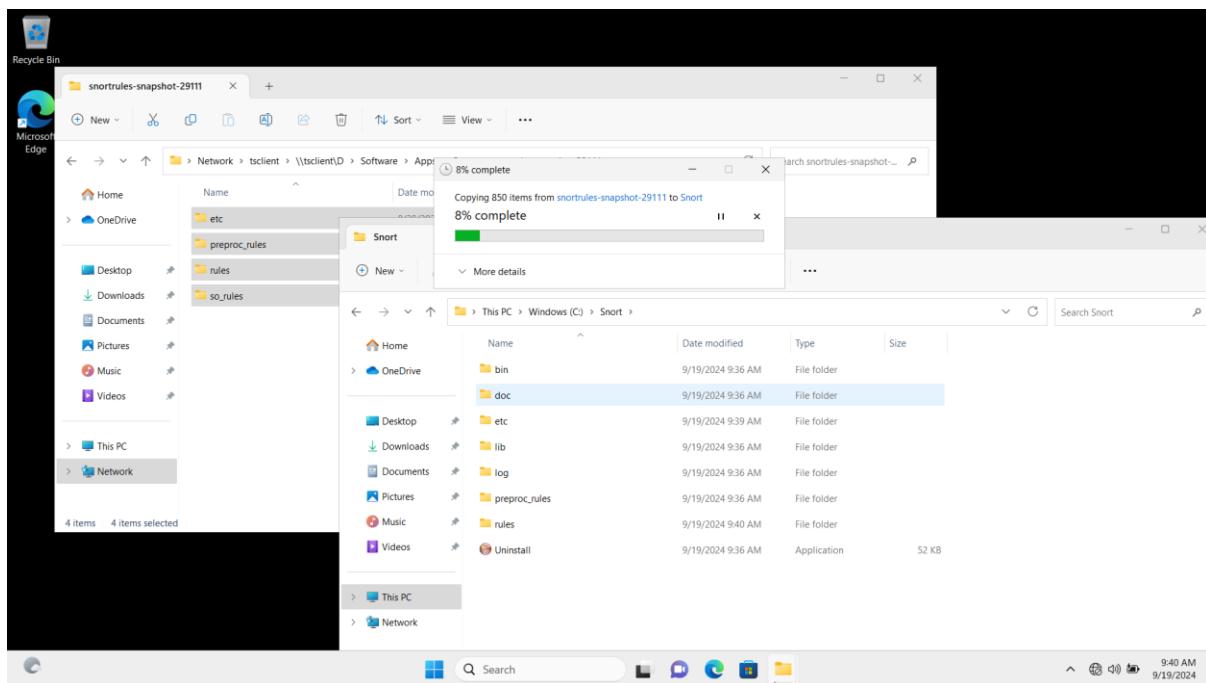






4. Download Snort Rules to local snort folder

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



5. Configure Snort

- Set the network variables

The screenshot shows a Windows desktop environment. In the background, there is a Command Prompt window titled "Windows IP Configuration" which displays basic network information for an "Ethernet adapter Ether". In the foreground, there is a Notepad window titled "*snort.conf - Notepad" containing the Snort configuration file. The file includes sections for setting network variables, defining protected networks, and listing DNS and SMTP servers.

```
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\spark>ipconfig

Windows IP Configuration

Ethernet adapter Ether

Connection-specific Link-local IPv6 Address . . .
IPv4 Address . . .
Subnet Mask . . .
Default Gateway . . .

C:\Users\spark>

*snort.conf - Notepad

File Edit View

# 1) Set the network variables.
# 2) Configure the decoder
# 3) Configure the base detection engine
# 4) Configure dynamic loaded libraries
# 5) Configure preprocessors
# 6) Configure output plugins
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####
#
# Step #1: Set the network variables. For more information, see README.variables
#####

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.1.0/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

Ln 46, Col 1
100% Unix (LF) UTF-8
ENG US 9:50 am 19/09/2024
```

