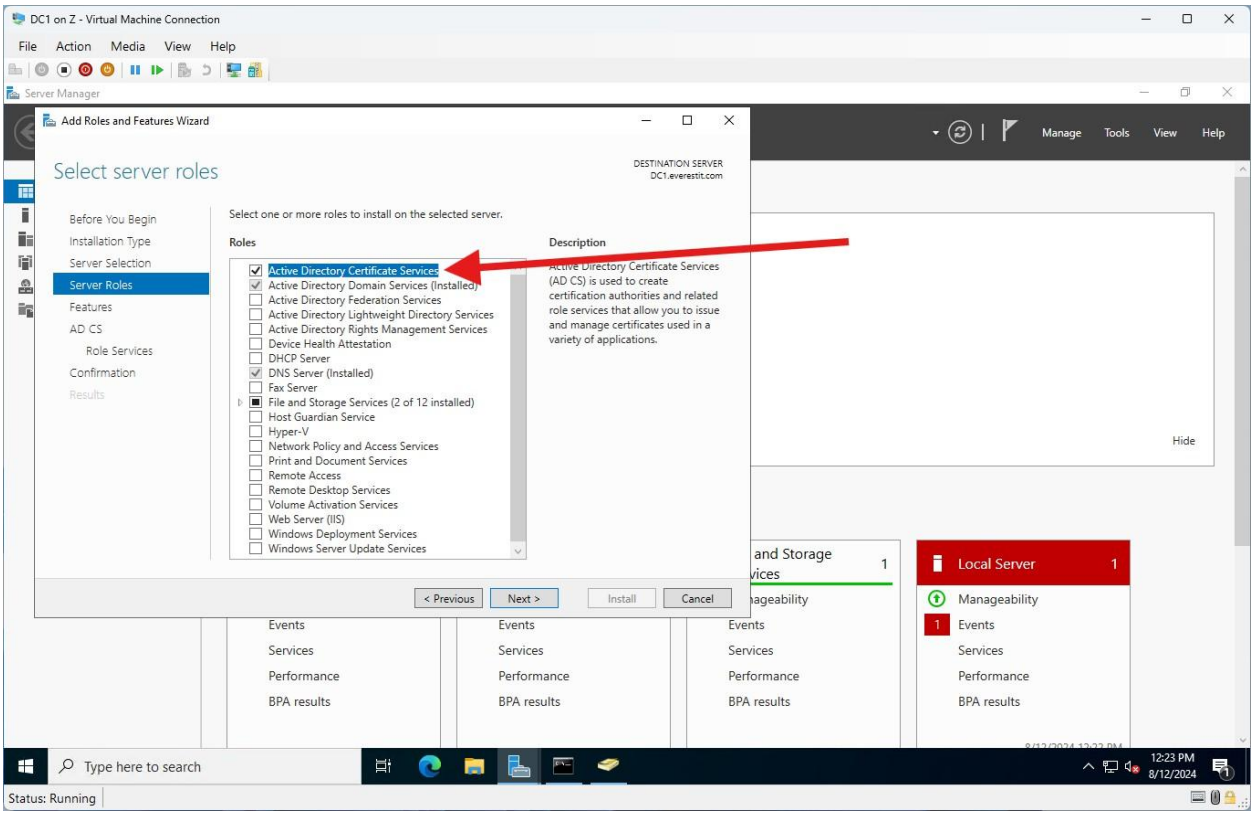
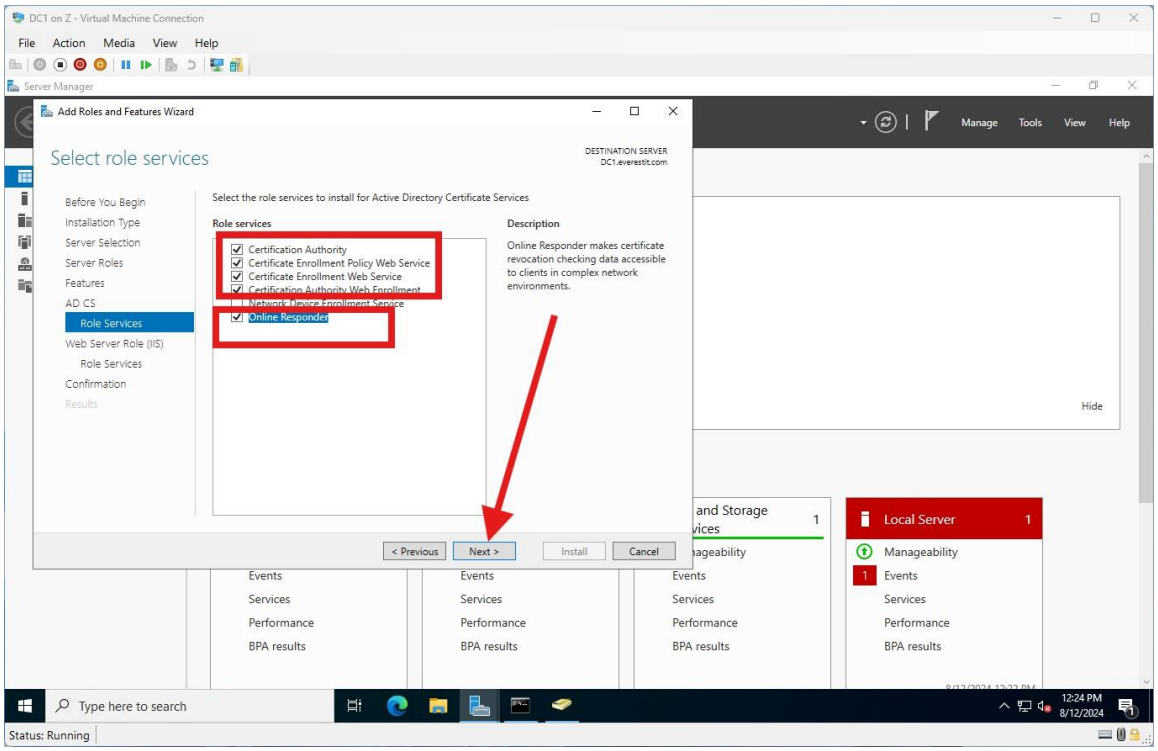
This project provides a step-by-step guide to deploy Active Directory Certificate Services and then create a self-signed SSL certificate for Microsoft Exchange Server 2019. Deploying the certificate ensures that the Exchange server can start its services properly and is ready to send and receive emails internally within the organization immediately after deployment. While a self-signed certificate is sufficient for internal mail flow and Outlook connectivity, external email communication requires a CA-signed SSL certificate to establish trusted connections with other mail servers and clients and to ensure secure email encryption. Even when using a public CA-signed certificate, the CSR (Certificate Signing Request) process must still be performed on the Exchange server so the steps following the creation of a self-signed certificate, including importing, enabling for services, and restarting IIS, remain the same. This guide helps configure certificates correctly to make the Exchange server fully operational and secure in a production-ready environment.

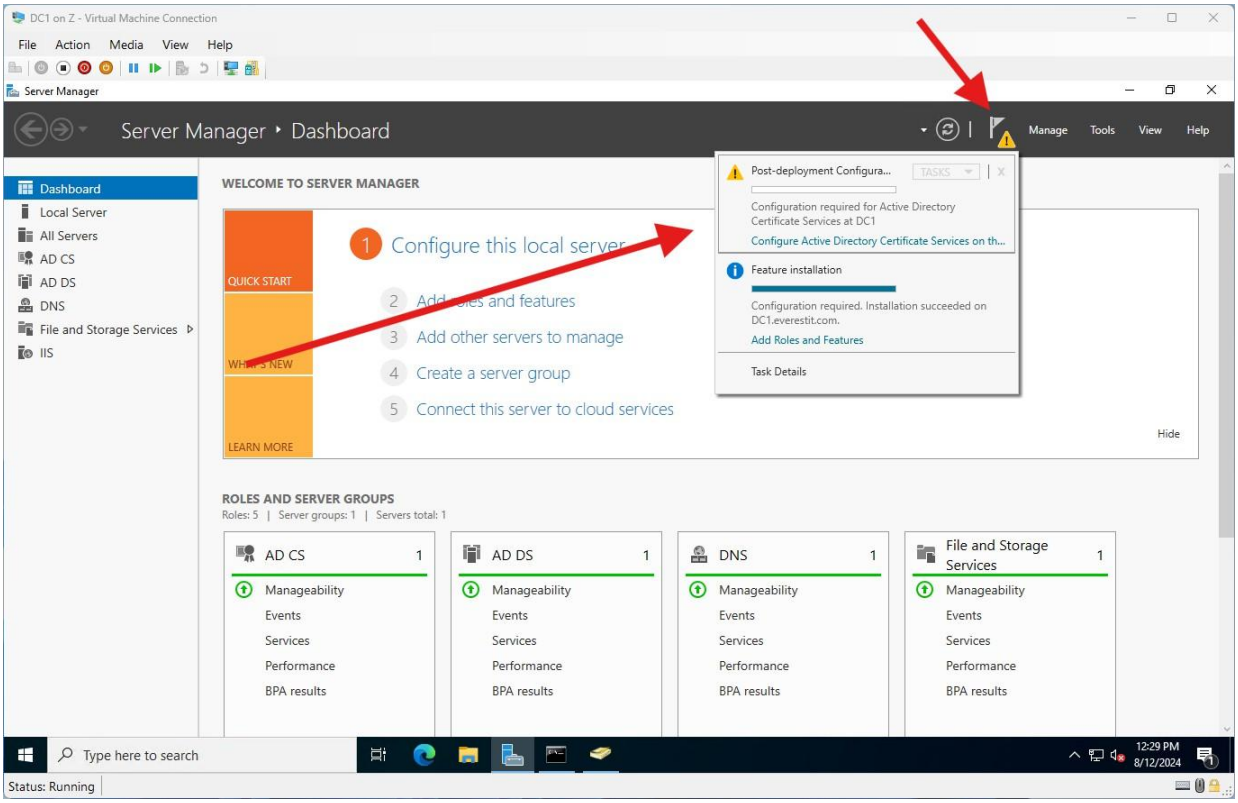
- DOMAIN CONTROLLER “DC1”
- EXCHANGE SERVER “MAIL”
- Go to the domain controller
- Manage>add roles and features
- Select active directory certificate services
- And install it

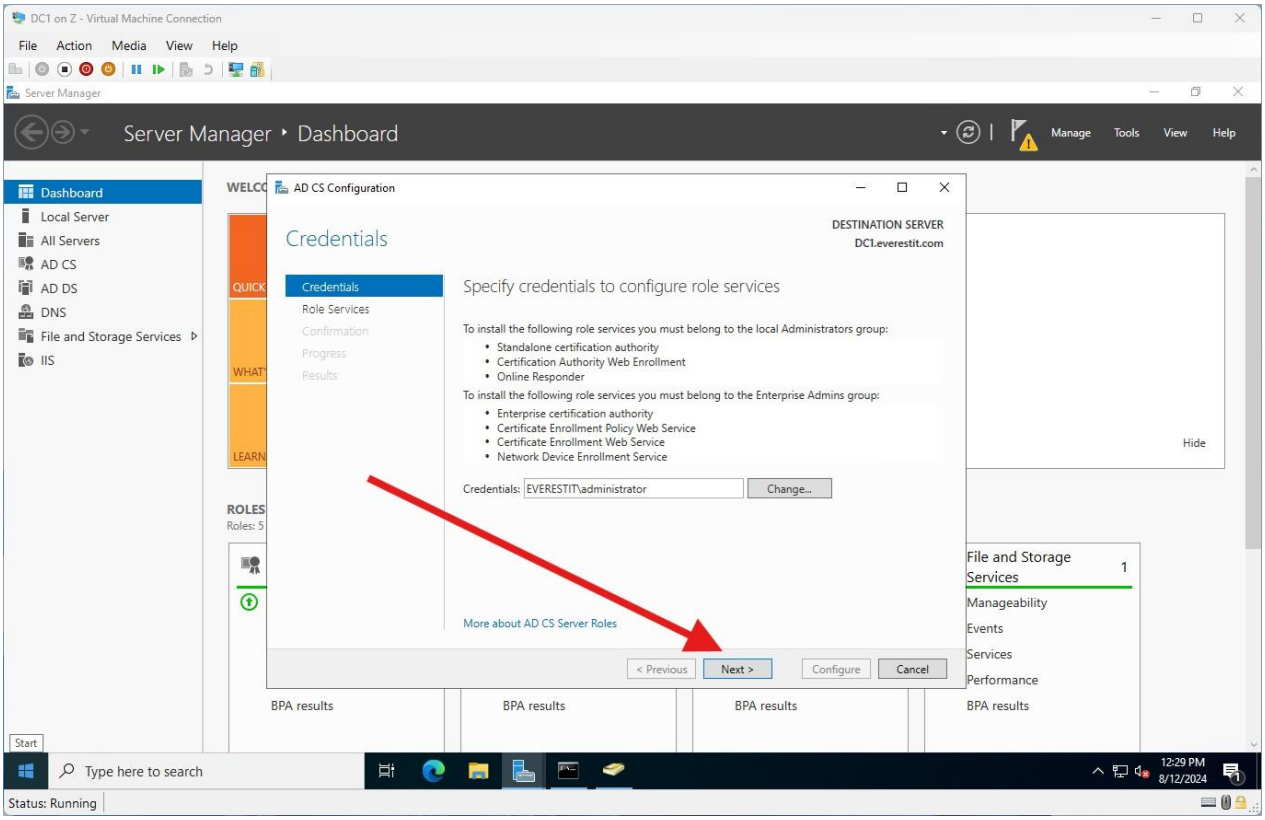


- Select these four options

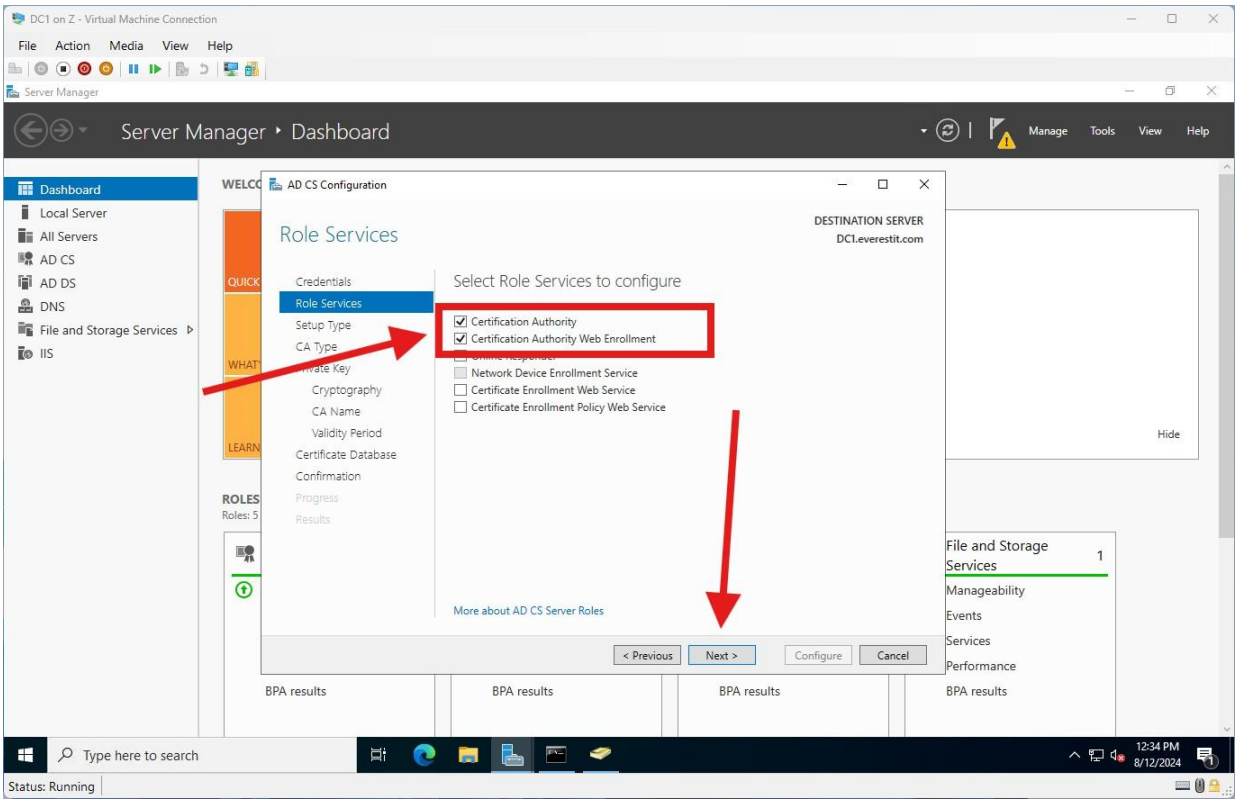


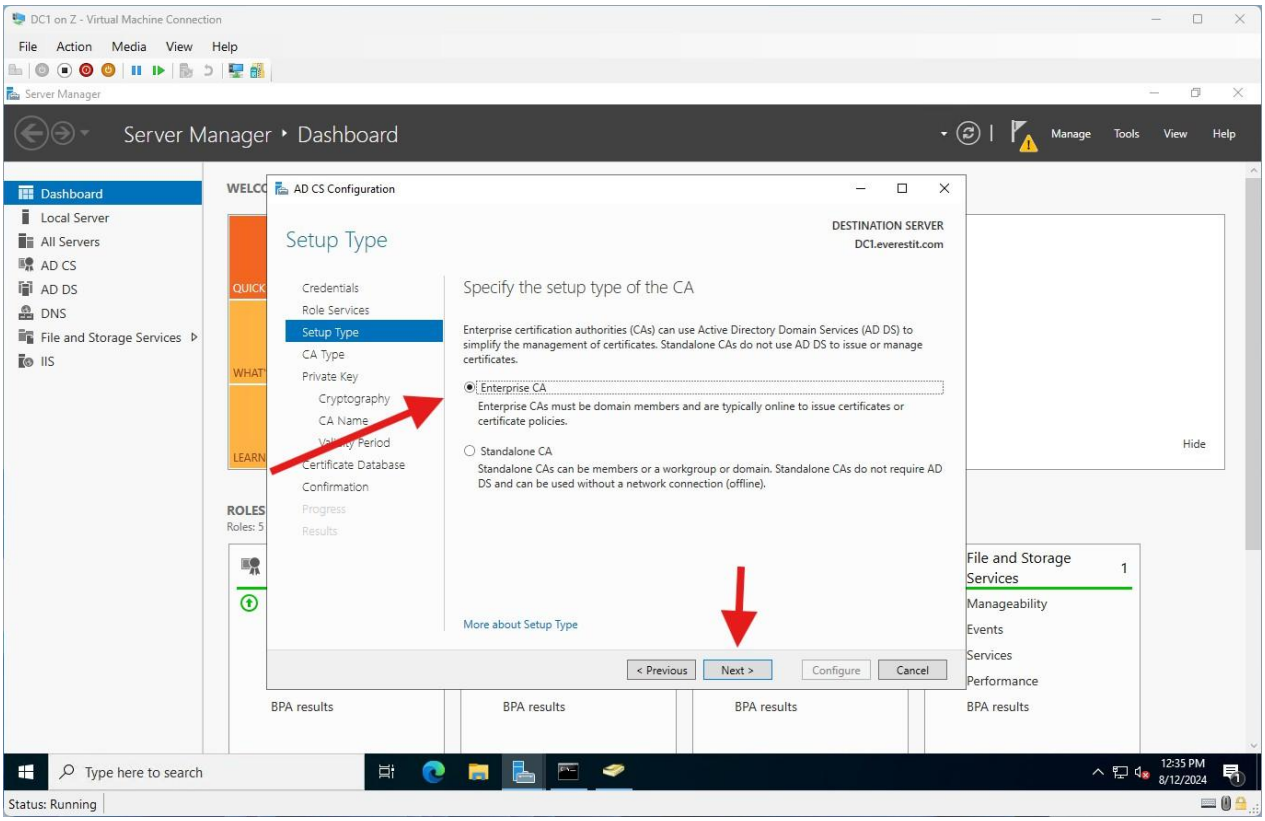
- Once installation is complete configure it

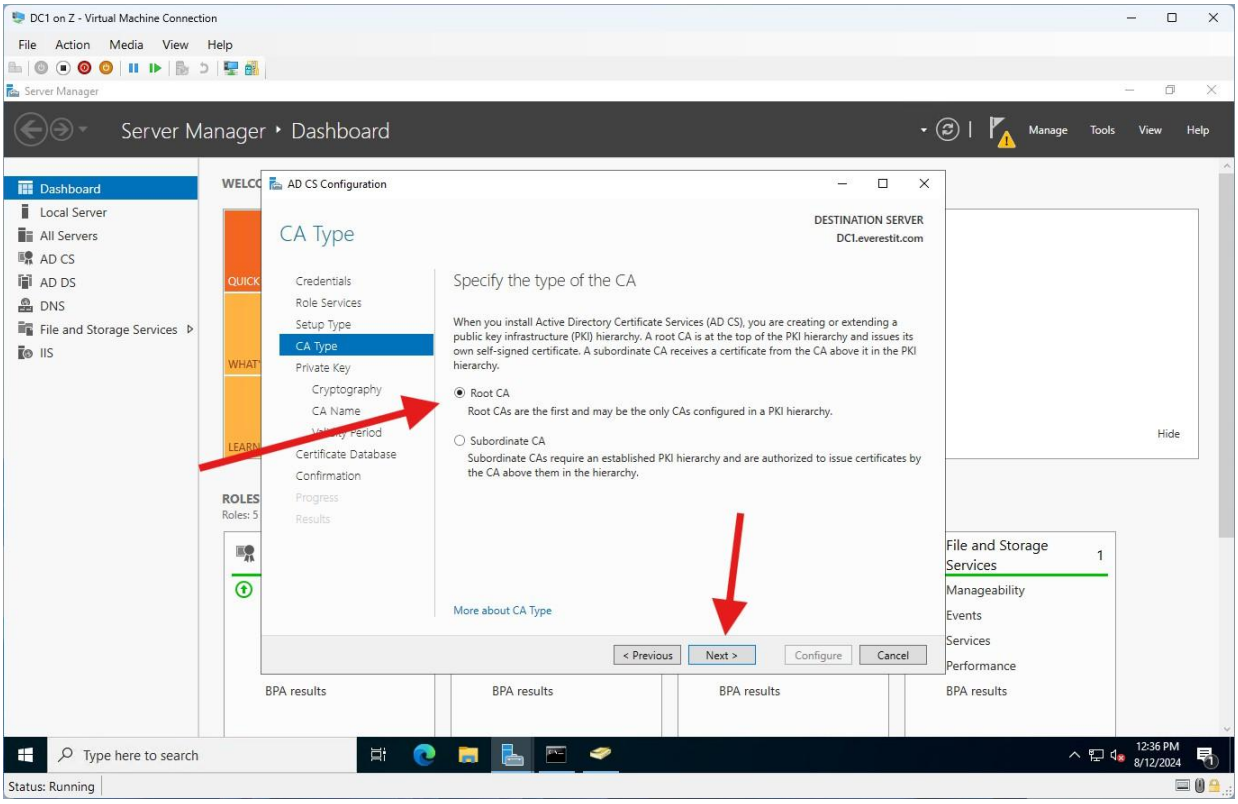


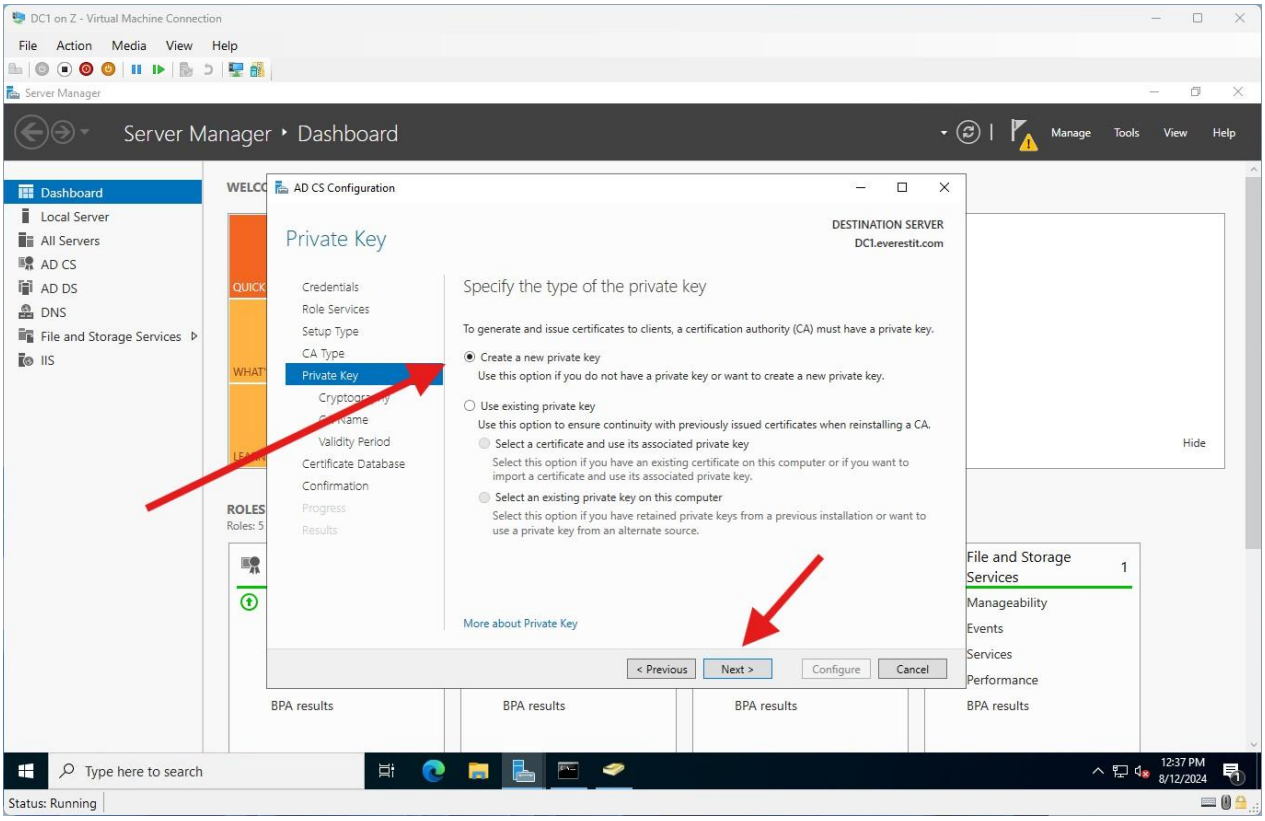


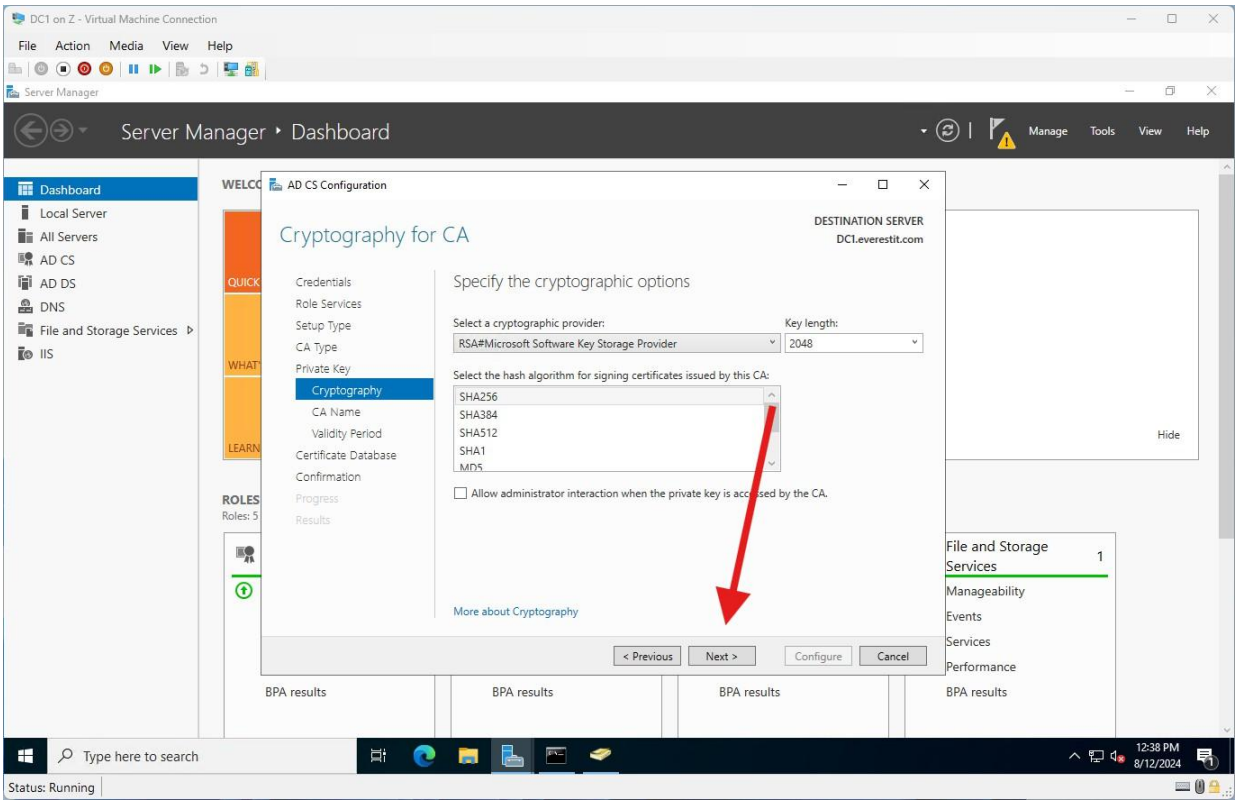
- Select the first two option

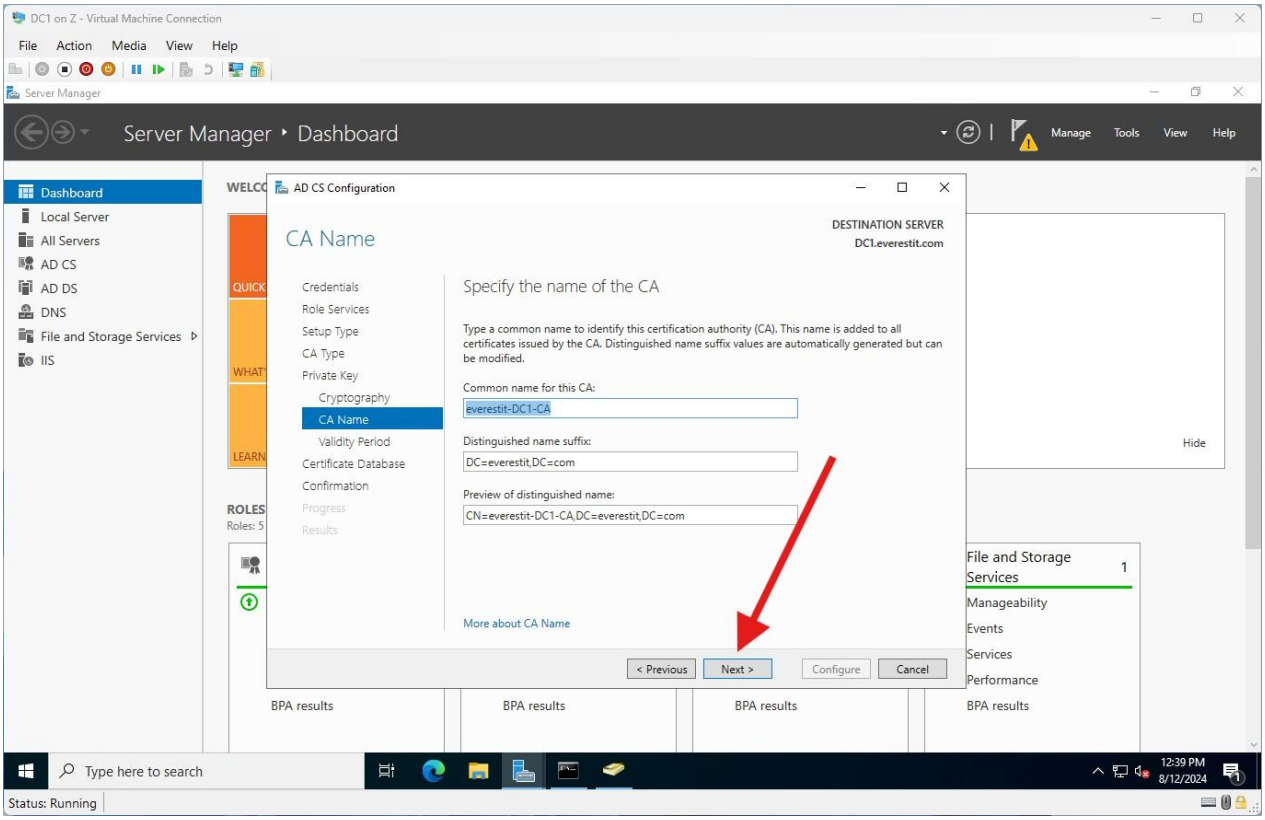


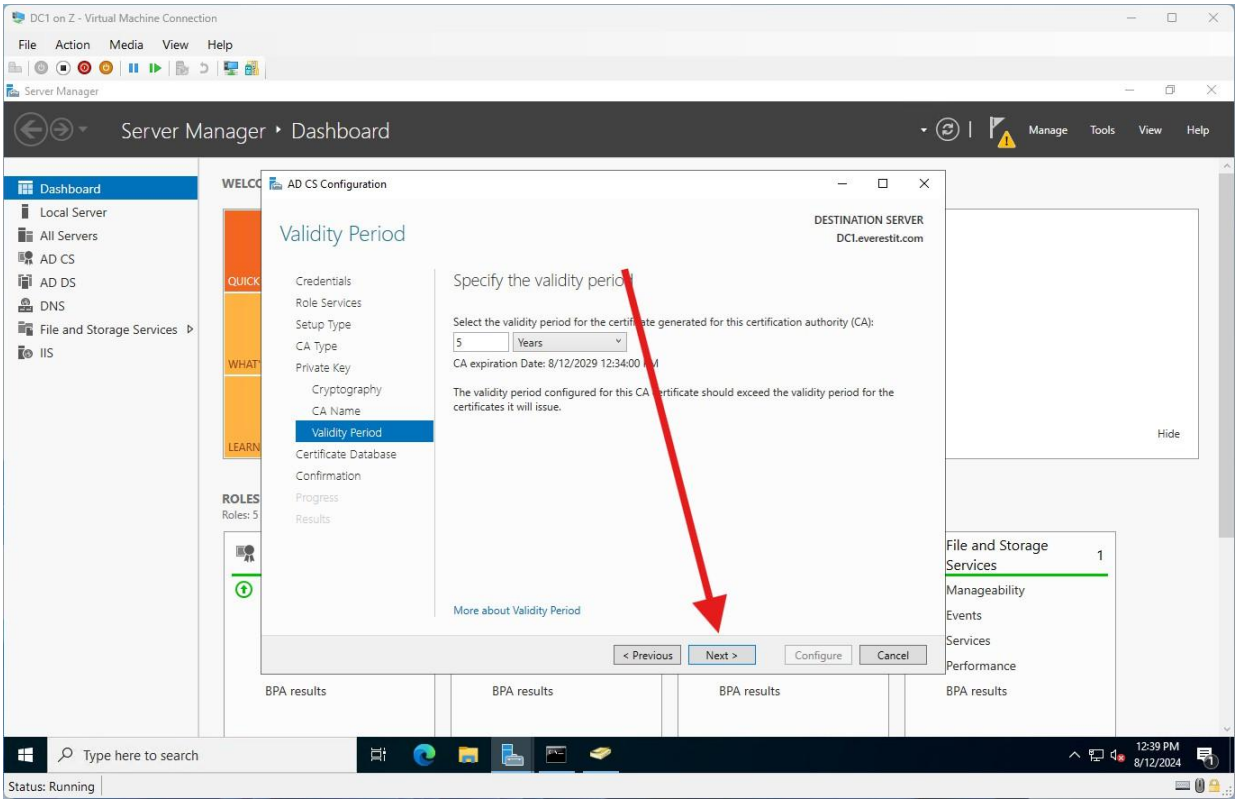

DC1 on Z - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
AD CS Configuration
Setup Type
DESTINATION SERVER
DC1.everestit.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the setup type of the CA
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.
Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.
Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).
More about Setup Type
< Previous
Next >
Configure
Cancel
Hide
ROLES
Roles: 5
File and Storage Services
1
Manageability
Events
Services
Performance
BPA results
BPA results
BPA results
BPA results
Type here to search
12:35 PM
8/12/2024
Status: Running

