

Exchange Server 2019 Configuration Step by Step Guide:

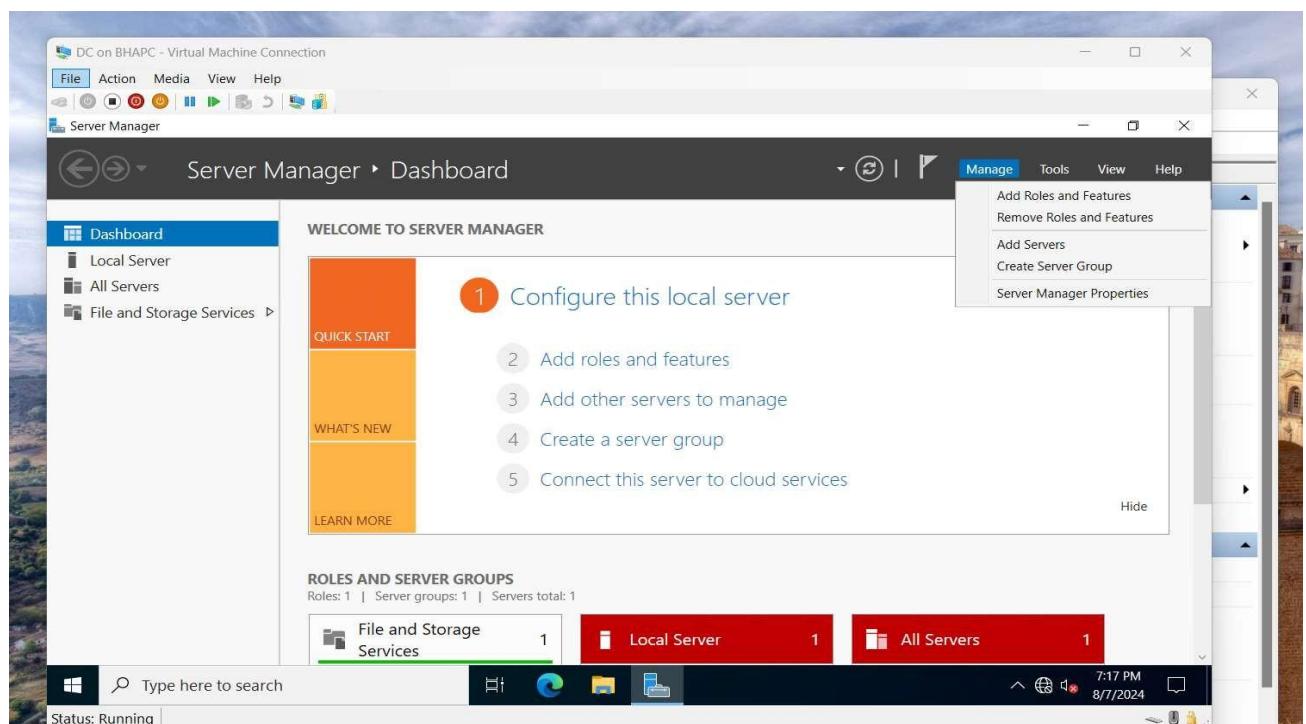
What is Exchange Server?

An Exchange Server is a mail server developed by Microsoft that enables organizations to manage emails, calendars, contacts, and tasks in a centralized and secure environment. It acts as the core of business communication, storing and organizing all messaging and scheduling data while ensuring employees can access their emails and calendars from multiple devices with synchronization and security. Before installing and configuring an Exchange Server, an organization must have a Domain Controller in place, because Exchange relies on Active Directory to manage user accounts, security permissions, and configuration settings. Without a Domain Controller, the organization would lack the necessary infrastructure to deploy Exchange Server efficiently or maintain control over its messaging environment. Having Active Directory in place ensures that Exchange can function properly, allowing seamless communication, collaboration, and task management across the organization.

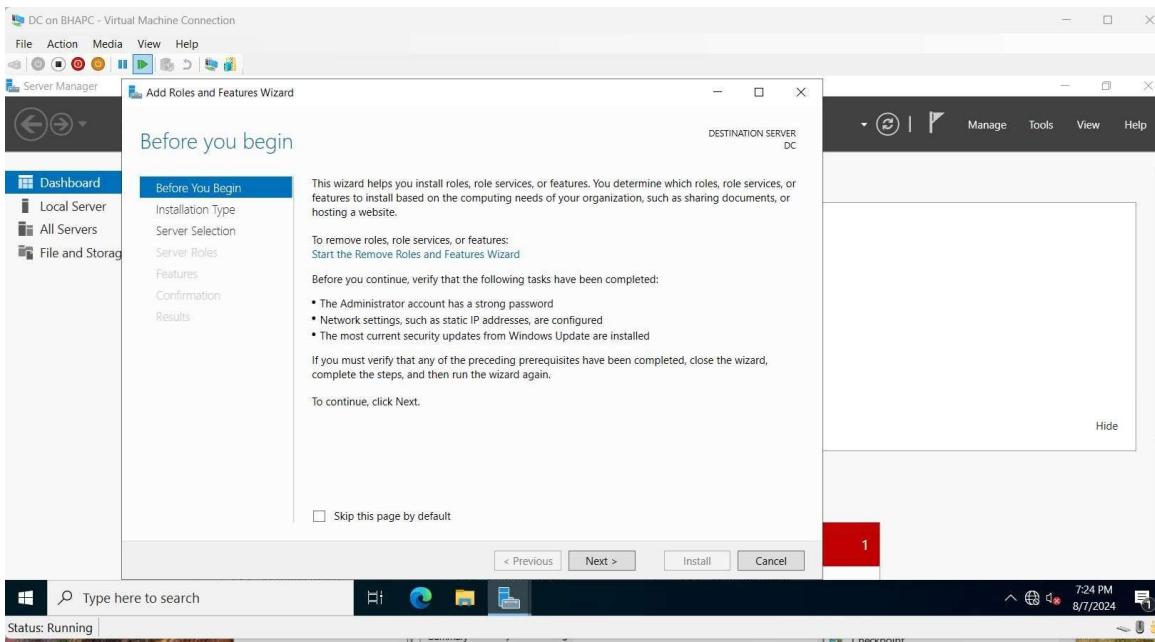
So, first let's configure Domain Controller.

IMPORTANT: Always assign Static IP address for Servers.

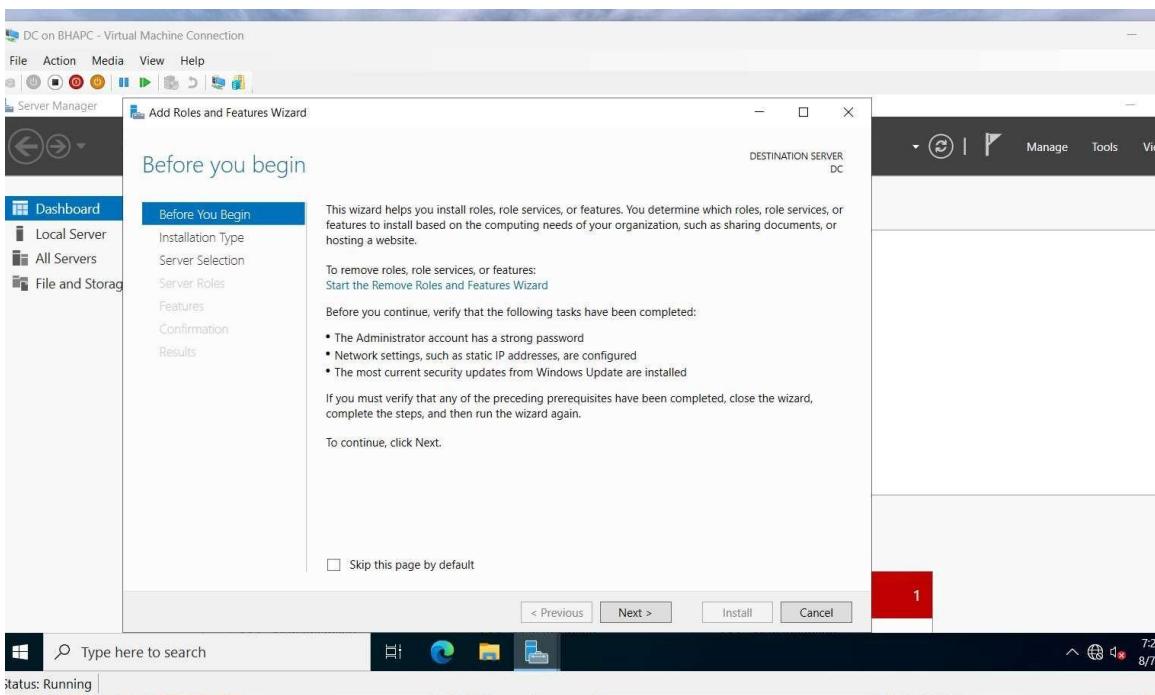
1. Click on Manage. Add Roles and Features. This is Windows Server, when first installed, has no roles assigned and functions only as a basic server. To give it a specific purpose, such as an Active Directory Domain Controller, File and Print Server, DNS Server, DHCP Server, Web Server, or WSUS Server, you must install the appropriate roles and features. Since we want this server to act as an Active Directory Domain Controller, we will add the Active Directory Domain Services role and then promote the server to a domain controller.



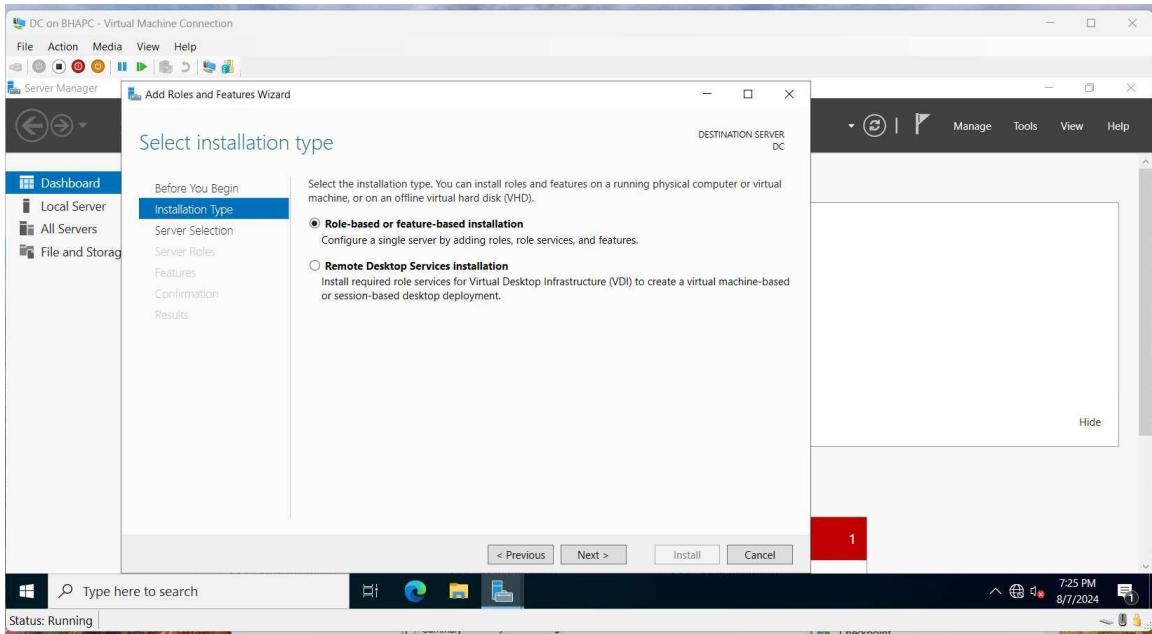
2. Click Next.



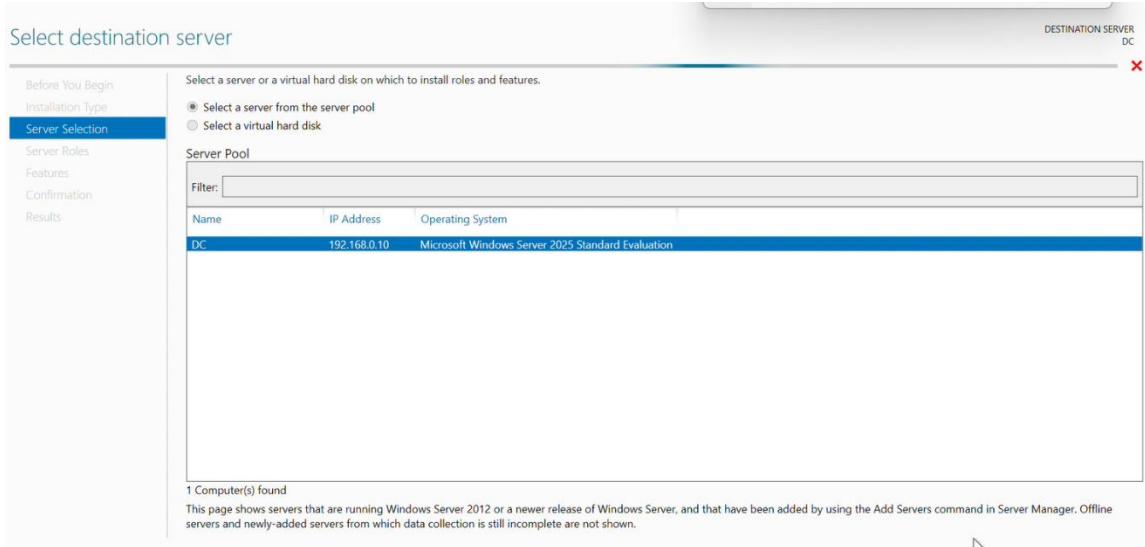
3. Click Next.



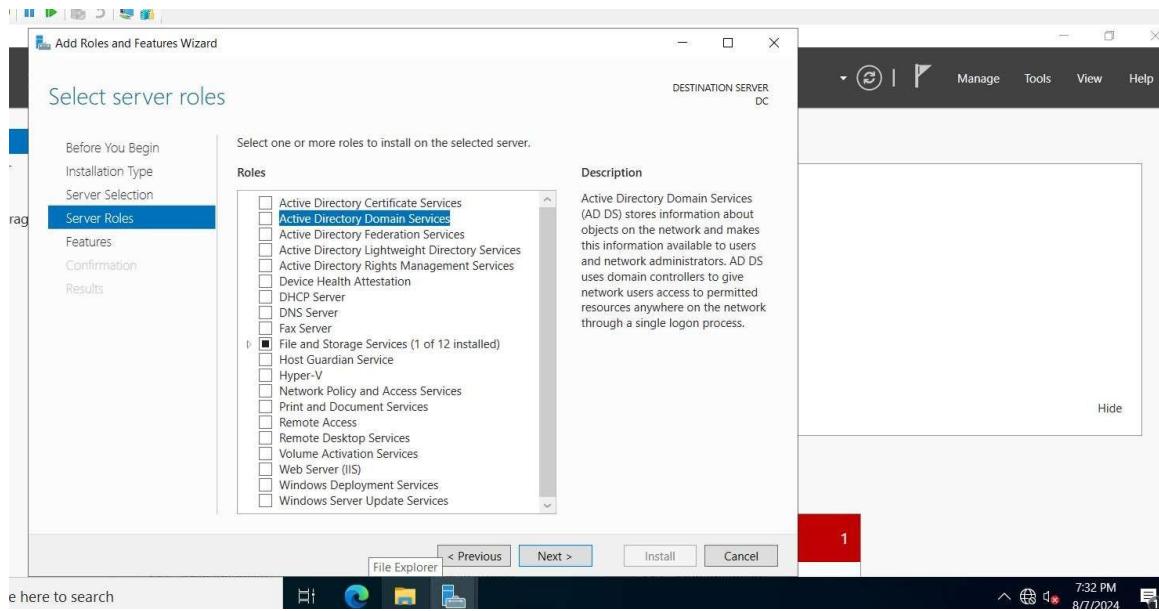
4. Click Role-Based or Feature-Based installation. (We want to add the role of Active Directory Domain Services) Click Next.