- Set the path of rules

The screenshot shows a Windows desktop environment. In the background, there is a Command Prompt window titled "Windows IP Configuration" which displays basic network information for an "Ethernet adapter Ether". In the foreground, there is a Notepad window titled "*snort.conf - Notepad" containing the Snort configuration file. The "Path to your rules files" section is highlighted with a blue selection bar.

```
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\spark>ipconfig

Windows IP Configuration

Ethernet adapter Ether

Connection-specific Link-local IPv6 Address . . .
IPv4 Address . . .
Subnet Mask . . .
Default Gateway . . .

C:\Users\spark>

*snort.conf - Notepad

File Edit View

portvar SIP_PORTS [5060,5061,5600]
# List of file data ports for file inspection
portvar FILE_DATA_PORTS [$HTTP_PORTS,110,143]

# List of GTP ports for GTP preprocessor
portvar GTP_PORTS [2123,2152,3386]

# other variables, these should not be modified
ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24]

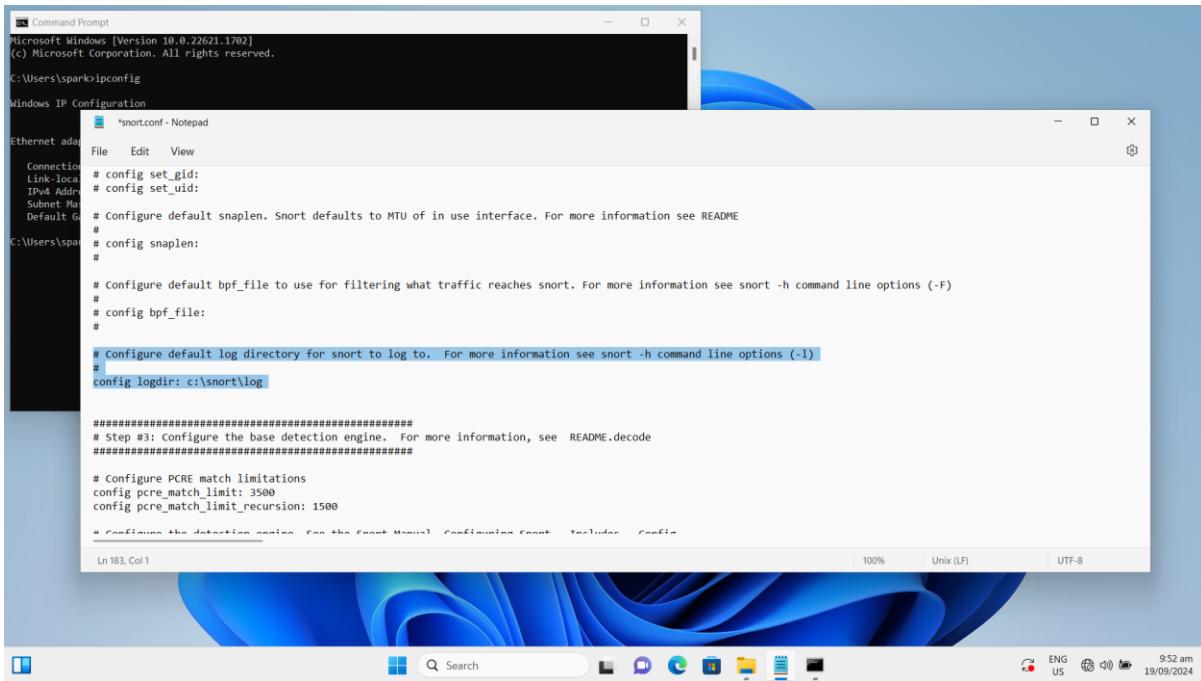
# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snort\rules
var RULE_PATH c:\snort\rules
var SO_RULE_PATH c:\snort\so_rules
var PREPROC_RULE_PATH c:\snort\preproc_rules

# If you are using reputation preprocessor set these
var WHITE_LIST_PATH c:\snort\rules
var BLACK_LIST_PATH c:\snort\rules

#####
#
# Step #2: Configure the decoder. For more information, see README.decode
#####

# Start snortrc, decode counter
Ln 112, Col 1
100% Unix (LF) UTF-8
ENG US 9:52 am 19/09/2024
```

- Set the path of log file



```

Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\spark>ipconfig

Windows IP Configuration

File Edit View
Connection Link-local IPv4 Address Subnet Mask Default Gateway
# config set_gid: # config set_uid:
# Configure default snaplen. Snort defaults to MTU of in use interface. For more information see README
# config snaplen:
#
# Configure default bpf_file to use for filtering what traffic reaches snort. For more information see snort -h command line options (-F)
# config bpf_file:
#
# Configure default log directory for snort to log to. For more information see snort -h command line options (-l)
# config logdir: c:\snort\log

#####
# Step #3: Configure the base detection engine. For more information, see README.decode
#####

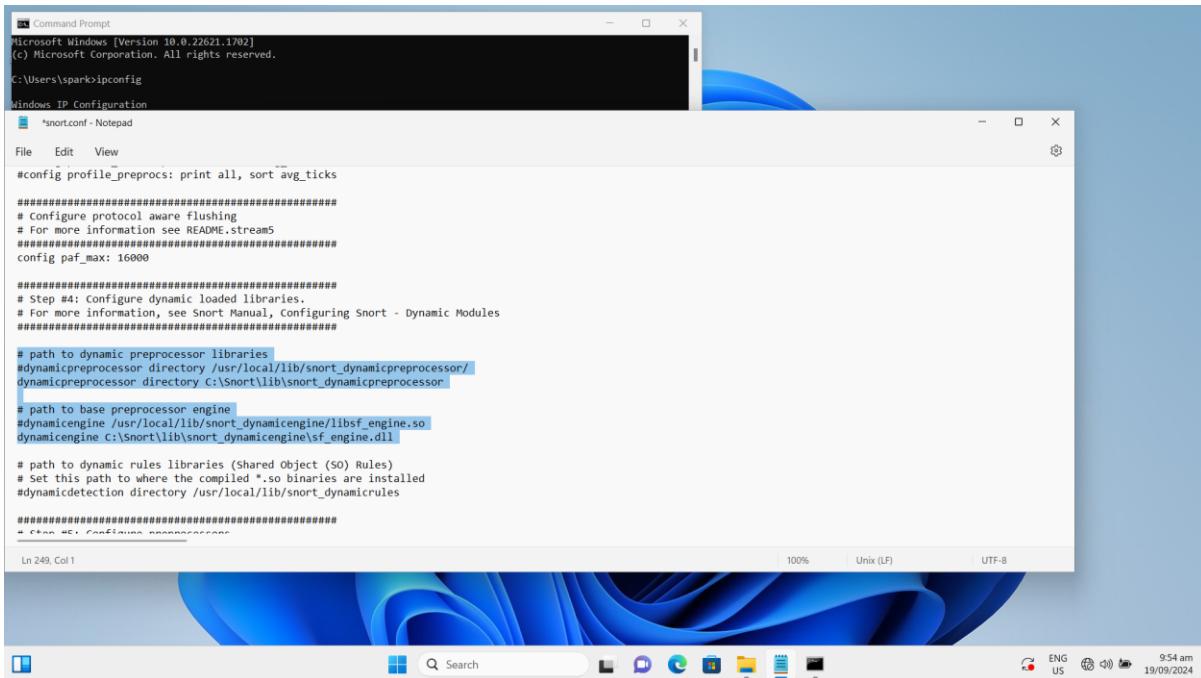
# Configure PCRE match limitations
config pcre_match_limit: 3500
config pcre_match_limit_recursion: 1500

# Configuring the detection engine. See the Snort Manual, Configuring Snort - Toolkit Configuration
# Configuring the detection engine. See the Snort Manual, Configuring Snort - Toolkit Configuration

Ln 183, Col 1