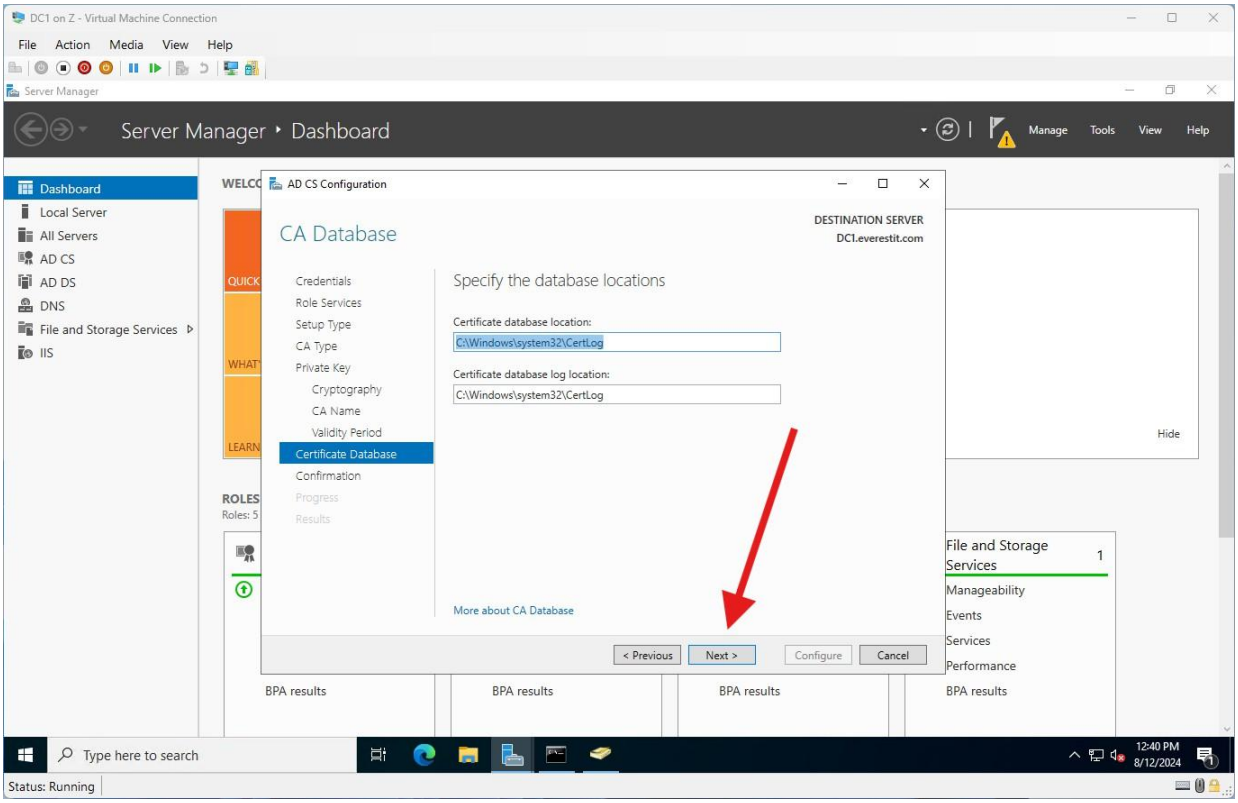

DC1 on Z - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
AD CS Configuration
CA Type
DESTINATION SERVER
DC1.everestit.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the type of the CA
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.
Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.
More about CA Type
< Previous
Next >
Configure
Cancel
Hide
ROLES
Roles: 5
File and Storage Services
1
Manageability
Events
Services
Performance
BPA results
BPA results
BPA results
BPA results
Type here to search
12:36 PM
8/12/2024
Status: Running

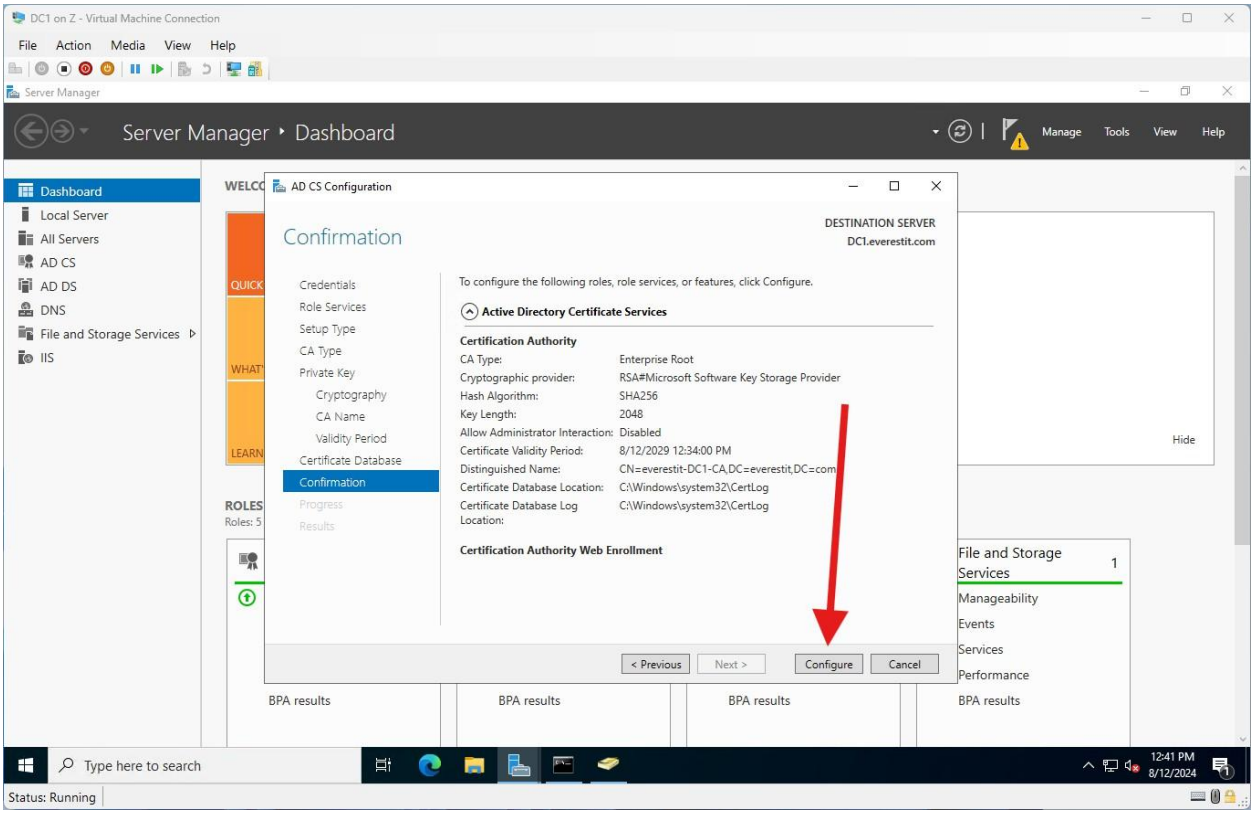

DC1 on Z - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager ‣ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
AD CS Configuration
Private Key
DESTINATION SERVER
DC1.everestit.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the type of the private key
To generate and issue certificates to clients, a certification authority (CA) must have a private key.
Create a new private key
Use this option if you do not have a private key or want to create a new private key.
Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.
Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.
Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.
More about Private Key
< Previous
Next >
Configure
Cancel
File and Storage Services
Manageability
Events
Services
Performance
BPA results
Type here to search
12:37 PM
8/12/2024
Status: Running

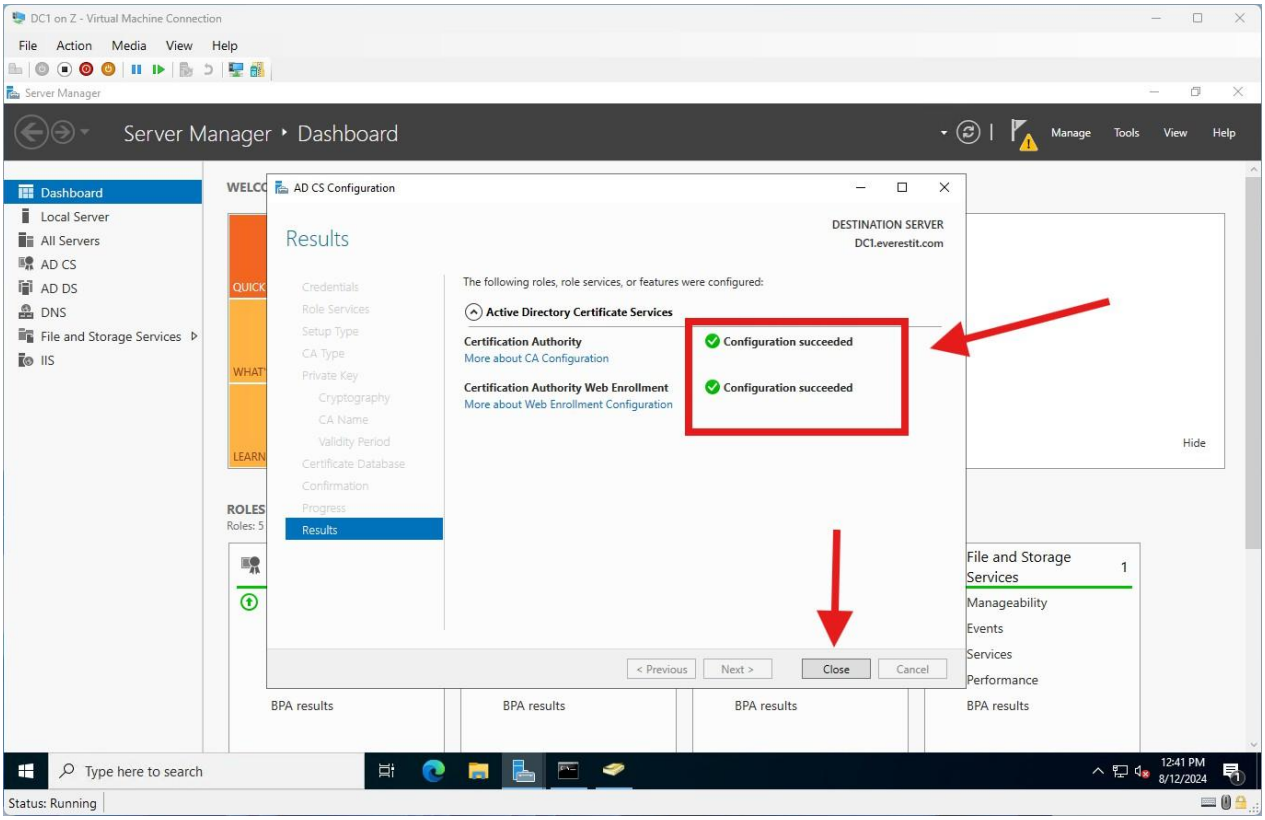

DC1 on Z - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager ‣ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
AD CS Configuration
Cryptography for CA
DESTINATION SERVER
DC1.everestit.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the cryptographic options
Select a cryptographic provider:
RSA#Microsoft Software Key Storage Provider
Key length:
2048
Select the hash algorithm for signing certificates issued by this CA:
SHA256
SHA384
SHA512
SHA1
MD5
Allow administrator interaction when the private key is accessed by the CA.
More about Cryptography
< Previous
Next >
Configure
Cancel
File and Storage Services
Manageability
Events
Services
Performance
BPA results
Type here to search
12:38 PM
8/12/2024
Status: Running


DC1 on Z - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager ‣ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
AD CS Configuration
CA Name
DESTINATION SERVER
DC1.everestit.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the name of the CA
Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.
Common name for this CA:
everestit-DC1-CA
Distinguished name suffix:
DC=everestit,DC=com
Preview of distinguished name:
CN=everestit-DC1-CA,DC=everestit,DC=com
More about CA Name
< Previous
Next >
Configure
Cancel
Hide
ROLES
Roles: 5
File and Storage Services
1
Manageability
Events
Services
Performance
BPA results
BPA results
BPA results
BPA results
Type here to search
12:39 PM
8/12/2024
Status: Running

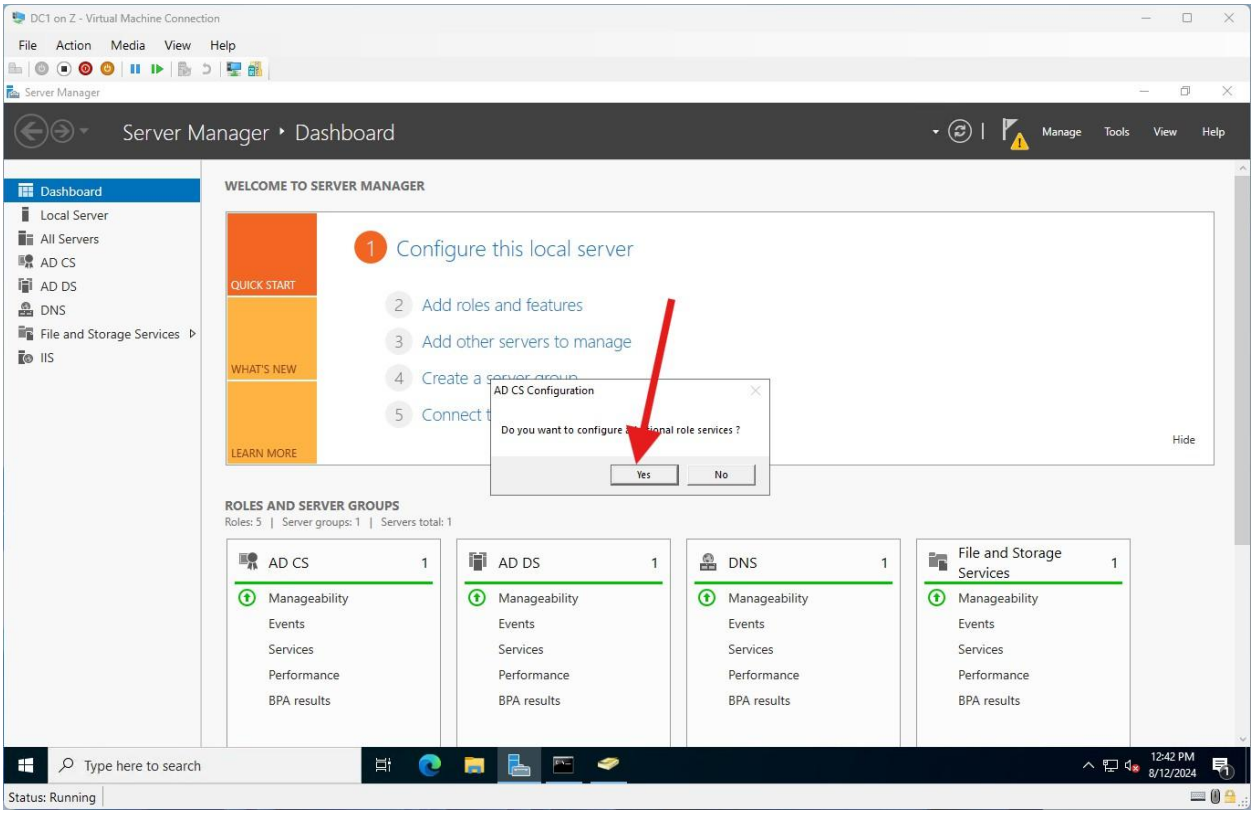

DC1 on Z - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager ‣ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
AD CS Configuration
Validity Period
DESTINATION SERVER
DC1.everestit.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the validity period
Select the validity period for the certificate generated for this certification authority (CA):
5
Years
CA expiration Date: 8/12/2029 12:34:00 PM
The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.
More about Validity Period
< Previous
Next >
Configure
Cancel
Hide
ROLES
Roles: 5
File and Storage Services
1
Manageability
Events
Services
Performance
BPA results
BPA results
BPA results
BPA results
Type here to search
12:39 PM
8/12/2024
Status: Running

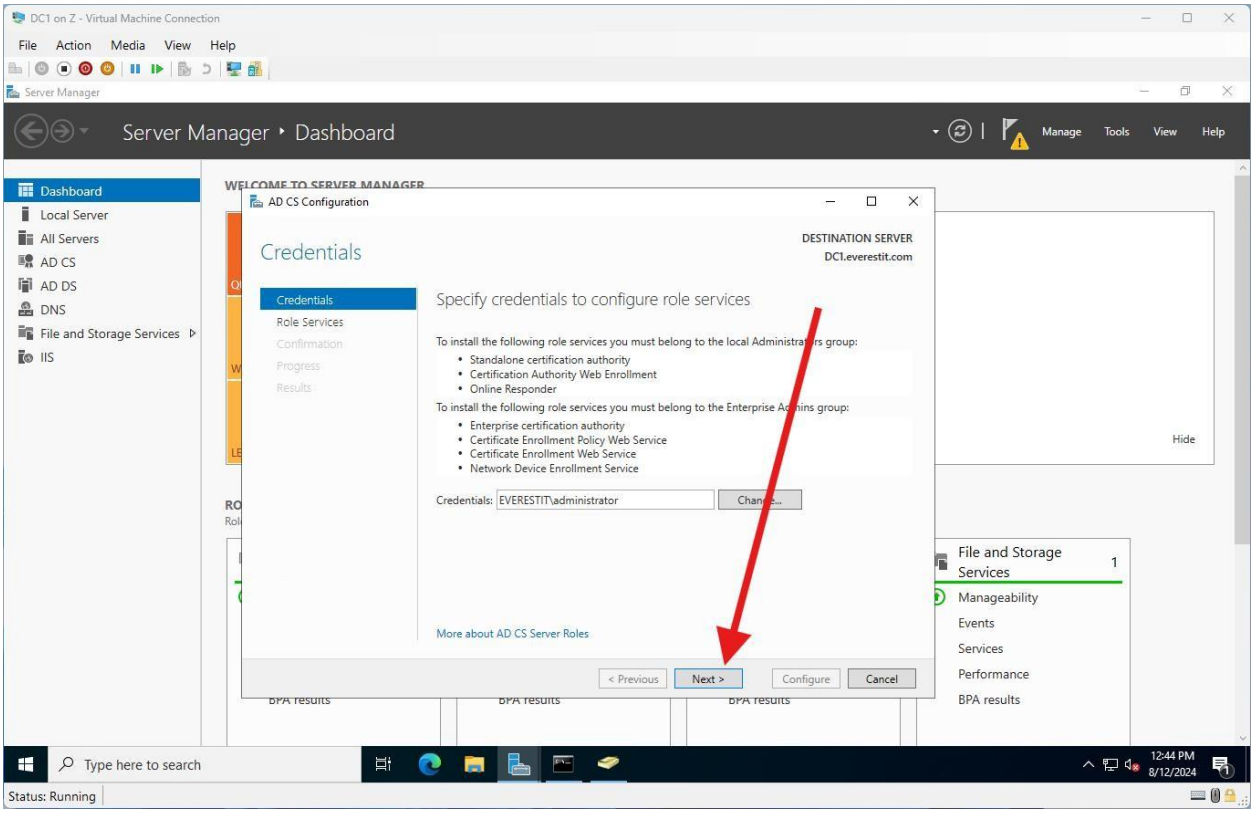

DC1 on Z - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager ‣ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
AD CS Configuration
CA Database
DESTINATION SERVER
DC1.everestit.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the database locations
Certificate database location:
C:\Windows\system32\CertLog
Certificate database log location:
C:\Windows\system32\CertLog
More about CA Database
< Previous
Next >
Configure
Cancel
Hide
File and Storage Services
Manageability
Events
Services
Performance
BPA results
Type here to search
12:40 PM
8/12/2024
Status: Running


DC1 on Z - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager ‣ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
AD CS Configuration
Confirmation
DESTINATION SERVER
DC1.everestit.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
To configure the following roles, role services, or features, click Configure.
Active Directory Certificate Services
Certification Authority
CA Type: Enterprise Root
Cryptographic provider: RSA#Microsoft Software Key Storage Provider
Hash Algorithm: SHA256
Key Length: 2048
Allow Administrator Interaction: Disabled
Certificate Validity Period: 8/12/2029 12:34:00 PM
Distinguished Name: CN=everestit-DC1-CA,DC=everestit,DC=com
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog
Certification Authority Web Enrollment
< Previous
Next >
Configure
Cancel
Hide
File and Storage Services
Manageability
Events
Services
Performance
BPA results
Type here to search
12:41 PM
8/12/2024
Status: Running

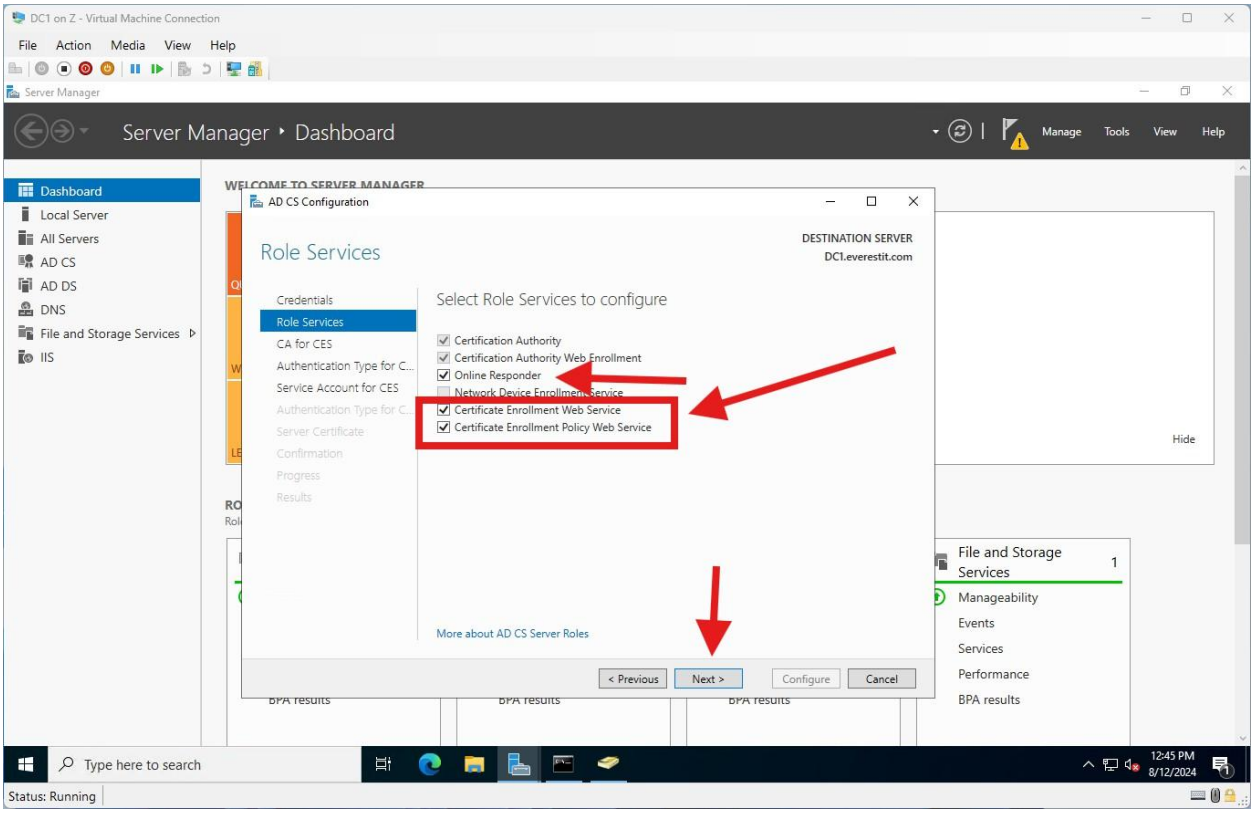


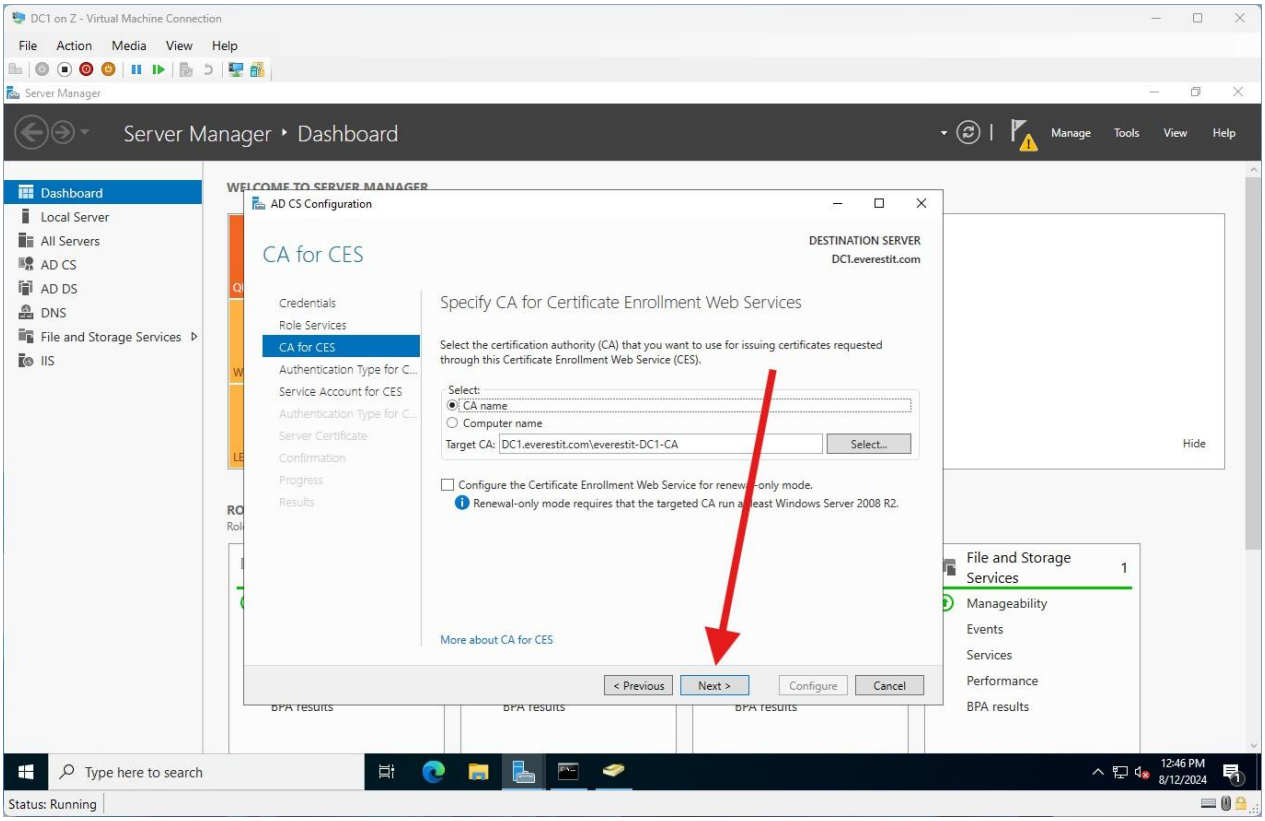
- Once the configuration is completed
- Confirmation screen will pop up
- Hit yes

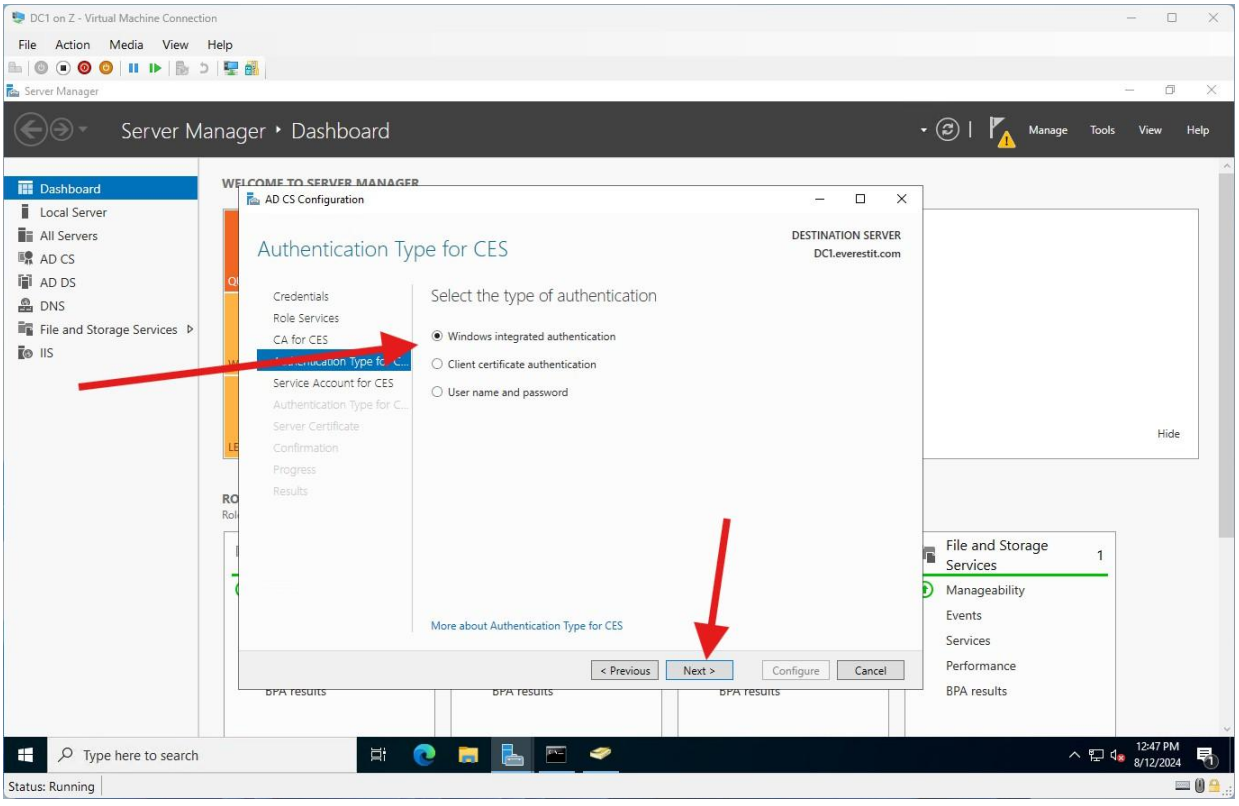




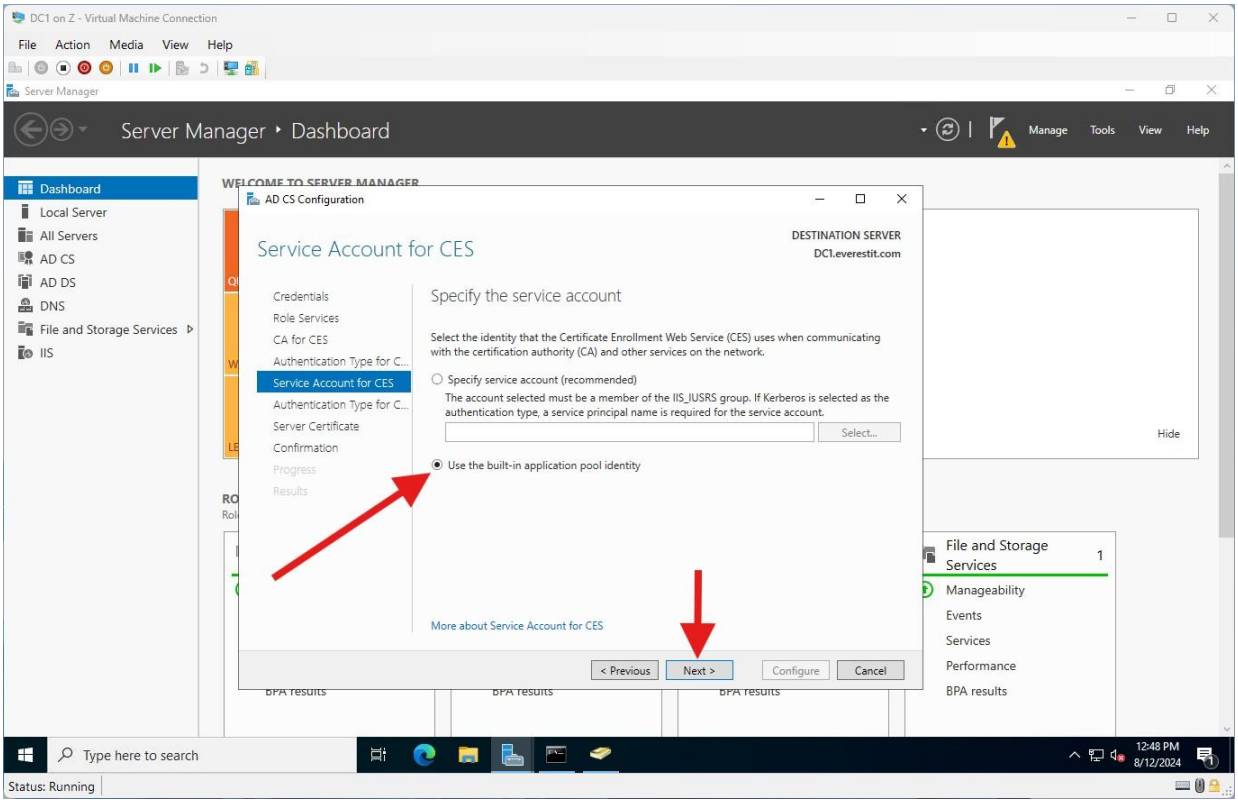
- Select the following three options in the next screen

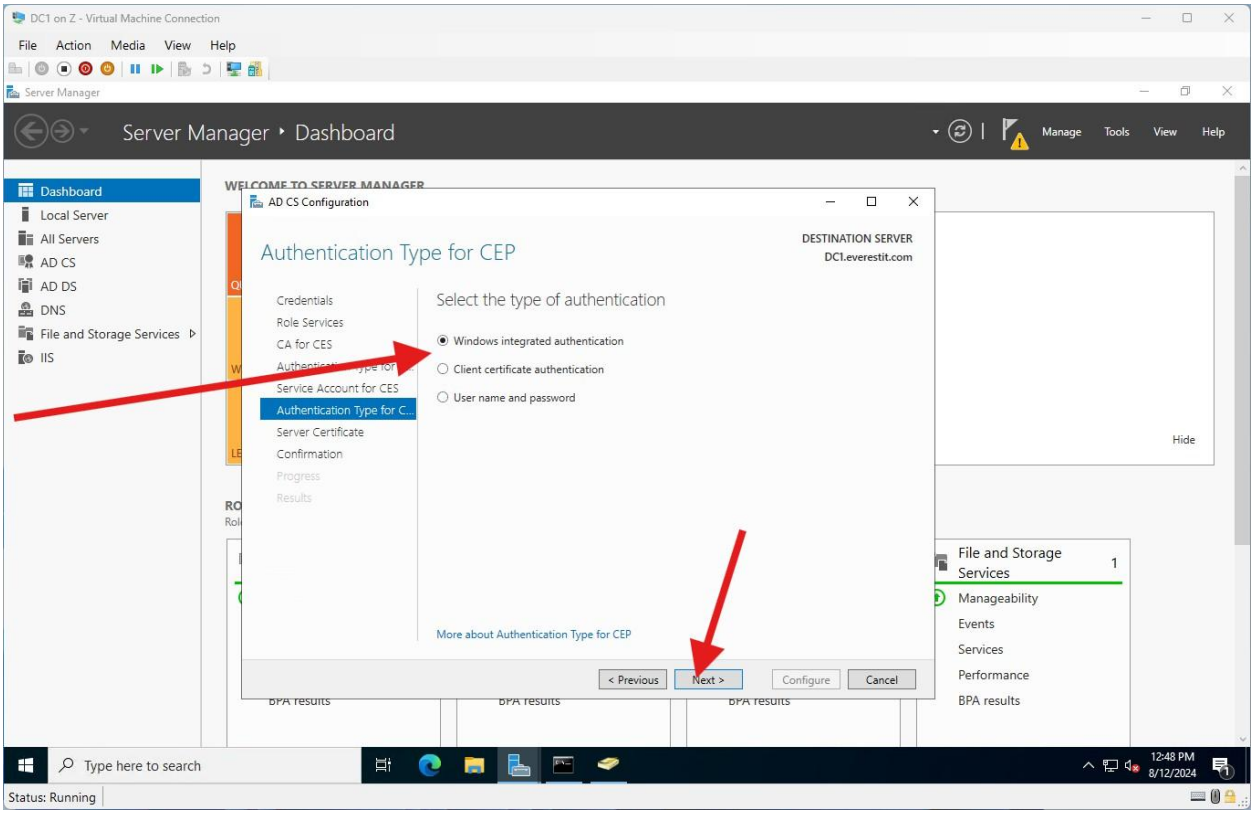



DC1 on Z - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager ‣ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
AD CS Configuration
CA for CES
DESTINATION SERVER
DC1.everestit.com
Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Server Certificate
Confirmation
Progress
Results
Specify CA for Certificate Enrollment Web Services
Select the certification authority (CA) that you want to use for issuing certificates requested through this Certificate Enrollment Web Service (CES).
Select:
CA name
Computer name
Target CA: DC1.everestit.com\everestit-DC1-CA
Select...
Configure the Certificate Enrollment Web Service for renewal-only mode.
Renewal-only mode requires that the targeted CA run at least Windows Server 2008 R2.
More about CA for CES
< Previous
Next >
Configure
Cancel
Hide
File and Storage Services
1
Manageability
Events
Services
Performance
BPA results
Type here to search
12:46 PM
8/12/2024
Status: Running