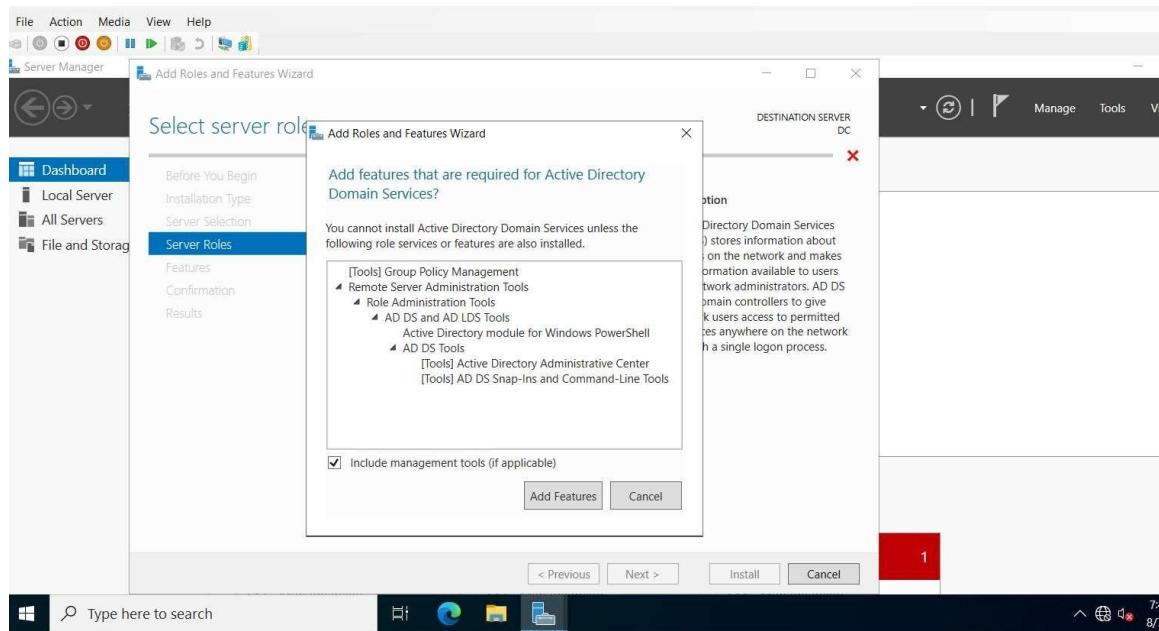
5. Ensure the IP address, server name, and operating system are correct. Click Next.



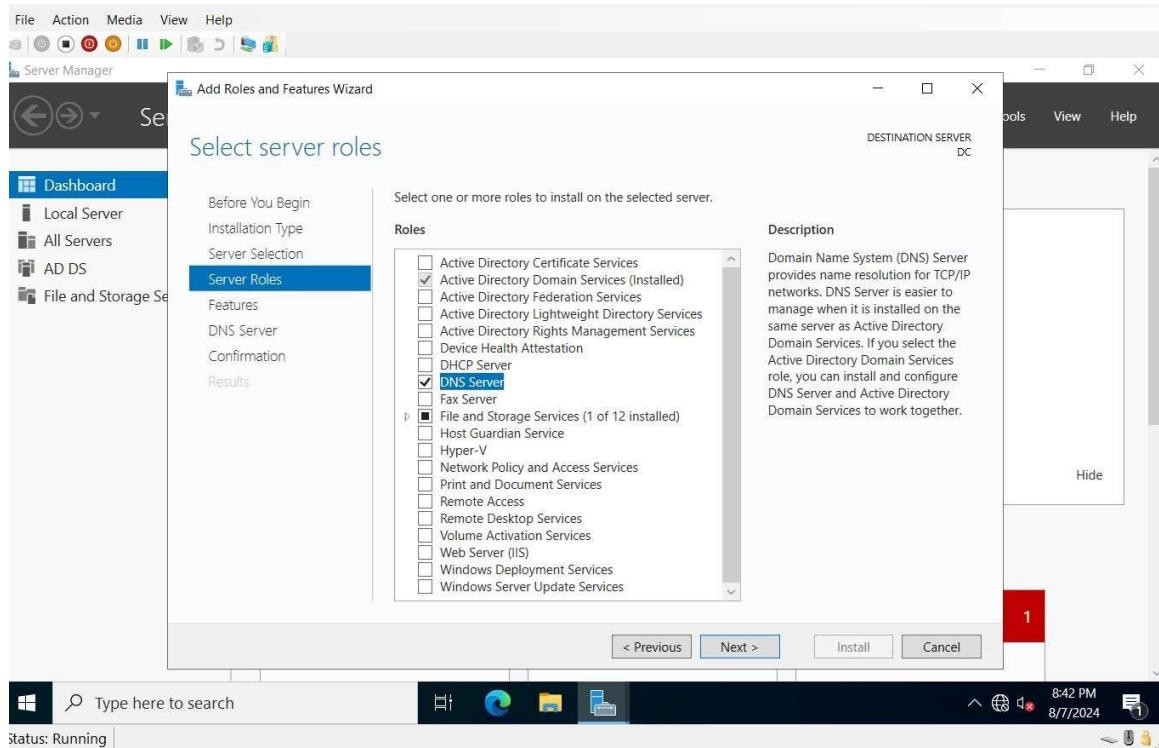
6. To configure this server as a Domain Controller, check the box for Active Directory Domain Services. When you add this role, DNS will be automatically installed and configured. The server's DNS will point to its own IP address because a Domain Controller needs to manage and resolve names for its domain internally. In the same way, if you were adding roles like Web Server or DHCP Server, you would select those boxes, since a server takes on the function of any role that is installed on it.



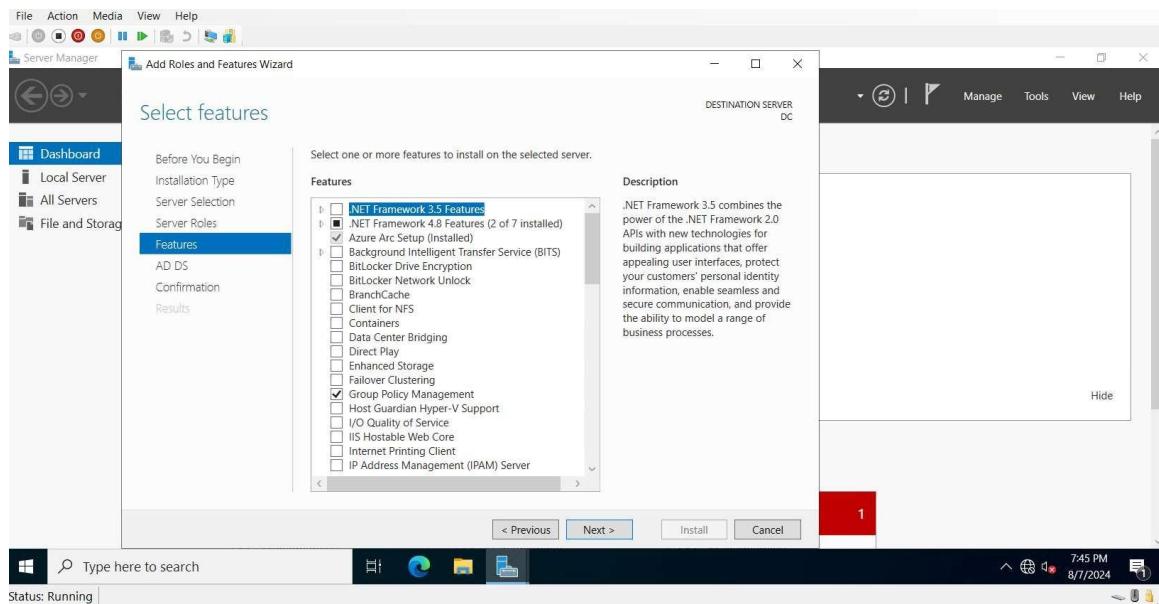
8. A box will POP-UP once you check the box. Click Add features.



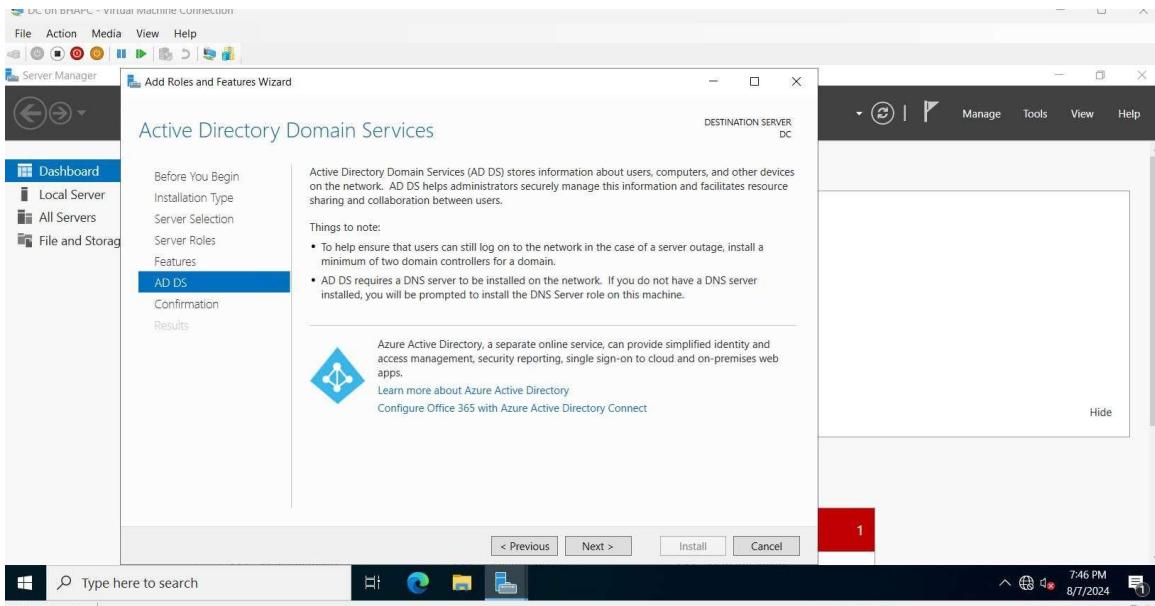
9. Also, add DNS. Click Next.



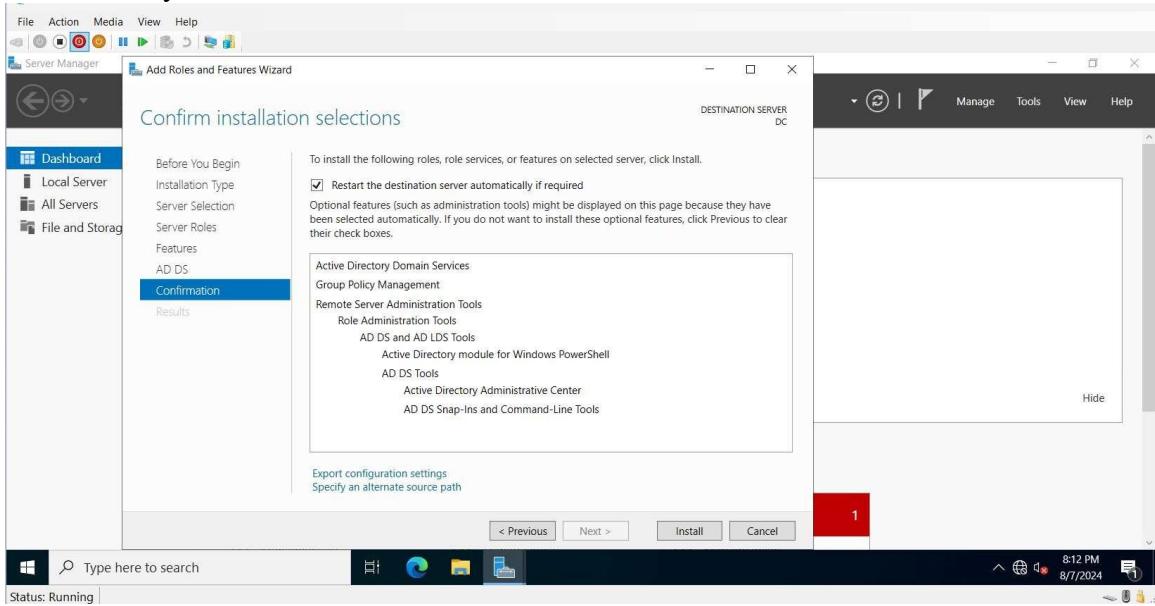
10. Click Next.



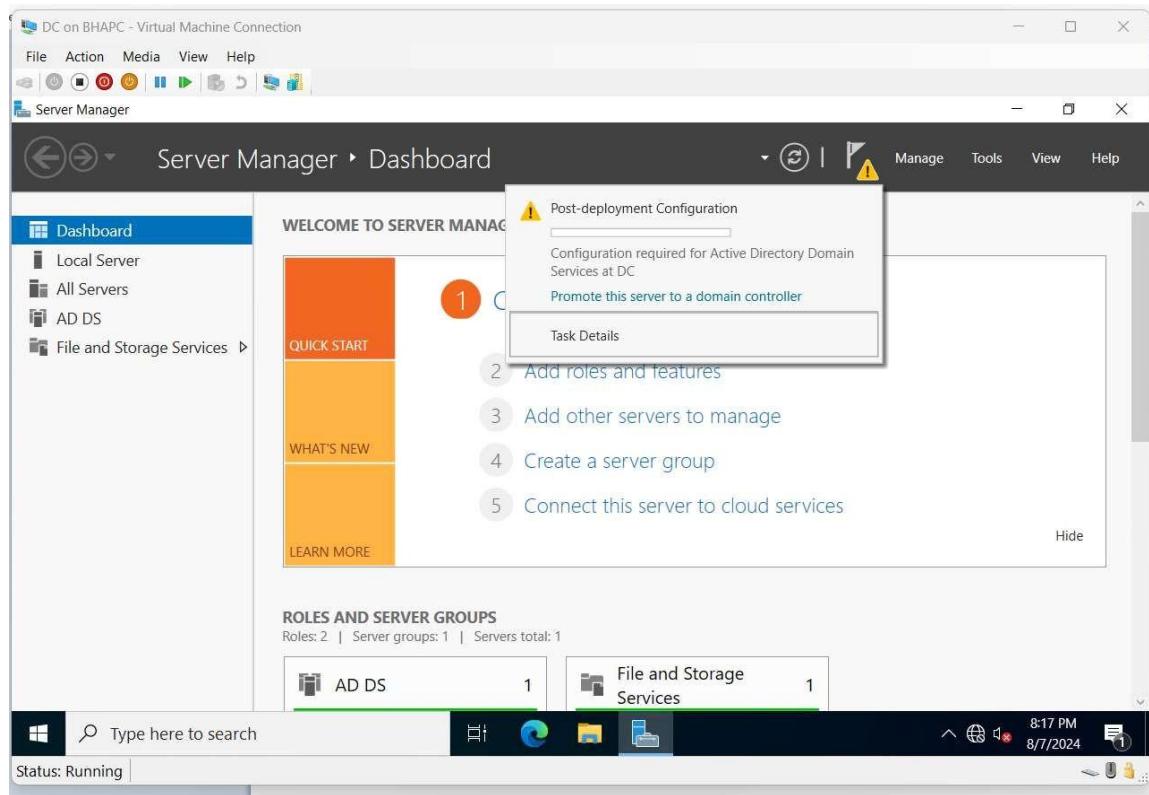
11. Click Next.



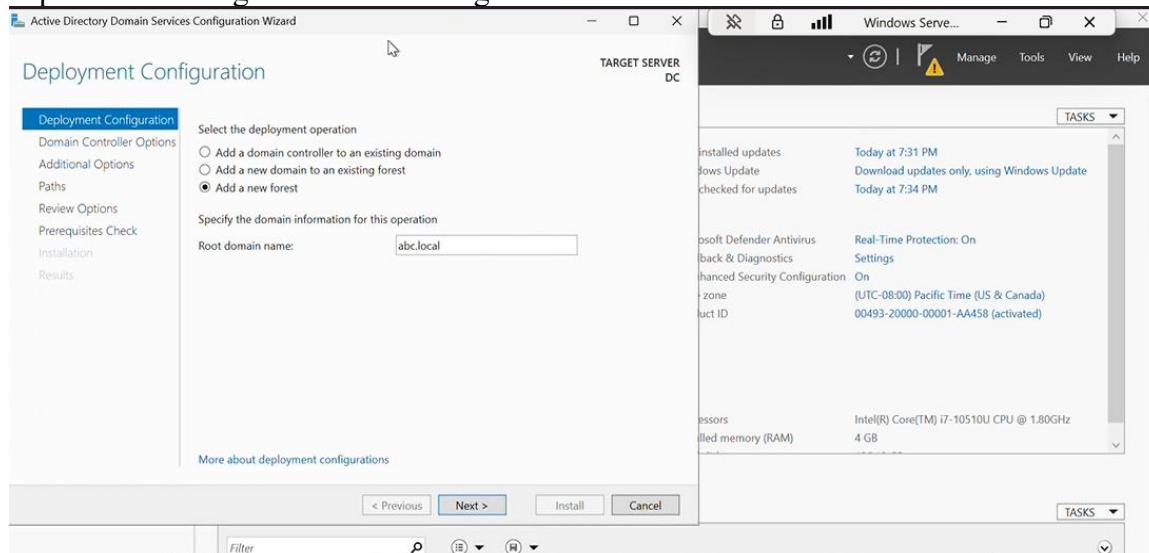
12. Check the box to allow the server to restart automatically if required, then click Install. During the installation, if a restart is needed, the system will restart the server automatically.