```

- Configure dynamic loaded libraries



```

Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.

C:\Users\spark>ipconfig

Windows IP Configuration

File Edit View
#config profile_preprocs: print all, sort avg_ticks

#####
# Configure protocol aware flushing
# For more information see README.stream5
#####
config paf_max: 16000

#####
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort - Dynamic Modules
#####

# path to dynamic preprocessor libraries
#dynamicpreprocessor_directory /usr/local/lib/snort_dynamicpreprocessor/
dynamicpreprocessor_directory C:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
#dynamicengine /usr/local/lib/snort_dynamicengine/libbsf_engine.so
dynamicengine C:\Snort\lib\snort_dynamicengine\bsf_engine.dll

# path to dynamic rules libraries (Shared Object (.SO) Rules)
# Set this path to where the compiled *.so binaries are installed
#dynamicrules_directory /usr/local/lib/snort_dynamicrules

#####
# Step #5: Configuring preprocessors
#####

Ln 249, Col 1

```

```

C:\Users\spark>ipconfig

Windows IP Configuration

Ethernet Adapter Local Area Connection:
  Connection-specific DNS Suffix: 
  Link Layer Protocol Stack Order: 1
  IP Address List:
    IP Address 1: 192.168.1.10
    Subnet Mask 1: 255.255.255.0
    Default Gateway 1: 192.168.1.1
  IP Address List:
    IP Address 2: 192.168.1.10
    Subnet Mask 2: 255.255.255.0
    Default Gateway 2: 192.168.1.1

C:\Users\spark>notepad snort.conf

# Snort.conf - Notepad

File Edit View

max_header_length 750 \
max_headers 100 \
max_spaces 200 \
small_chunk_length { 10 5 } \
ports { 36 80 81 82 83 84 85 86 87 88 89 90 311 323 383 443 444 555 591 593 623 631 664 801 808 818 901 972 1158 1220 1270 1414 1533 1581 1719 1720 1741 1801 1812
9 49152 49153 50000 50002 50452 51423 53331 54444 55252 55555 56712 } \
non_rfc_char { 0x00 0x01 0x02 0x03 0x04 0x05 0x06 0x07 } \
enable_cookie \
extended_response_inspection \
inspect_gzip \
normalize_utf \
unlimited_decompress \
normalize_javascript \
apache_whitespace no \
ascii no \
bare_byte no \
directory no \
double_decode no \
iis_backslash no \
iis_delimiter no \
iis_unicode no \
multi_slash no \
utf_8 no \
u_encode yes \
webroot no \
# decompress_swf { deflate lzma } \
decompress_pdf { deflate }

# ONC-RPC normalization and anomaly detection. For more information, see the Snort Manual, Configuring Snort - Preprocessors - RPC Decode
preprocessor rpc_decode: 111 32770 32771 32772 32773 32774 32775 32776 32777 32778 32779 no_alert_multiple_requests no_alert_large_fragments no_alert_incomplete

Ln 325, Col 1
100% Unix (LF) UTF-8