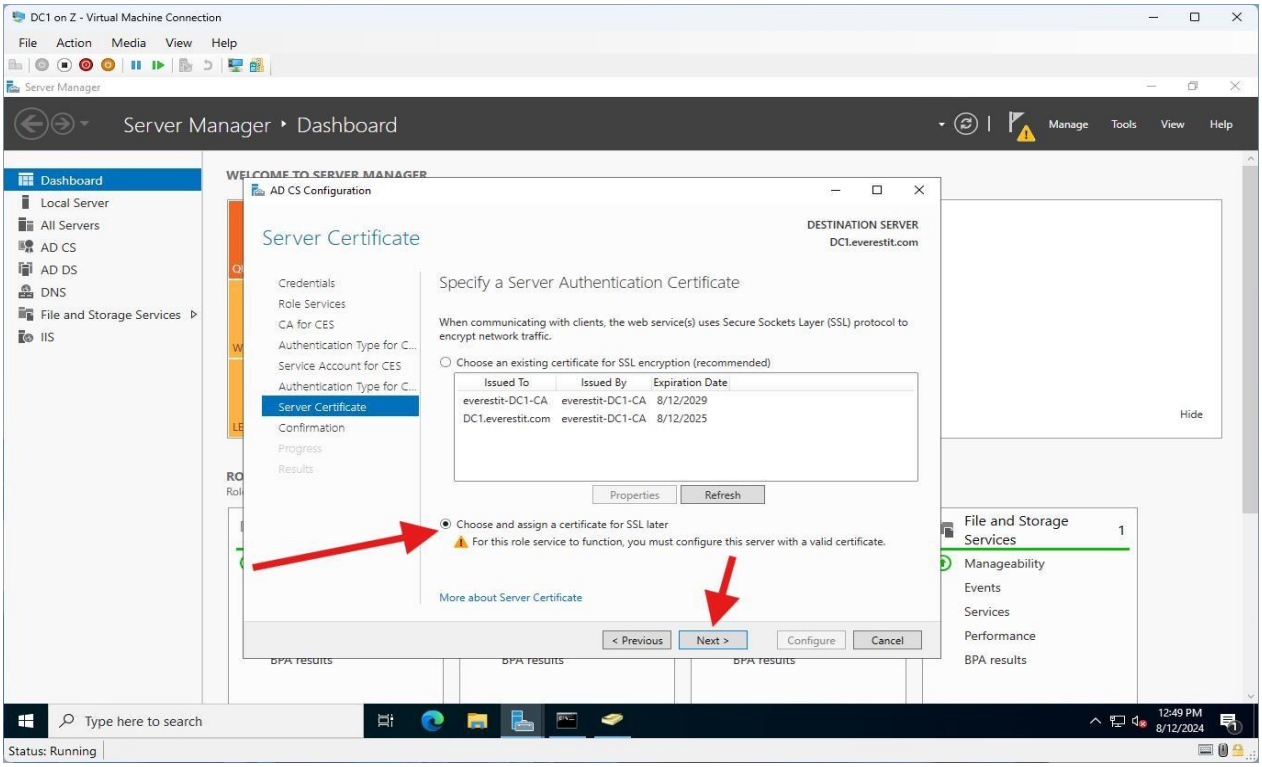

DC1 on Z - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager ‣ Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
AD CS Configuration
Authentication Type for CES
DESTINATION SERVER
DC1.everestit.com
Credentials
Role Services
CA for CES
Service Account for CES
Server Certificate
Confirmation
Progress
Results
Select the type of authentication
Windows integrated authentication
Client certificate authentication
User name and password
More about Authentication Type for CES
< Previous
Next >
Configure
Cancel
Hide
File and Storage Services
1
Manageability
Events
Services
Performance
BPA results
Type here to search
12:47 PM
8/12/2024
Status: Running

- Select built-in application pool identity

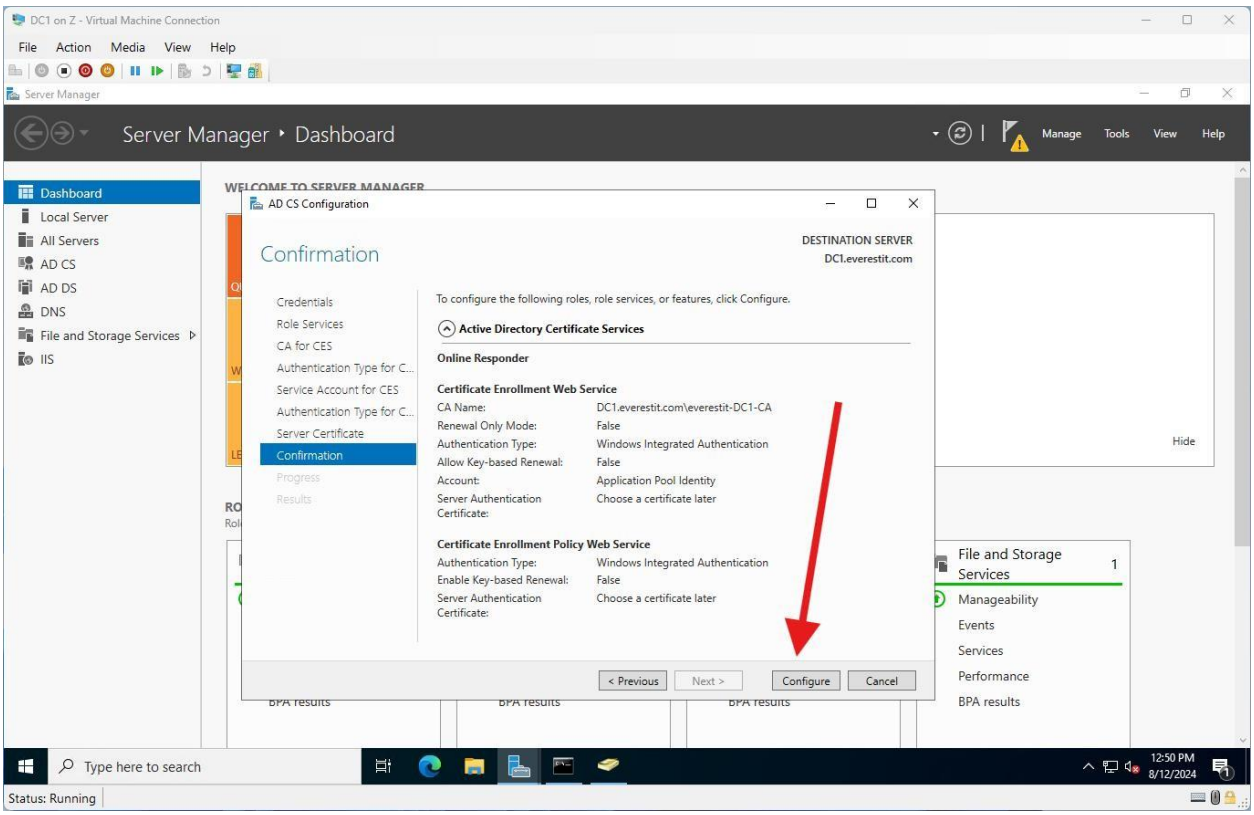


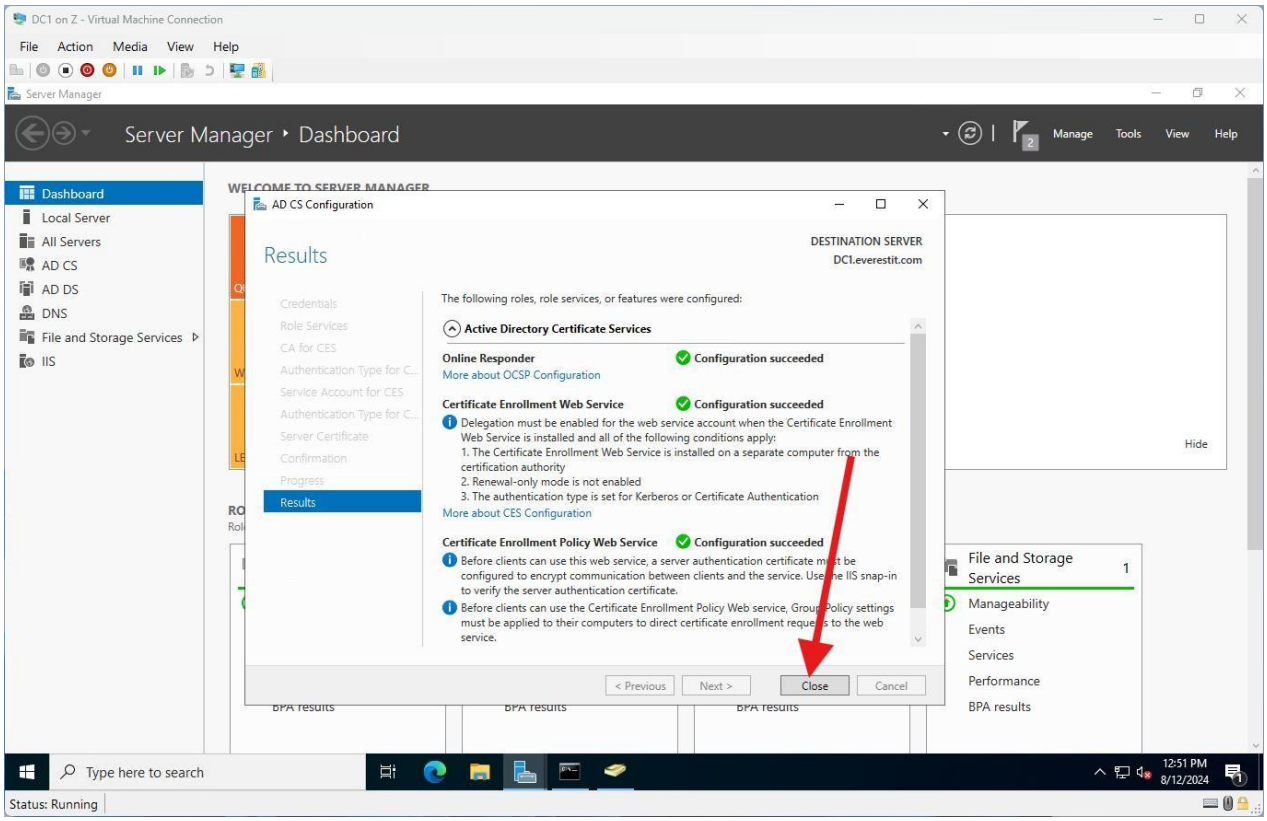


- Here select the option on the bottom of the screen



- Hit configure

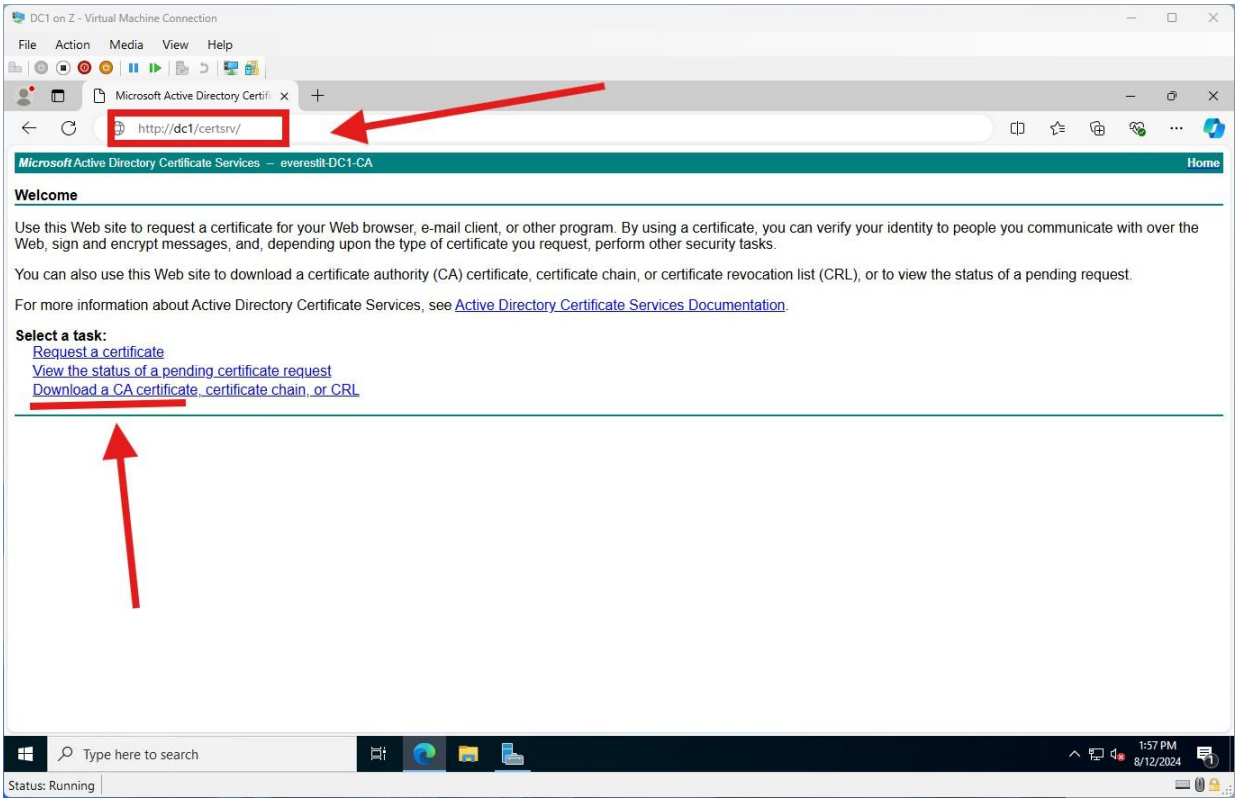


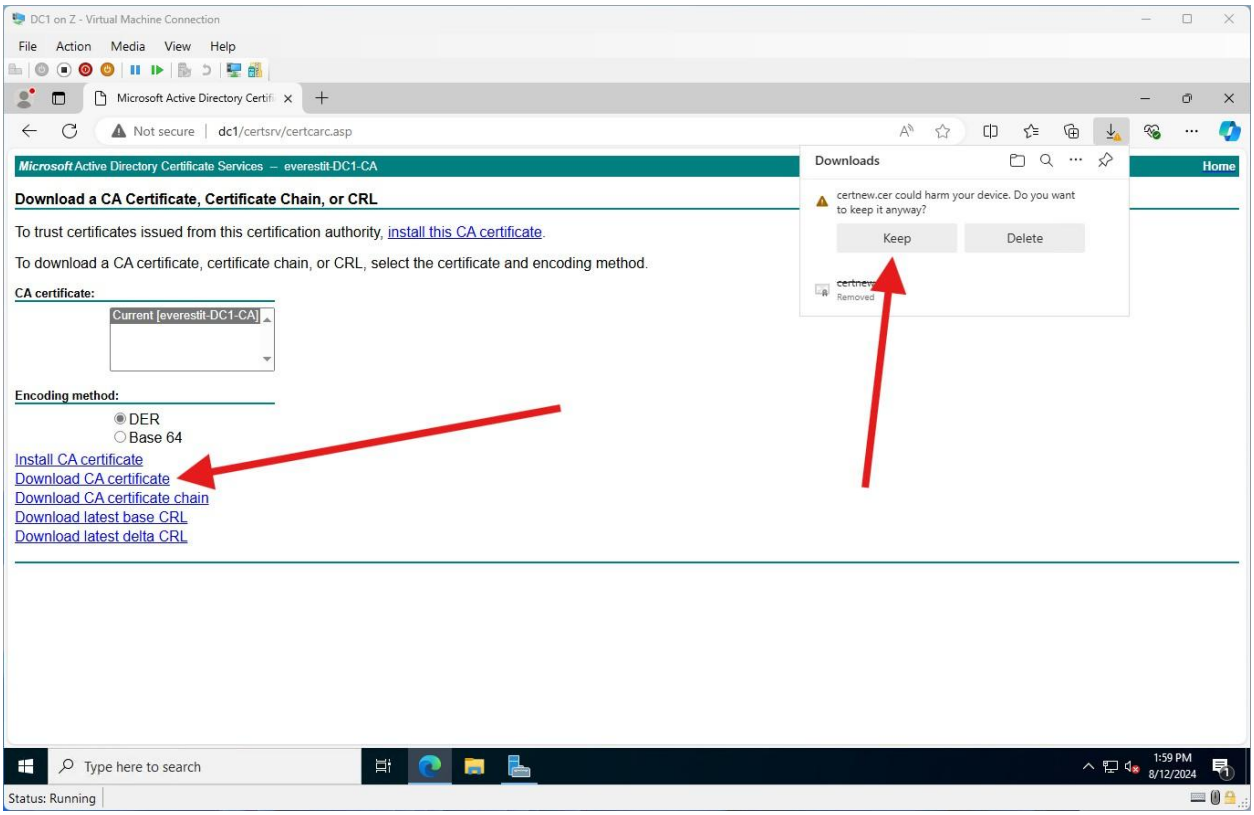


- Close out of this screen
- We just made dc1 our certificate authority so now it can issue the certificates

- In the domain controller pc
- Open a browser and go to
- http://dc1/certsrv
- Make sure to type in http not https
- In my case here dc1 is the hostname of my domain controller so this is a variable depending on what name is your domain controller type accordingly.

- Click on download a CA certificate

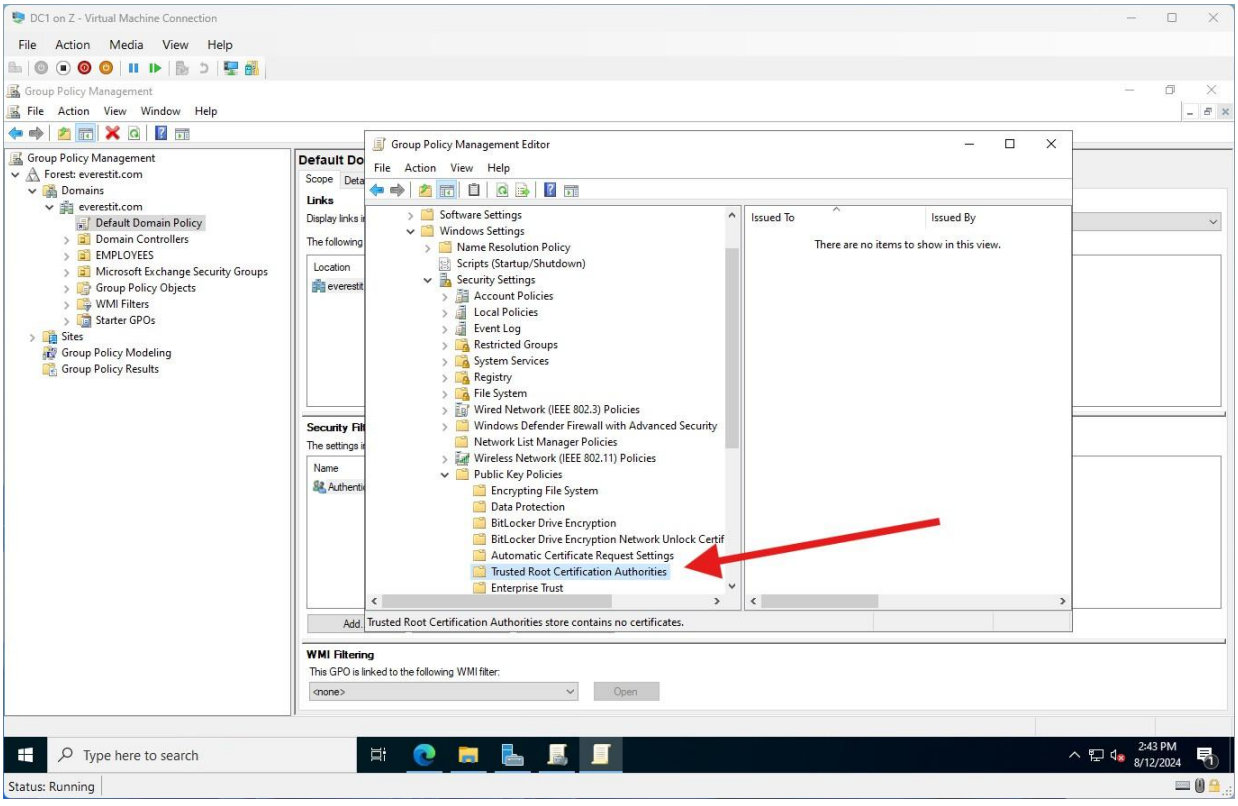




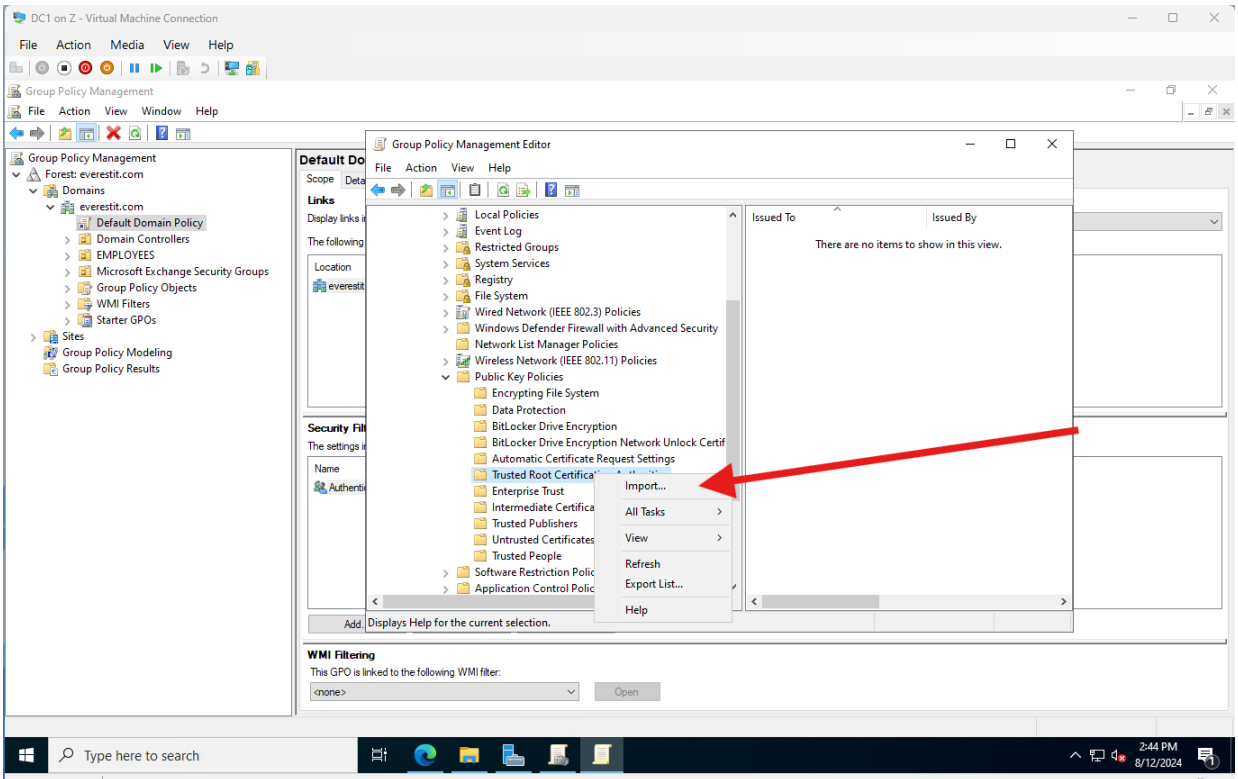
- Warning will pop up just click save
- This certificate we just downloaded
- We need to push it to all the client pcs that are connected to the domain
- In order to do that we need to use group policy

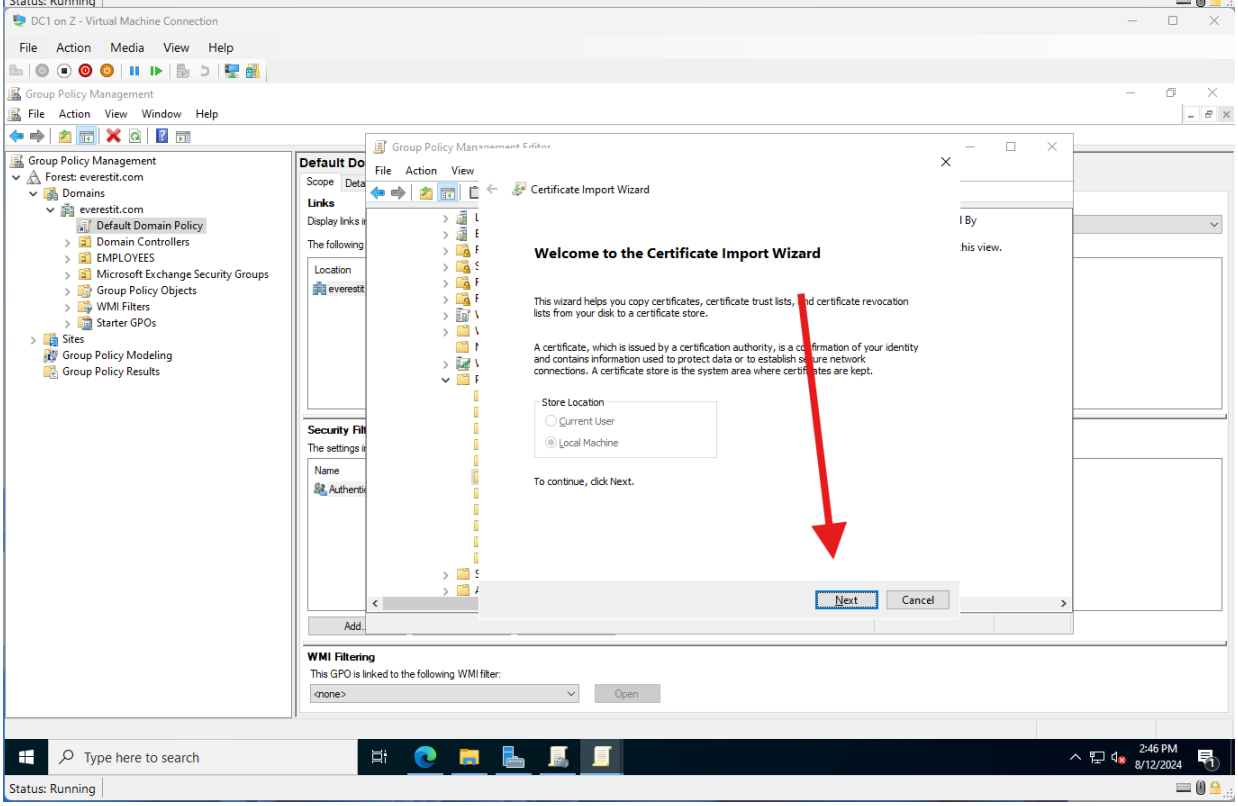
CONFIGURE GROUP POLICY

- Open group policy management
- Go to default domain policy and edit
- Under computer configuration >policies>windows settings>security settings>public key policies>trusted root certification authiorities

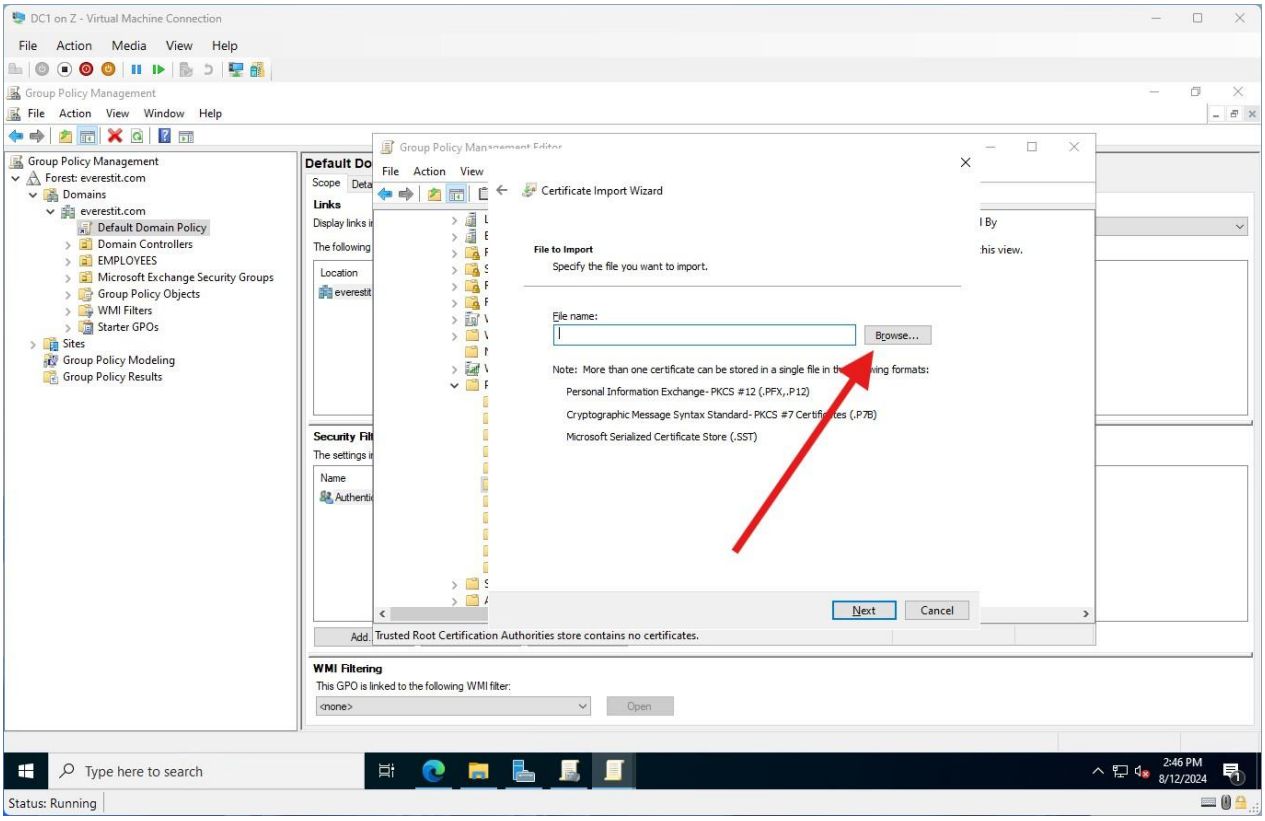


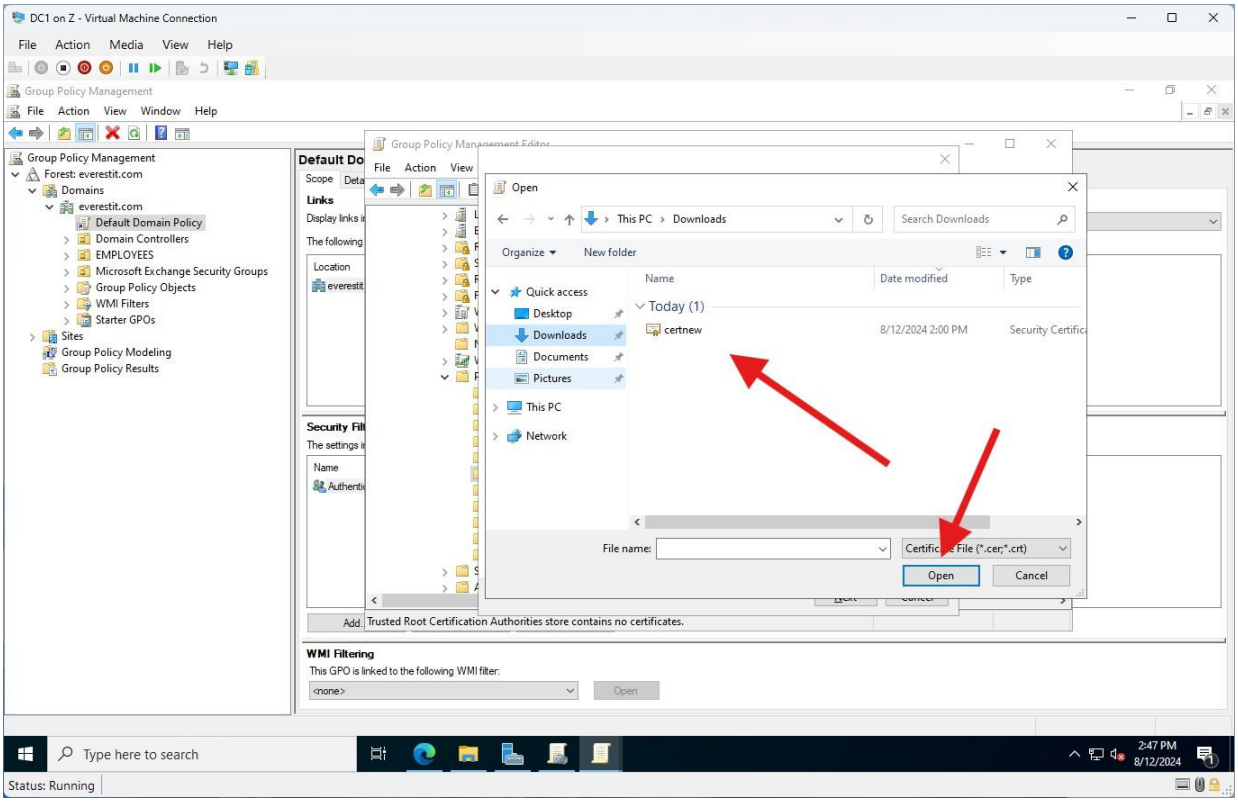
- Rt click on trusted root certification authority and import