13. After the server reboots, click on the Notifications flag. You will see a yellow warning triangle indicating that further configuration is required. Since our server has the Active Directory Domain Services role installed, we now need to promote it to a Domain Controller. To do this, click on Promote this server to a domain controller.

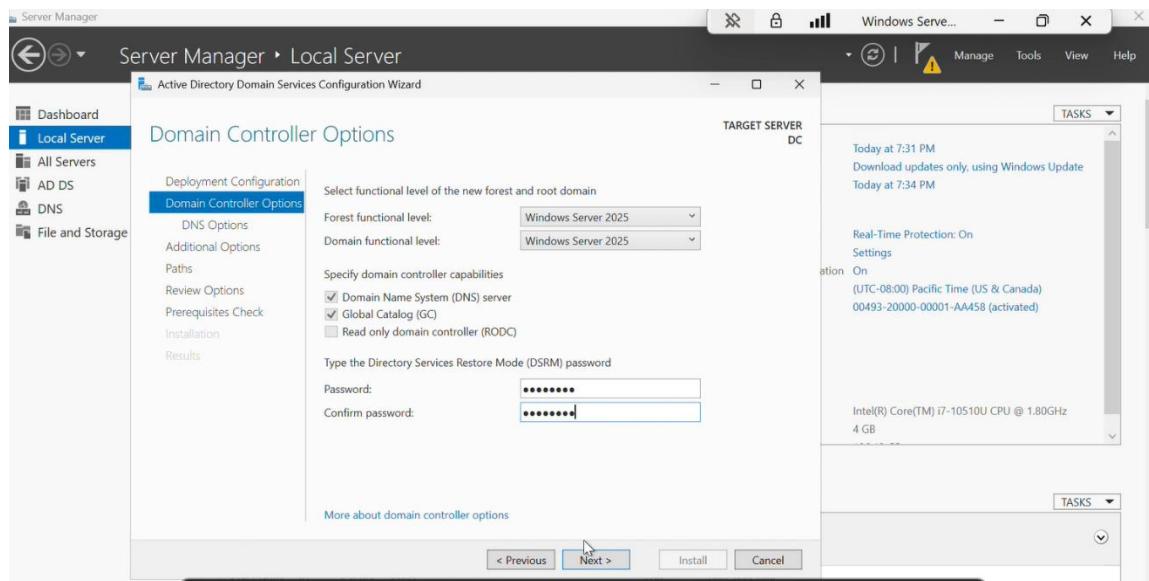


14. Click on Add a Forest and then enter your Root Domain Name. The forest is the top-level container in Active Directory that holds all domains within an organization, and the root domain is the first domain created in the forest. For example, if your organization's name is ABC, you can name the forest abc.local. Within this forest, you can have multiple domain trees, such as sales.abc.local or hr.abc.local, which are separate domains that share the same forest and can communicate securely. The root domain, ABC.local, serves as the main domain, while trees can represent different departments or regions within the organization.

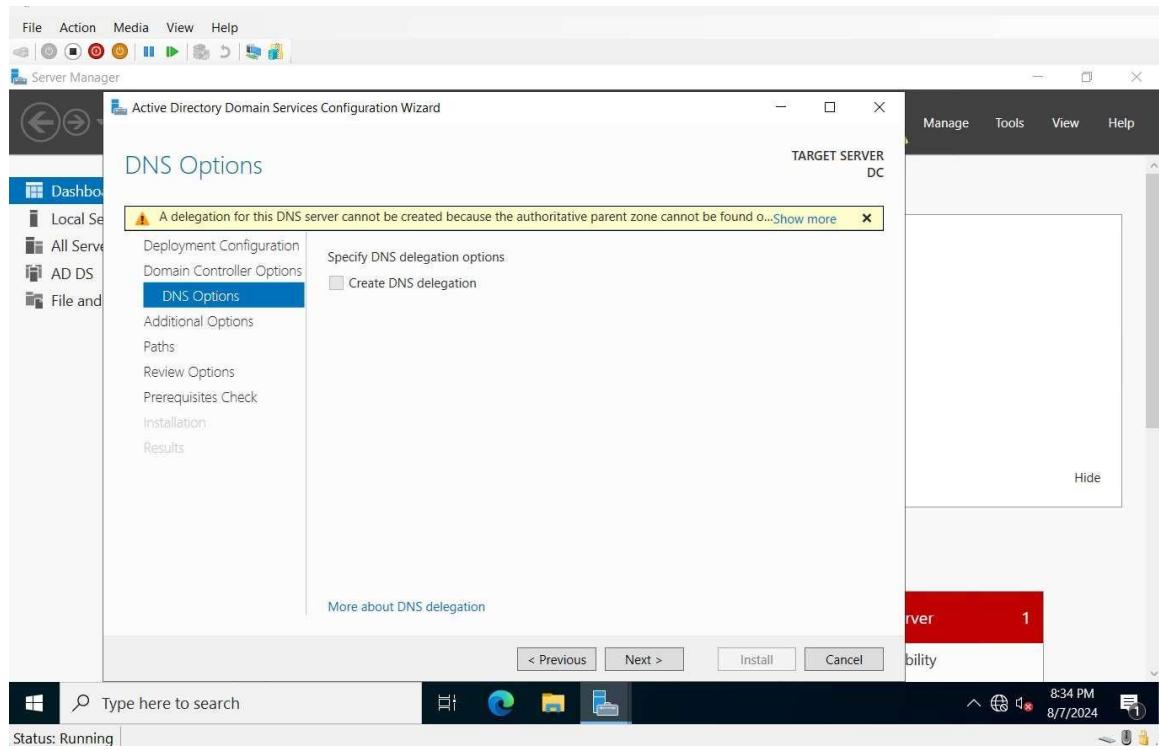


15. The Forest Functional Level determines which version of Windows Server your Active Directory forest will use. Choose the latest version so you can take advantage of all the newest features, such as enhanced security, better replication, and advanced administrative tools.

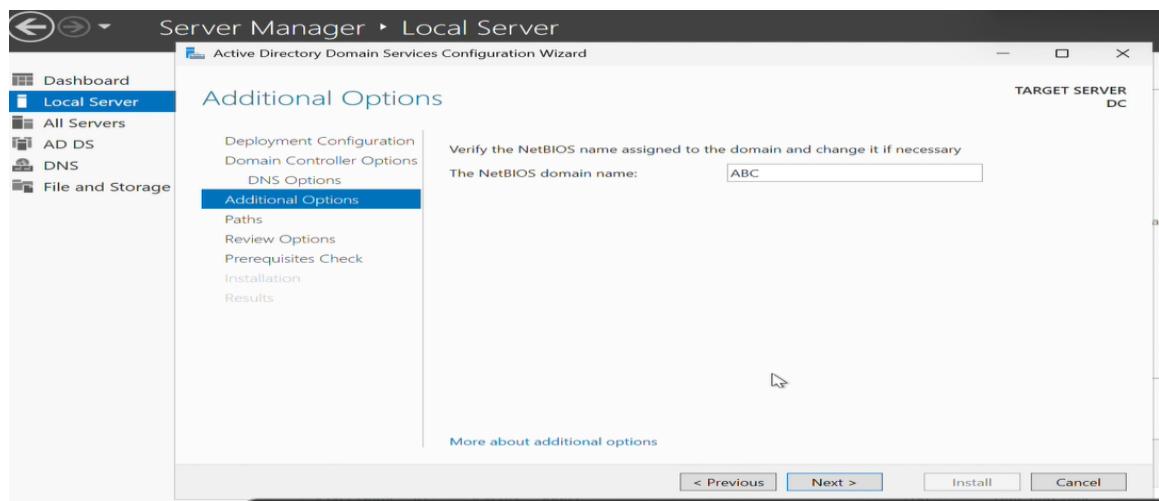
Next, set the Directory Services Restore Mode (DSRM) password. You will use this password whenever you need to perform maintenance or recover the Active Directory database. For example, if the domain controller becomes corrupted or someone accidentally deletes critical AD objects, you can restart the server in Directory Services Restore Mode and use this password to log in and fix the problem. Without it, you cannot access Active Directory for recovery. After you enter the password, click Next to continue promoting the server to a domain controller.

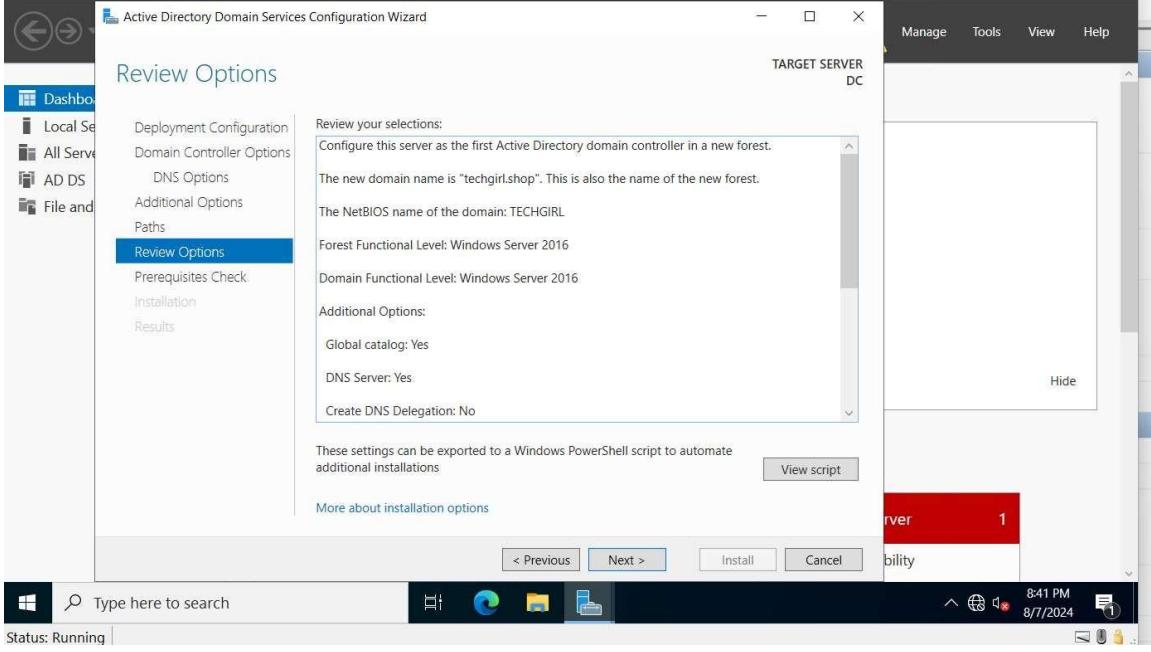


16. Click Next.

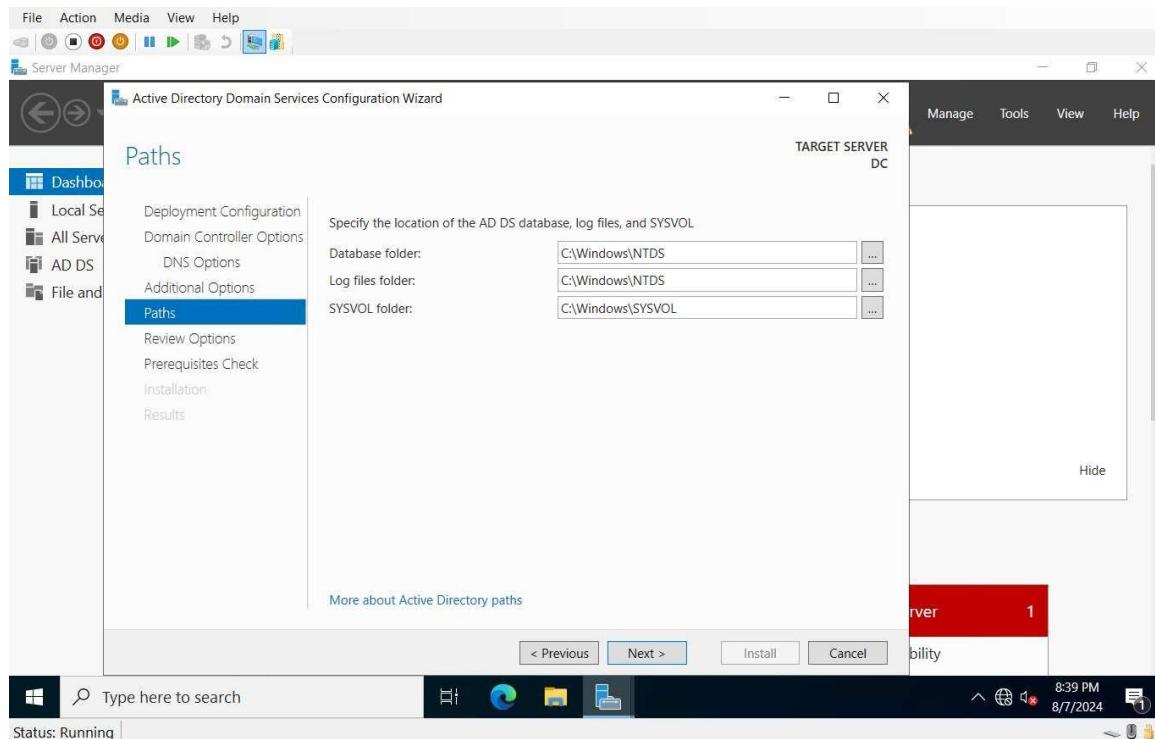


17. Your domain name should appear on this screen. The NETBIOS name is a short identifier for your Windows domain that is used within the local network to simplify name resolution and communication between computers. After verifying the domain and NETBIOS names, click Next to continue.