```

- Change slash for Windows path

```

# POP preprocessor. For more information see README.pop
preprocessor pop: \
ports { 110 } \
b64_decode_depth 0 \
qp_decode_depth 0 \
bitenc_decode_depth 0 \
uu_decode_depth 0

# Modbus preprocessor. For more information see README.modbus
preprocessor modbus: ports { 502 }

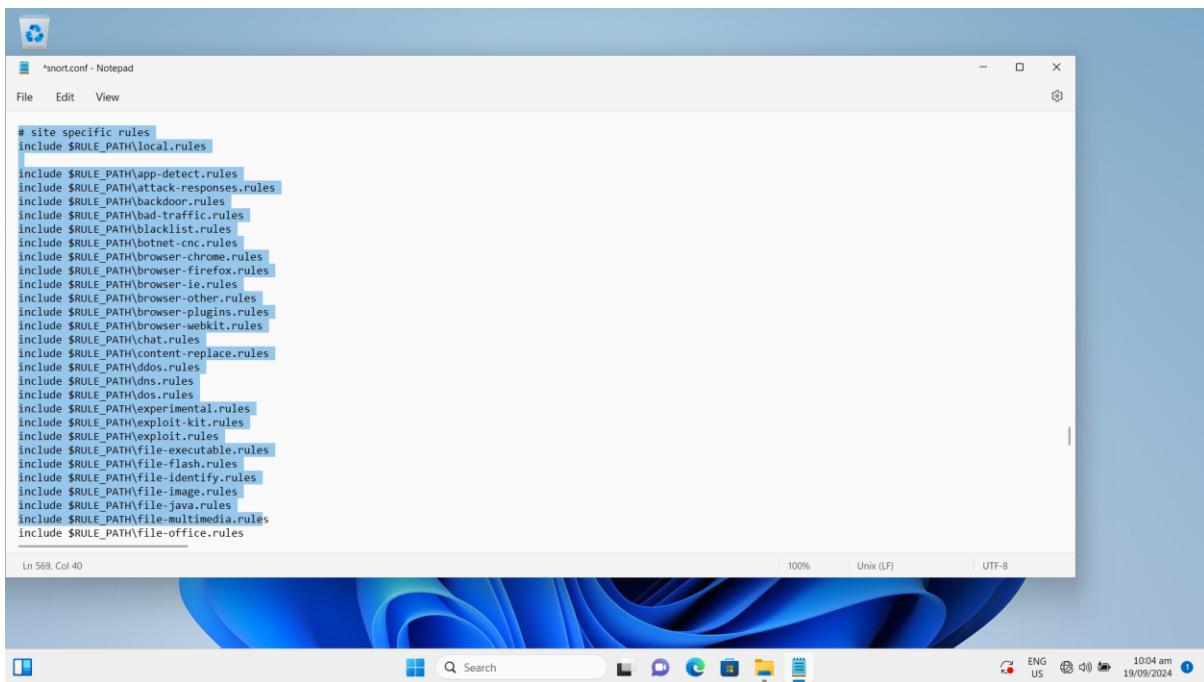
# DNP3 preprocessor. For more information see README.dnp3
preprocessor dnp3: ports { 20000 } \
memcap 262144 \
check_crc

# Reputation preprocessor. For more information see README.reputation
preprocessor reputation: \
memcap 500, \
priority whitelist, \
nested_ip inner, \
whitelist $WHITE_LIST_PATHwhite_list.rules, \
blacklist $BLACK_LIST_PATHblack_list.rules

#####
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
#####

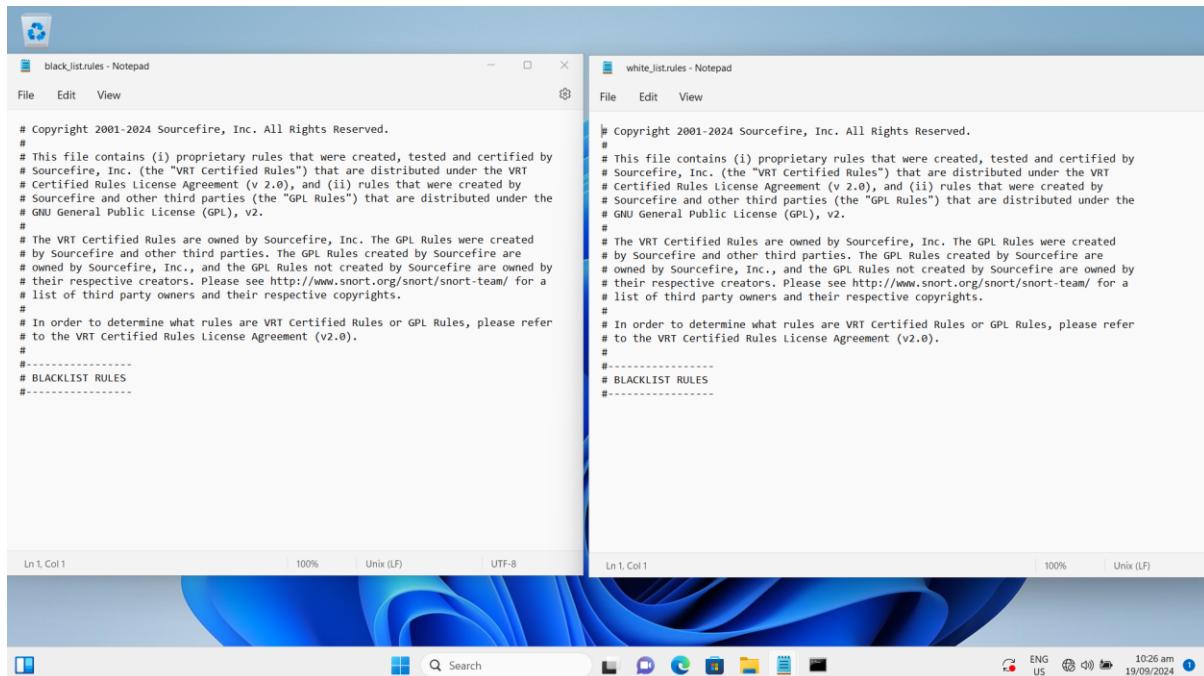
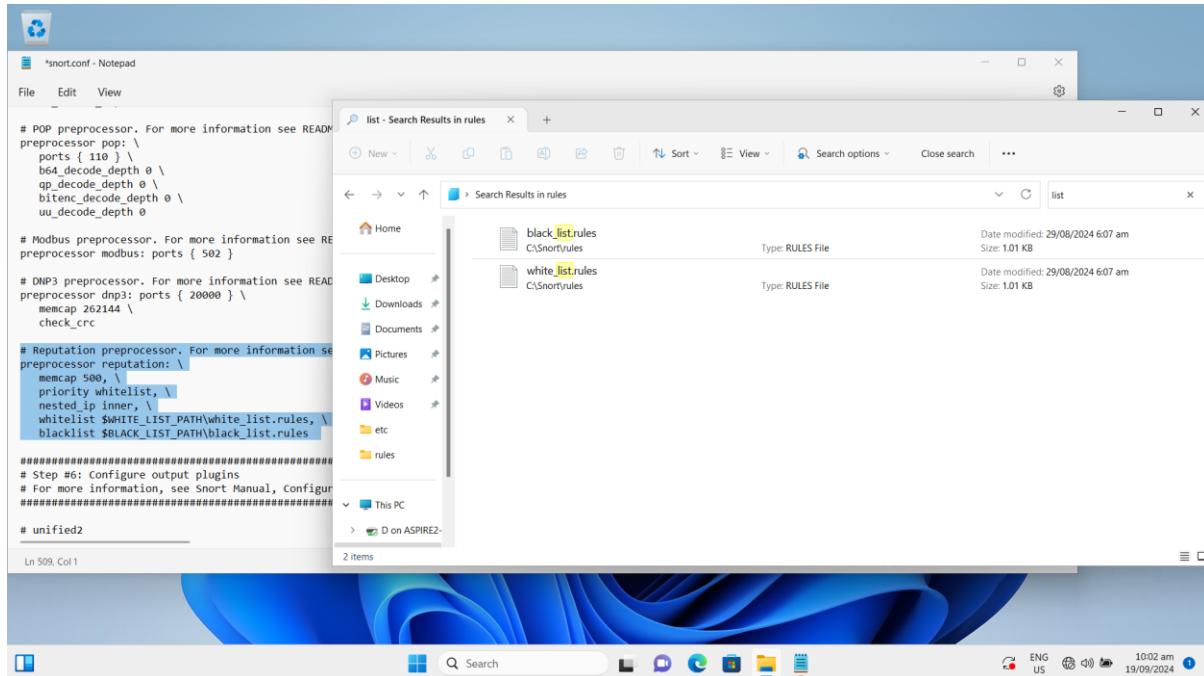
# unified2