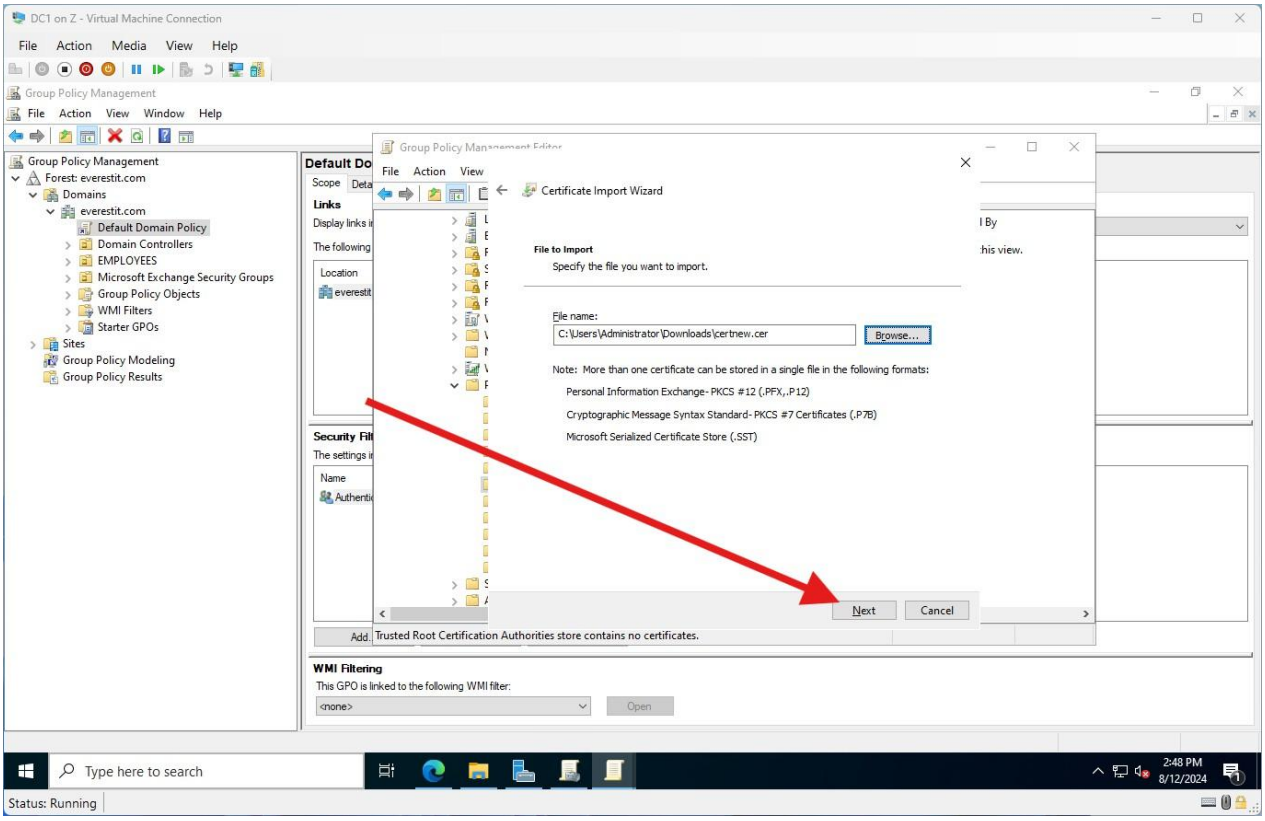


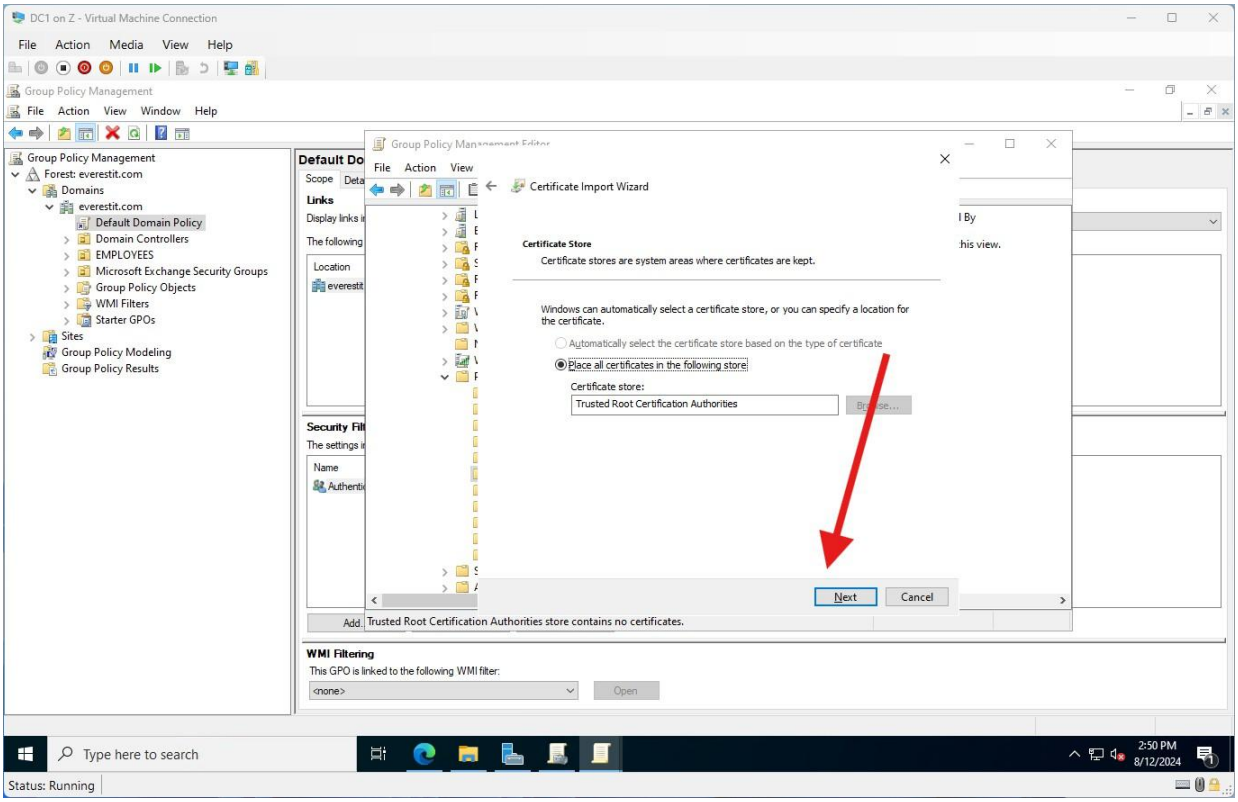


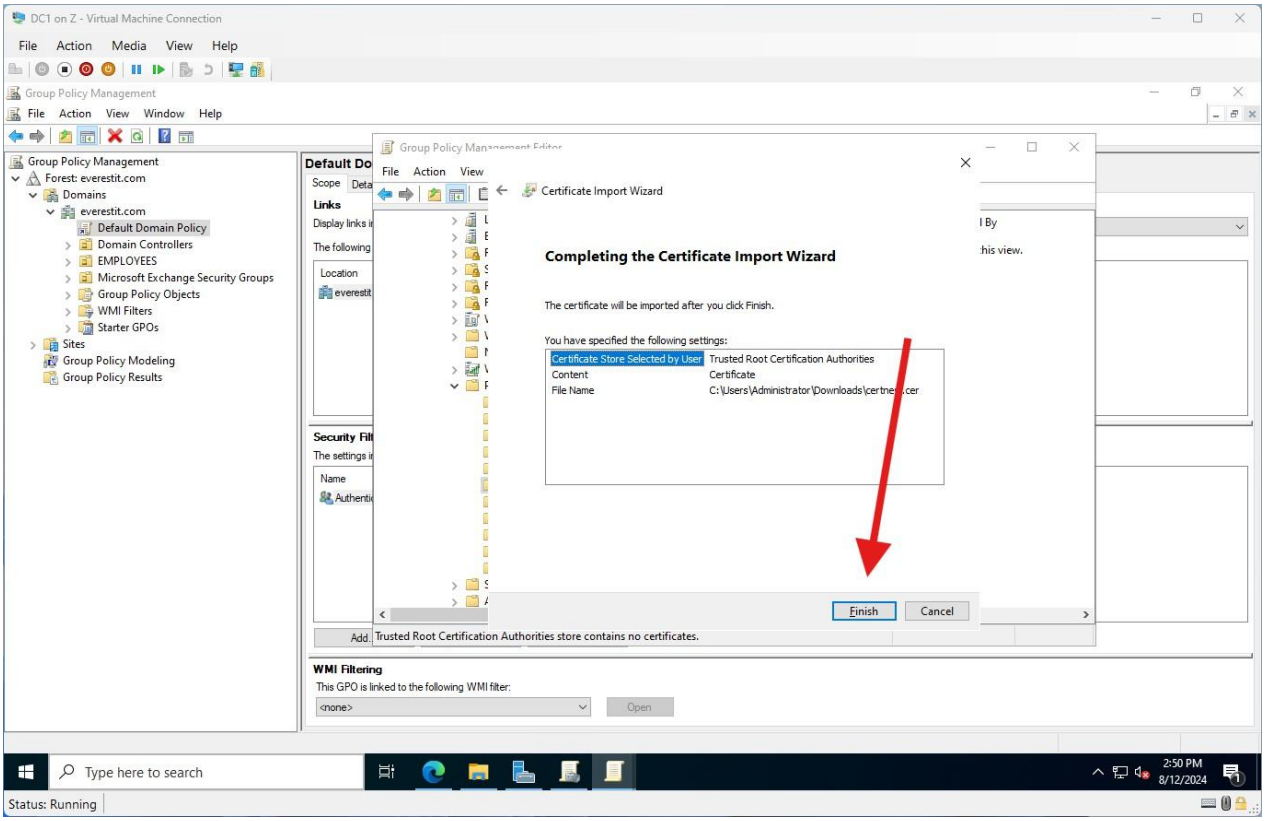
- Select browse and go to the folder where you downloaded it earlier select it and open

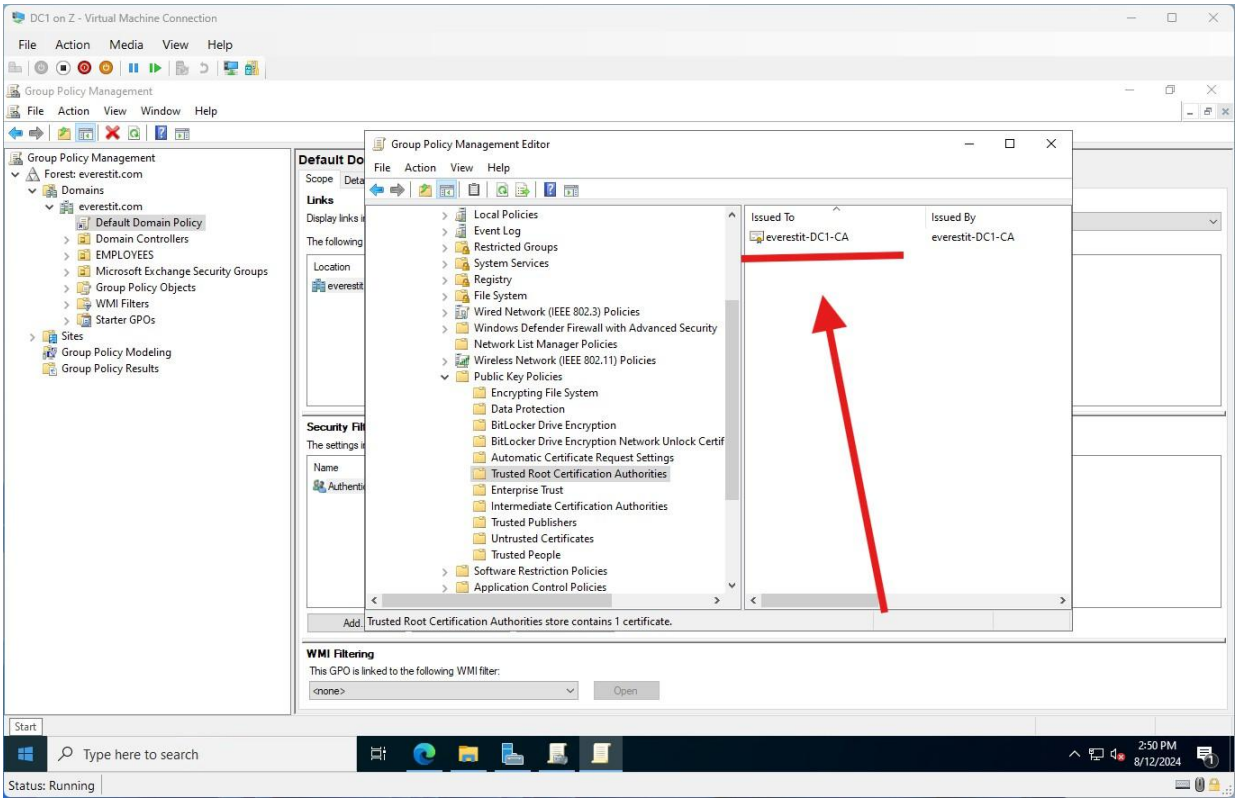




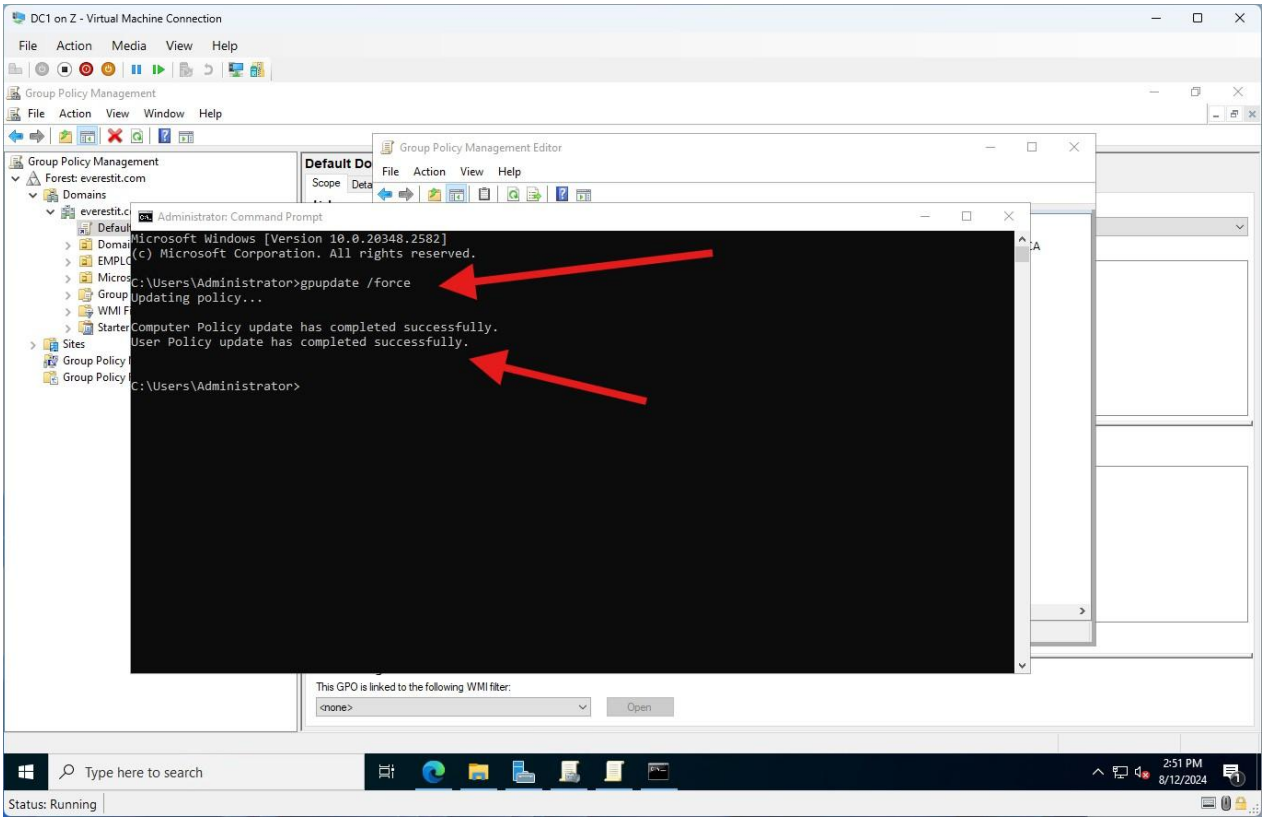

DC1 on Z - Virtual Machine Connection
File Action Media View Help
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: everestit.com
Domains
everestit.com
Default Domain Policy
Domain Controllers
EMPLOYEES
Microsoft Exchange Security Groups
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View
Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
C:\Users\Administrator\Downloads\certnew.cer
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Next
Cancel
Trusted Root Certification Authorities store contains no certificates.
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
Type here to search
2:48 PM
8/12/2024
Status: Running


DC1 on Z - Virtual Machine Connection
File Action Media View Help
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: everestit.com
Domains
everestit.com
Default Domain Policy
Domain Controllers
EMPLOYEES
Microsoft Exchange Security Groups
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities
Browse...
Next
Cancel
Trusted Root Certification Authorities store contains no certificates.
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
Type here to search
2:50 PM
8/12/2024
Status: Running

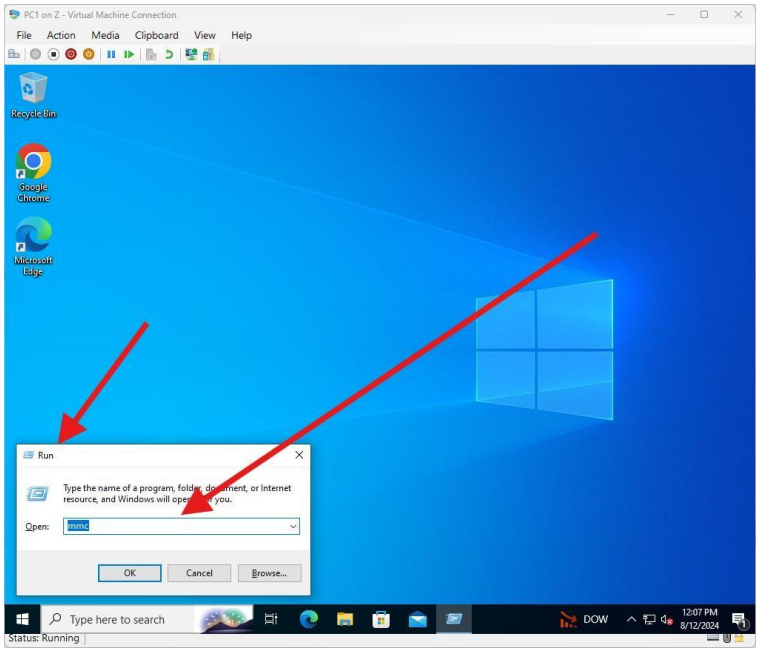

DC1 on Z - Virtual Machine Connection
File Action Media View Help
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: everestit.com
Domains
everestit.com
Default Domain Policy
Domain Controllers
EMPLOYEES
Microsoft Exchange Security Groups
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View
Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certification Authorities
Content
Certificate
File Name
Finish
Cancel
Trusted Root Certification Authorities store contains no certificates.
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
Type here to search
2:50 PM
8/12/2024
Status: Running


DC1 on Z - Virtual Machine Connection
File Action Media View Help
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: everestit.com
Domains
everestit.com
Default Domain Policy
Domain Controllers
EMPLOYEES
Microsoft Exchange Security Groups
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlock Certif
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Software Restriction Policies
Application Control Policies
Issued To
Issued By
everestit-DC1-CA
everestit-DC1-CA
Trusted Root Certification Authorities store contains 1 certificate.
WMI Filtering
This GPO is linked to the following WMI filter:
<none>
Open
Start
Type here to search
2:50 PM
8/12/2024
Status: Running

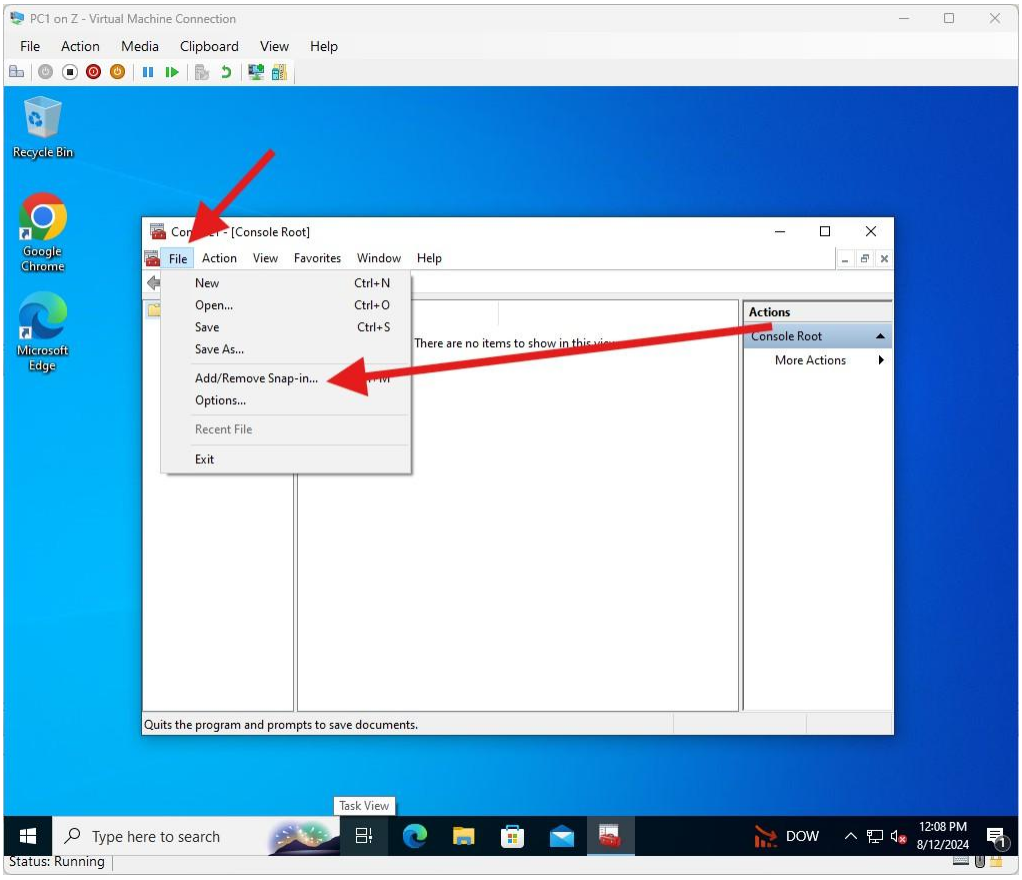
- Once that’s done open cmd prompt in admin mode
- And update the group policy



- If u want to see if this policy got updated in your client pc
- Login to it
- Run >mmc

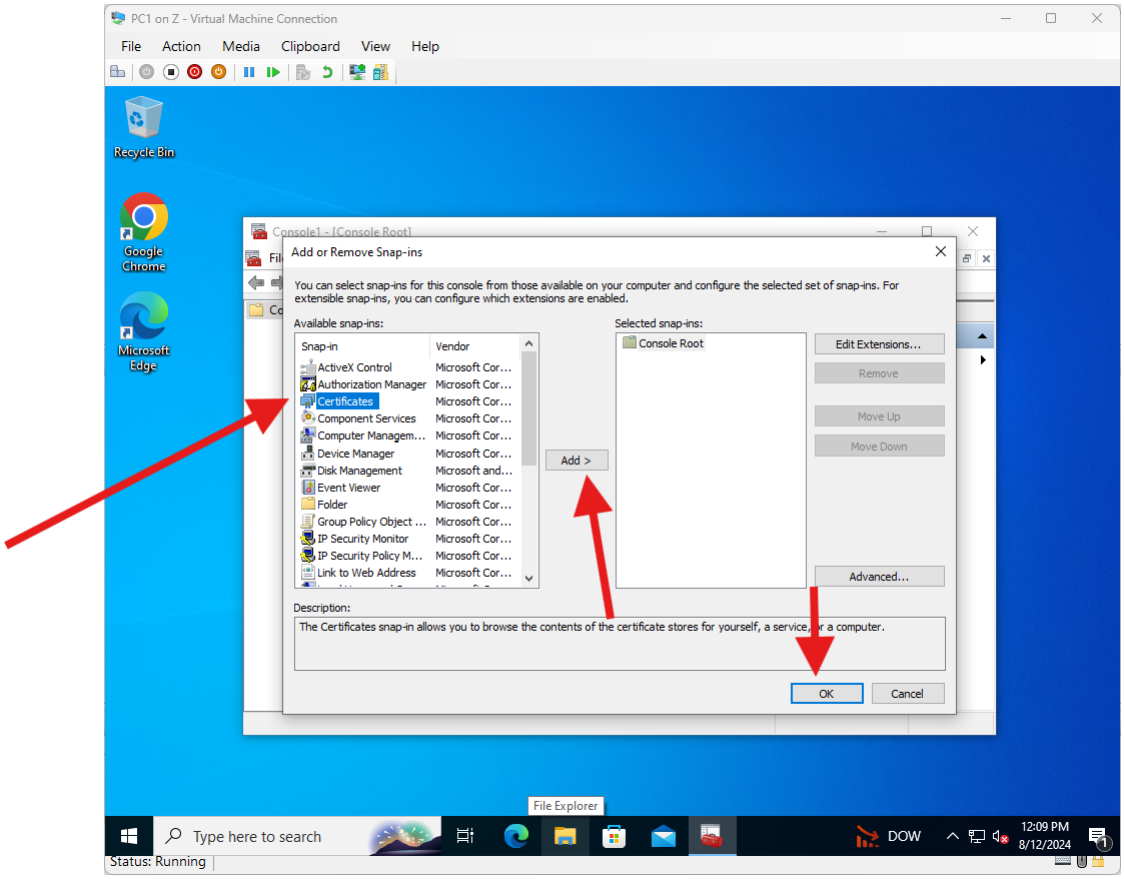


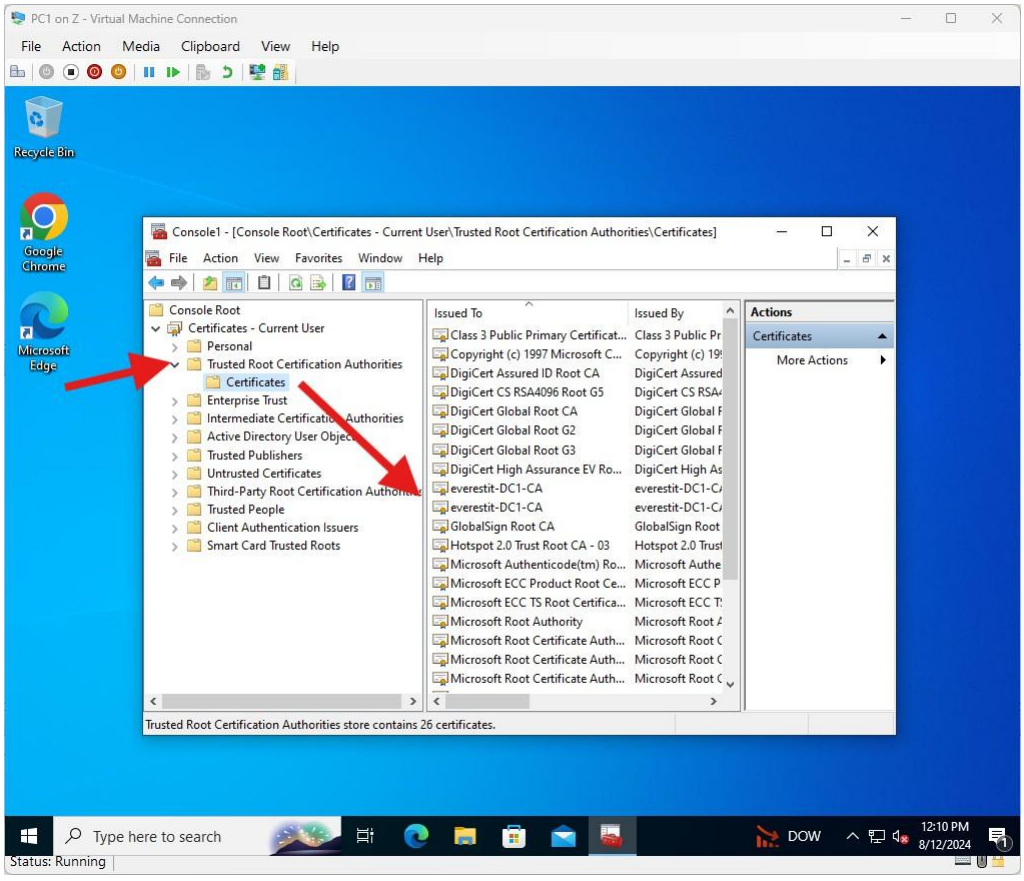
- File>add/remove snapin



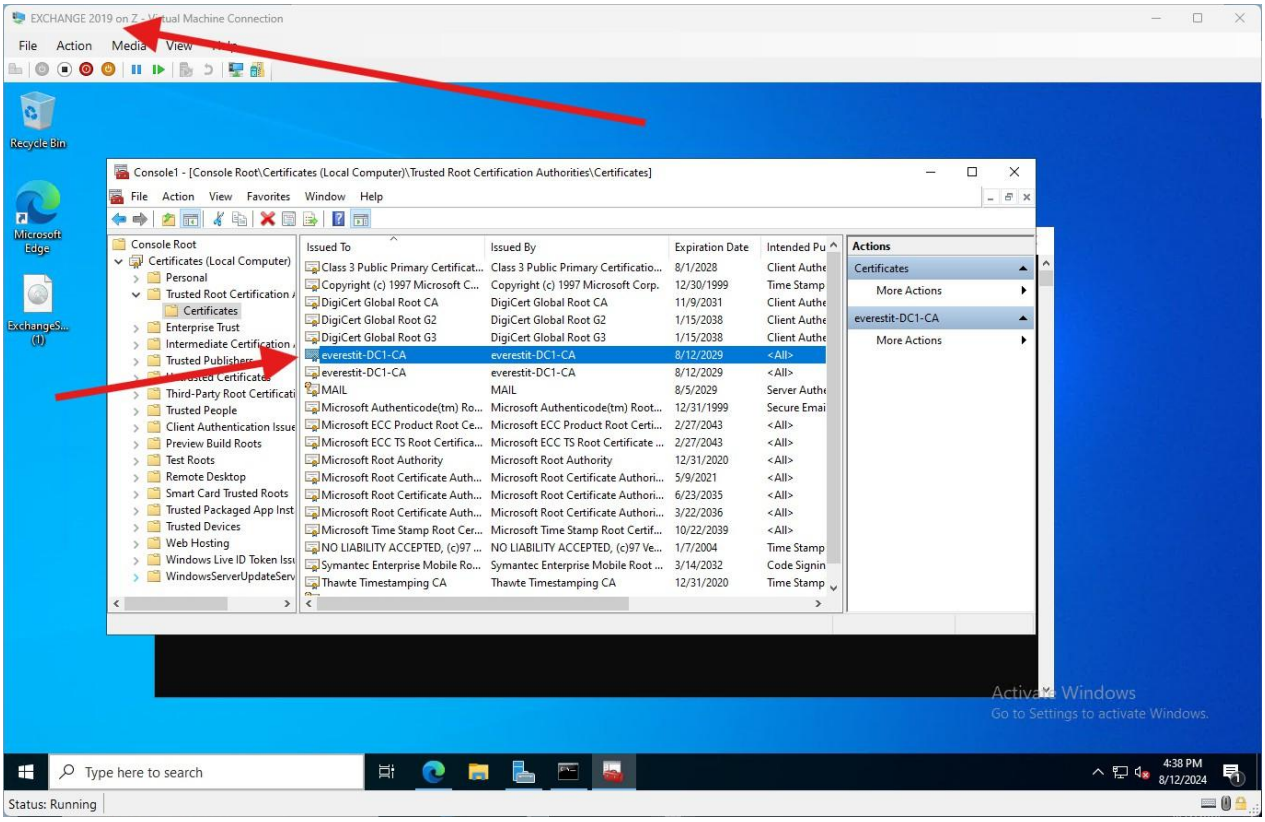
- Select certificates
- add
- ok

- Once out
- Go to trusted root certification authorities > certificates
- Here you can see the new certificates

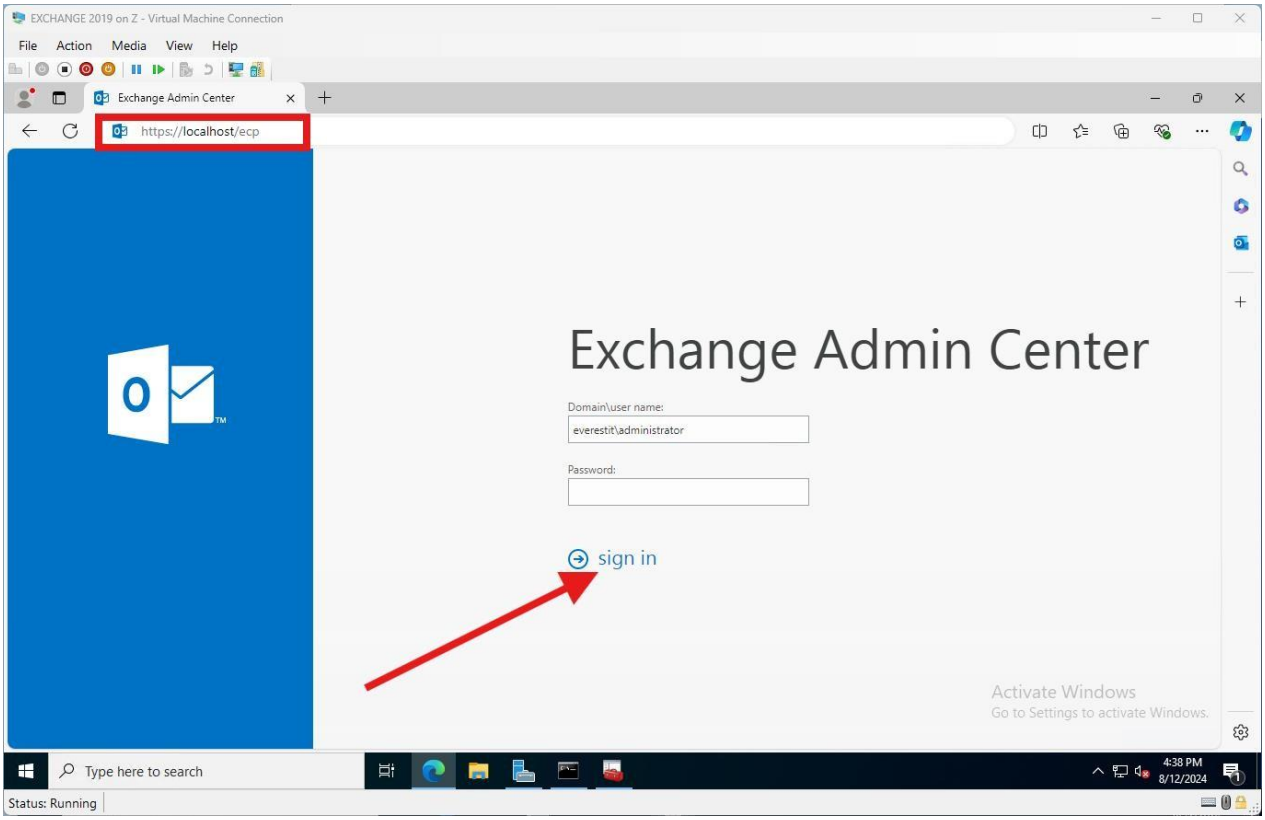

PC1 on Z - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Google Chrome
Microsoft Edge
Console1 - [Console Root]
Add or Remove Snap-ins
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.
Available snap-ins:
Snap-in
Vendor
ActiveX Control
Authorization Manager
Certificates
Component Services
Computer Managem...
Device Manager
Disk Management
Event Viewer
Folder
Group Policy Object ...
IP Security Monitor
IP Security Policy M...
Link to Web Address
Add >
Selected snap-ins:
Console Root
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
Description:
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.
OK
Cancel
File Explorer
Type here to search
DOW
12:09 PM
8/12/2024
Status: Running