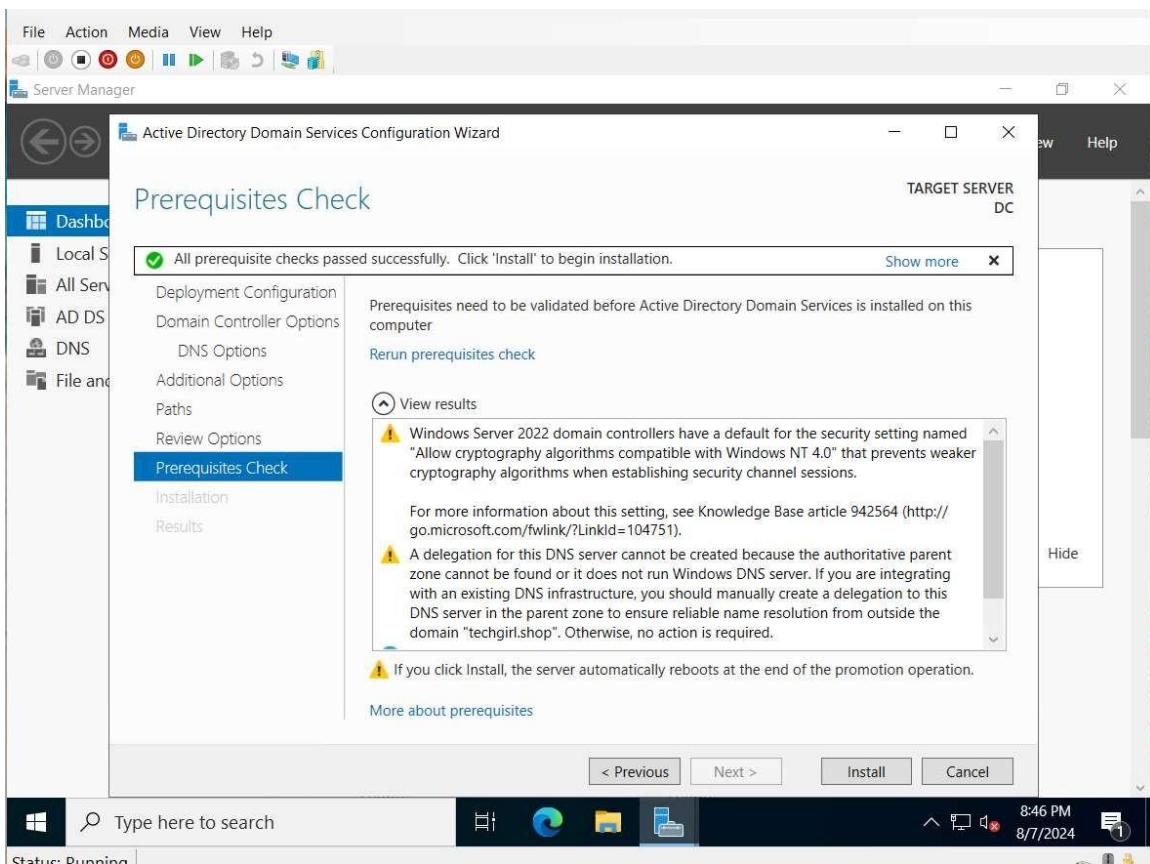




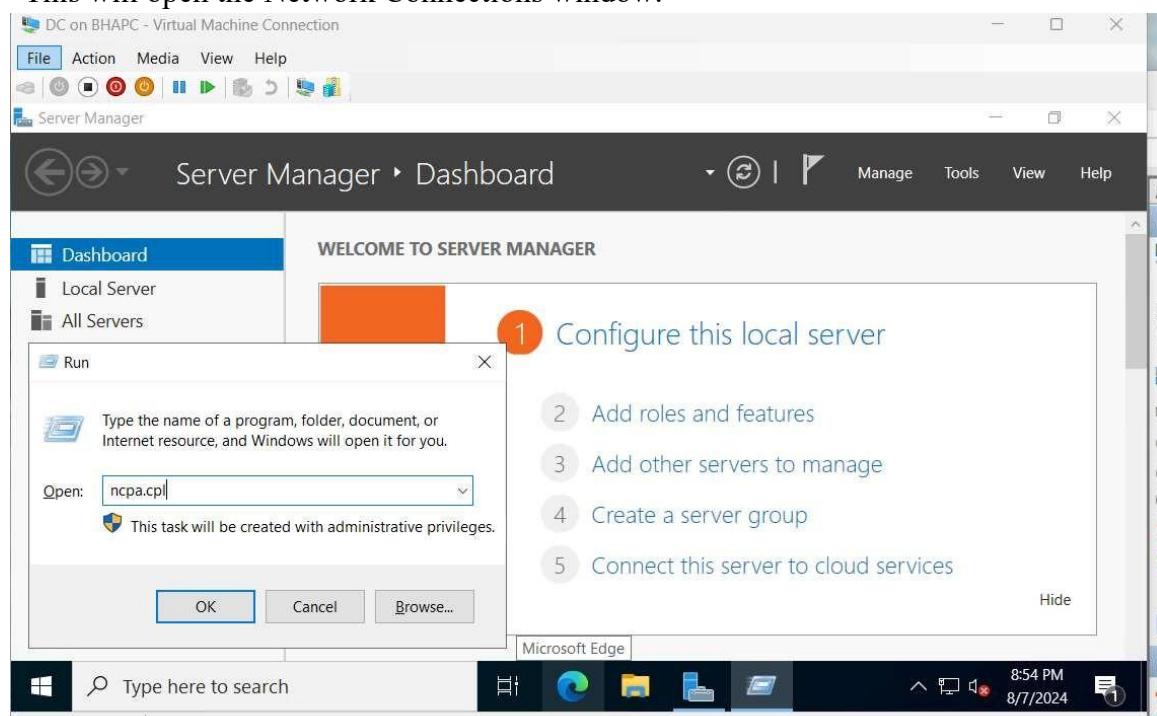
16. This screen shows the path on your server where the Active Directory database will be stored. The database files are called NTDS files. NTDS, or NT Directory Services, holds all the Active Directory information for your domain, including user accounts, groups, computer accounts, passwords, and security policies. The server needs this database to manage authentication, authorization, and directory services for all users and devices in the domain. By default, Windows stores the NTDS database at C:\Windows\NTDS, but you can change the location if required. After verifying or modifying the path, click Next to continue.



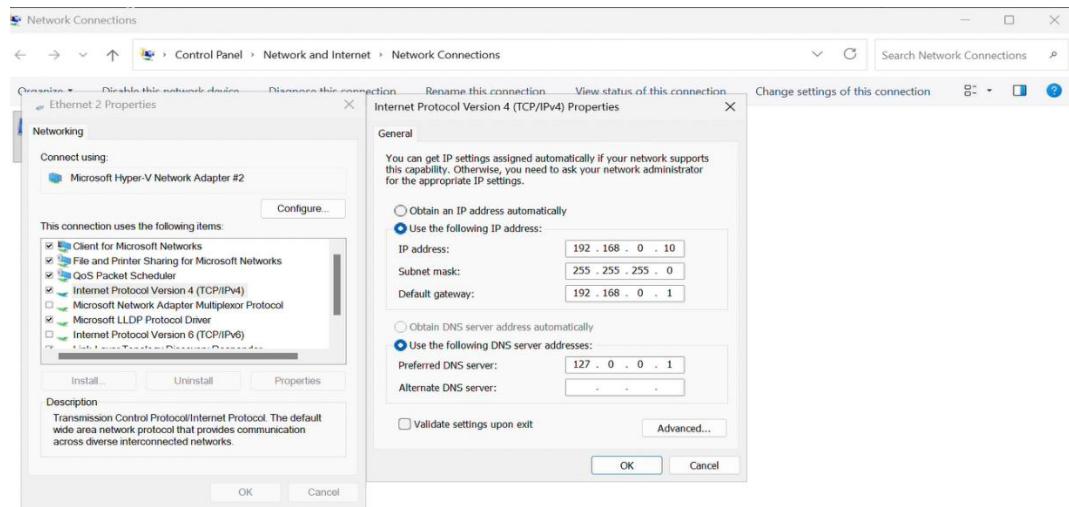
18. Click Install.



19. Now log in to the server as a Domain Admin. After installing the Active Directory and DNS roles and completing the deployment, the server becomes a Domain Controller. The Domain Admins group manages the domain and has full administrative rights over all users, computers, and policies. You must log in as a Domain Admin to manage the domain properly.
20. Open the Run dialog by pressing Windows + R, then type ncpa.cpl and press Enter. This will open the Network Connections window.

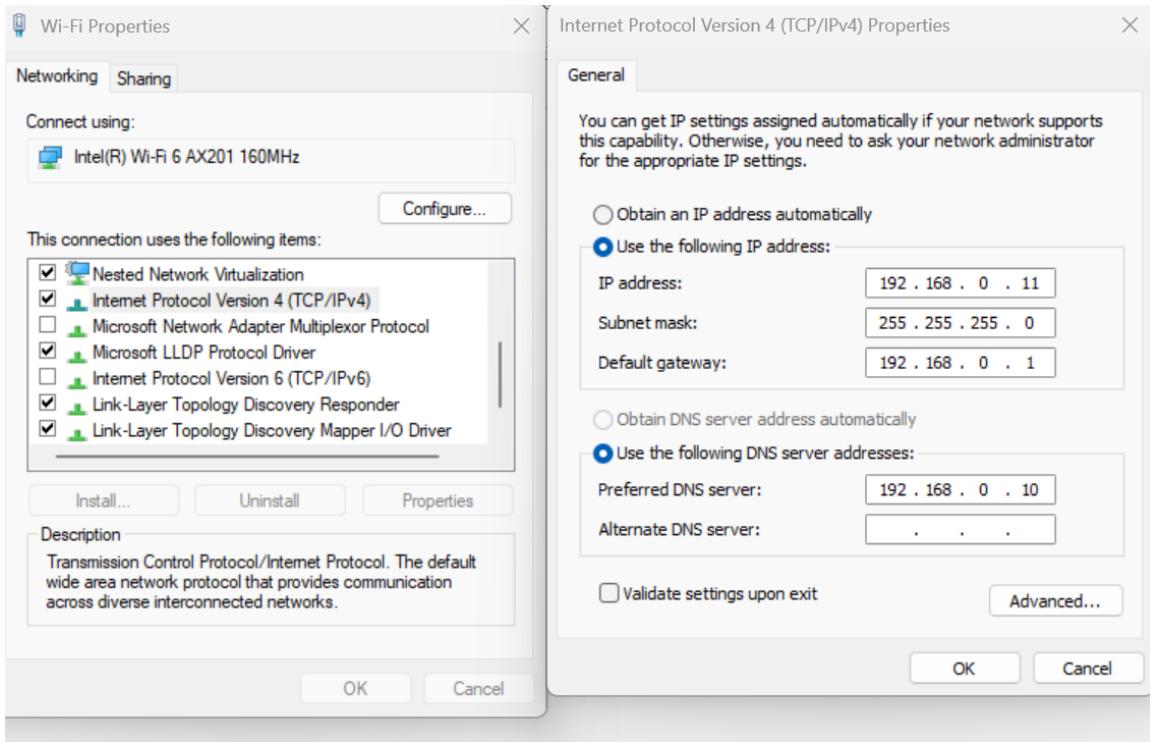


21. Right-click your network connection (here, Ethernet) and select Properties. Then select IPv4 and click Properties. In the DNS server address field, you will see 127.0.0.1. This is the loopback IP address, which means the server is pointing to itself for DNS. Since this server is now a Domain Controller, it also acts as the DNS server for the domain. Active Directory relies on DNS to locate domain resources, authenticate users, and manage network services, so the server must resolve DNS queries for its own domain. All devices that join this domain will also use the Domain Controller's IP address as their DNS server to ensure they can locate domain services and communicate properly with Active Directory.

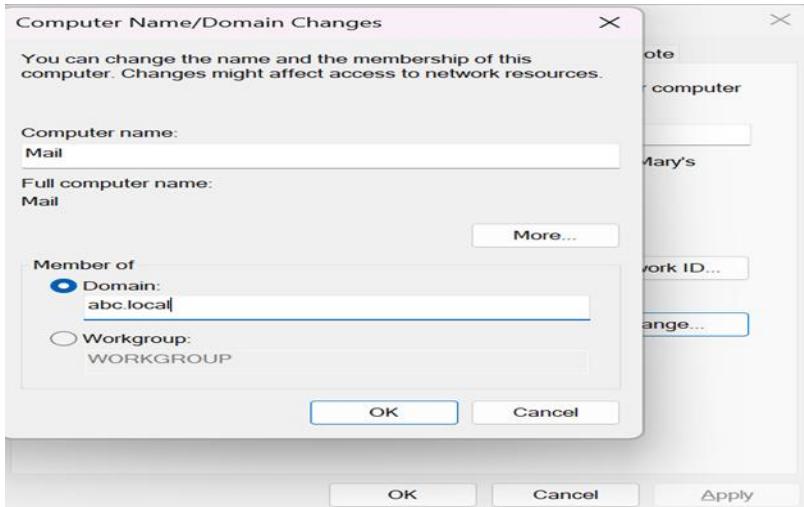


You have now configured Active Directory and set up a Domain Controller in your network. Next, we will configure the Exchange Server. Before starting, download and install the three required Exchange files. Also, make sure you have a separate drive (other than C:) available. Exchange uses this separate drive to store its databases and logs, which improves performance, simplifies backup and recovery, and prevents the system drive from filling up. Having a dedicated drive ensures the Exchange environment runs efficiently and remains easier to manage.

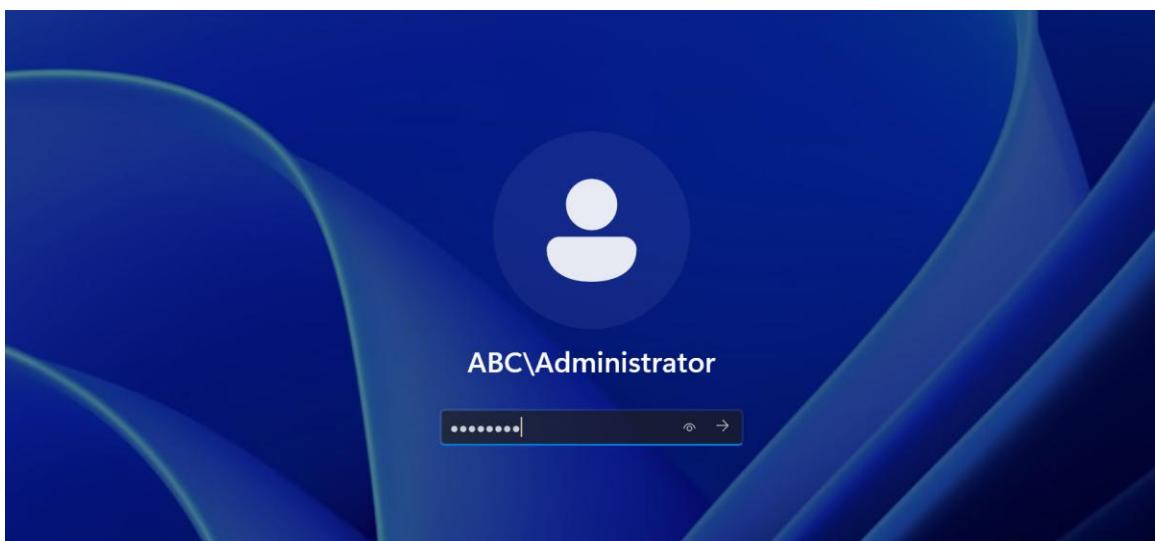
1. The first step is to assign a static IP address to the server. Press Win + R, type ncpa.cpl, and press Enter to open the Network Connections window. Right-click your network adapter (here, Ethernet) and select Properties. Uncheck IPv6, then select IPv4 and click Properties. Assign a static IP address to the server. In the DNS settings, enter the IP address of your Domain Controller as the Preferred DNS. If you have additional Domain Controllers, add their IP addresses as Alternate DNS by clicking Advanced. This ensures that the Exchange Server can reliably communicate with the Domain Controller and resolve Active Directory DNS records.



2. The second step is to change the server name. Press Win + R, type sysdm.cpl, and press Enter to open the System Properties window. Click Change and enter the new server name. In this example, the server is named Mail. Using a short and simple name makes it easier to identify and manage internally. It also needs to be updated in the public DNS records with your domain registrar. This ensures that external mail servers can locate your Exchange Server to deliver emails into your organization and that your server can send emails to external domains reliably. Proper DNS configuration connects your internal Exchange Server with the global email network. Click OK, then click OK again. The server will automatically reboot to apply the new name.



3. The third step is to join the server to the domain. After the server reboots from the previous step, press Win + R, type sysdm.cpl, and press Enter to open the System Properties window. Click Change, then select Domain and enter the name of your domain. When prompted, enter the Domain Administrator's credentials. After completing this, the server will automatically reboot again. Once it restarts, your server will be joined to the domain and fully recognized as part of your network.
4. Now, login as Domain Admin. If you have not downloaded the Package files for Server, do it now. Make sure you are logged in as Domain Administrator. Here is the link:
<https://download.microsoft.com/download/b/f/7/bf7700c9-c2fd-40be-82cc-7c5330b5f981/ExchangeServer2019-x64-CU14.ISO>