```

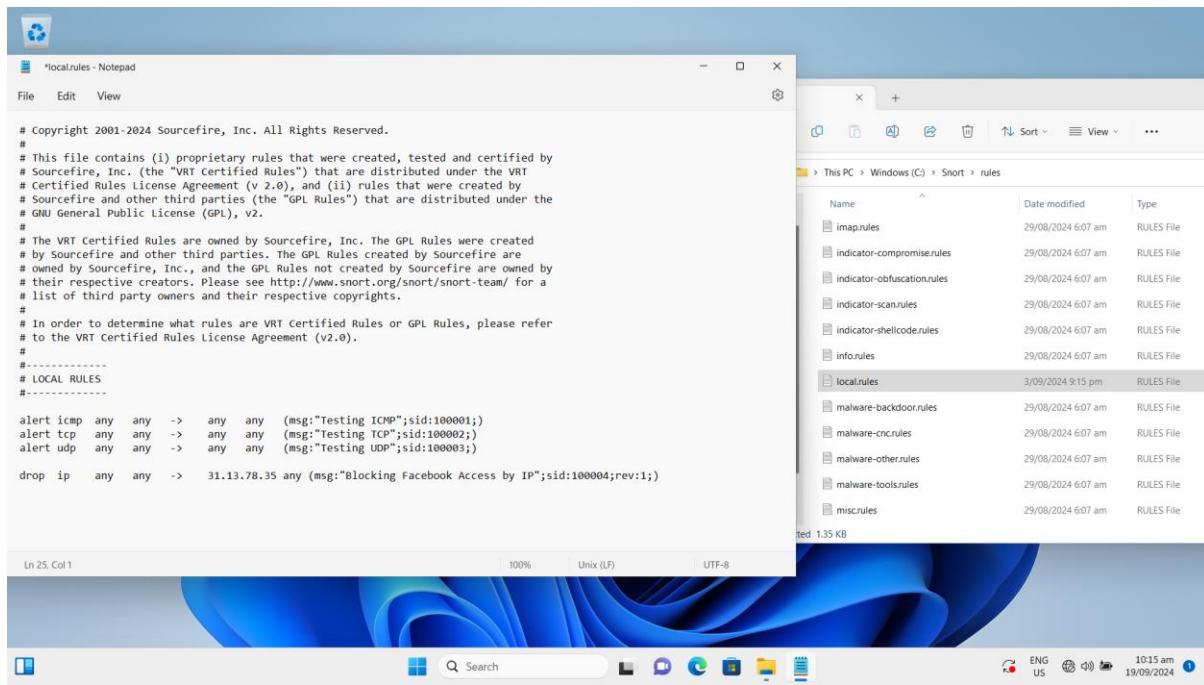


Task 6.2: Integration, Testing, and Documentation

1. Add blacklist.rules and whitelist.rules

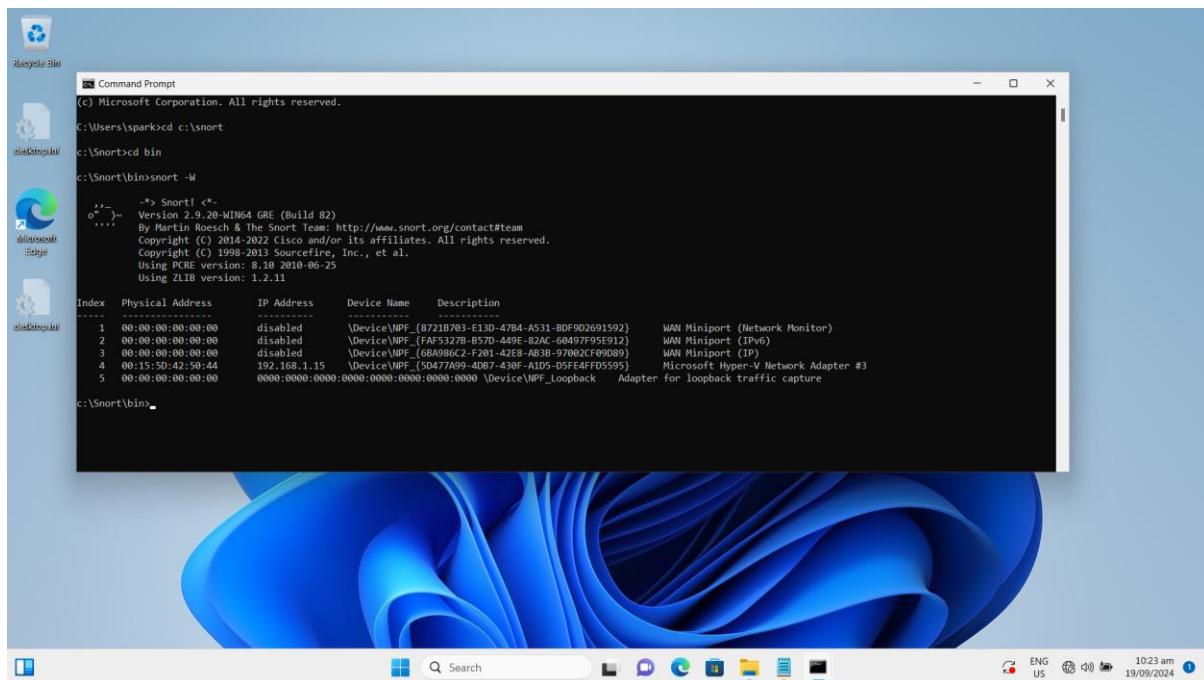


2. Add local.rules



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
Running in IDS mode
=====
Initializing Snort ====
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plugins!
Parsing Rule File "c:\snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined : [ 36 88:98 311 323 383 443:444 555 591 593 623 631 664 801 808 818 901 972 1158 1220 1270 1414 1533 1581 1719:1720 1741 1801 1812
1838 1942 2231 2301 2375 2381 2578 2809 2869 2908 3000 3029 3037 3057 3128 3323 3443 3702 4000 4343 4444 4592 4848 5000 5054 5060:5061 5117 5222 5250 5416 5443 54
50 5480 5555 5600 5814 5894 5984:5986 6060 6088 6173 6988 7000:7001 7005 7071 7080 7144:7145 7180:7181 7510 7777:7779 8000:8001 8008 8014:8015 8020 802
8048 8080:8082 8085 8088 8098 8095 8118 8123 8161 8180:8182 8222 8243 8280 8300 8333 8344 8393 8400 8443 8484 8500 8509 8511 8694 8787 8800 8848 8852 8880 8888 888
899 8983 9000:9002 9050 9060 9080 9090:9091 9111 9260:9261 9290 9443 9447 9502 9700 9710 9788 9830 9850 9900 9999:10000 10088 10100 10255 10297 10443 11371
12601 13014 14592 15489 16000 16992:16993 17000 18081 19980 20000 29991 30007 30018 30888 33300 34412 34443:34444 36099 37215 40007 41080 44449 49152 50000
50602 50451 51423 53331 54444 55252 55555 56712 ]
PortVar 'MIME_TYPES' defined : [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined : [ 1:1024:65535 ]
PortVar 'SSH_PORTS' defined : [ 21 22 ]
PortVar 'FTP_PORTS' defined : [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined : [ 5060:5061 5060 ]