PC1 on Z - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Google Chrome
Microsoft Edge
Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File Action View Favorites Window Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Smart Card Trusted Roots
Issued To
Issued By
Class 3 Public Primary Certificat...
Copyright (c) 1997 Microsoft C...
DigiCert Assured ID Root CA
DigiCert CS RSA4096 Root G5
DigiCert Global Root CA
DigiCert Global Root G2
DigiCert Global Root G3
DigiCert High Assurance EV Ro...
everestit-DC1-CA
everestit-DC1-CA
GlobalSign Root CA
Hotspot 2.0 Trust Root CA - 03
Microsoft Authenticode(tm) Ro...
Microsoft ECC Product Root Ce...
Microsoft ECC TS Root Certifica...
Microsoft Root Authority
Microsoft Root Certificate Auth...
Microsoft Root Certificate Auth...
Microsoft Root Certificate Auth...
Actions
Certificates
More Actions
Trusted Root Certification Authorities store contains 26 certificates.
Type here to search
DOW
12:10 PM
8/12/2024
Status: Running

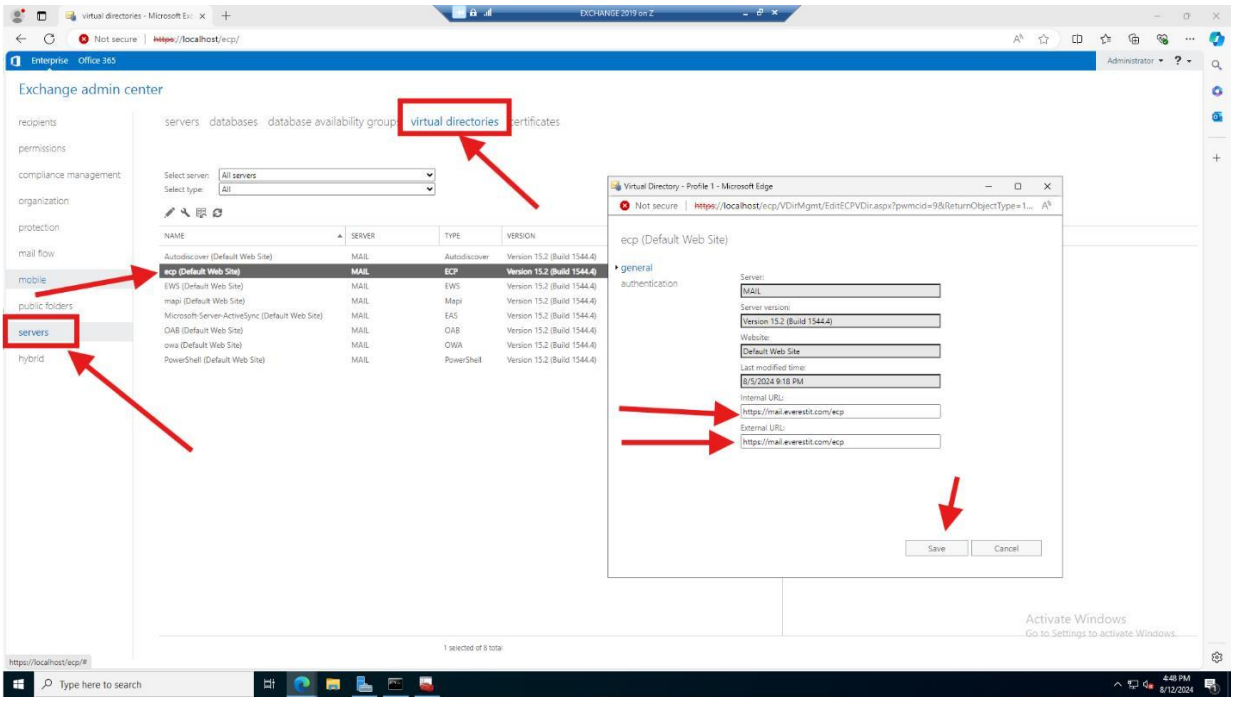
- Now go to exchange server
- Check to see if the certificate we pushed out using group policy is updated here or not
- Follow the same process as before but this time in exchange server to check the certificate
- And verify the certificate

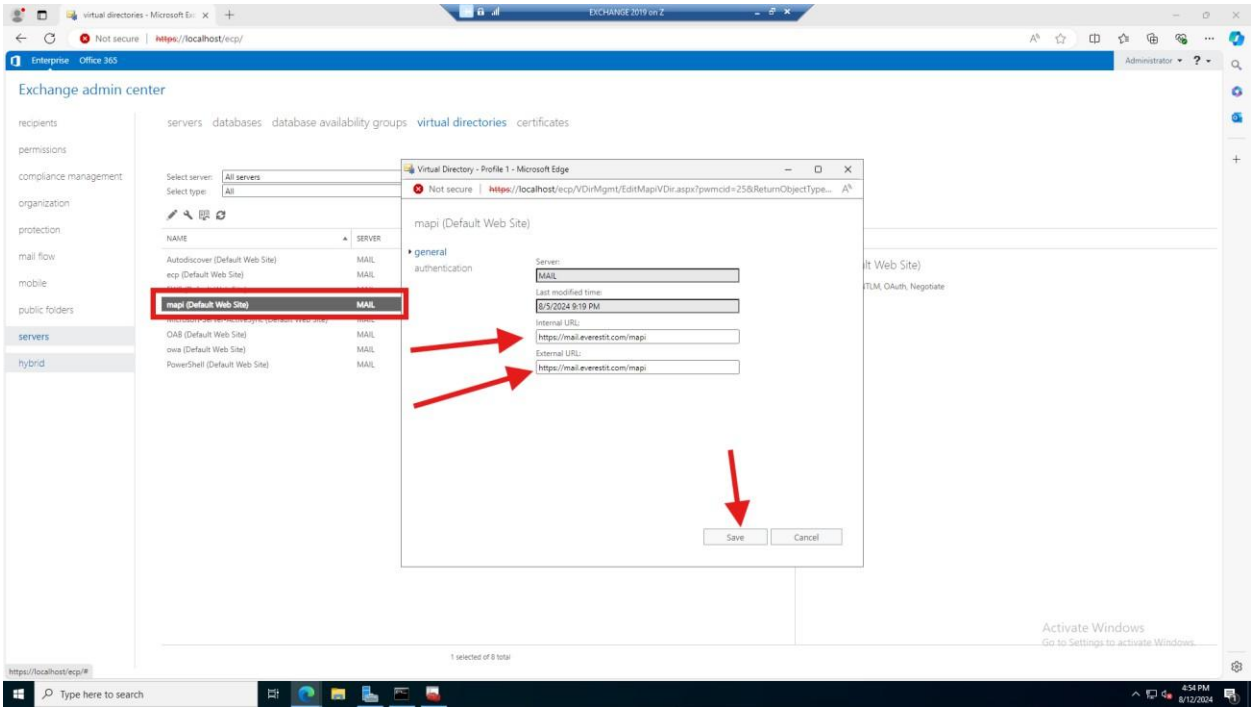


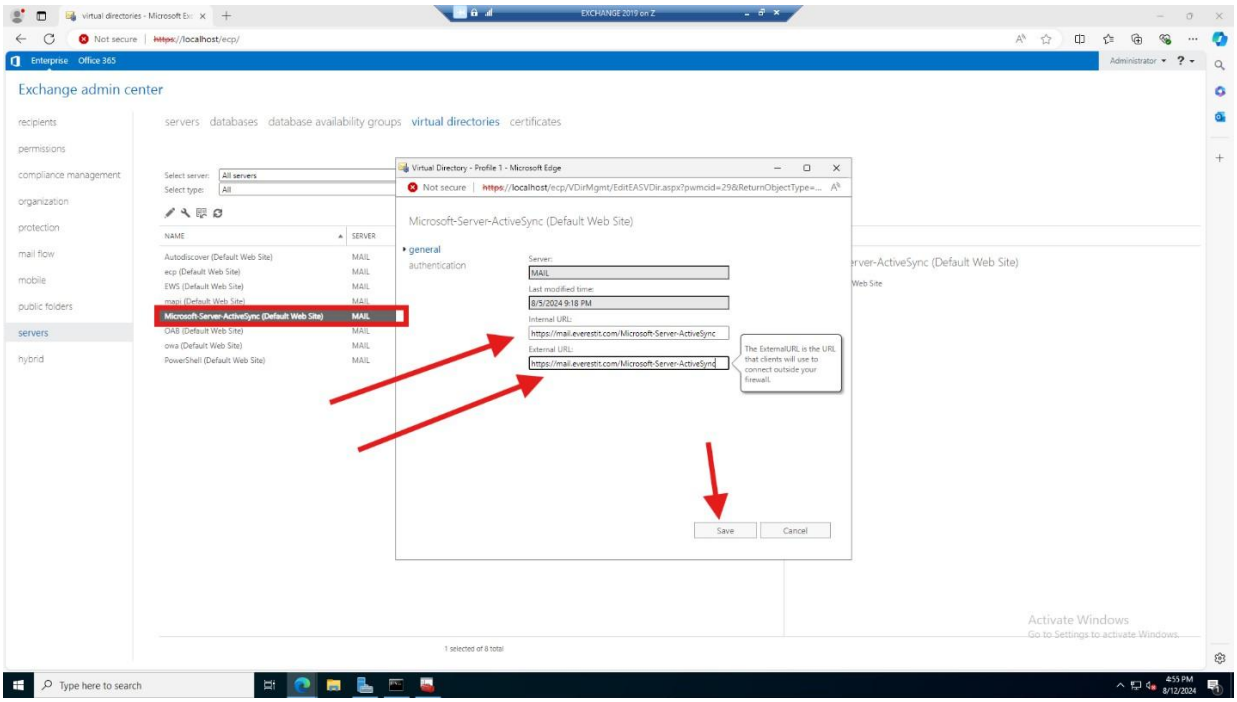
- While in the exchange server
- Open a browser and login to ecp

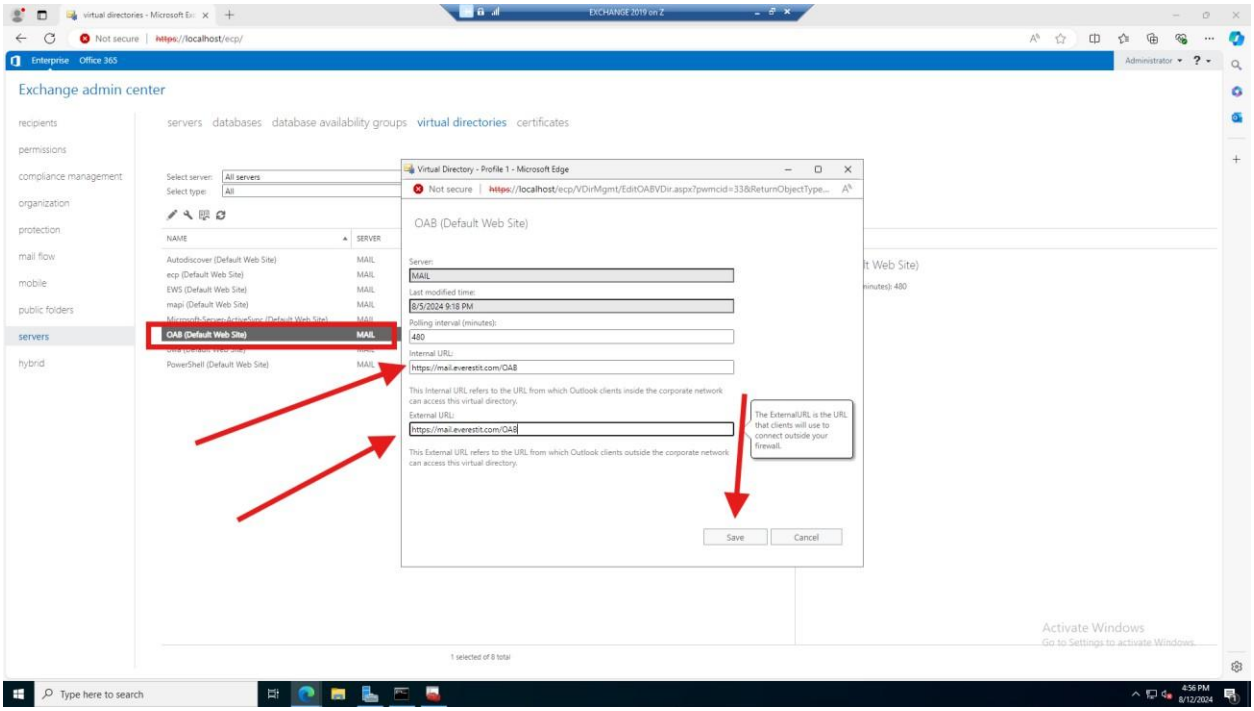


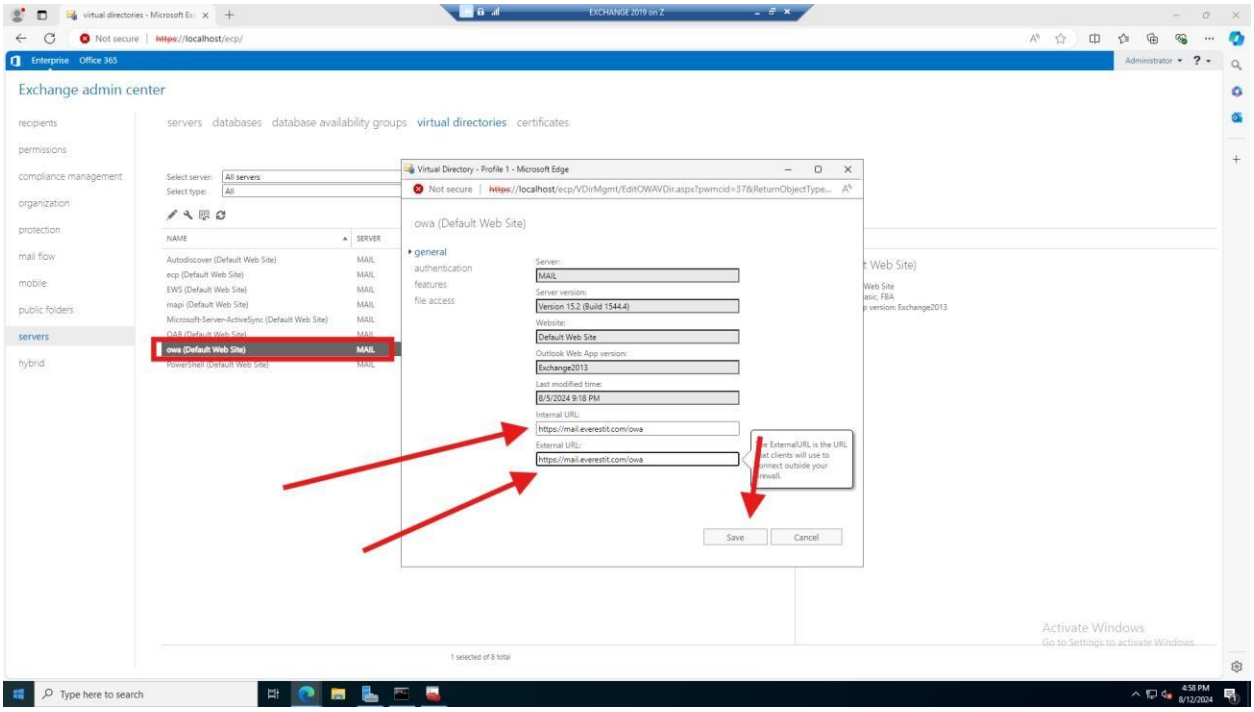
- Once inside
- Click on servers then virtual directories
- Since at this time we are not configuring mail from outside of the firewall
- For each of the options below copy the internal url and paste in the external url
- Make it the same



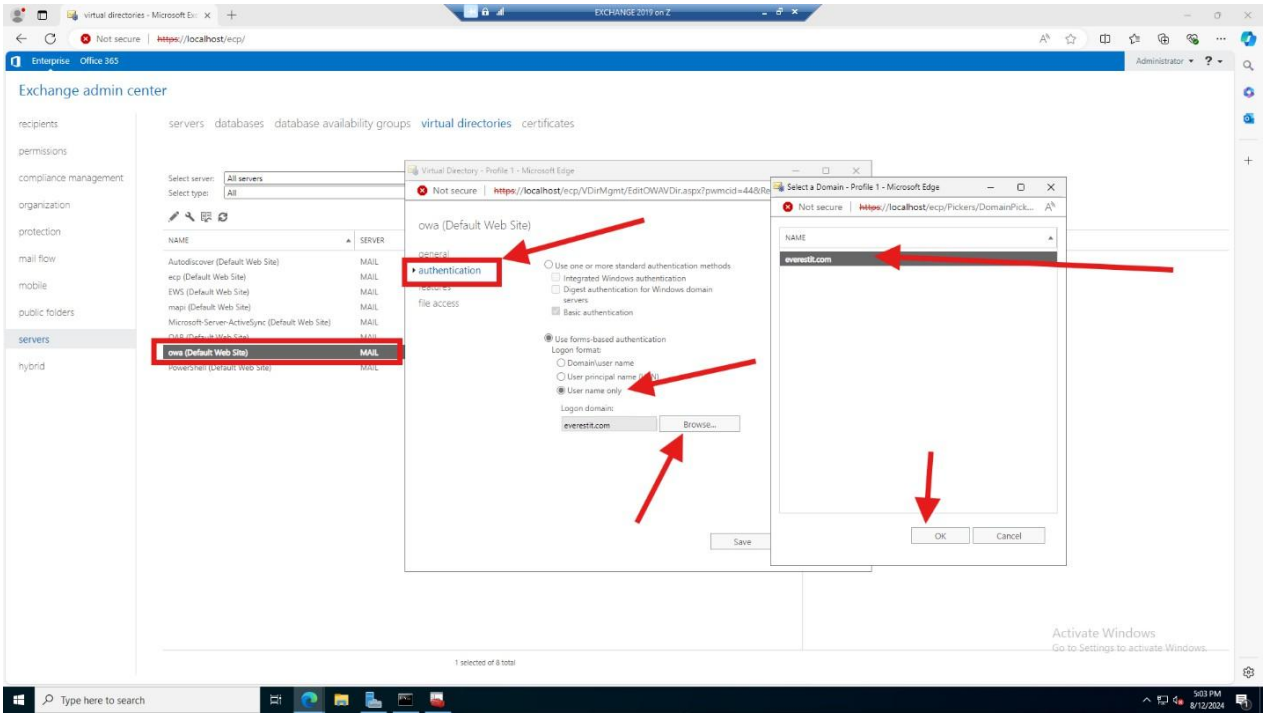

Exchange admin center
servers databases database availability groups virtual directories certificates
Virtual Directory - Profile 1 - Microsoft Edge
mapi (Default Web Site)
general
authentication
Server:
MAIL
Last modified time:
8/5/2024 9:19 PM
Internal URL:
https://mail.everestit.com/mapi
External URL:
https://mail.everestit.com/mapi
Save
Cancel


Exchange admin center
servers databases database availability groups virtual directories certificates
Virtual Directory - Profile 1 - Microsoft Edge
Microsoft-Server-ActiveSync (Default Web Site)
general
authentication
Server:
MAIL
Last modified time:
8/5/2024 9:18 PM
Internal URL:
https://mail.everestit.com/Microsoft-Server-ActiveSync
External URL:
https://mail.everestit.com/Microsoft-Server-ActiveSync
The ExternalURL is the URL that clients will use to connect outside your firewall.
Save
Cancel

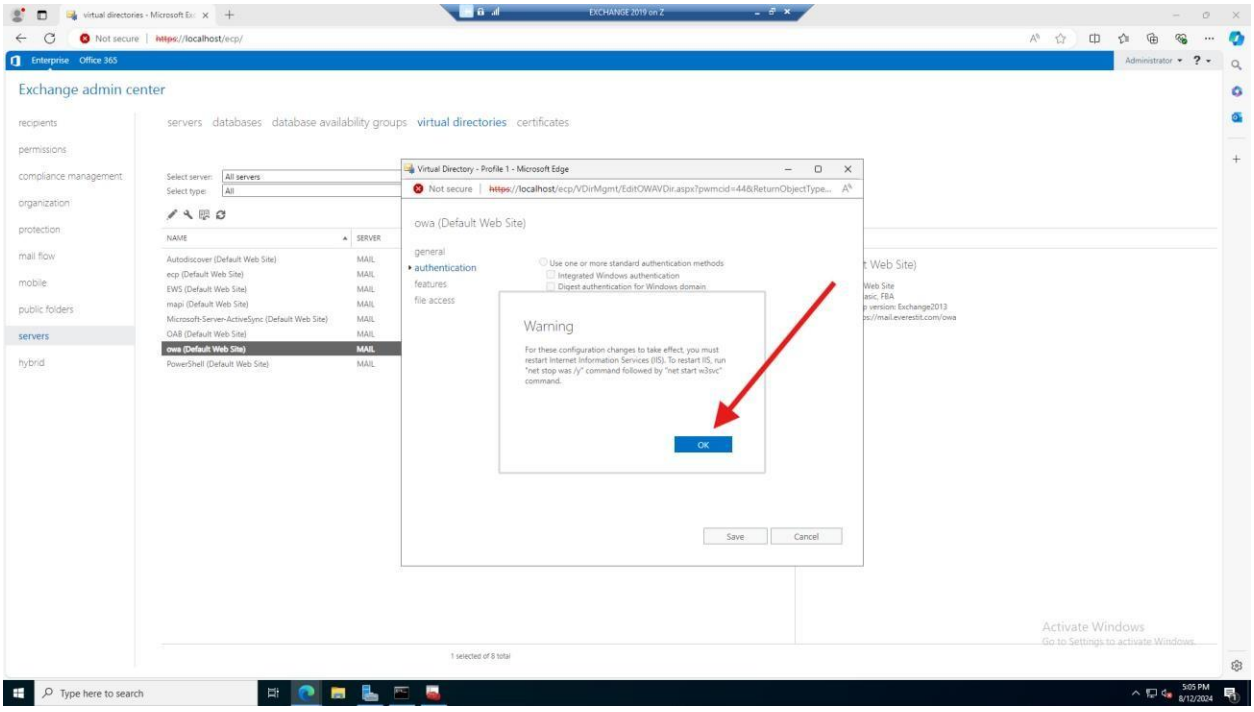

Exchange admin center
servers databases database availability groups virtual directories certificates
Virtual Directory - Profile 1 - Microsoft Edge
OAB (Default Web Site)
Server:
MAIL
Last modified time:
8/5/2024 9:18 PM
Polling interval (minutes):
480
Internal URL:
https://mail.everestit.com/OAB
External URL:
https://mail.everestit.com/OAB
The ExternalURL is the URL that clients will use to connect outside your firewall.
Save
Cancel


Exchange admin center
servers databases database availability groups virtual directories certificates
Virtual Directory - Profile 1 - Microsoft Edge
owa (Default Web Site)
general
authentication
features
file access
Server:
MAIL
Server version:
Version 15.2 (Build 1544.4)
Website:
Default Web Site
Outlook Web App version:
Exchange2013
Last modified time:
8/5/2024 9:18 PM
Internal URL:
https://mail.everestit.com/owa
External URL:
https://mail.everestit.com/owa
Save
Cancel

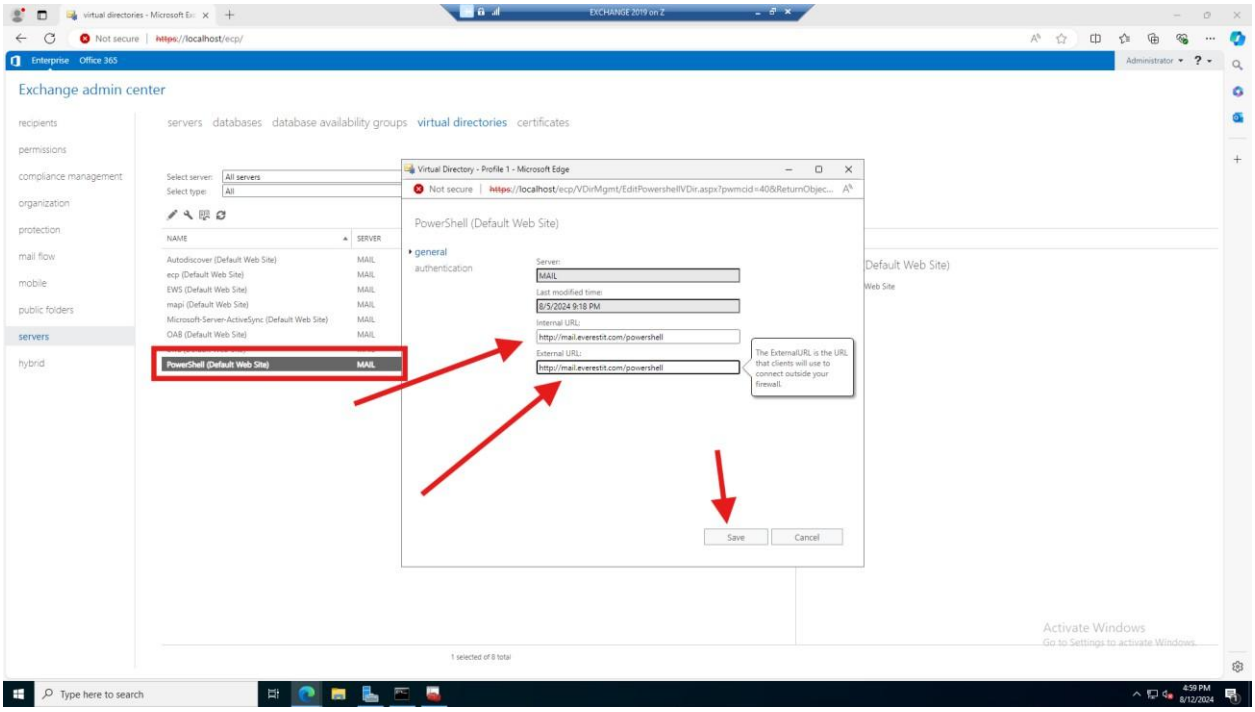
- In owa window go to authentication and also select user name only so it removes the hassle of typing the domain name all the time
- Select browse and select the domain and hit ok



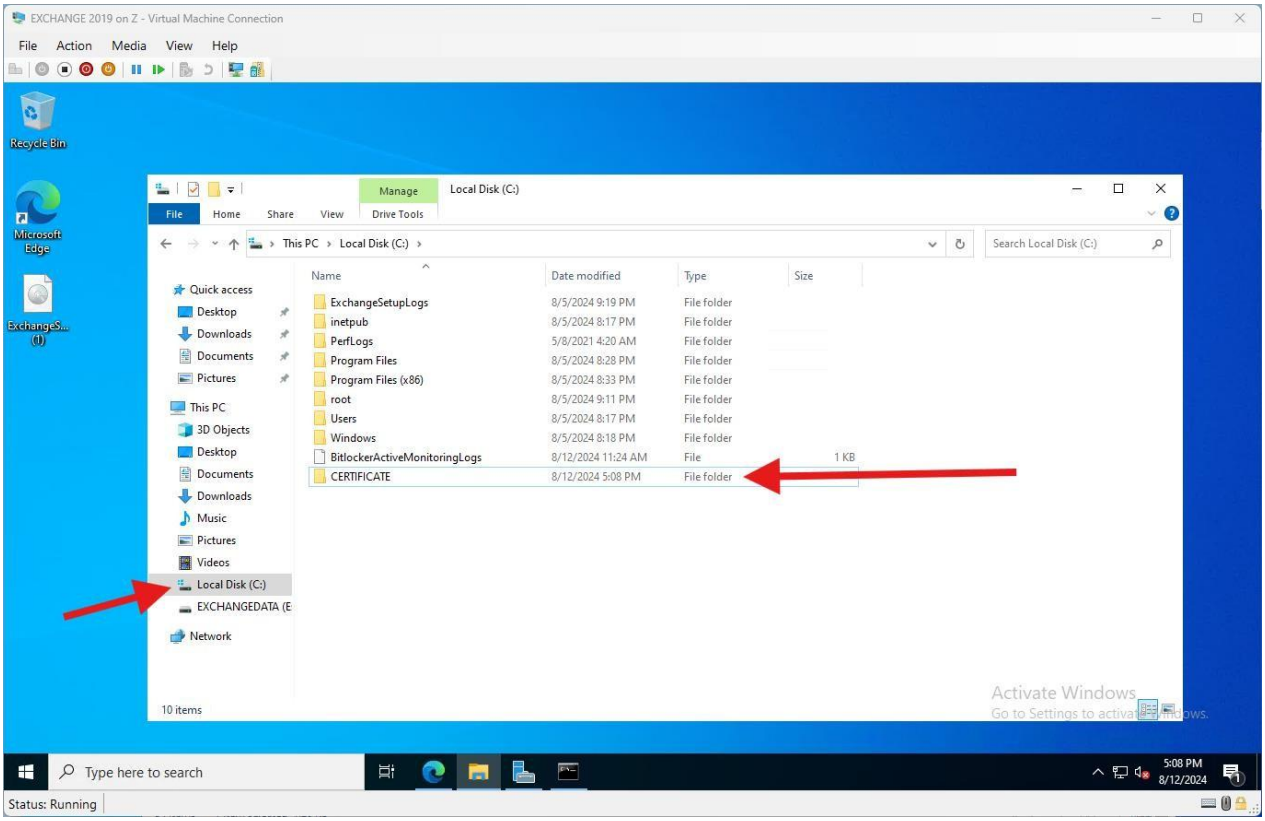
- Following warning will pop up, select ok



- Continue to the last option



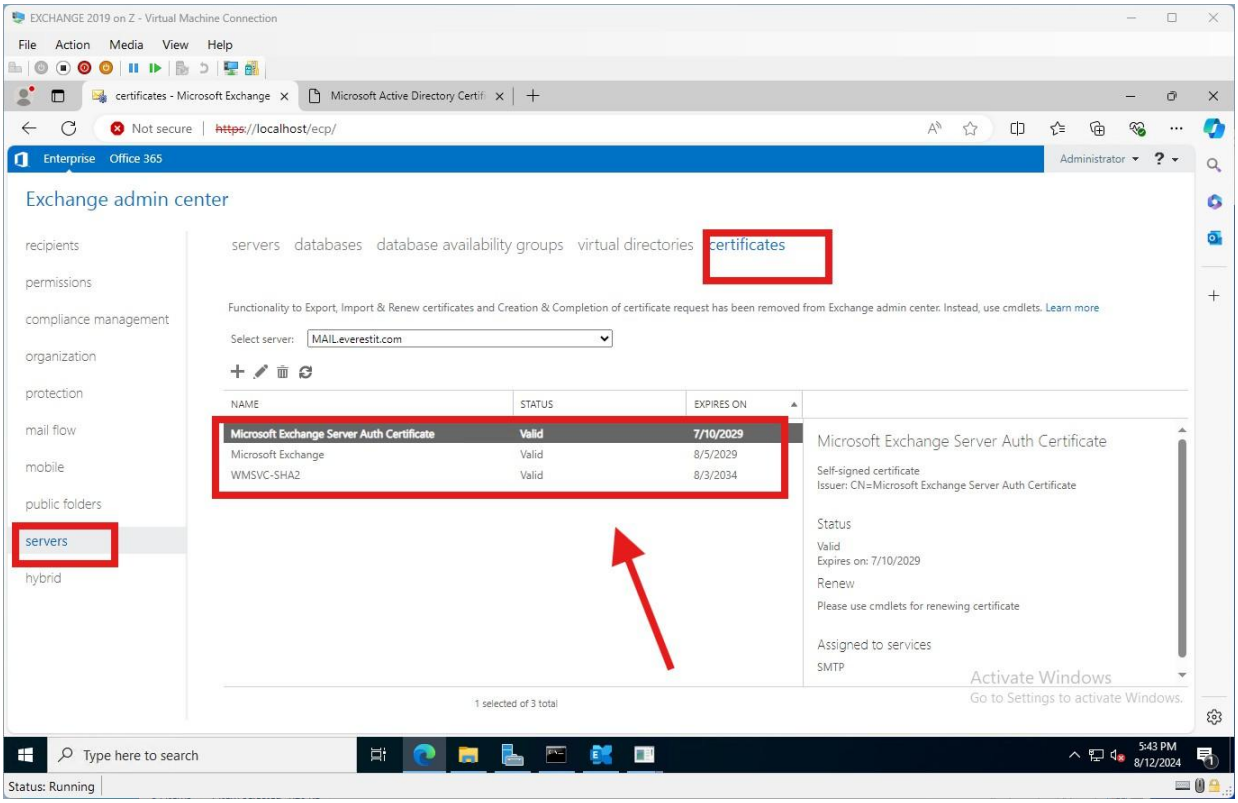
NOW GO TO C DRIVE AND CREATE A FOLDER AND SHARE IT WITH DOMAIN ADMIN



- RT CLICK /PROPERTIES /SHARING /SHARE
- Share it with the domain admins only

AFTER THAT GO BACK TO EXCHANGE ADMIN CENTER

- In a browser login to ecp
- Go to servers / certificates, here we see only 3 certificated but now our task is to add another certificate issued by our own certificate authority that is in the domain controller

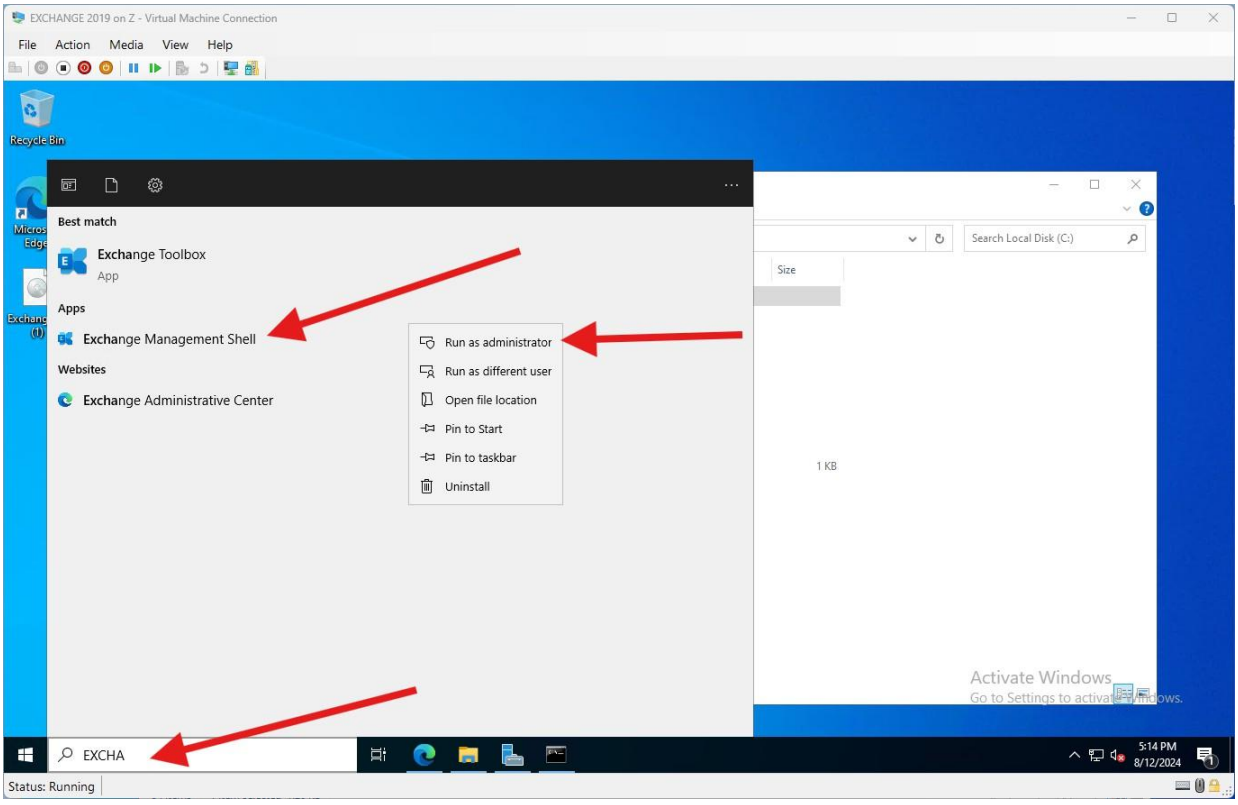


- To complete that task
- We need to create a random key
- In order to do that copy and paste the code below in to exchange Management shell