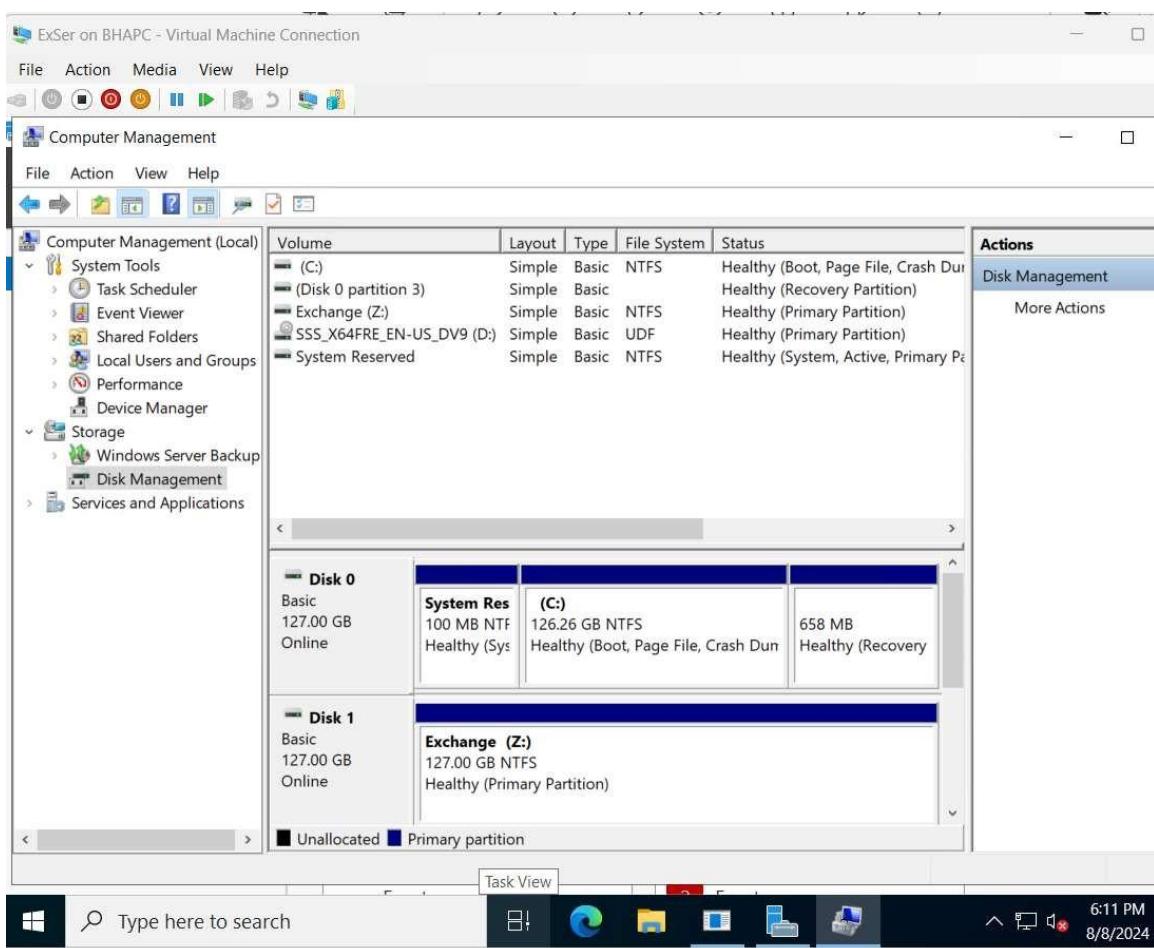
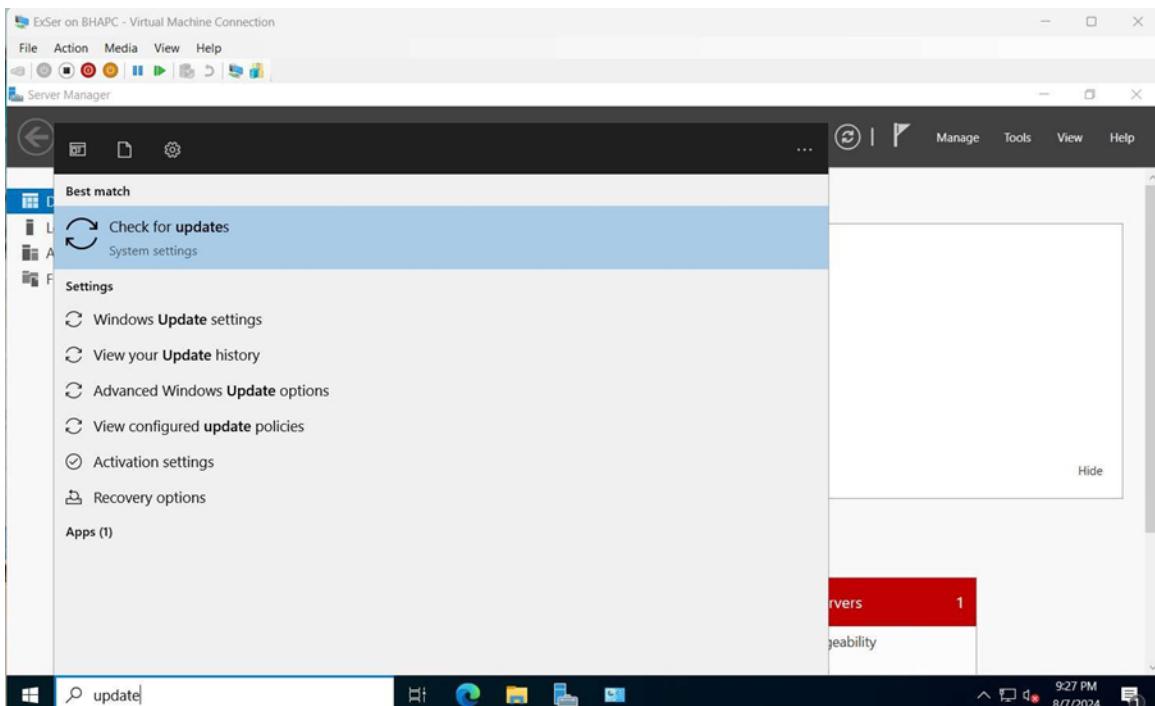
5. After joining the server to the domain, you need to verify network connectivity between the Domain Controller and the Exchange Server. Open a command prompt and use the ping command to test connectivity. For example, type ping abc.local to check domain name resolution, or ping 192.168.0.10 to verify that the Exchange Server can reach the Domain Controller. This communication is essential because the Exchange Server relies on the Domain Controller to authenticate users, resolve domain names, and function properly as an email server.

6. There are some prerequisites to complete before installing Exchange Server: The first and most important requirement is to log in as a Domain Administrator. Only a Domain Admin account has the necessary permissions to install and configure Exchange Server in a domain environment.

The next prerequisite is to check for and install any pending Windows updates. On the Exchange Server, search for updates and install all cumulative updates. If Windows updates are pending, the server may not be compatible with Exchange, which can cause errors or issues during installation. Make sure the server is fully updated before starting the Exchange Server installation.

7. Create a separate drive for Exchange Server installation: It is recommended to install Exchange Server on a drive other than C: While you can install it on C: doing so creates a risk: if the system drive experiences issues, your Exchange Server, including its databases and logs, could be affected. By using a separate drive, you ensure that the Exchange Server remains functional even if the C: drive encounters problems. This is especially important because Exchange stores critical mail data, logs, and configuration files that must always remain protected and accessible.

8. Prepare the new drive: Open Computer Management, and under Disk Management, right-click the available disk and select Online, then Initialize it. Next, right-click the unallocated space, choose New Simple Volume, and follow the wizard to assign a drive letter (avoid using letters A to G), set the volume size, and give the drive a name. Wait until the system shows the new drive with the name you assigned. This drive will be used to install and mount Exchange Server. Exchange Server relies on Active Directory for user accounts, security, and configuration. The server also acts as a mail hub for the organization, sending and receiving emails both internally and externally. Using a dedicated drive ensures that all Exchange data, including mailbox databases and logs, is kept separate from the system drive, reducing the risk of corruption or downtime. Together with a proper hostname (like Mail) and correct DNS configuration, this setup ensures that your Exchange Server is reliable, manageable, and fully integrated into your domain network.



9. Before installing (mounting) the Exchange Server, you must download and install three required software packages on your server. These are prerequisites for Exchange and must be installed first to ensure a smooth installation.

Important: After installing these three software packages, restart the server before proceeding any further. This ensures all updates and configurations are properly applied and the server is ready for Exchange installation.

Here is the link:

Visual C++ Redistributable Packages for Visual Studio 2013 (64 Bit)

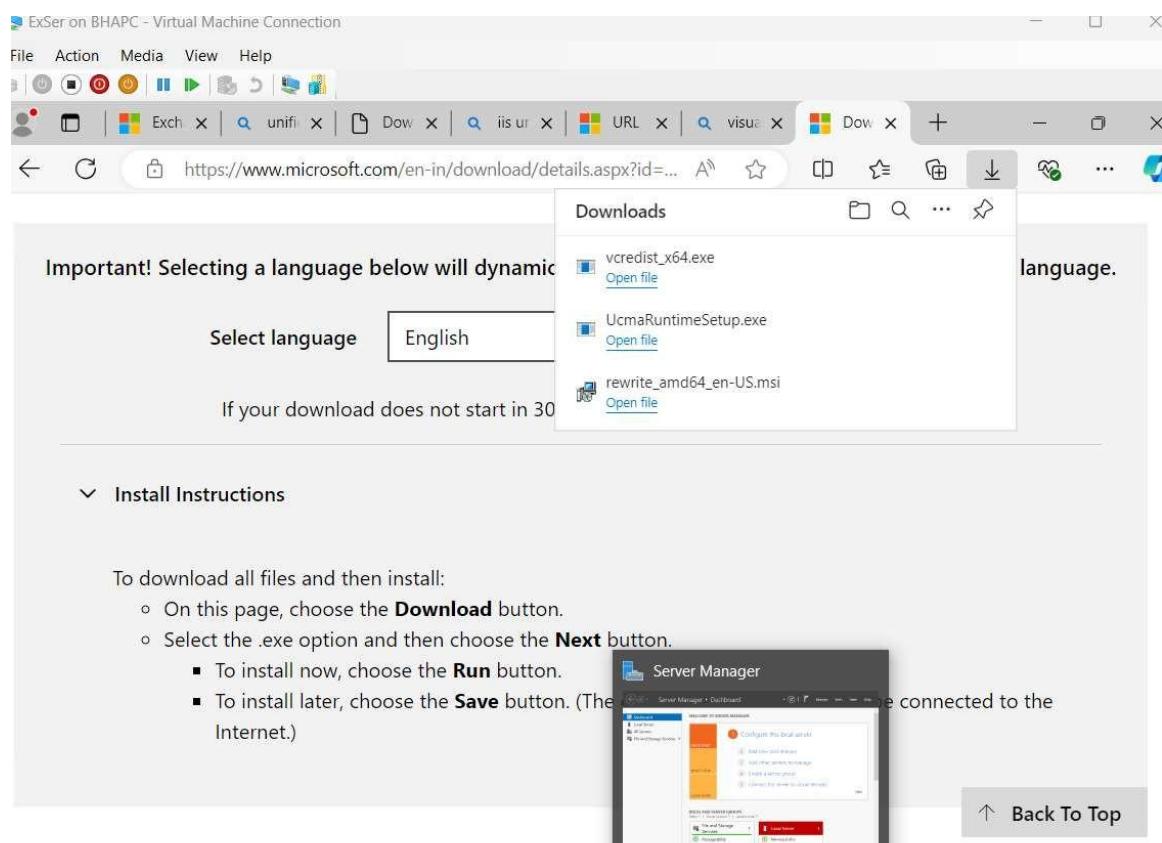
<https://www.microsoft.com/en-in/download/details.aspx?id=40784&msockid=1b04bc26064f6b7d0324a8f0070f6adf>

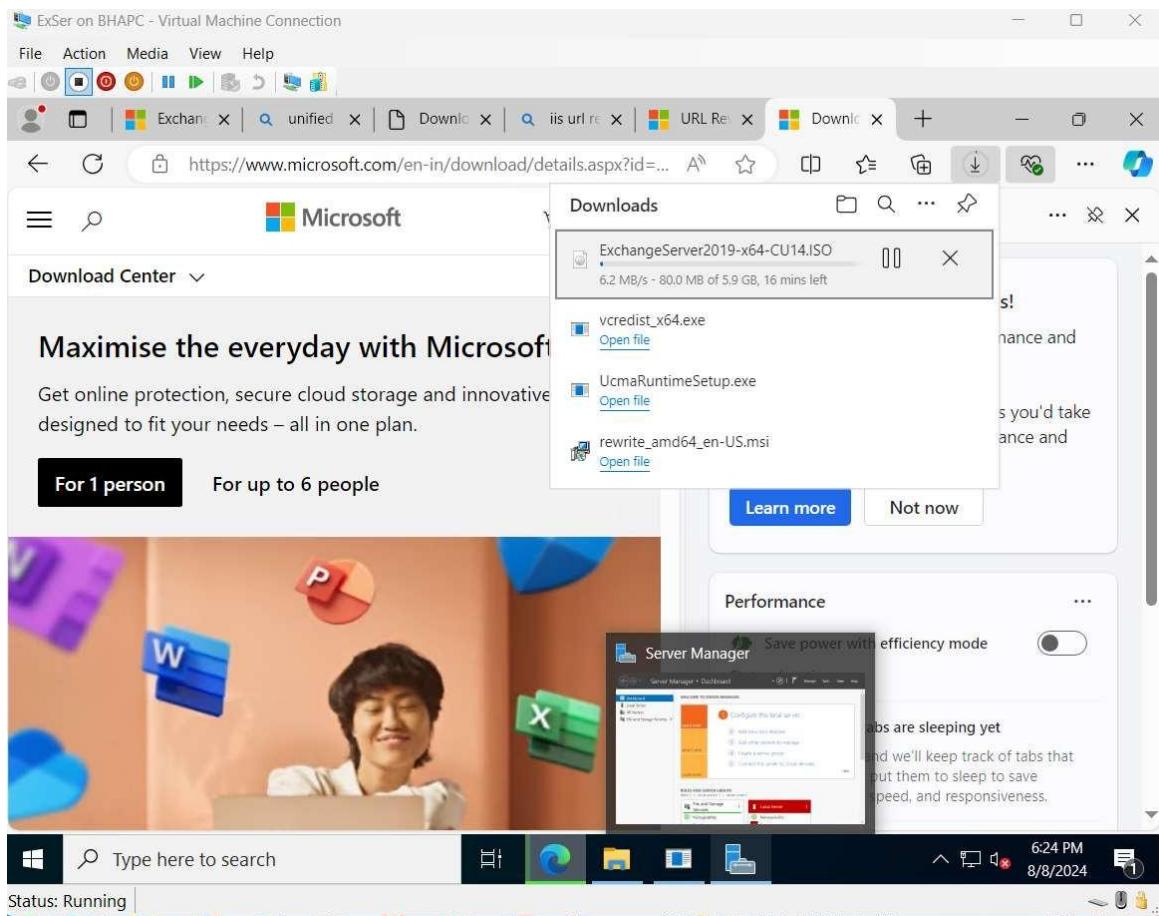
IIS URL Rewrite Module (64 Bit Installer)

<https://www.iis.net/downloads/microsoft/url-rewrite>

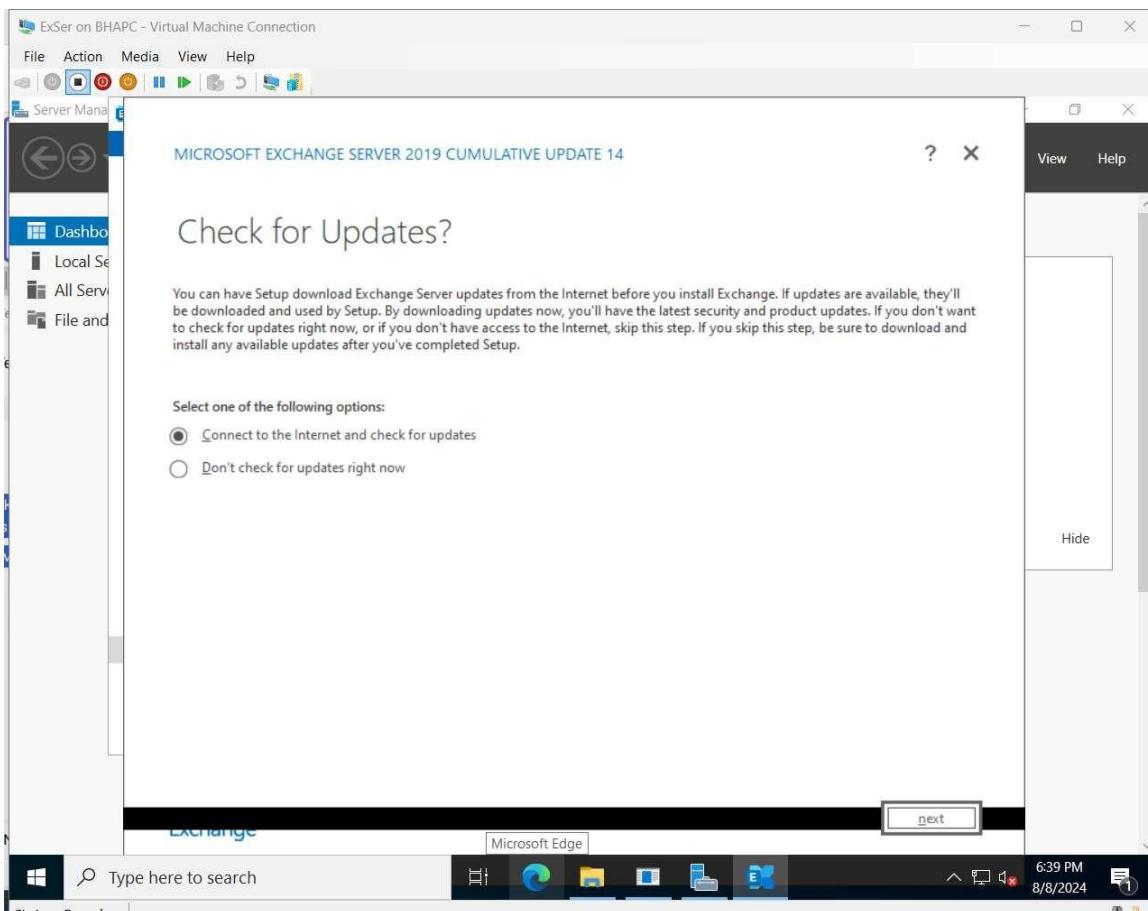
Unified Communications Managed API 4.0 Runtime