PortVar 'FILE_DATA_PORTS' defined : [ 36 88:98 110 143 311 323 383 443:444 555 591 593 623 631 664 801 808 818 901 972 1158 1220 1270 1414 1533 1581 1719:1720 17
41 1801 1812 1830 1942 2231 2301 2375 2381 2578 2809 2869 2908 3000 3029 3037 3057 3128 3323 3443 3702 4000 4343 4444 4592 4848 5000 5054 5060:5061 5117 5222 5250
5416 5443 5450 5480 5555 5600 5814 5894 5984:5986 6060 6088 6173 6988 7000:7001 7005 7070:7071 7080 7144:7145 7180:7181 7510 7777:7779 8000:8001 8008 8014:8
015 8020 8028 8040 8080:8082 8085 8088 8095 8118 8123 8161 8180:8182 8222 8243 8280 8300 8333 8344 8393 8400 8443 8484 8500 8509 8511 8694 8787 8800 8848 8852
8880 8888 8889 8983 9000:9002 9050 9060 9080 9090:9091 9111 9200:9201 9290 9443 9447 9502 9700 9710 9788 9830 9850 9900 9999:10000 10088 10100 10255 10297
10443 11371 12601 13014 14592 15489 16000 16992:16993 17000 18081 19980 20000 29991 30007 30018 30888 33300 34412 34443:34444 36099 37215 40007 41080 44449 49152
:49153 50000 50602 50451 51423 53331 54444 55252 55555 56712 ]
PortVar 'GTP_PORTS' defined : [ 2123 2152 5386 ]
Detection:
  Search-Method = AC-Full-Q
  Split Any/Any group = enabled
  Search-Method-Optimizations = enabled
  Maximum pattern length = 20
```

```

Administrator: Command Prompt - snort -i 4 -c c:\snort\etc\snort.conf -A Console
Nested IP: inner (Default)
White action: unblock (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->drop->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.mmv' is set but not ever checked.
WARNING: flowbits key 'Malware_ClassroomSpyPro_detection3' is set but not ever checked.
WARNING: flowbits key 'netwird' is set but not ever checked.