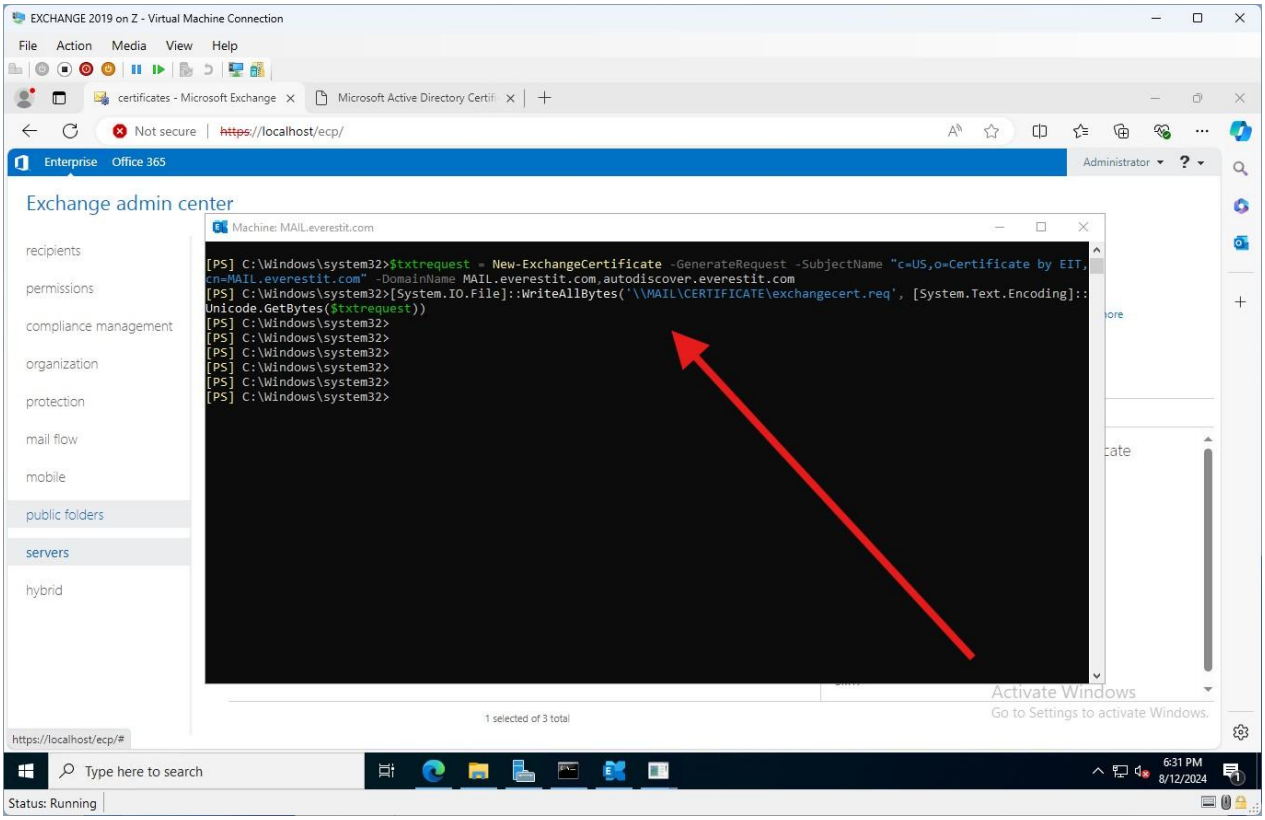
$txtrequest = New-ExchangeCertificate -GenerateRequest -SubjectName "c=US,o=Certificate by EIT,cn=MAIL.everestit.com" -DomainName MAIL.everestit.com,autodiscover.everestit.com
[System.IO.File]::WriteAllBytes('\\MAIL\CERTIFICATE\exchangecert.req',
[System.Text.Encoding]::Unicode.GetBytes($txtrequest))

- In my case the "CERTIFICATE" in the red is the name of the folder I created in C drive earlier so be careful and update the code as necessary

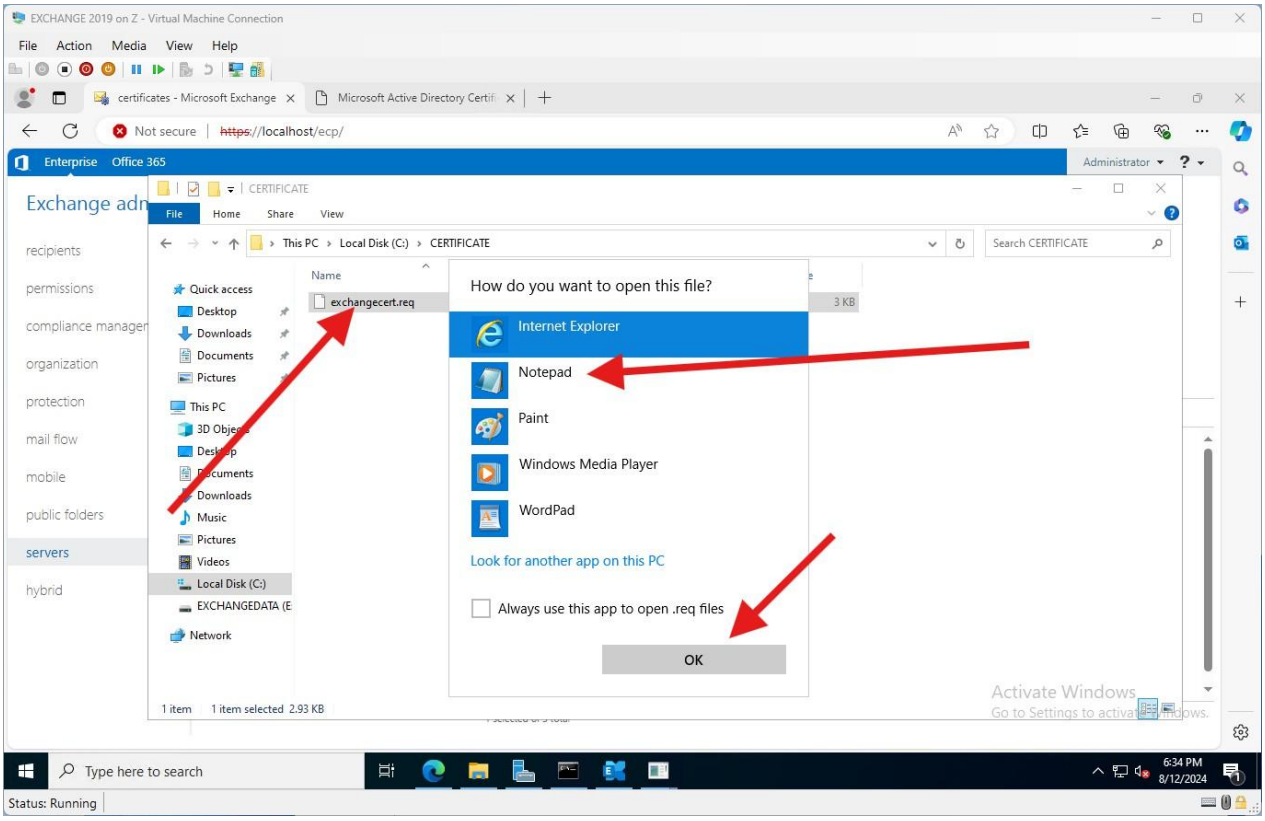
- Open exchange management shell



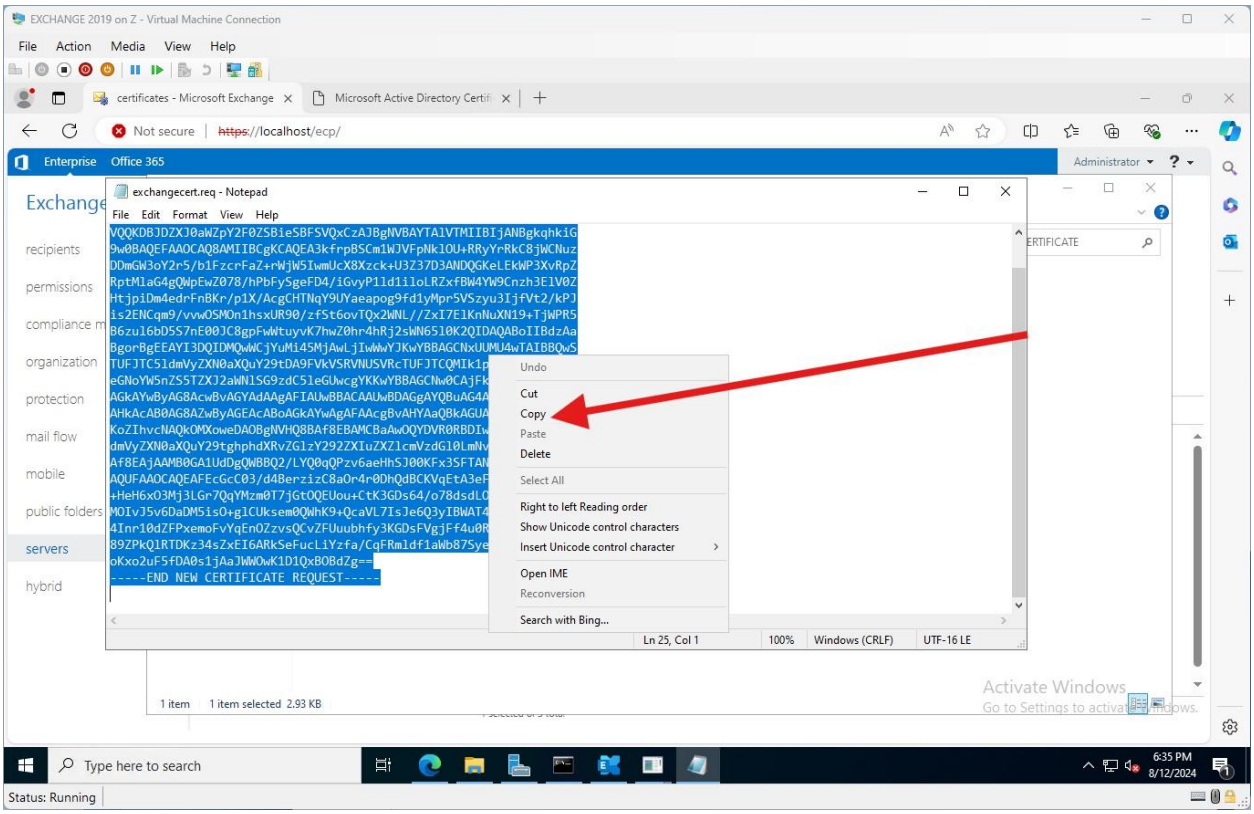
- It will take a few moments for the window to become active for taking in commands
- So be patient
- Once the window becomes active hit enter a few times
- In order to paste the copied code just rt click in the window and it will automatically paste
- Hit enter, this will execute the code



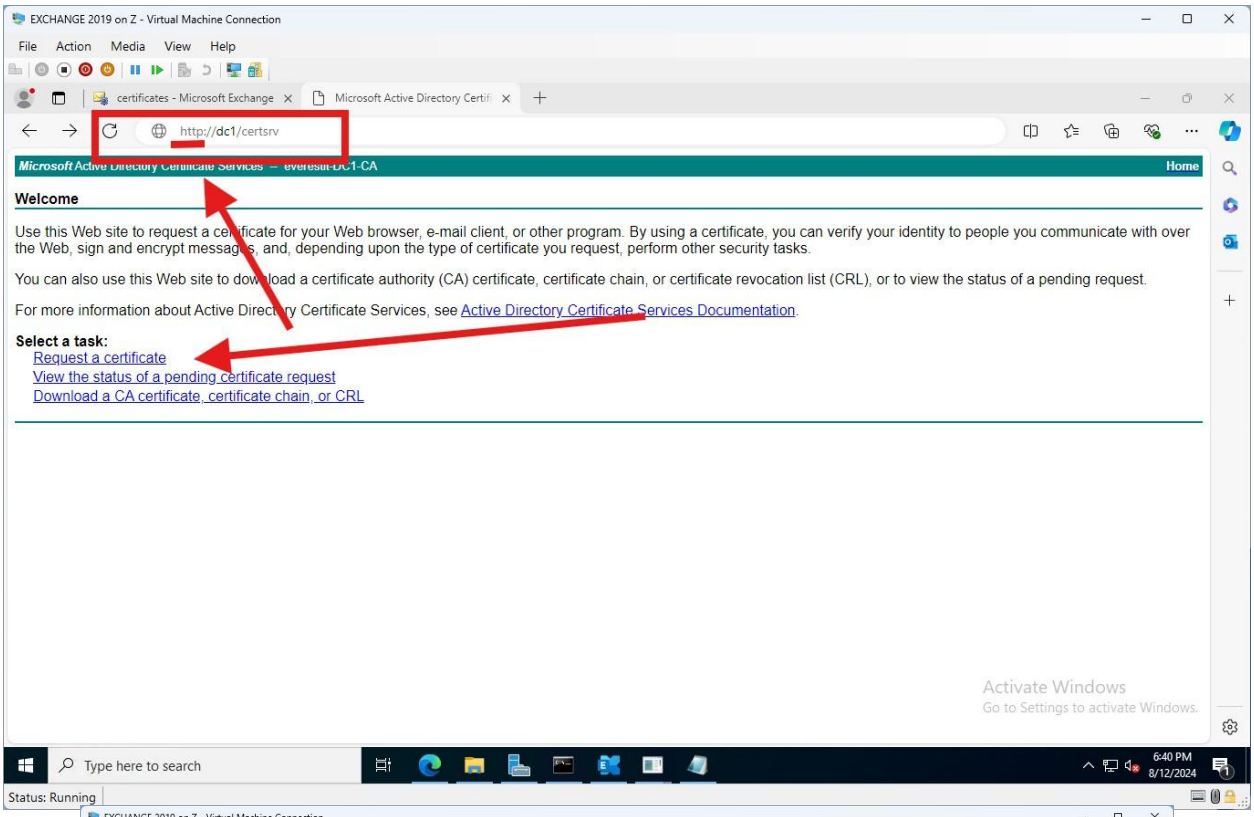
- once the code is executed go back out to the CERTIFICATE folder in C drive and you will see the file
- open that file in notepad

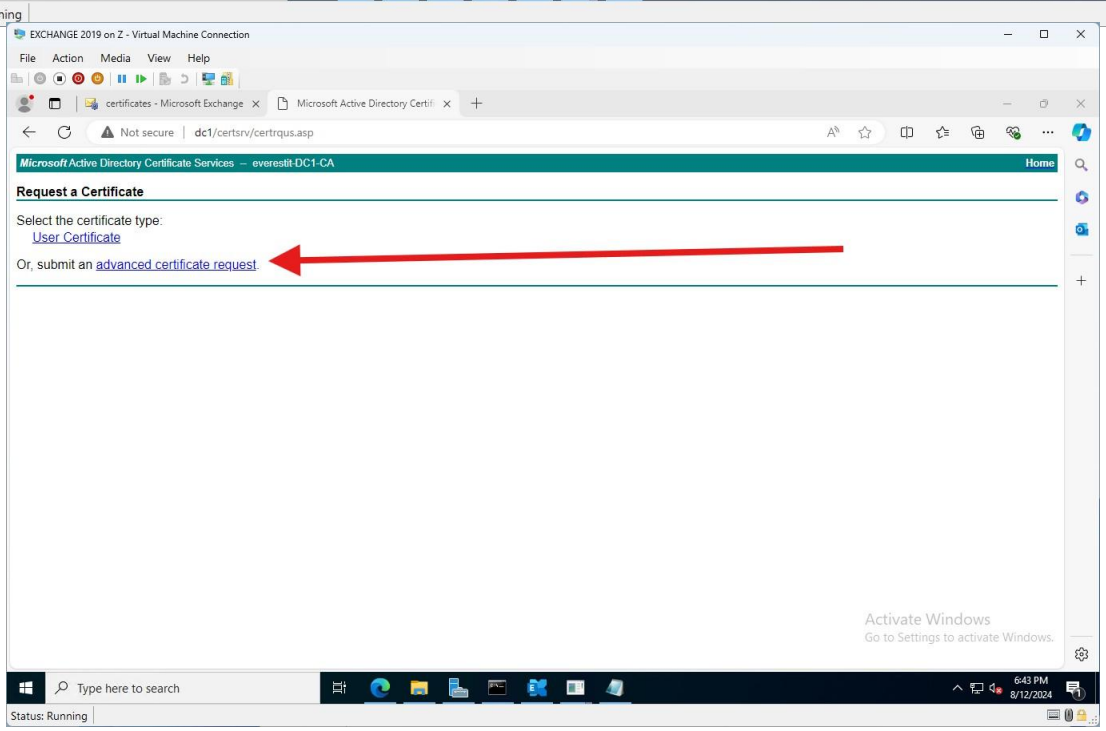


- Next copy all the content in there

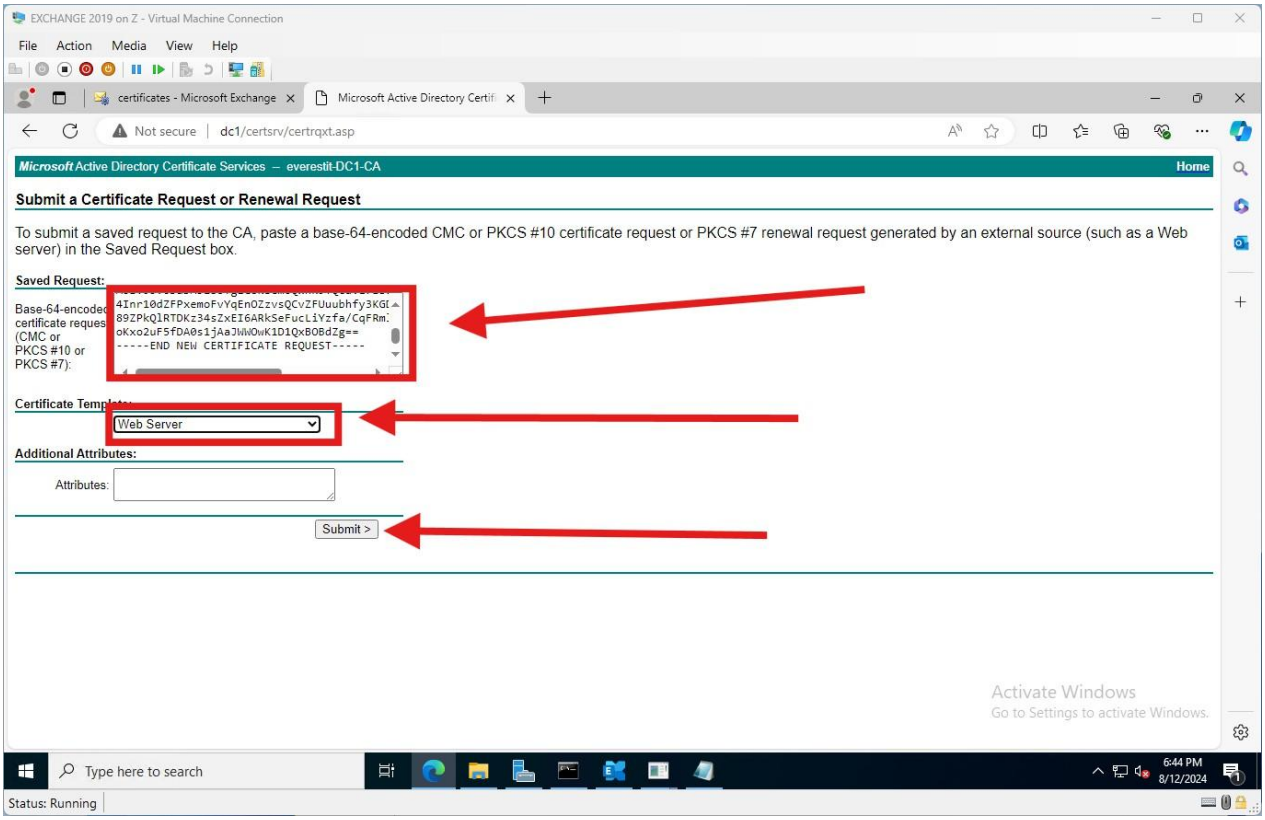


- Now go to the exchange server browser and type
- http://dc1/certsrv
- click on request certificate
- Then advanced certificate request

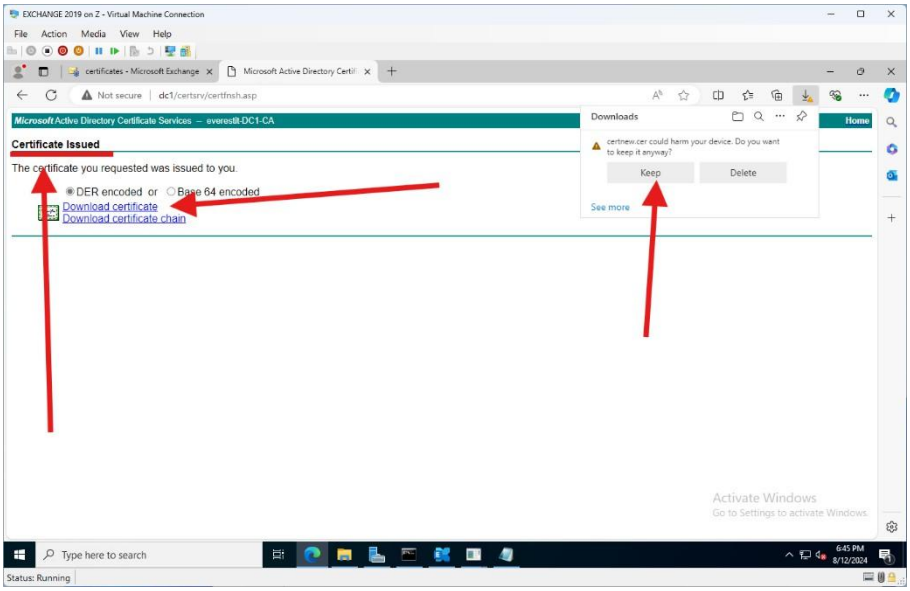




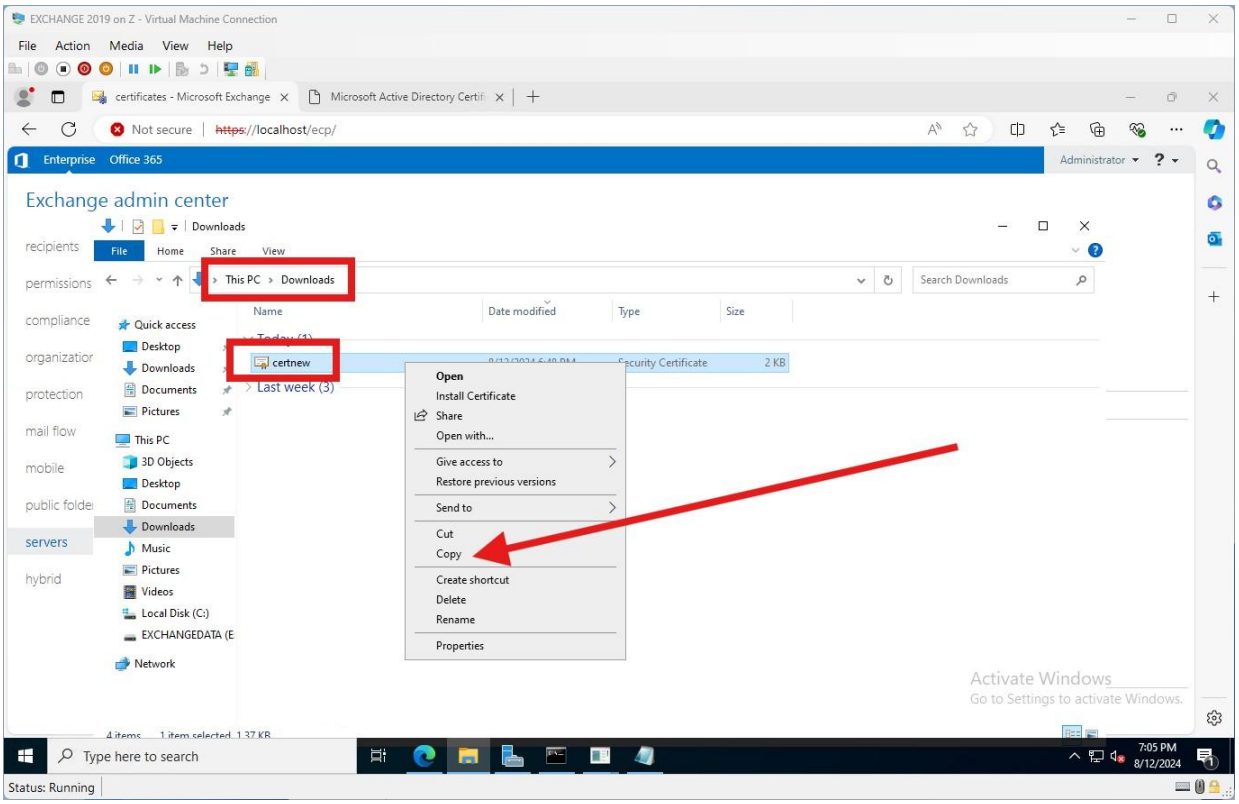
- Paste the content of the notepad that we had copied earlier, in the box that says saved requests
- Select the template as web server
- submit

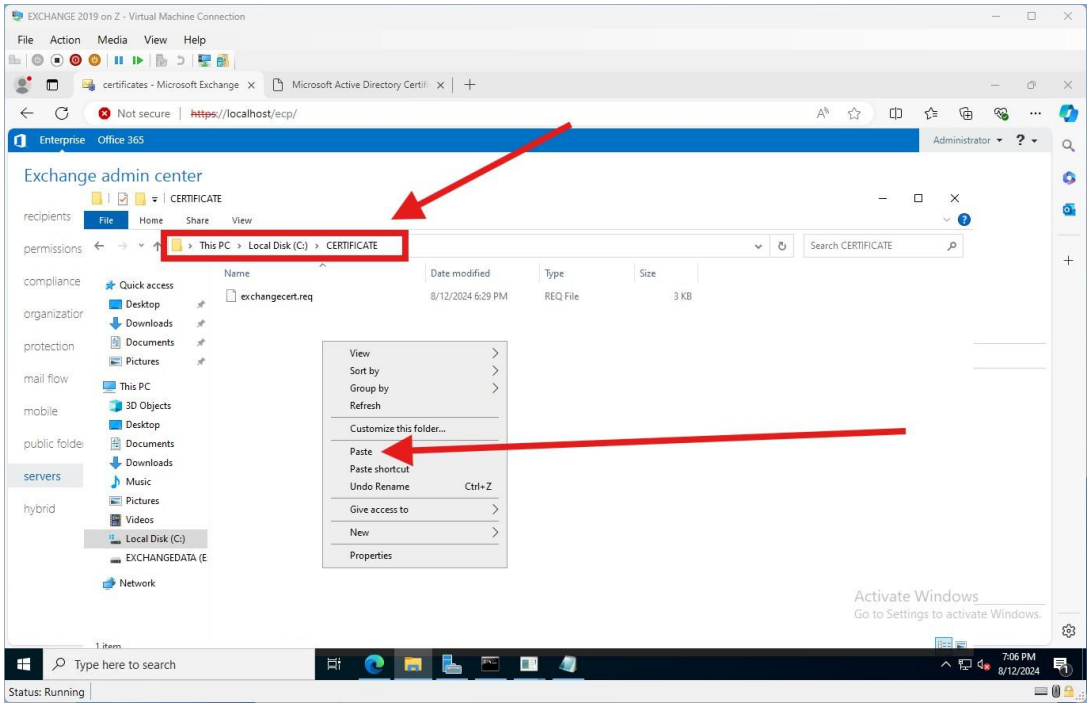


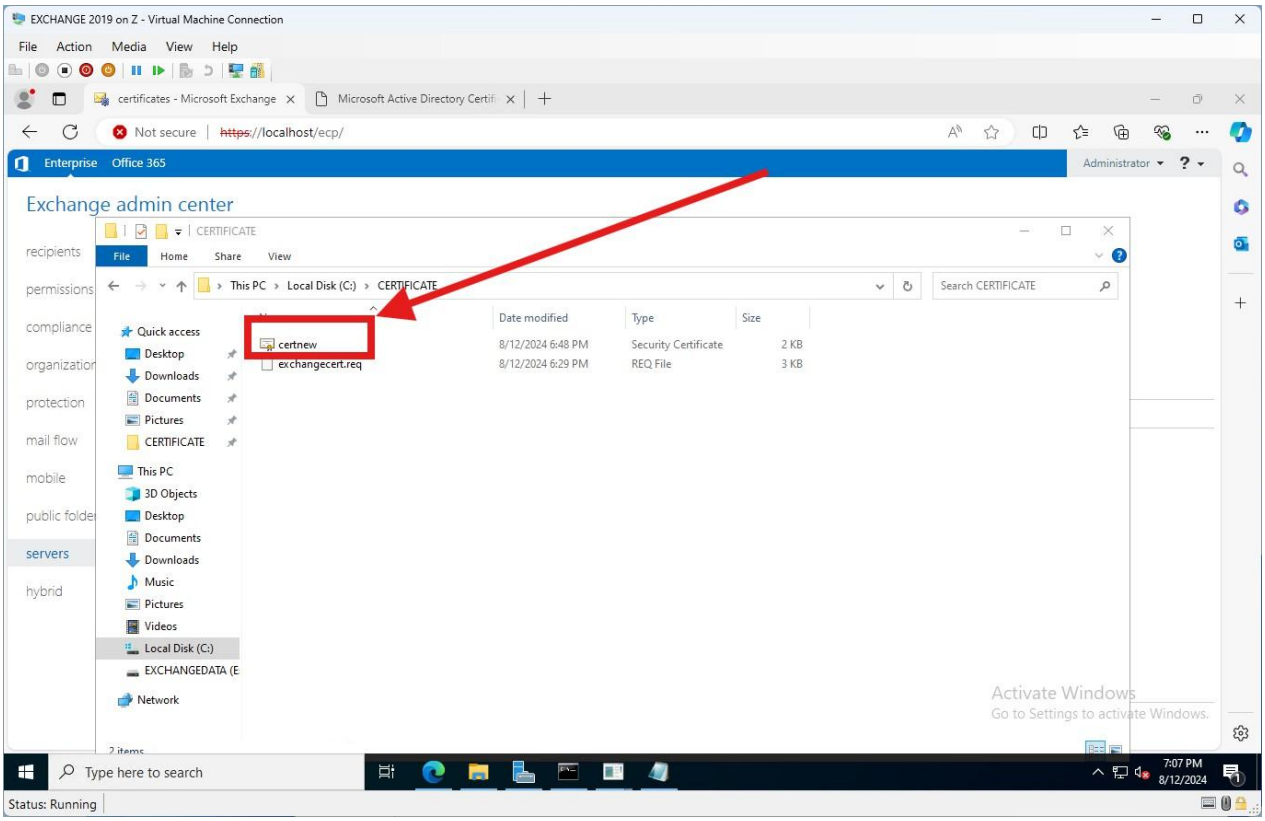
- Hit submit
- A certificate we requested will be issued



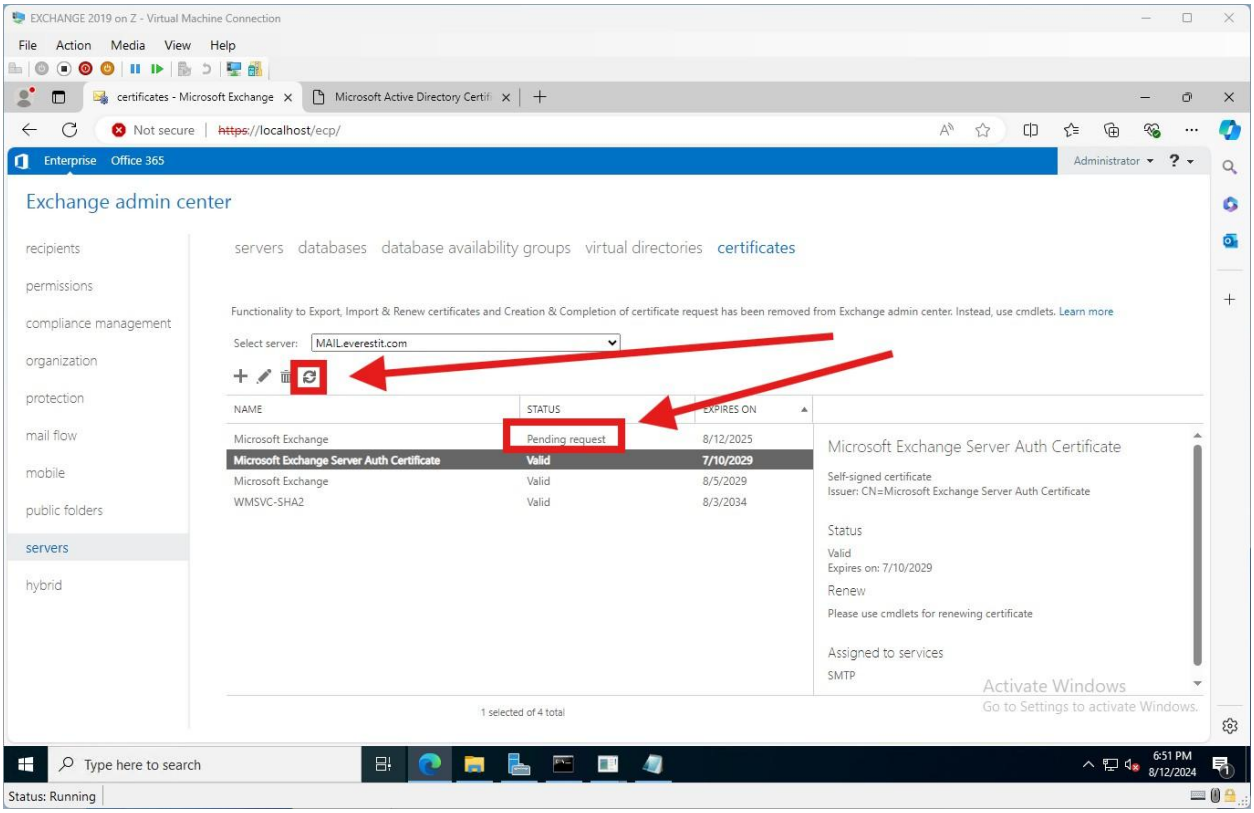
- Click on download
- And keep
- Once downloaded go to the download folder and copy it and take it to the C drive where we had created the certificate folder and paste it there