<https://www.microsoft.com/en-us/download/details.aspx?id=34992>

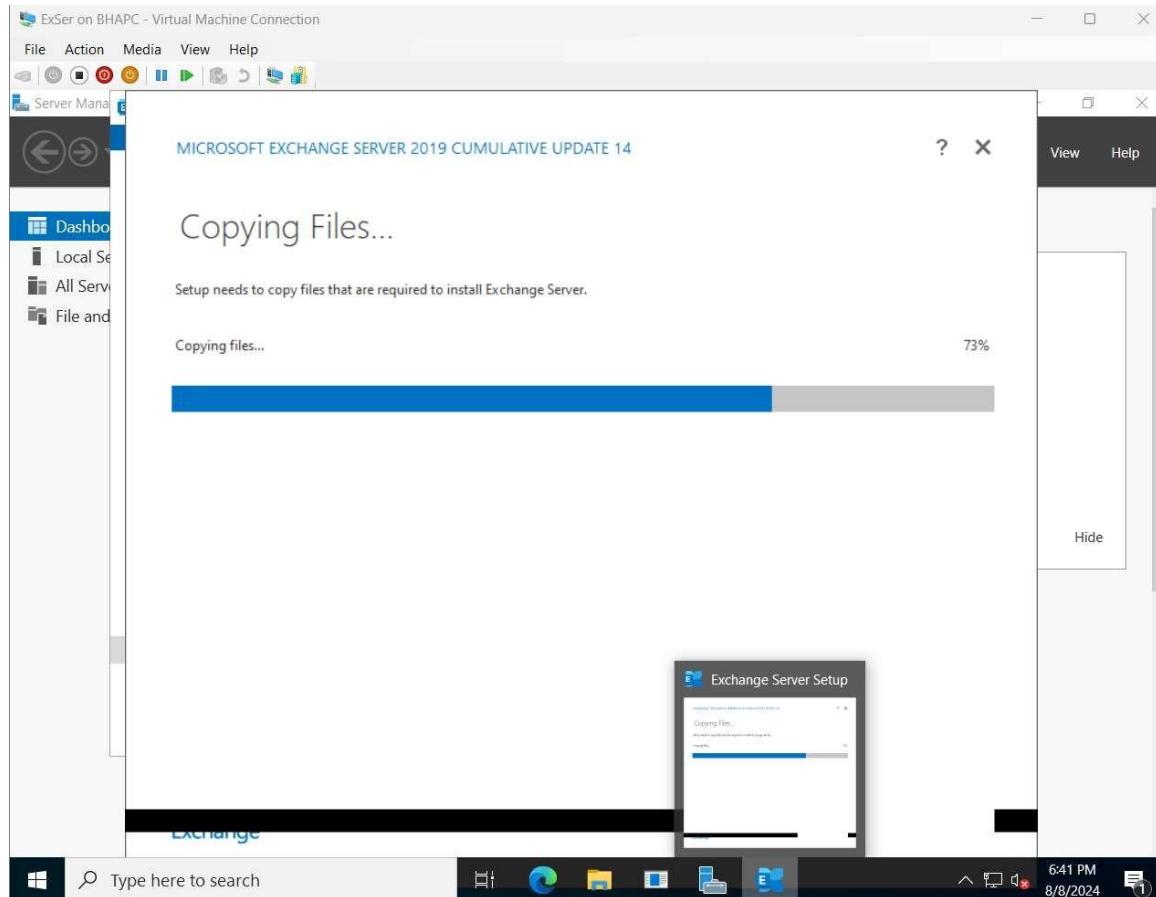




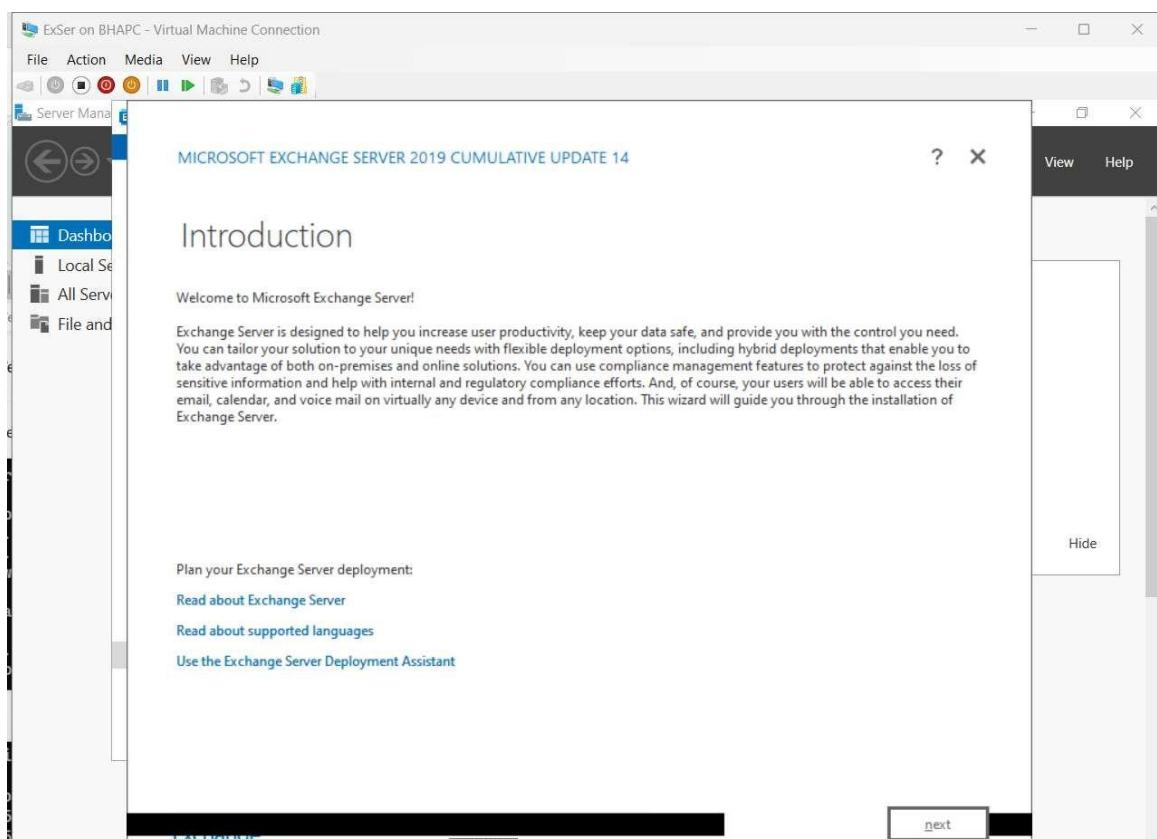
10. Right-click the Exchange Server installation file and mount it on the prepared drive (for example, drive Z:). Open the mounted drive, right-click Setup.exe, and select Run as Administrator. Click Next to begin the installation process.



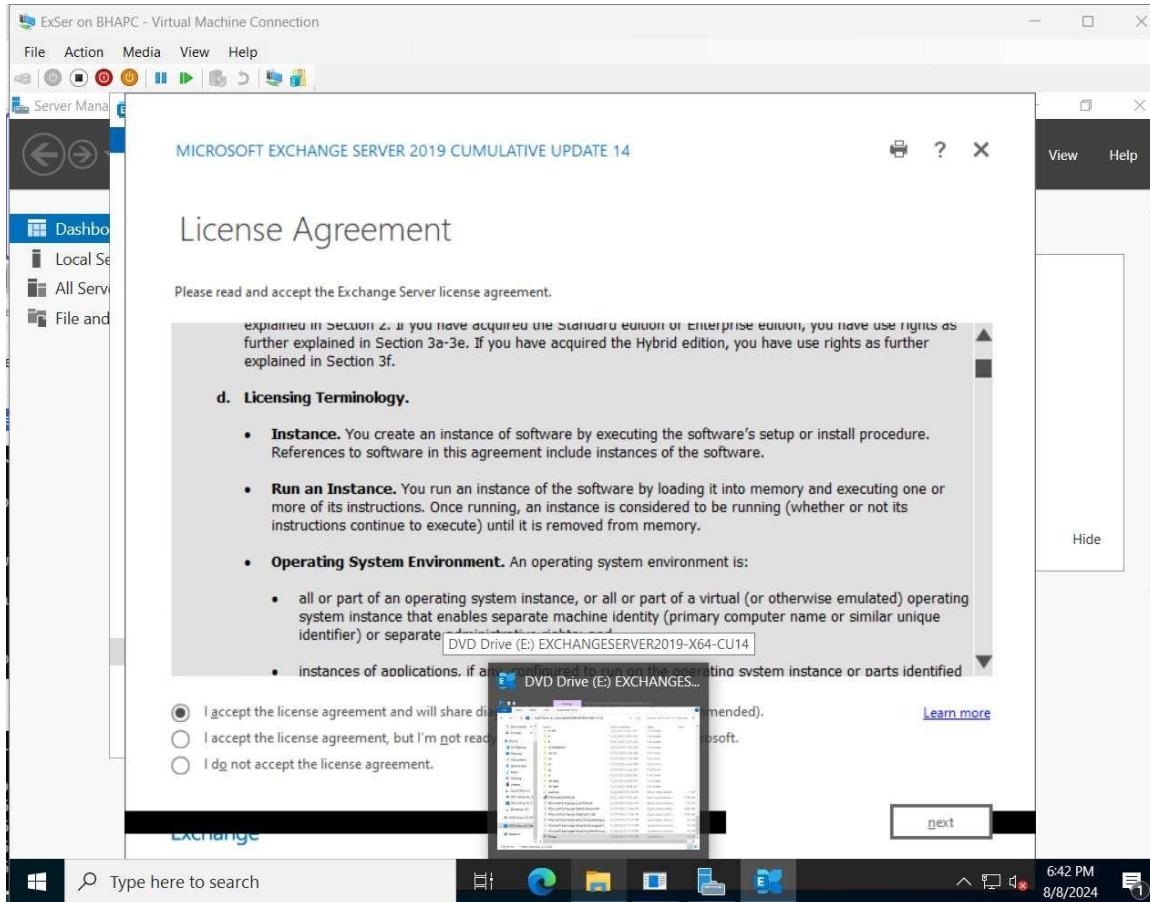
11. Click Next. The setup will now copy all the necessary files required to install Exchange Server. This prepares the server for the actual installation process.

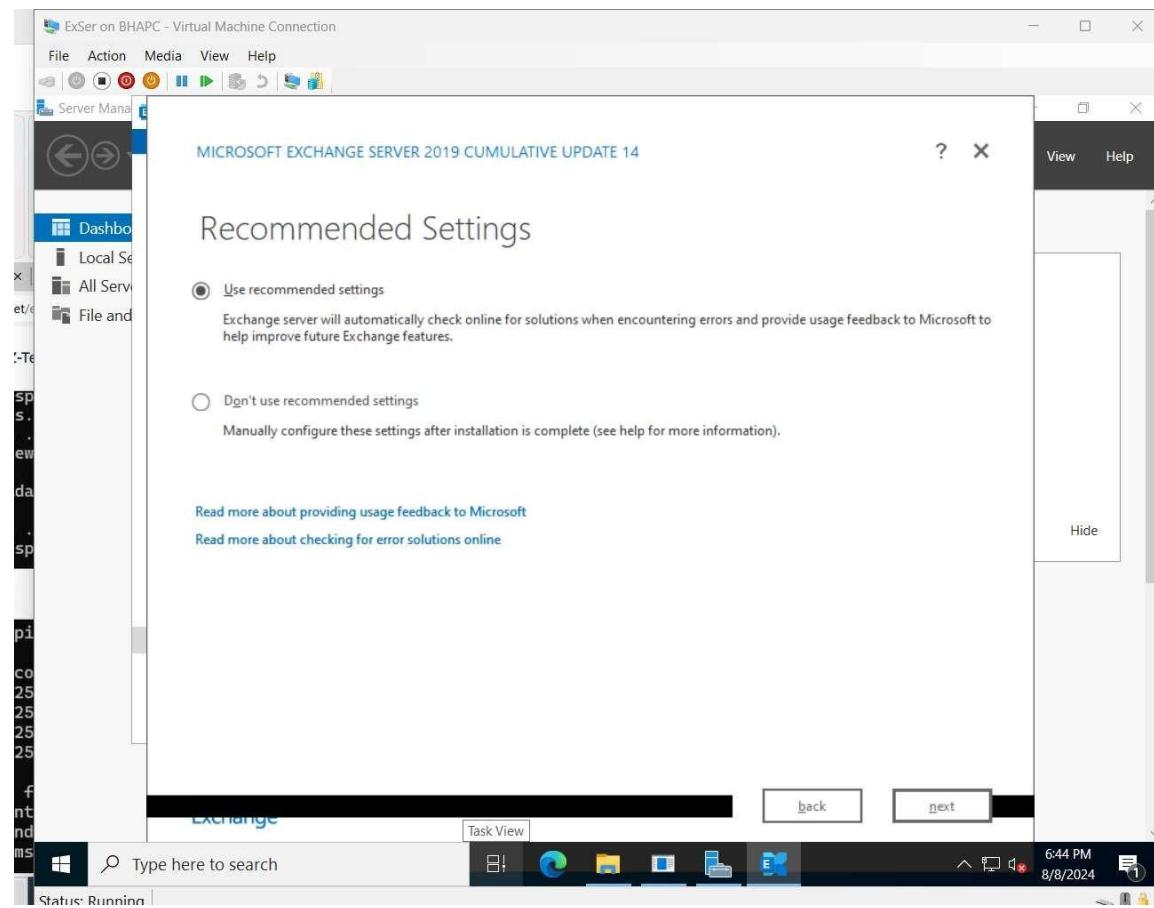


12. Click Next

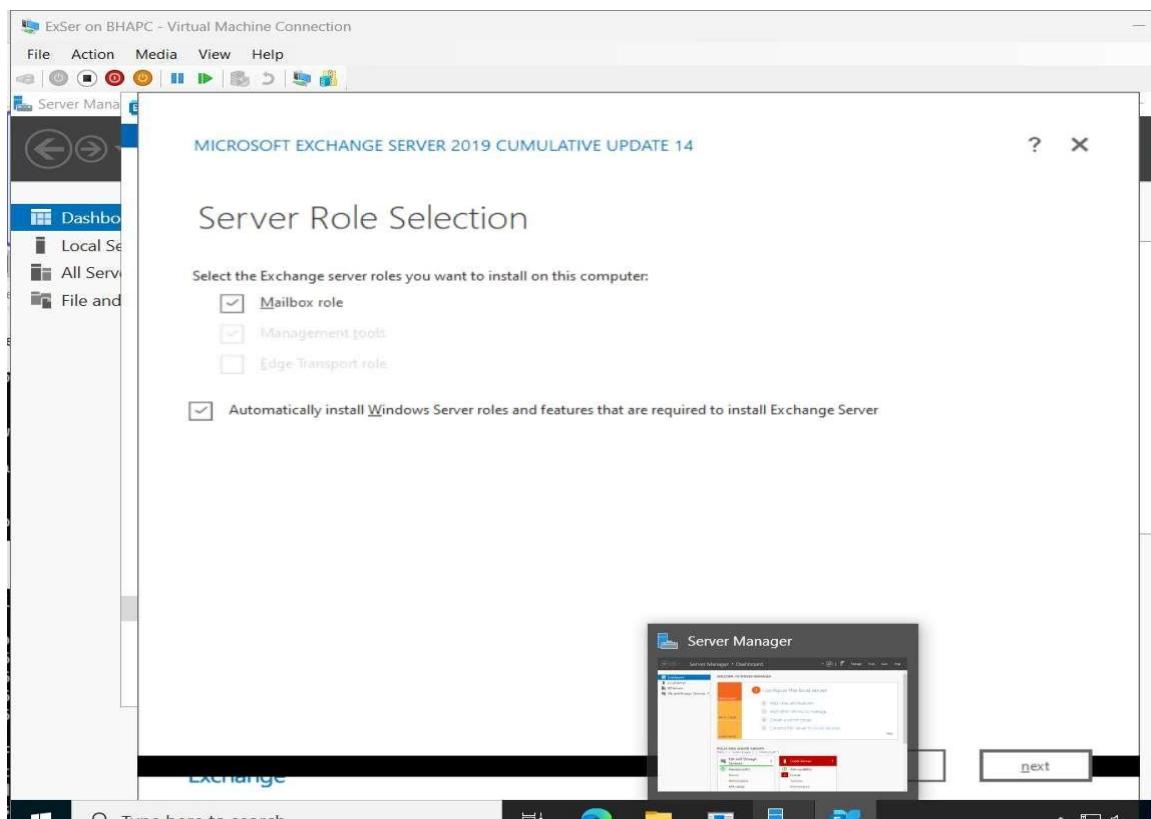


- 13.** The setup will now display the License Agreement. Read the agreement, check the box I accept the terms in the License Agreement, and then click Next to proceed.