10:31 am 19/09/2024

```

```

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
|   DPD : 1
|     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_{5D477A99-4D87-438F-AIDS-05FE4FFD5595}".
Decoding Ethernet
==== Initialization Complete ====
-> Snort! <-
o" .> Version 2.9.26-WIN64 GRE (Build 82)
By Martin Roess & 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_SDP Version 1.1 <Build 1>
Preprocessor Object: SF_TELNET Version 1.0 <Build 1>
Preprocessor Object: SF_PPP_VJSESSION Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.0 <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_DCERP2 Version 1.0 <Build 3>

Commencing packet processing (pid=4848)

10:39 am 19/09/2024

```

4. Check logs

- ICMP detected.

```
Select Administrator: Command Prompt - snort -i 4 -c c:\snort\etc\snort.conf -A Console
Using ZLIB version: 1.2.11

Rules Engine: SF-SNORT-DETECTION-ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 1>
Preprocessor Object: SF_SNTP 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_POP3 Version 1.0 <Build 1>
Preprocessor Object: SF_FTPBIO Version 1.0 <Build 1>
Preprocessor Object: SF_IMPP 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 (process 0)
[1:100000:0] [1:100000:0] Testing ICMP [**] [Priority: 0] (ICMP) 192.168.1.1->192.168.1.15
09/19/10:35:47.570455 [*]:[1:100001:0] Testing ICMP [**] [Priority: 0] (ICMP) 192.168.1.1->192.168.1.15
09/19/10:35:48.381454 [*]:[1:100001:0] Testing ICMP [**] [Priority: 0] (ICMP) 192.168.1.1->192.168.1.15
09/19/10:35:49.991790 [*]:[1:100001:0] Testing ICMP [**] [Priority: 0] (ICMP) 192.168.1.1->192.168.1.15
09/19/10:35:54.330730 [*]:[1:100000:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:52624
09/19/10:36:00.564728 [*]:[1:100000:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:63535
09/19/10:35:54.565001 [*]:[1:100000:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:63490
09/19/10:36:00.136052 [*]:[1:100001:0] Testing ICMP [**] [Priority: 0] (ICMP) 192.168.1.1->192.168.1.15
09/19/10:36:00.140723 [*]:[1:100001:0] Testing ICMP [**] [Priority: 0] (ICMP) 192.168.1.1->192.168.1.15
09/19/10:36:00.25.255.255.255 [*]:[1:100001:0] Testing ICMP [**] [Priority: 0] (ICMP) 192.168.1.1->192.168.1.15
09/19/10:36:01.151196 [*]:[1:100001:0] Testing ICMP [**] [Priority: 0] (ICMP) 192.168.1.1->192.168.1.15
09/19/10:36:09.565615 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:10800
09/19/10:36:09.565615 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:63490
09/19/10:36:12.284256 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:63535
09/19/10:36:36.896629 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:63490
09/19/10:36:46.084187 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:57414->239.255.255.256:1900
09/19/10:36:46.084187 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:57414->239.255.255.256:1900
09/19/10:36:46.084187 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:57414->239.255.255.256:1900
09/19/10:36:46.084187 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:57414->239.255.255.256:1900
09/19/10:36:46.084187 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:57414->239.255.255.256:1900
09/19/10:37:09.577711 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:52517
09/19/10:37:09.577711 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:51080
09/19/10:37:16.249183 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:7339
09/19/10:37:17.421072 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:49837
09/19/10:37:17.421072 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:56860
09/19/10:37:17.421072 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:56860