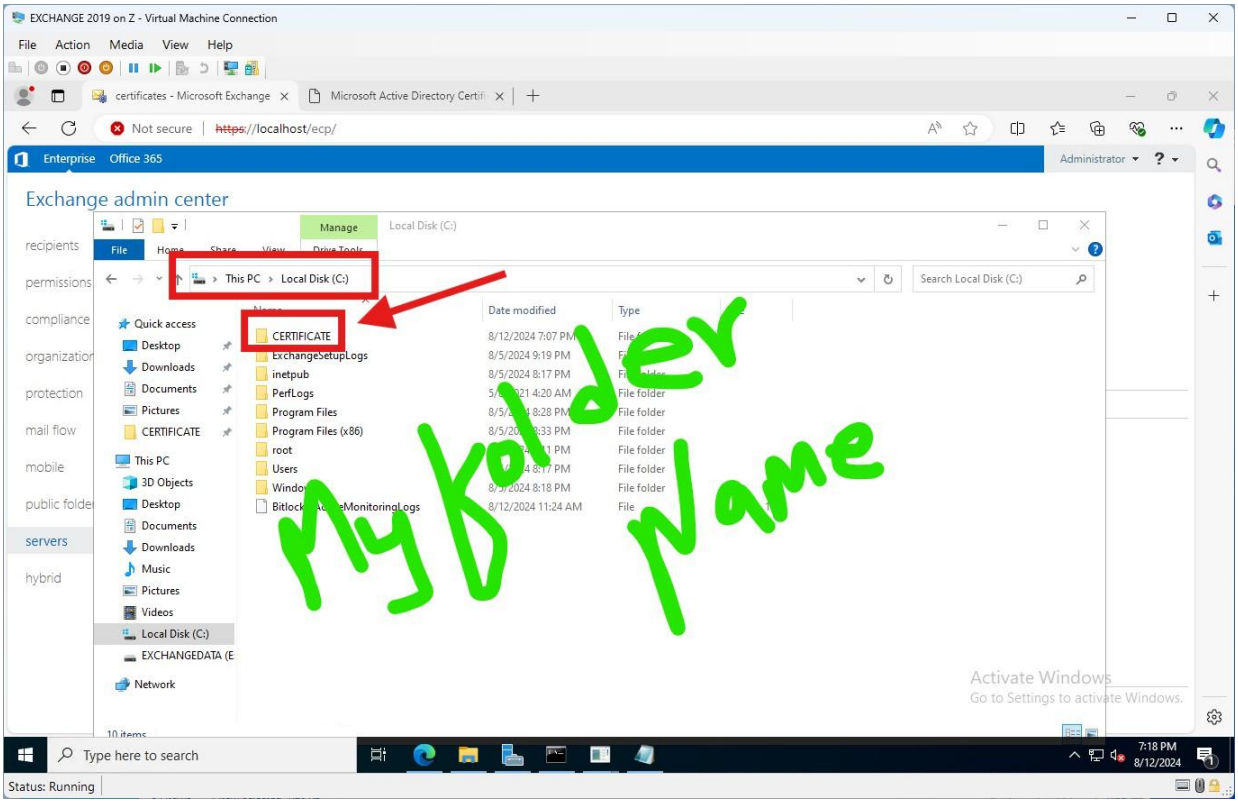
- Go back to exchange admin center and hit refresh
- There you will see a pending request

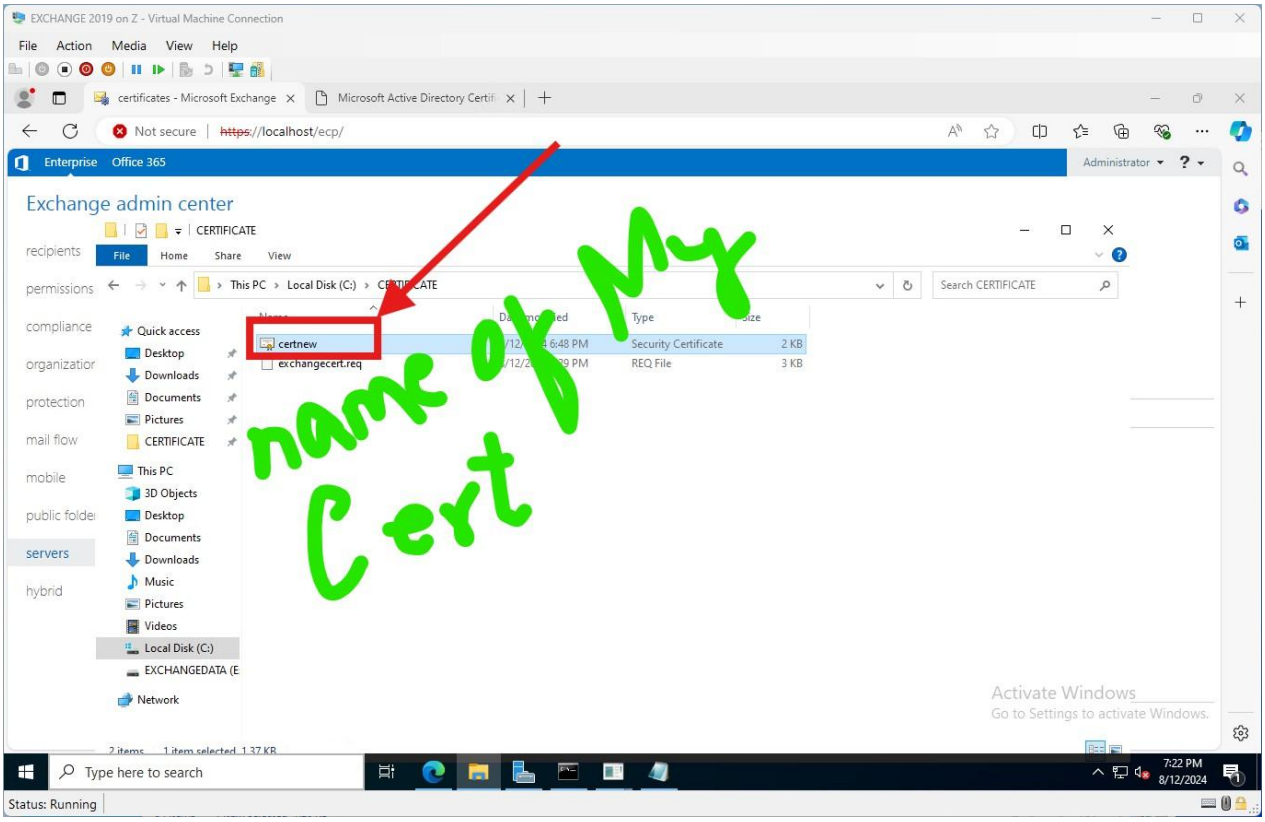


- Now once u see the pending request, we need to import this certificate into the exchange server
- For that we need to run some PowerShell script
- my code is

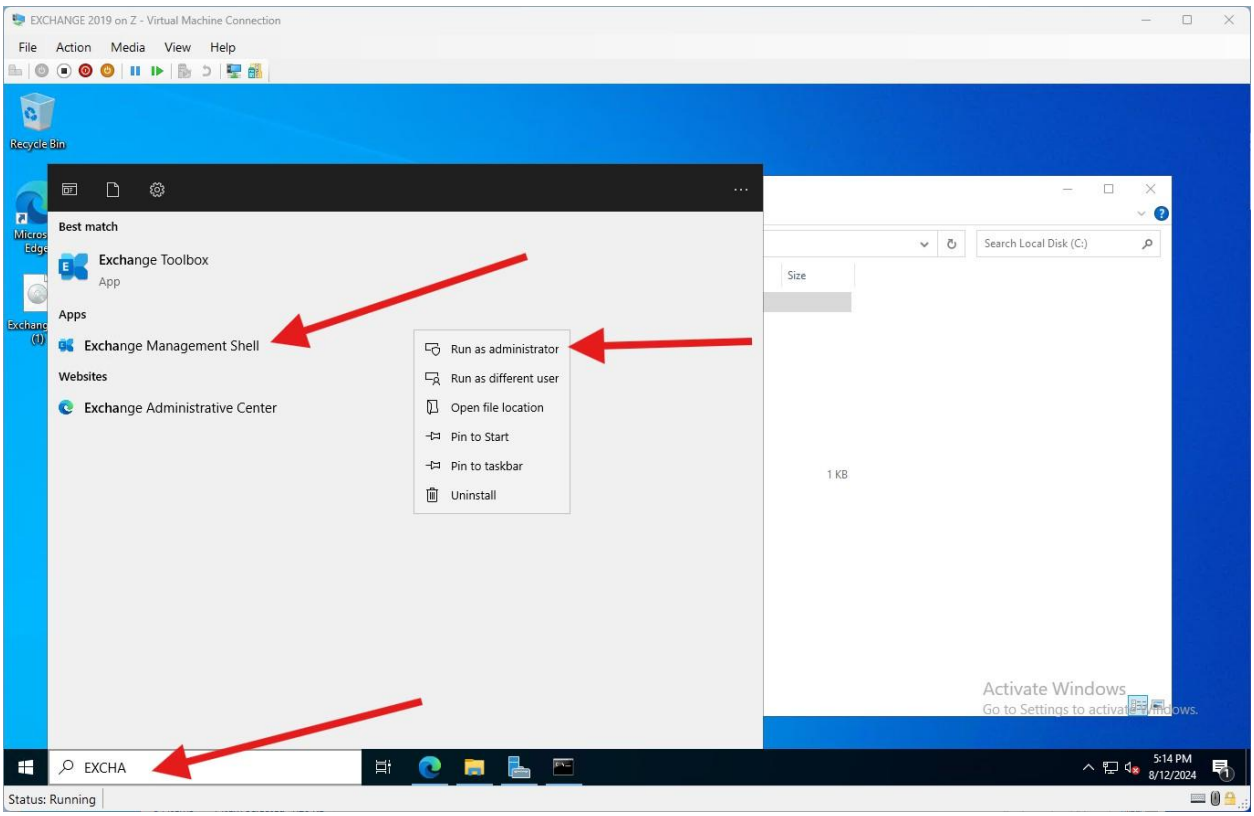
$cert = Import-ExchangeCertificate -FileData ([System.IO.File]::ReadAllBytes("\\MAIL\CERTIFICATE\certnew.cer")) -Password (Get-Credential).password

- In the following 2 pictures take a look and make sure to update your code to match the names accordingly. In my case since the name of my folder for the certificate I created was “CERTIFICATE” I updated the code accordingly. also, the name of the certificate

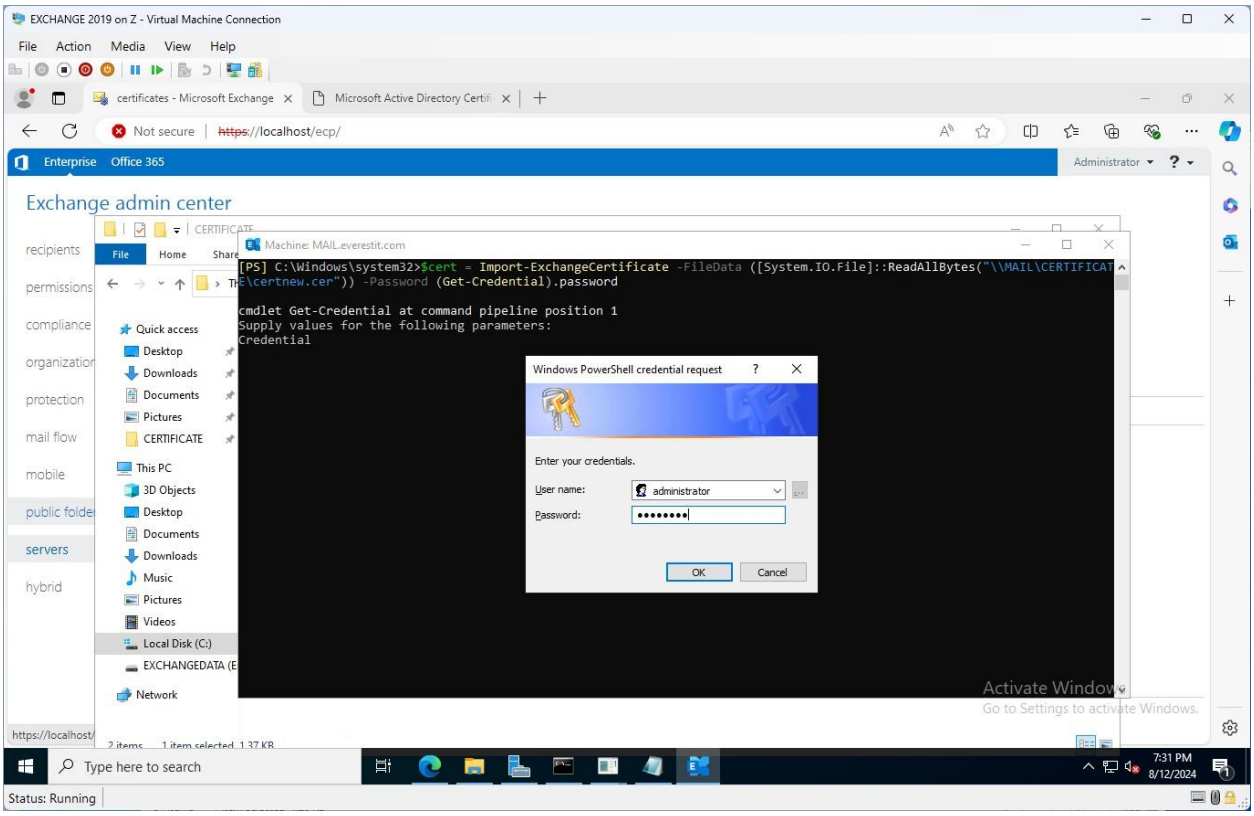




- Open exchange management Shell
- Wait for it to load first / takes time

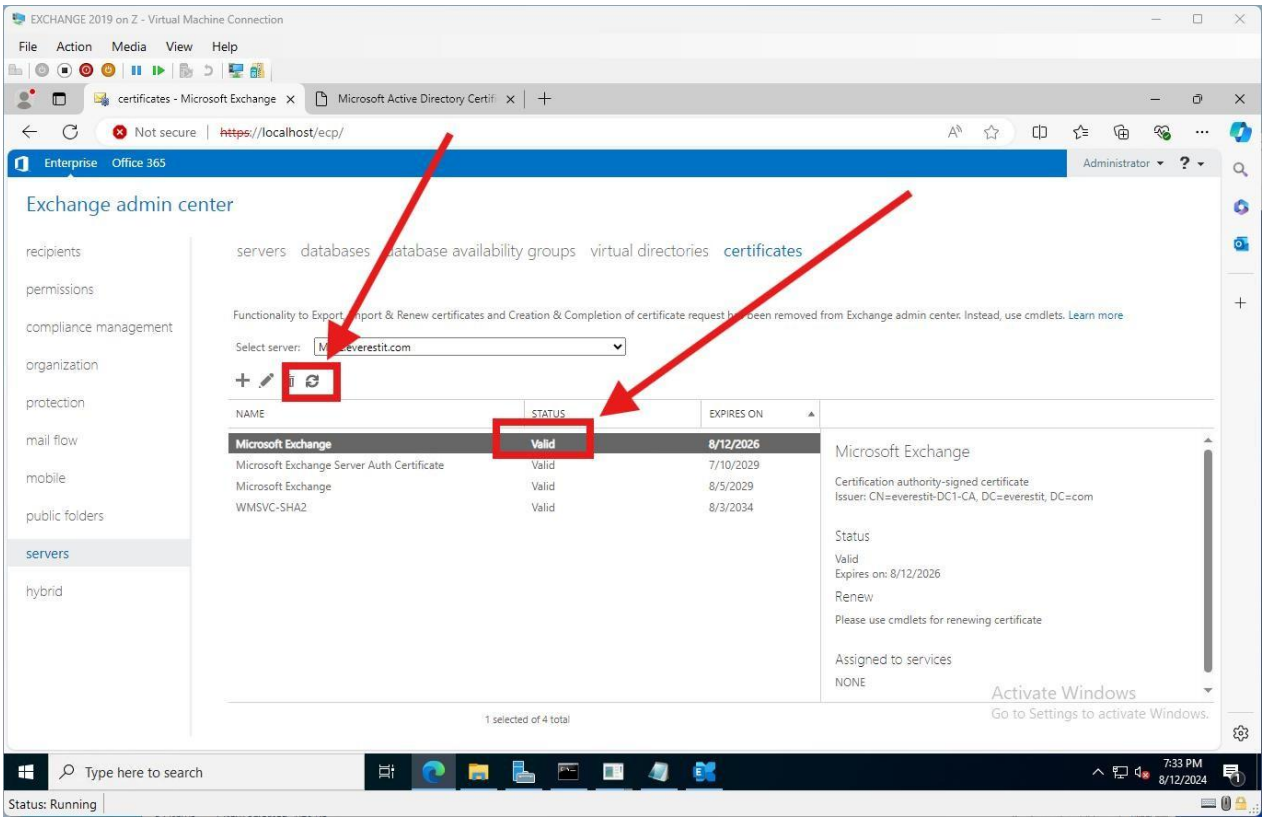


- Paste and run the code
- Once you do that
- It will ask you for the credentials



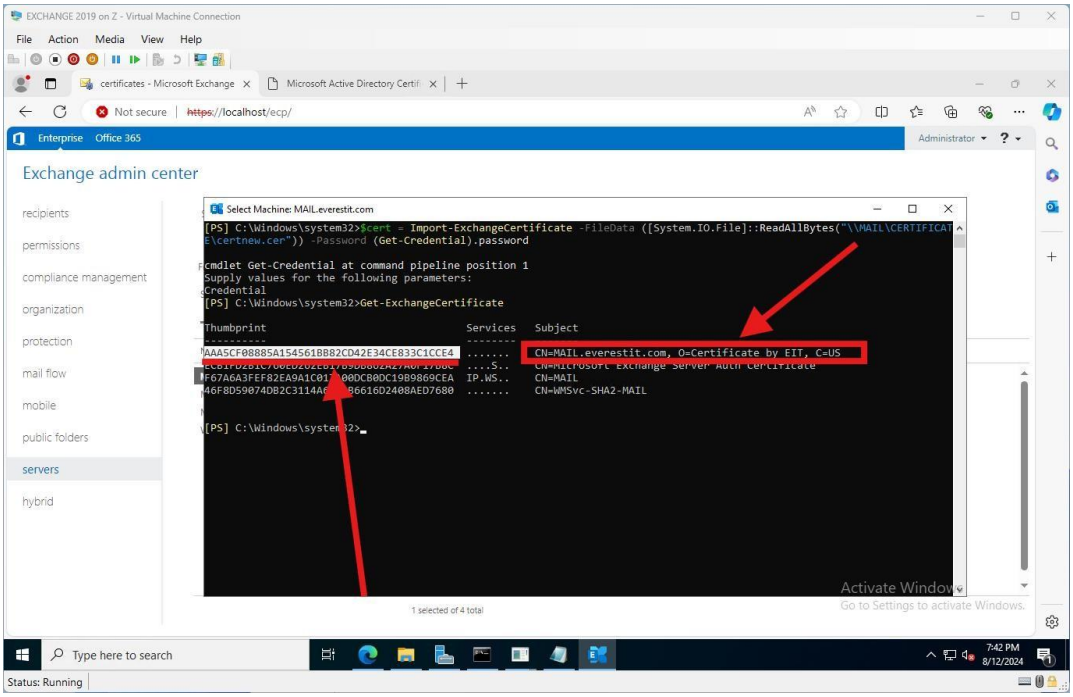
Now go back to exchange admin center and hit refresh

It should change the status from pending to valid



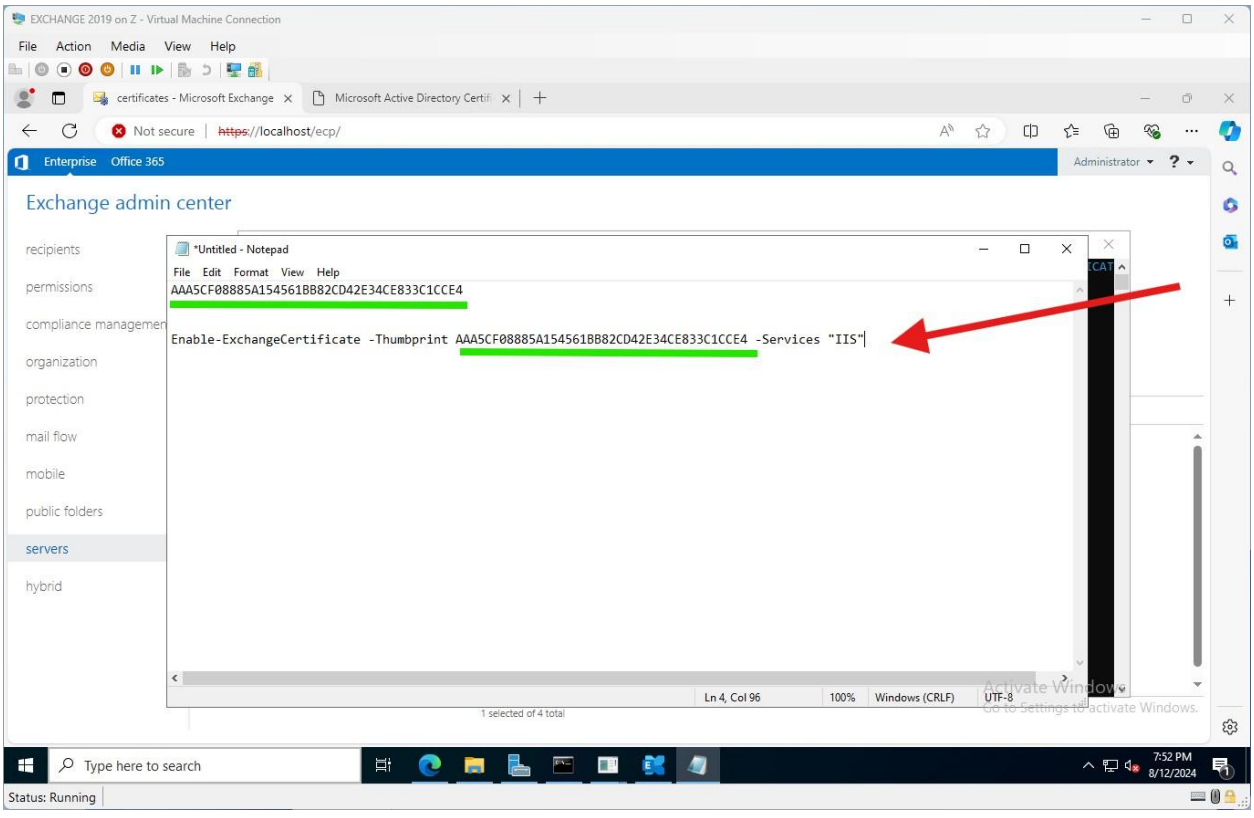
More steps to follow

- Go back to exchange management Shell and type
- Get-ExchangeCertificate
- This will give us a snapshot of all the certificates
- We need to copy the thumbprint Infront of the new certificate we created and just validated earlier
- In order to do that DoubleClick, the thumbprint it will be highlighted white and
- Copy with the command CTRL+C

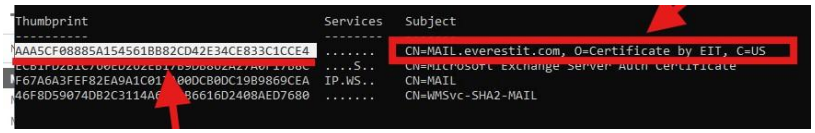


- Go out and open notepad and paste this thumbprint code in there
- Now copy the code below and paste in in the notepad just below the thumbpad like you see in the next picture

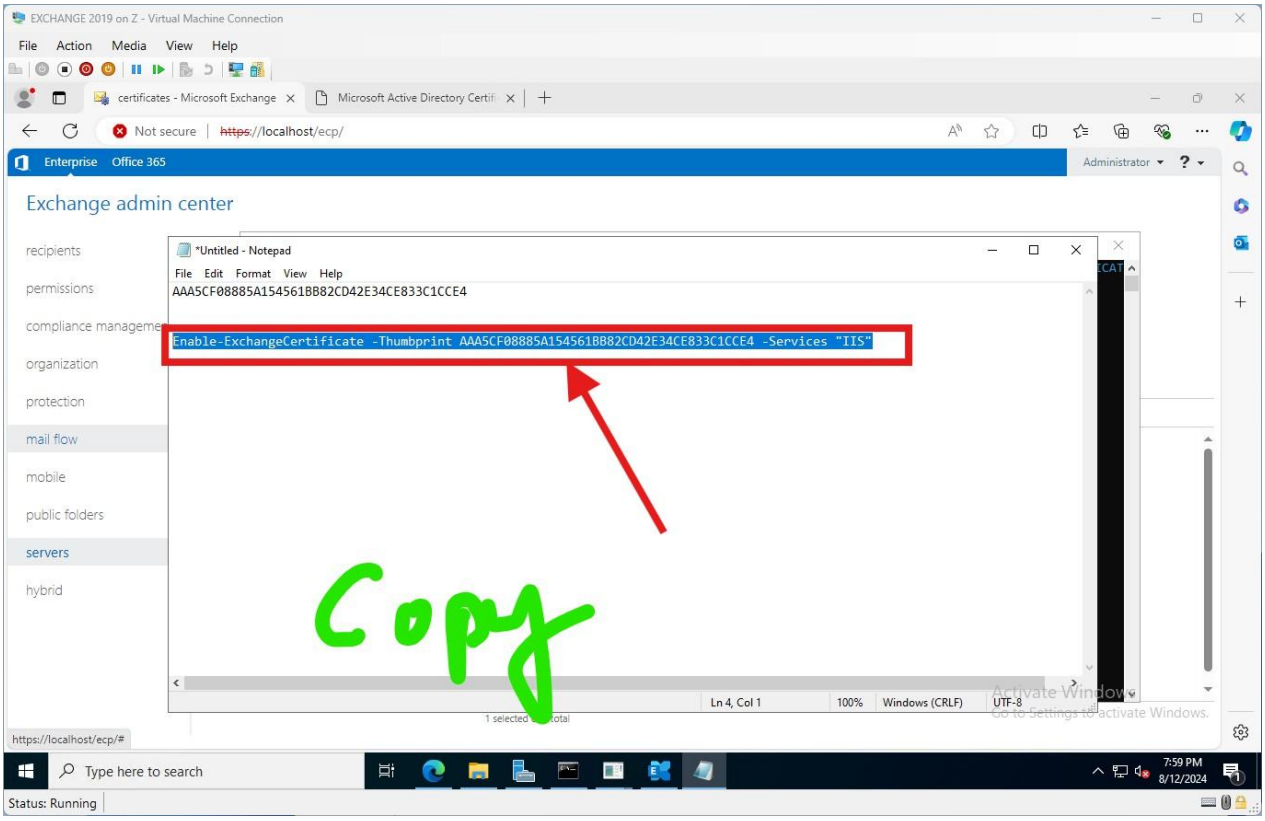
Enable-Exchange Certificate -Thumbprint AAA5CF08885A154561BB82CD42E34CE833C1CCE4 -Services "IIS"



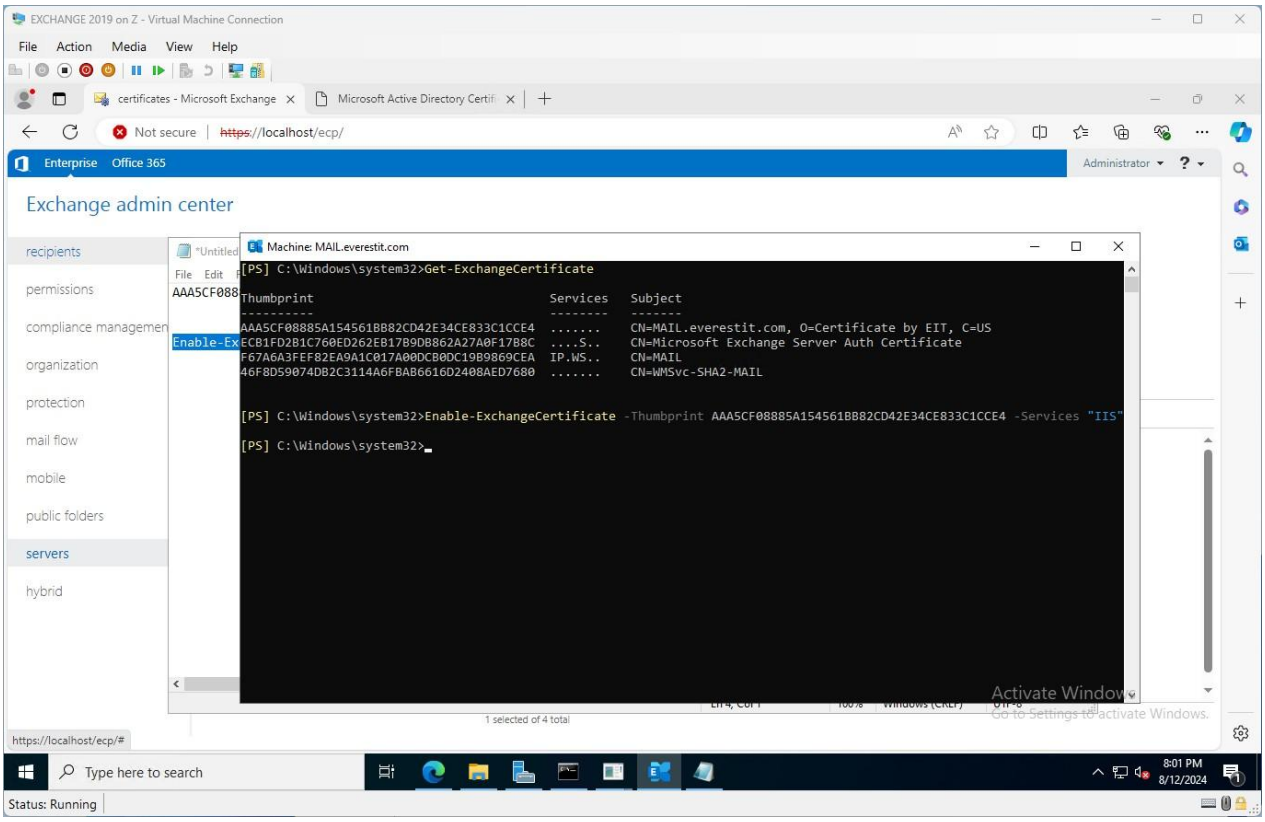
- Replace the code underlined with your unique code
- In the second line shown by the red arrow the underlined thumbprint in green should match from the ones you copied earlier
- Everyone has a unique code so do not copy this as is: it should be whatever the code shown by the PowerShell command earlier.



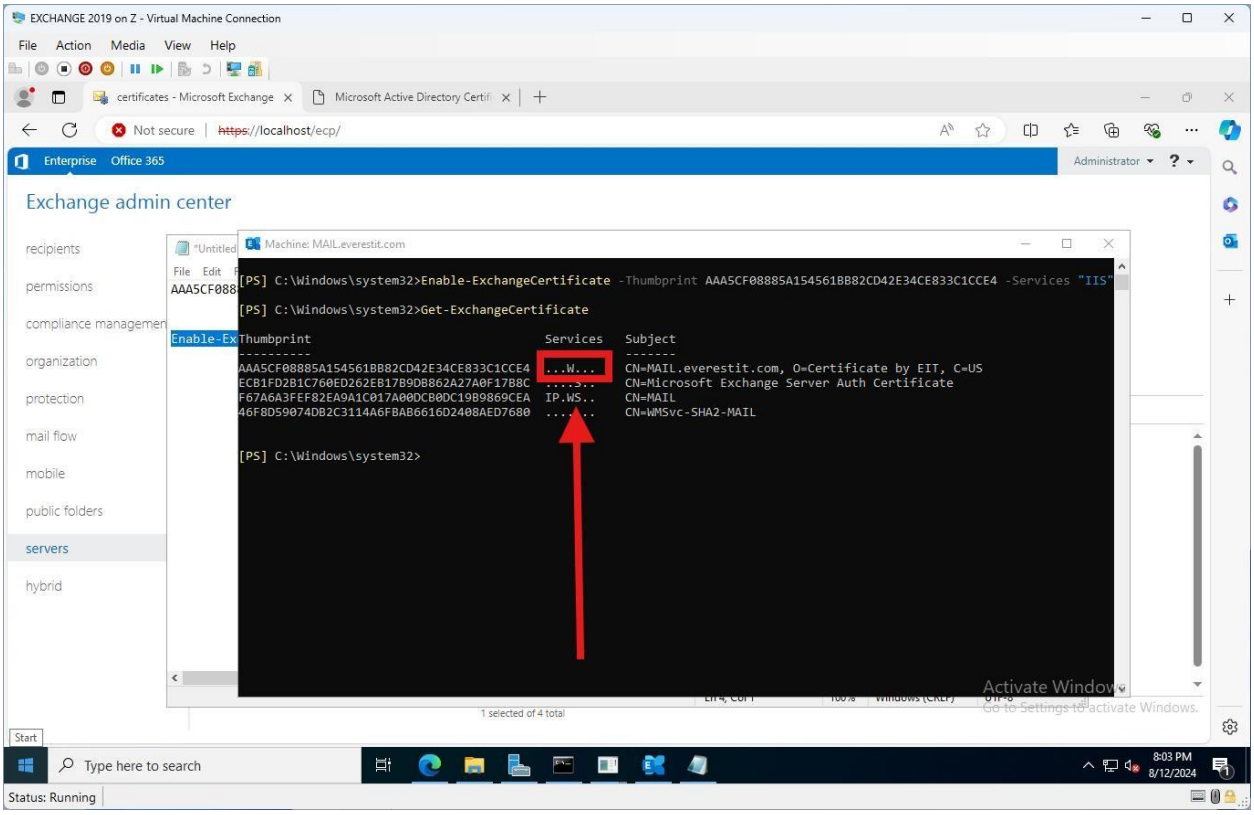
- Once the code is ready copy the code shown in the red box only



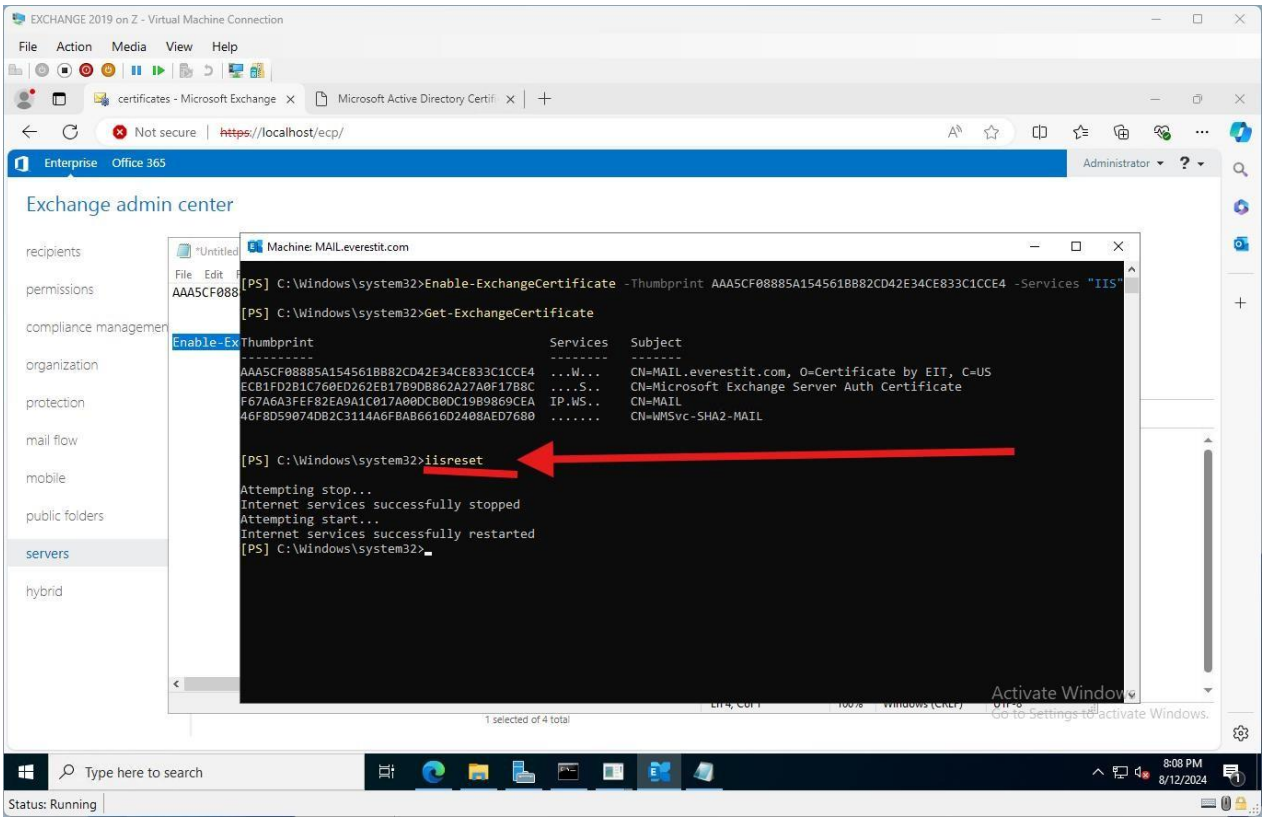
- Go to the exchange management Shell again and rt click there
- It will automatically paste
- Just hit enter