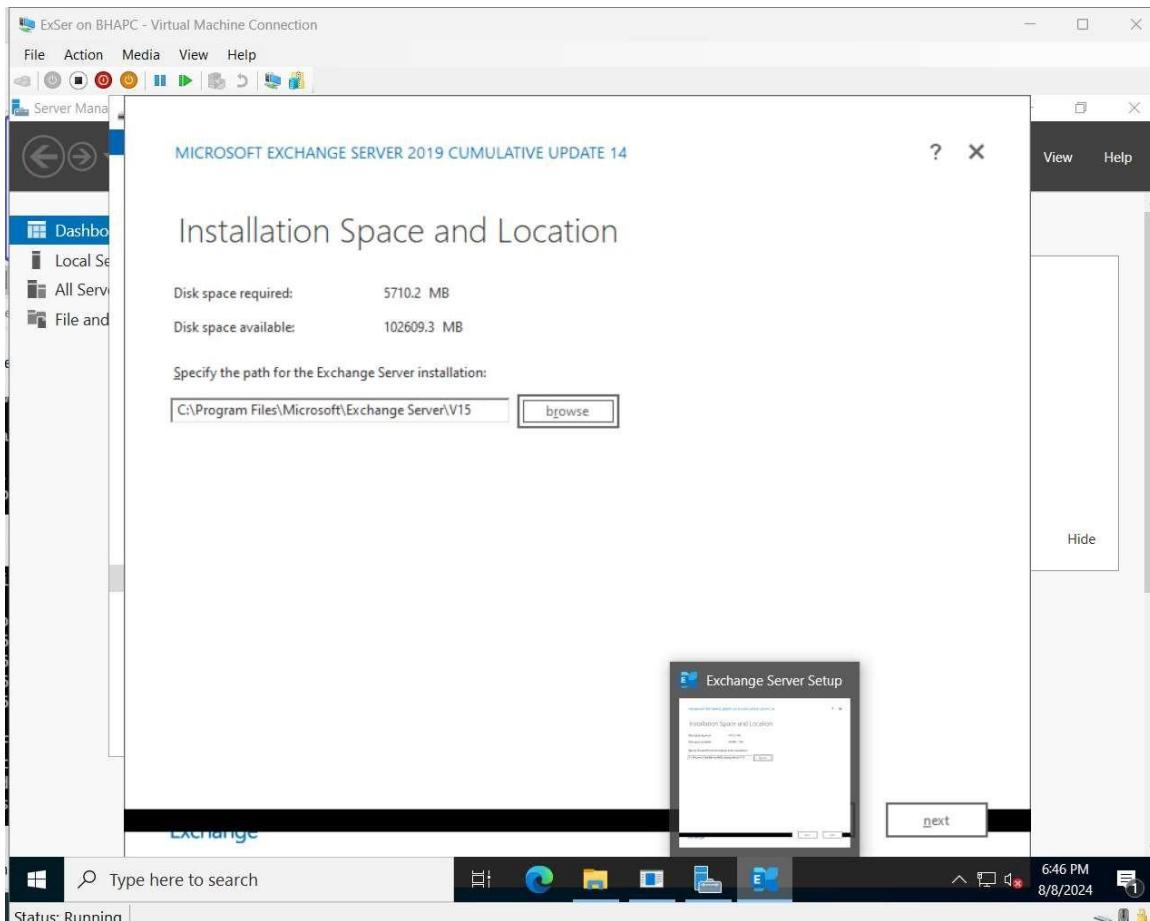




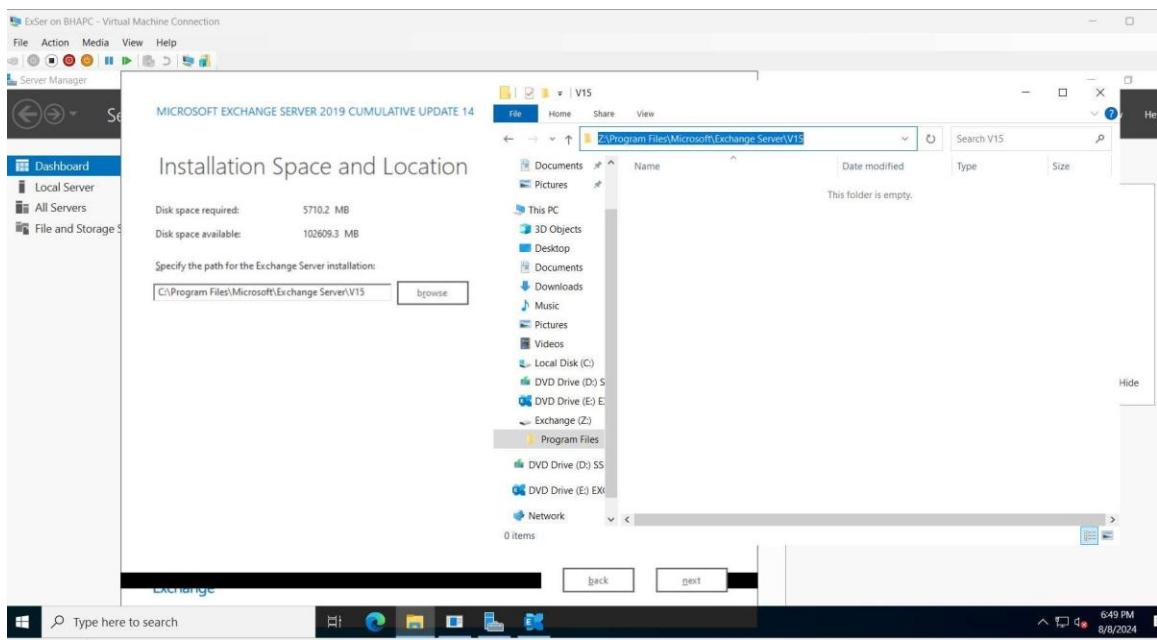
- 14.** Select the Mailbox role (a feature of the Exchange Server) and check the Automatically option. Then, click Next to proceed.



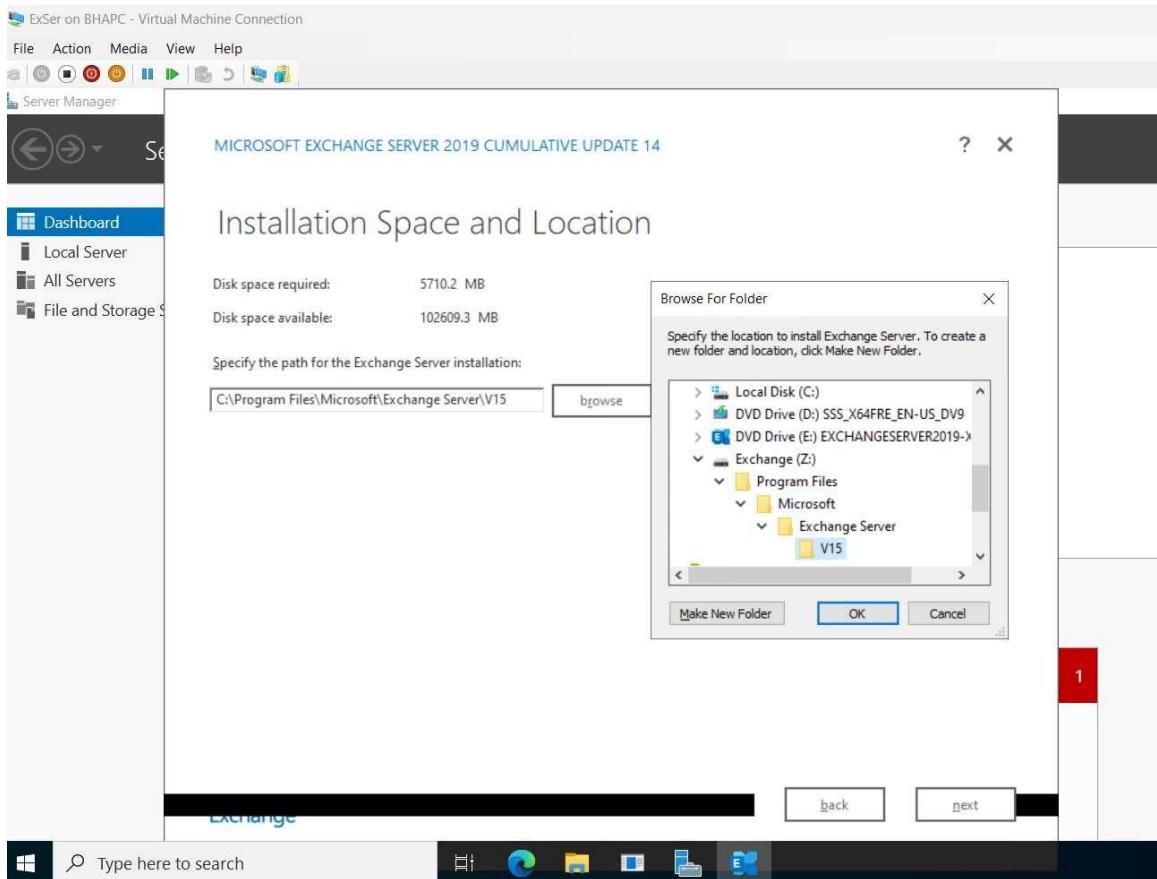
- 15.** In the setup, click Browse to specify the location where Exchange Server will be installed. Navigate to the prepared drive (for example, Z:) and create a folder that matches the installation path shown in the setup. This ensures that Exchange is installed on the separate drive instead of the C: drive, keeping system files and Exchange data separate for better performance and easier management.



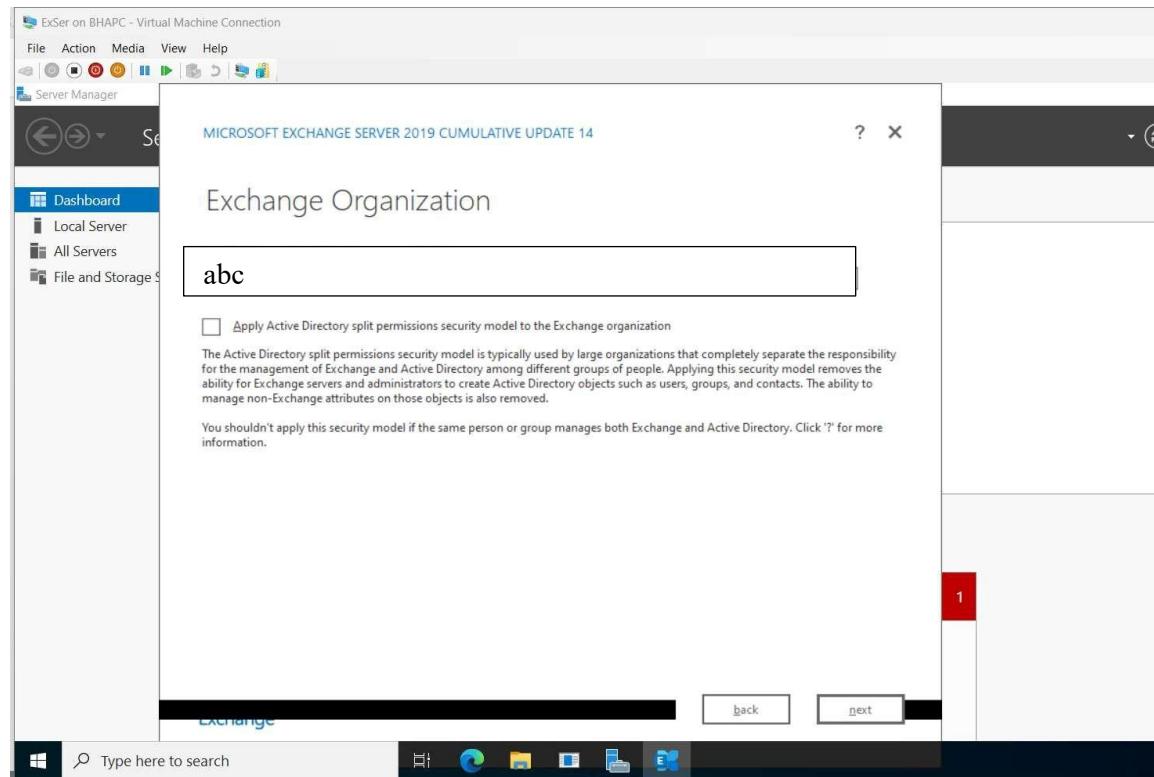
- 16.** Open File Explorer and navigate to your new drive (for example, Z:). Create the folder path: Program Files > Microsoft > Exchange Server > V15. This exact path is what you need to specify during the installation. Note: Be careful with spaces, capitalization, and spelling in the folder names, as any mistake can cause issues during installation.



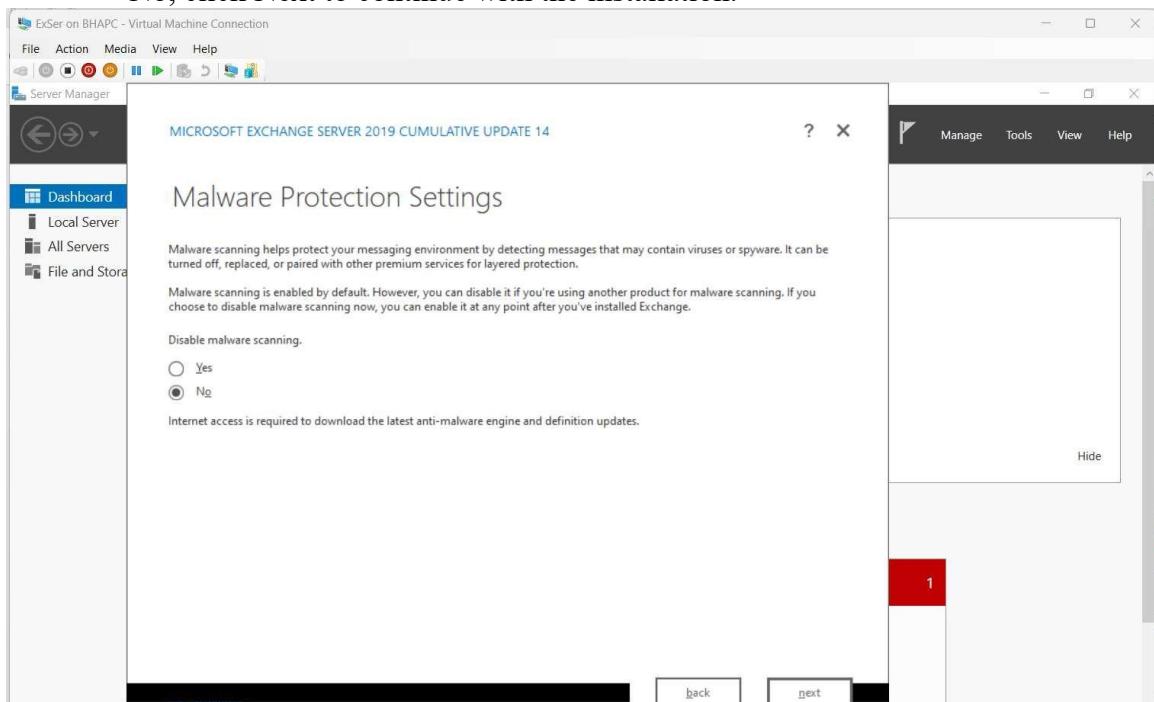
17. Browse the Location and Click Ok.