09/19/10:37:17.421072 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:51394
09/19/10:37:17.421072 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:60644
09/19/10:37:17.421072 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:53693
09/19/10:37:17.421072 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:58622
09/19/10:37:17.421072 [*]:[1:100003:0] Testing UDP [**] [Priority: 0] (UDP) 192.168.1.1:53->192.168.1.15:54429
```

- UDP detected

Select Administrator Command Prompt - snort -i -c c:\snort\etc\snort.conf -A Console

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_TELNET Version 1.1 <Build 3>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_IMDUS 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_MP3 Version 1.1 <Build 1>
Preprocessor Object: SF_RPC Version 1.0 <Build 3>

Commencing packet processing (pid:668)

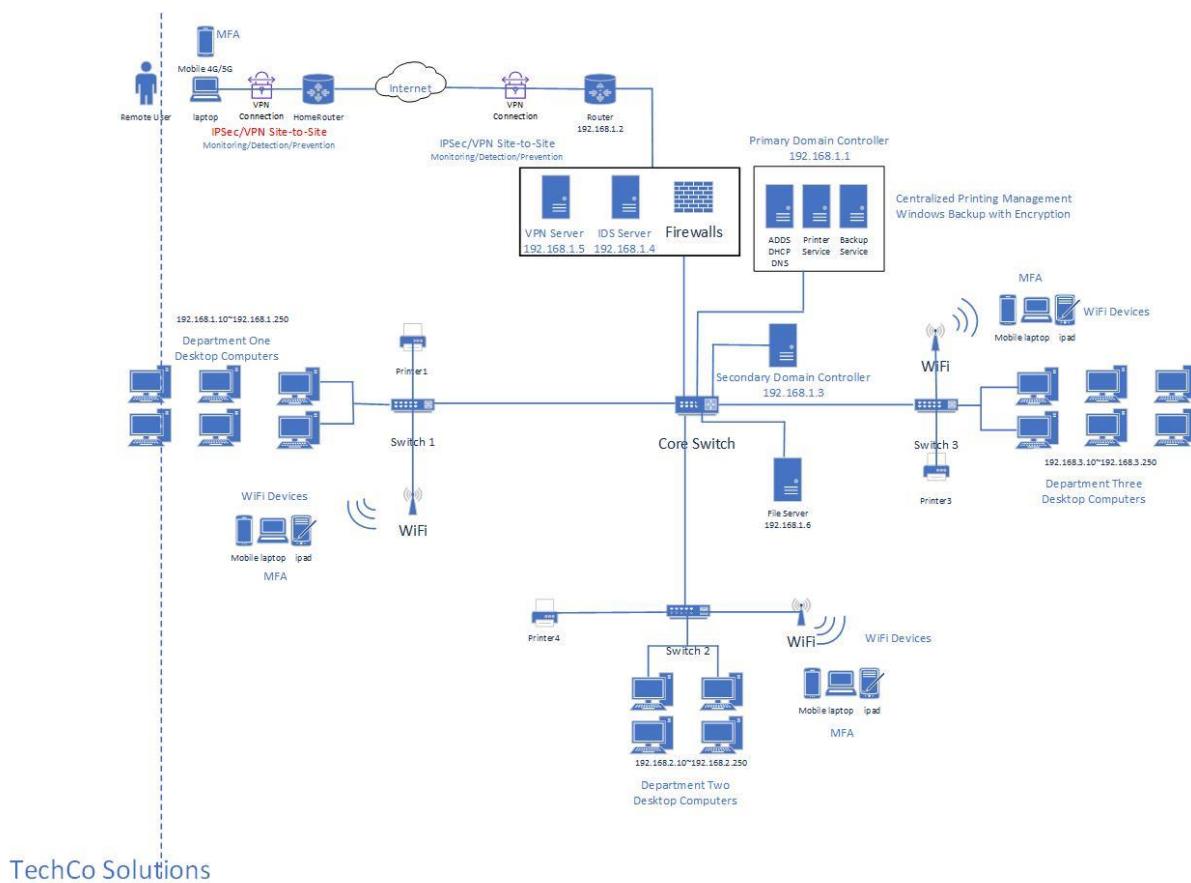
09/19/10:35:46.956408 [**] [1:100001:0] Testing ICMP [**] [Priority: 0] [ICMP] 192.168.1.1 -> 192.168.1.15
09/19/10:35:47.970455 [**] [1:100001:0] Testing ICMP [**] [Priority: 0] [ICMP] 192.168.1.1 -> 192.168.1.15
09/19/10:35:48.981454 [**] [1:100001:0] Testing ICMP [**] [Priority: 0] [ICMP] 192.168.1.1 -> 192.168.1.15
09/19/10:35:49.991799 [**] [1:100001:0] Testing ICMP [**] [Priority: 0] [ICMP] 192.168.1.1 -> 192.168.1.15
09/19/10:35:54.530730 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:52624
09/19/10:35:54.554728 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:63535
09/19/10:35:54.554728 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:63490
09/19/10:36:01.136052 [**] [1:100001:0] Testing ICMP [**] [Priority: 0] [ICMP] 192.168.1.1 -> 192.168.1.15
09/19/10:36:01.140273 [**] [1:100001:0] Testing ICMP [**] [Priority: 0] [ICMP] 192.168.1.1 -> 192.168.1.15
09/19/10:36:02.146186 [**] [1:100001:0] Testing ICMP [**] [Priority: 0] [ICMP] 192.168.1.1 -> 192.168.1.15
09/19/10:36:03.151906 [**] [1:100001:0] Testing ICMP [**] [Priority: 0] [ICMP] 192.168.1.1 -> 192.168.1.15
09/19/10:36:00.565615 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:51088
09/19/10:36:00.565615 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:63490
09/19/10:36:12.584256 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:63535
09/19/10:36:36.806629 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:63490
09/19/10:36:47.813229 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 239.255.255.256:1998
09/19/10:36:47.813229 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 239.255.255.256:1998
09/19/10:36:48.616474 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:575414 -> 239.255.255.256:1998
09/19/10:36:48.616474 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:575414 -> 239.255.255.256:1998
09/19/10:37:08.2.263849 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:51088
09/19/10:37:09.557711 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:52517
09/19/10:37:09.557711 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:51088
09/19/10:37:16.249183 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:57339
09/19/10:37:17.422072 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:58660
09/19/10:37:17.422072 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:58660
09/19/10:37:17.422072 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:59514
09/19/10:37:17.422072 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:51394
09/19/10:37:17.422072 [**] [1:100003:0] Testing UDP [**] [Priority: 0] [UDP] 192.168.1.1:53 -> 192.168.1.15:66664

- 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



TechCo Solutions