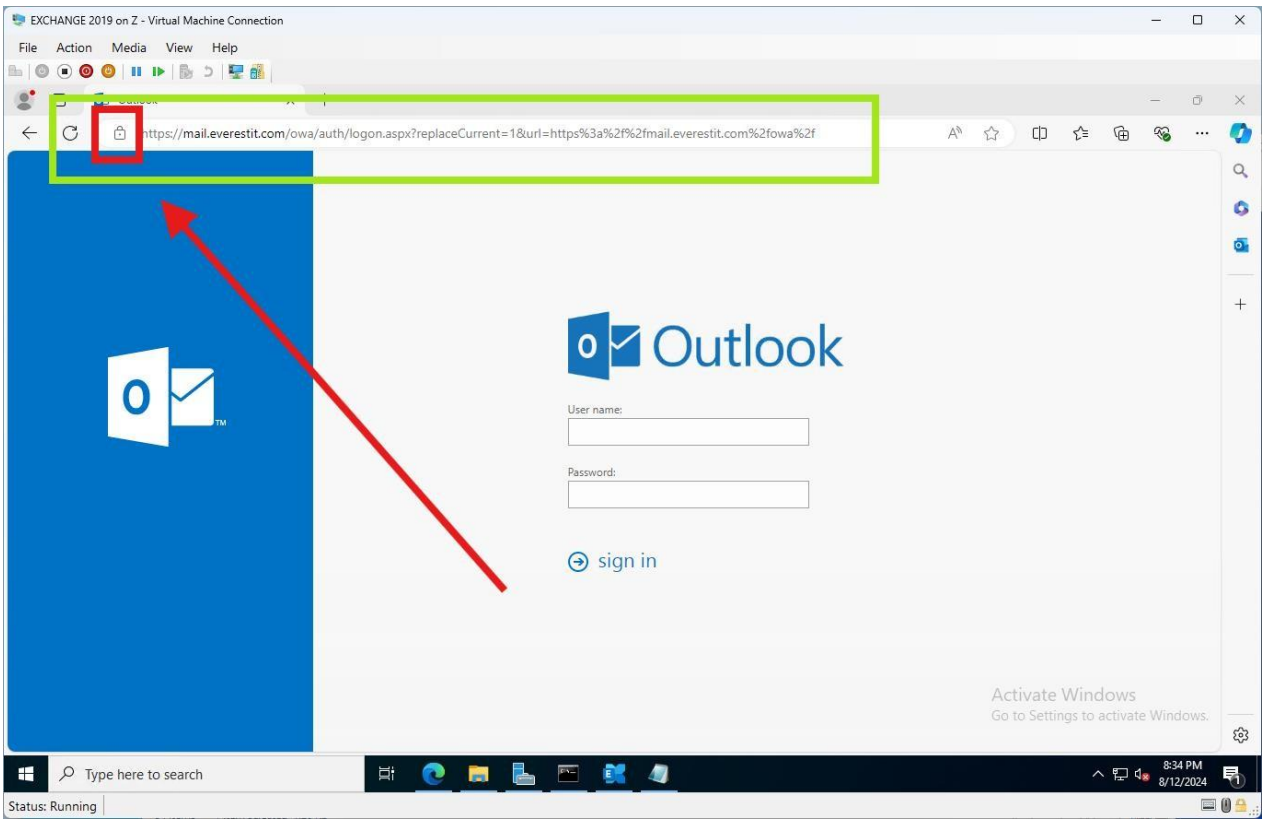
- Now just to verify type
- Get-ExchangeCertificate
- Hit enter / you should see the W in the services column

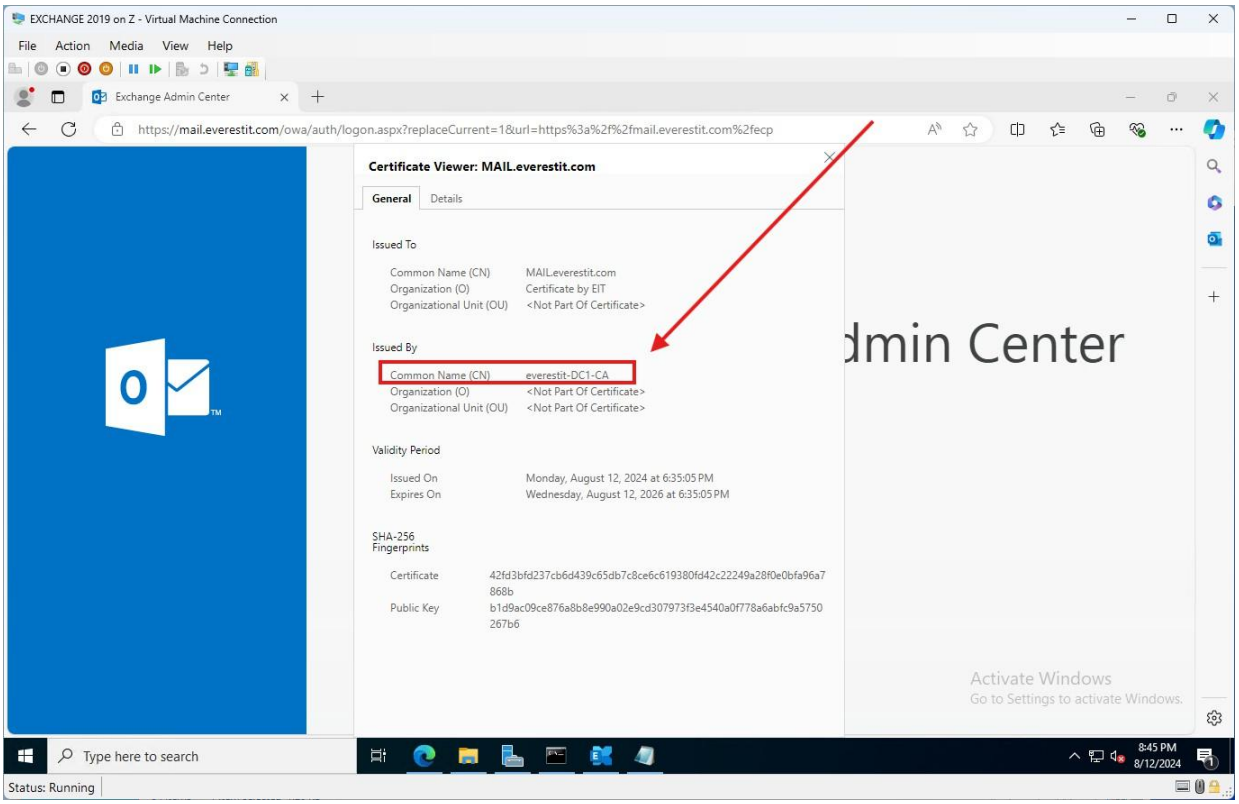


- Once you see that restart the webservices with the command below
- iisreset

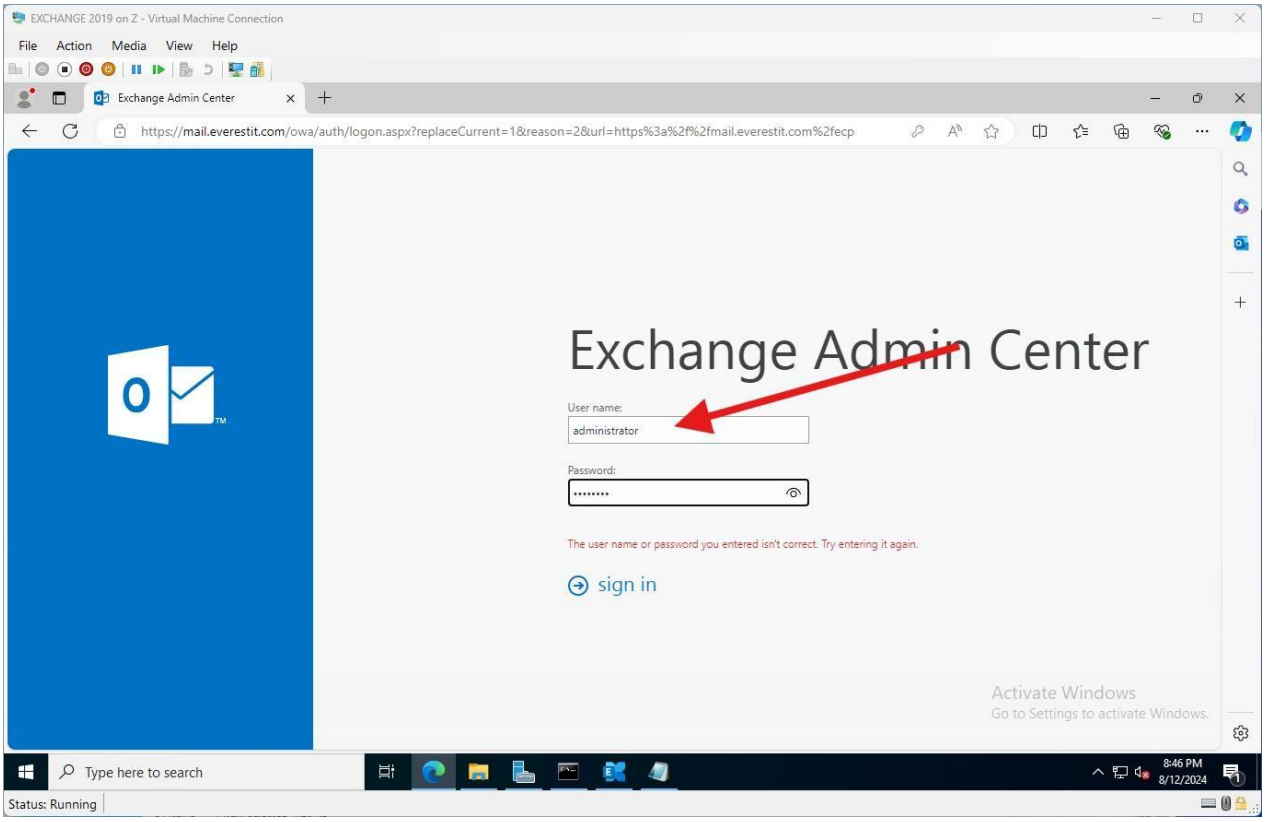


- Open web browser in the exchange server pc and type in the new address
- https://mail.everestit.com/ecp
- We can verify the lock sign signifying the implementation of https certificate

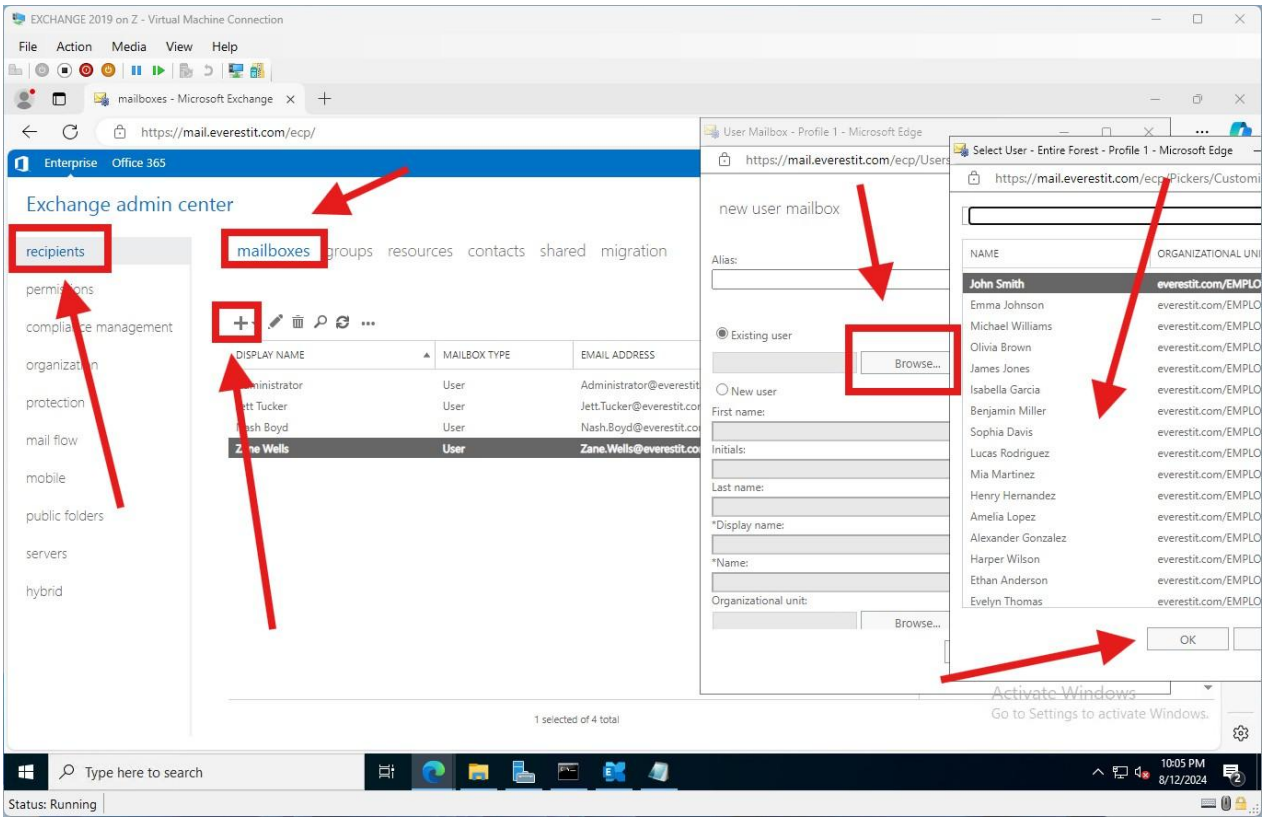

EXCHANGE 2019 on Z - Virtual Machine Connection
File Action Media View Help
https://mail.everestit.com/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.everestit.com%2fowa%2f
Outlook
User name:
Password:
sign in
Activate Windows
Go to Settings to activate Windows.
Type here to search
8:34 PM
8/12/2024
Status: Running


EXCHANGE 2019 on Z - Virtual Machine Connection
File Action Media View Help
Exchange Admin Center
https://mail.everestit.com/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fmail.everestit.com%2fecp
Certificate Viewer: MAIL.everestit.com
General
Details
Issued To
Common Name (CN) MAIL.everestit.com
Organization (O) Certificate by EIT
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) everestit-DC1-CA
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Monday, August 12, 2024 at 6:35:05 PM
Expires On Wednesday, August 12, 2026 at 6:35:05 PM
SHA-256 Fingerprints
Certificate 42fd3bfd237cb6d439c65db7c8ce6c619380fd42c22249a28f0e0bfa96a7868b
Public Key b1d9ac09ce876a8b8e990a02e9cd307973f3e4540a0f778a6abfc9a5750267b6
dmin Center
Activate Windows
Go to Settings to activate Windows.
Type here to search
8:45 PM
8/12/2024
Status: Running

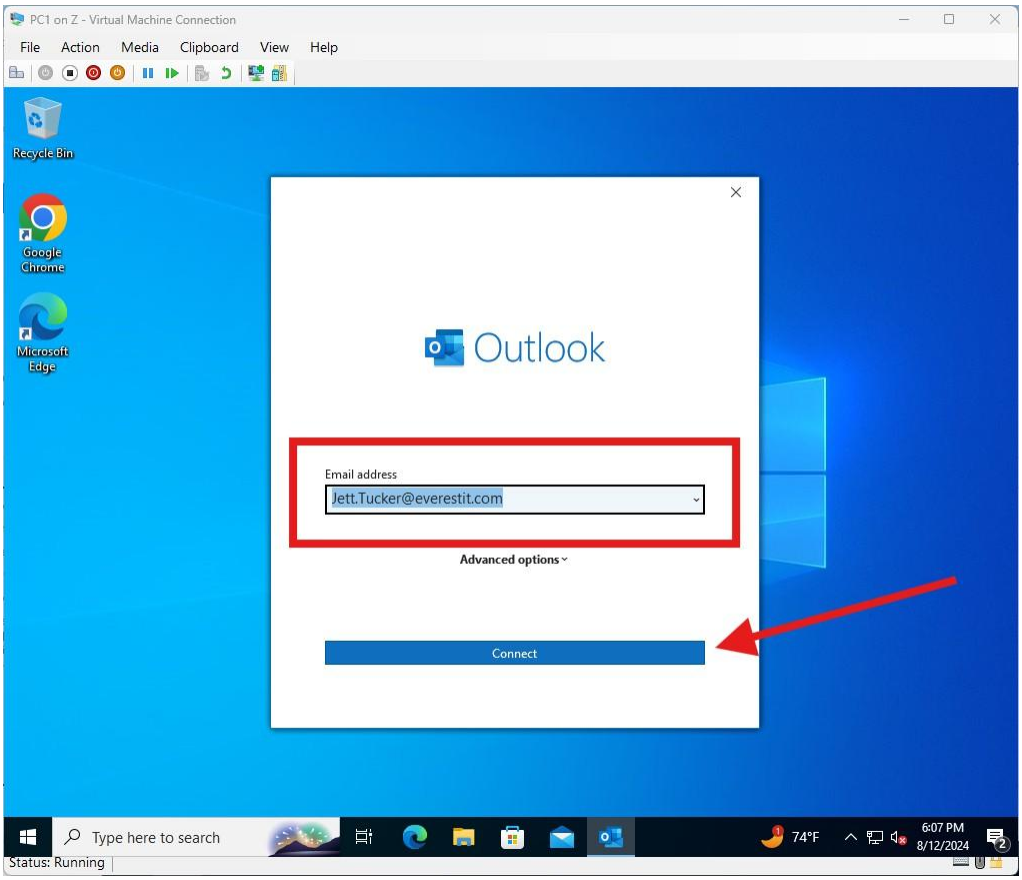
- You can use only the name now
- Since we had fixed the setting earlier



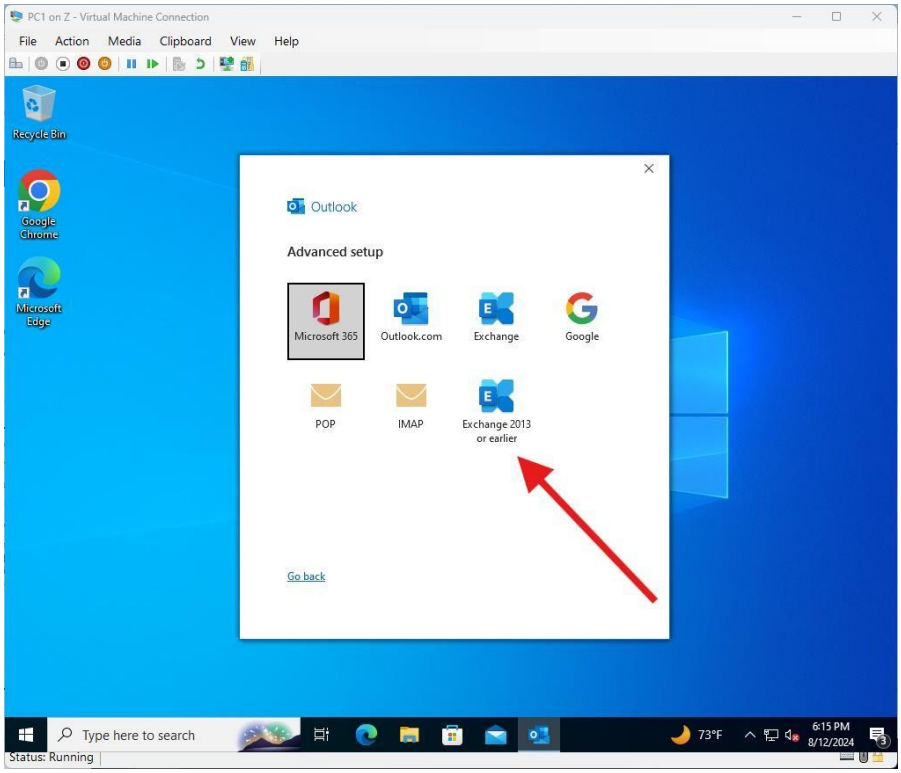
- Make a few mailbox accounts of some domain users which we are going to use to test the email server
- Click on recipients / mailboxes
- Hit the plus sign
- Select existing user
- Browse
- Choose the user and hit ok
- Do this process few times for a few more additional user



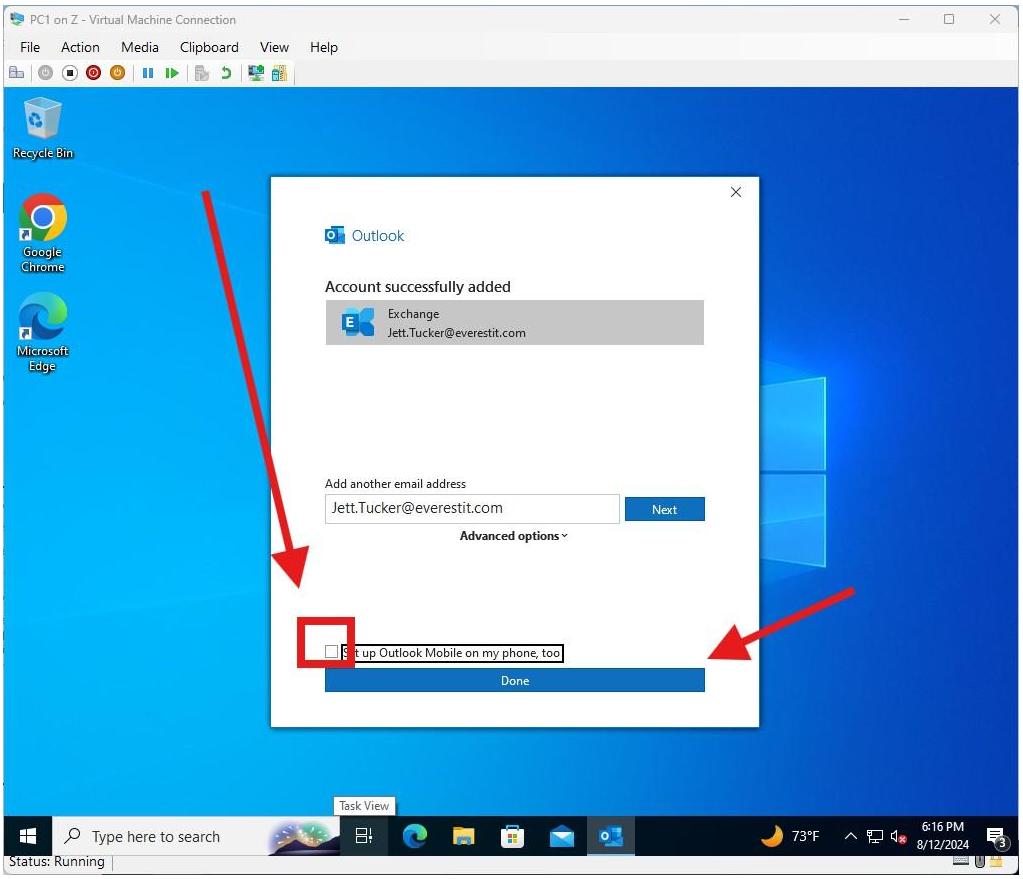
- Now go to one of the domain joined pc
- Login as admin and once in
- Restart the pc and
- Login using one of the users account
- And open outlook app
- It should automatically populate the email address for the current user

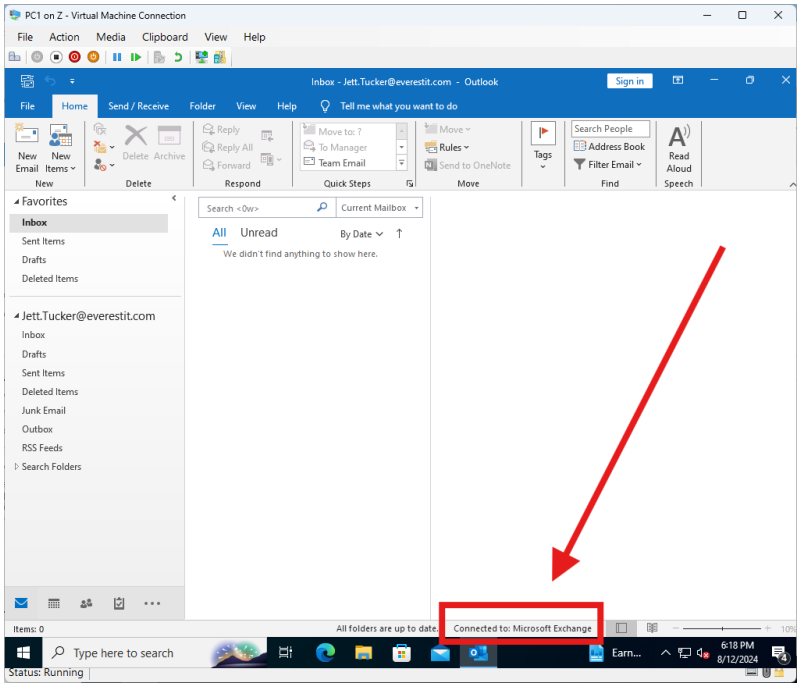


- Click connect > Select the 2013 or earlier

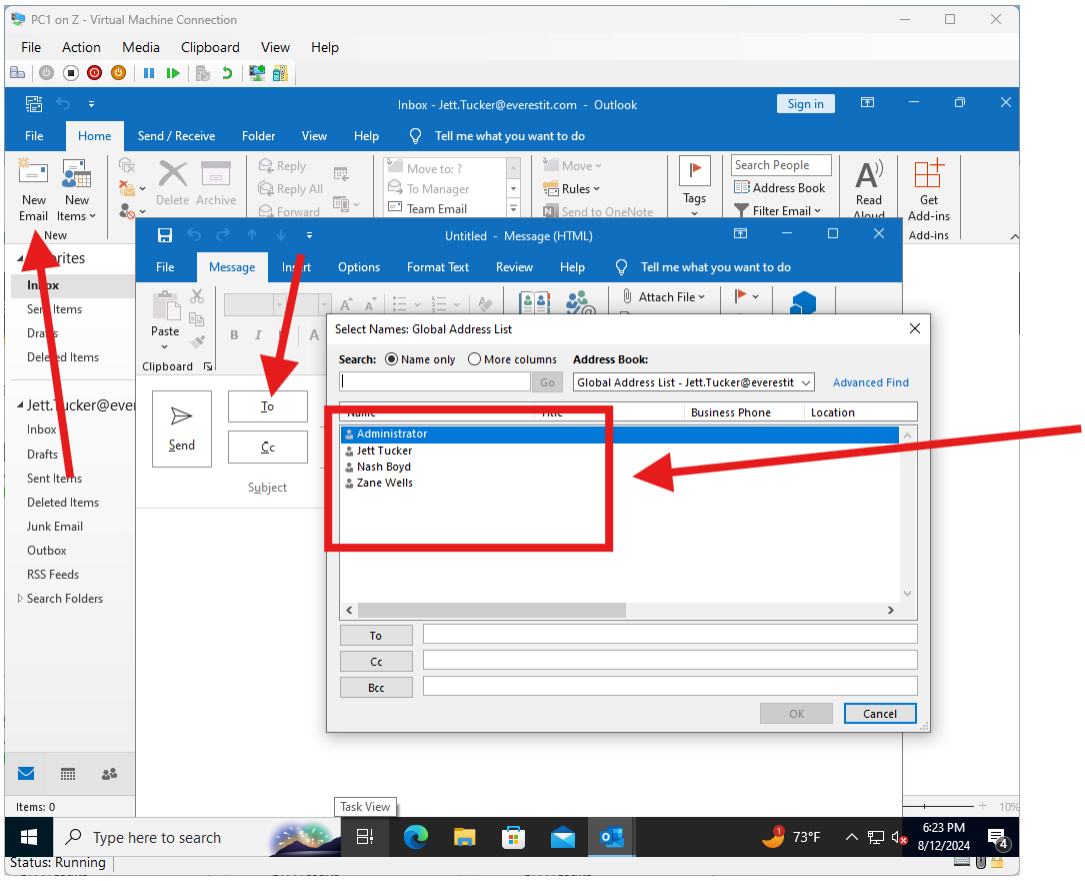


- Uncheck the mobile phone
- Hit done

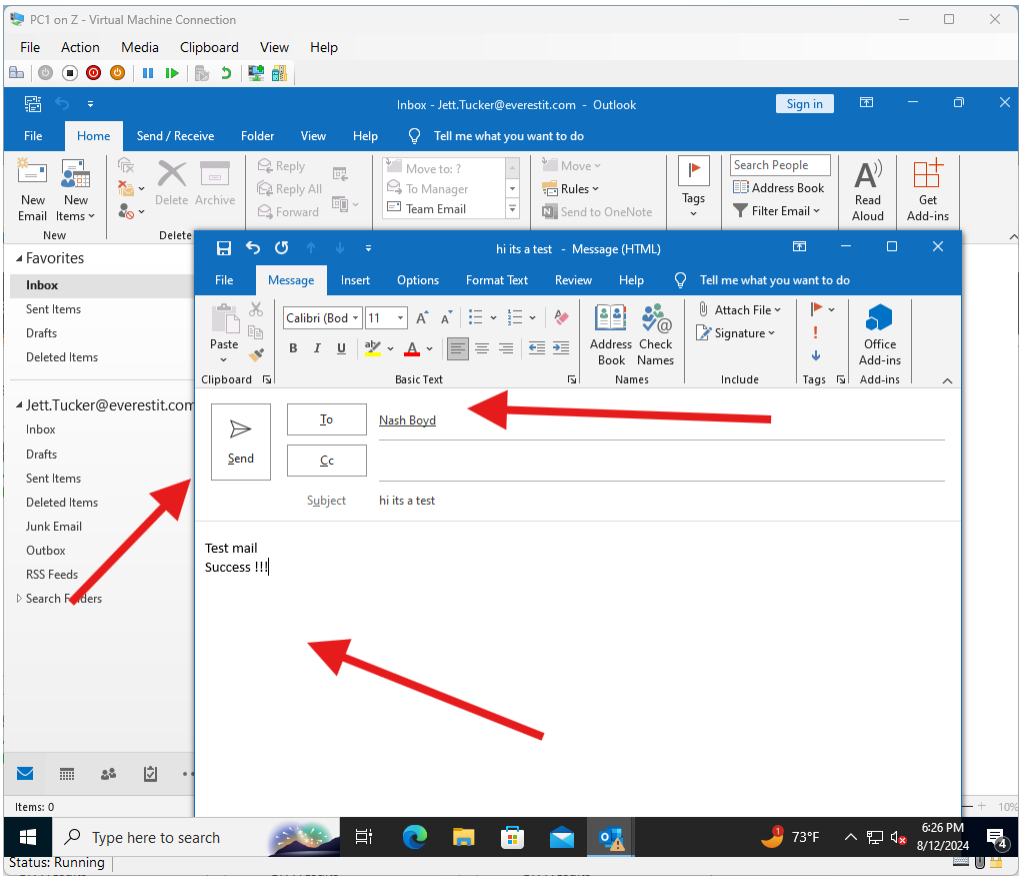




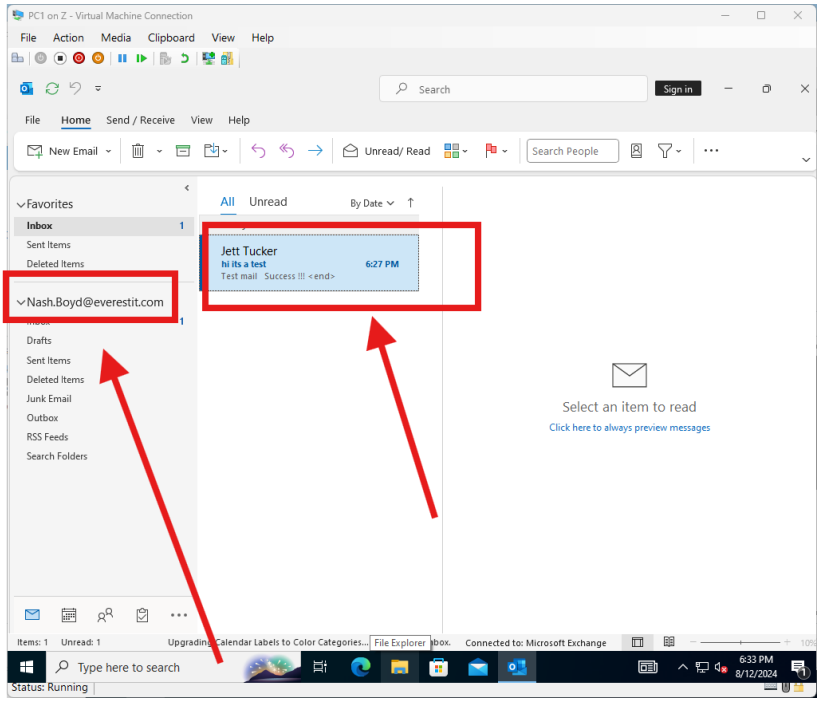
- Once you see its connected to Microsoft exchange
- Send an email to a different user



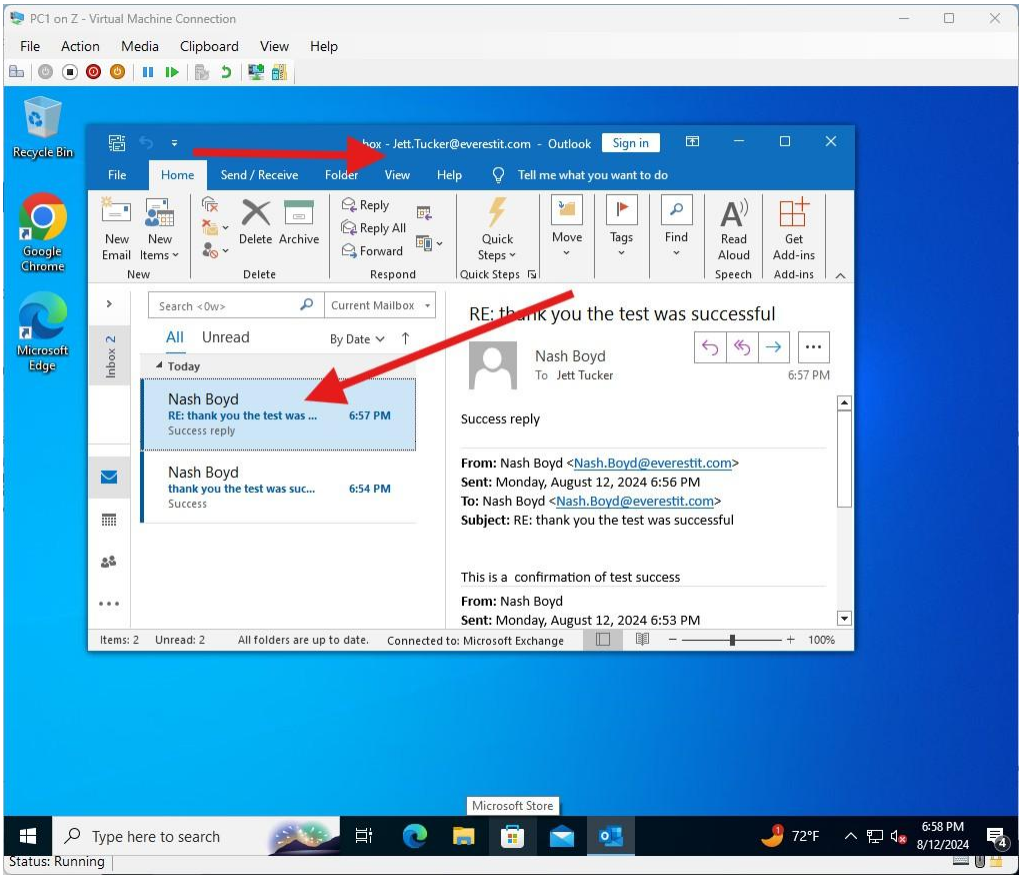
- Hit the TO button
- It should pop up a window with all the available recipients in the organization we added earlier
- Select one and hit ok
- Once the email is sent to that domain user



- Log off of this user account in the client pc
- Login as that user who we just sent the email to
- He should have his email in the outlook



- Now send a reply to the email to test if it's working the other way around then
- Log off the pc and
- Login as a user account to whom we just replied to



- Once we open outlook it will automatically login to the users outlook
- We can see the email in the inbox
- Its working both ways
- Sending and receiving