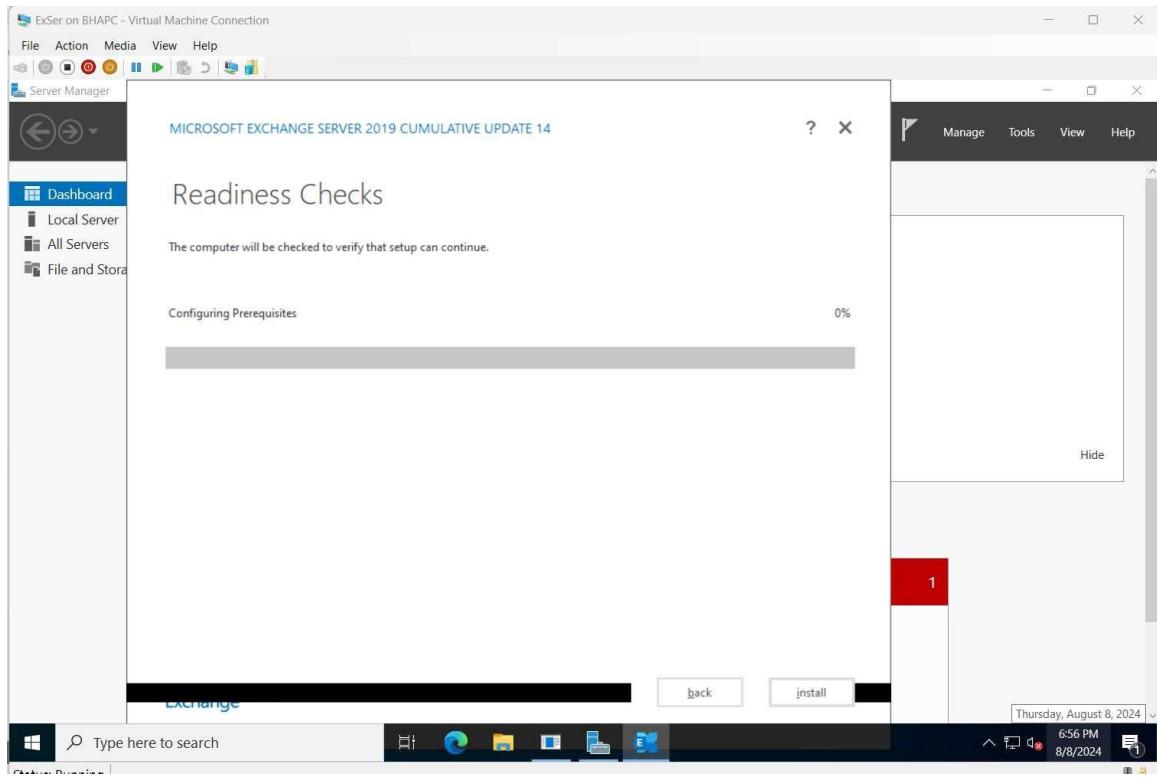
- 18.** When prompted during setup, enter the Exchange Organization name. For example, you can type ABC. This name identifies your Exchange environment and groups all Exchange servers and mailboxes under a single administrative organization. Important: This is not the same as your Active Directory domain name (e.g., abc.local). You can choose a name like your domain for consistency, but it is primarily used by Exchange internally for management purposes.



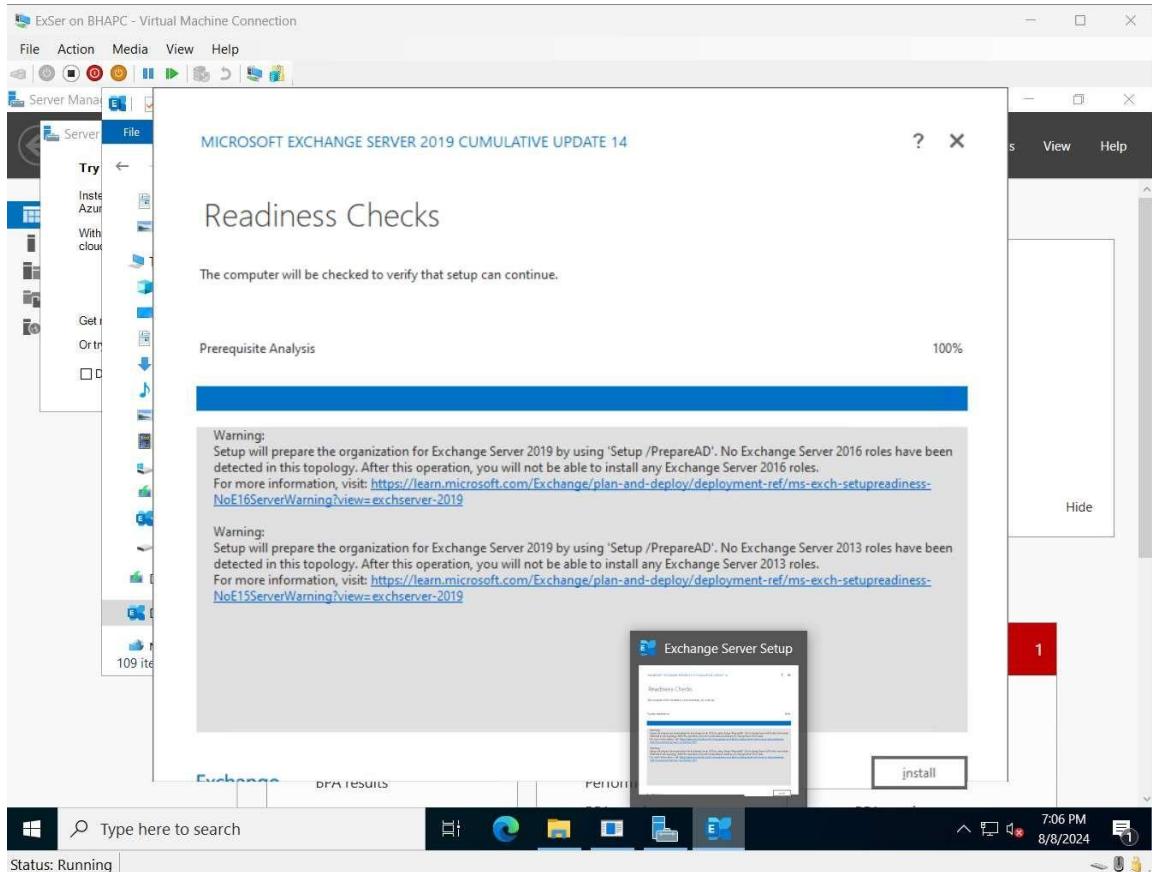
- 19.** When prompted about Malware Scanning, always select No. You want Exchange Server to be able to scan all incoming and outgoing emails for malware, so disabling this feature could leave your organization vulnerable. After selecting No, click Next to continue with the installation.



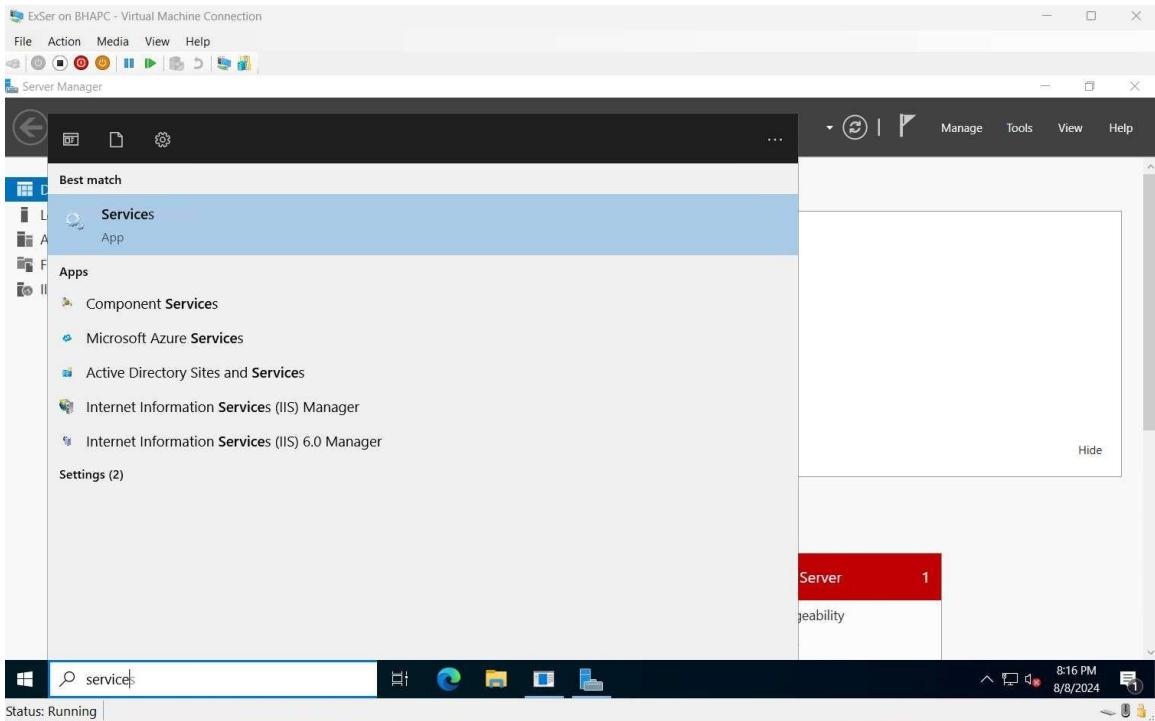
20. It will check for Pre-Requisites.



21. After clicking Install, the setup will begin installing Exchange Server. This process may take some time, so be patient. If the installation completes without any errors, you can proceed to the next steps. However, if any errors appear, carefully review the installation documentation, as it usually indicates that a prerequisite or configuration step was missed. Once the installation finishes, do not forget to reboot the server to ensure all Exchange services and settings are applied correctly before moving on to service verification.



22. After the installation, verify that all Exchange services are running properly. Open Services and check that all Microsoft Exchange Mailbox services set to Automatic are running. If any service is not running, right-click it and select Start. Even if the services appear to be running but you are unable to access mailboxes, try stopping and restarting the services. This can resolve any startup issues and ensure that all Exchange components are functioning correctly.



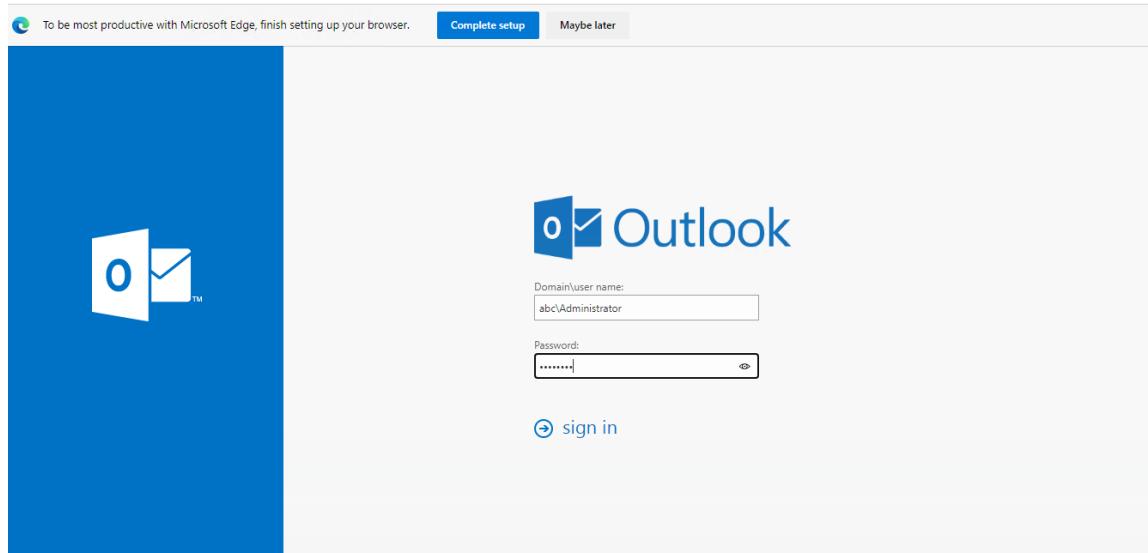
The screenshot shows the "Services (Local)" management interface in the Server Manager. The left sidebar has "Dashboard" selected. In the center pane, under "Microsoft Exchange Active Directory Topology", there are links to "Stop the service" and "Restart the service". A detailed description follows: "Provides Active Directory topology information to Exchange services. If this service is stopped, most Exchange services are unable to start." Below this, a table lists numerous Microsoft Exchange services, all of which are currently running. The columns in the table are Name, Description, Status, Startup Type, and Log On As. The "Name" column lists items such as Microsoft Account Sign-in A..., Microsoft App-V Client, Microsoft Defender Antivirus, Microsoft Defender Antivirus, Microsoft Edge Elevation Se..., Microsoft Edge Update Serv..., Microsoft Edge Update Serv..., Microsoft Exchange Active D..., Microsoft Exchange Anti-sp..., Microsoft Exchange Complia..., Microsoft Exchange Complia..., Microsoft Exchange DAG Ma..., Microsoft Exchange Diagnos..., Microsoft Exchange EdgeSync, Microsoft Exchange Emergen..., Microsoft Exchange Fronten..., Microsoft Exchange Health..., Microsoft Exchange Health..., Microsoft Exchange IMAP4, Microsoft Exchange IMAP4 B..., Microsoft Exchange Informa..., Microsoft Exchange Mailbox..., and Microsoft Exchange Mailbox... . The "Status" column shows "Running" for all services. The "Startup Type" column includes "Manual (Trigg...", "Disabled", "Running", "Automatic", and "Automatic (De...". The "Log On As" column shows "Local System" for most services, with a few exceptions like "Network Se...".

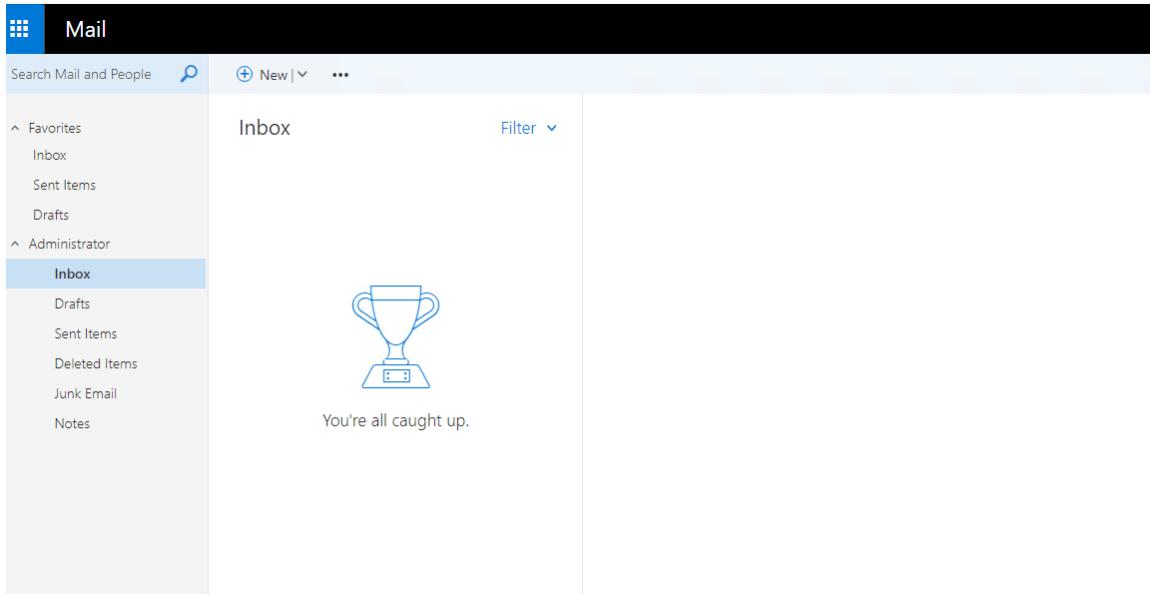
23. Open a web browser on the server and type:

- <https://localhost/ecp>: This opens the Exchange Control Panel (ECP), which is used for administrative tasks.
- If ECP does not work, try <https://localhost/owa>: This opens Outlook Web Access (OWA), which allows email users, including Exchange admins, to access their mailboxes via the web.

Log in using your Exchange or Domain Administrator credentials. This step verifies that the Exchange Server is accessible and that both administrative and user web access are functioning correctly.

24. After the server reboots and all Exchange services are running, you should now be able to access the mailboxes. If you are still unable to access them, it usually means that one or more steps were missed during the setup. In that case, carefully review the entire installation guide again, ensuring that all prerequisites, configurations, and installation steps were completed correctly.





The screenshot shows the Exchange admin center interface. The left sidebar includes links for recipients, permissions (which is selected), compliance management, organization, protection, mail flow, mobile, public folders, servers, and hybrid. The main content area shows the 'admin roles' section with tabs for 'admin roles', 'user roles', and 'Outlook Web App policies'. A 'Compliance Management' role group is selected. The details pane on the right provides a description: 'This role group will allow a specified user, responsible for compliance, to properly configure and manage compliance settings within Exchange in accordance with their policy.' It lists 'Assigned Roles' including Audit Logs, Compliance Admin, Data Loss Prevention, Information Rights Management, Journaling, Message Tracking, Retention Management, Transport Rules, View-Only Audit Logs, View-Only Configuration, and View-Only Organization Management. A note at the bottom states '1 selected of 14 total'.