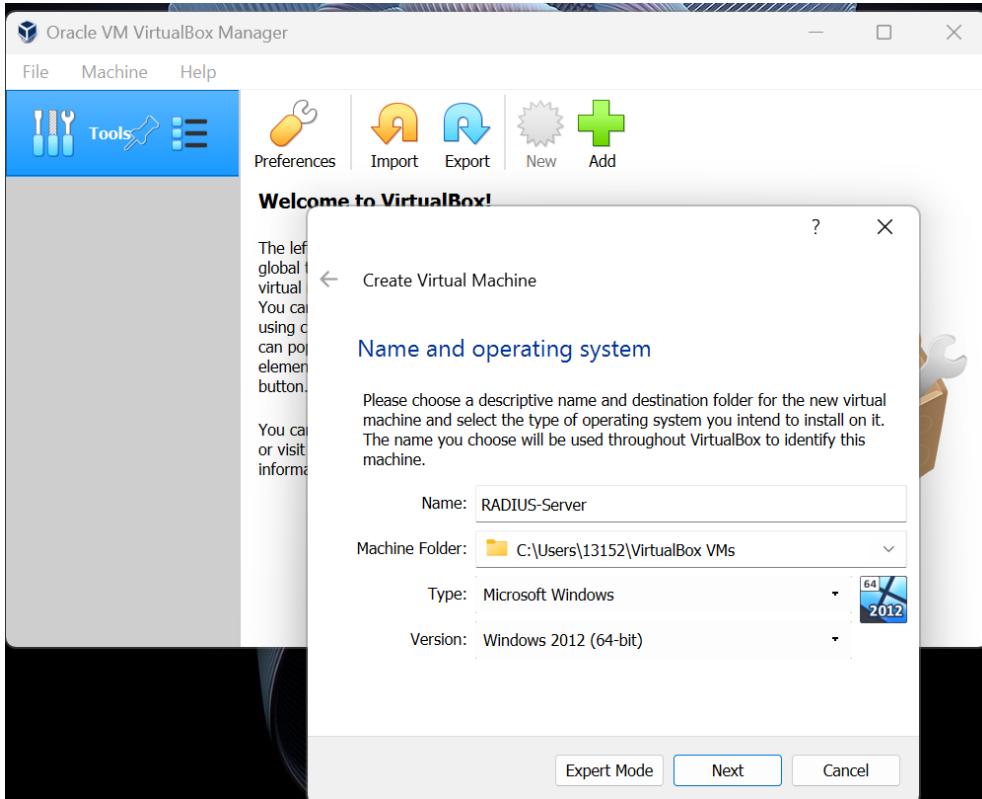


Justin Linder

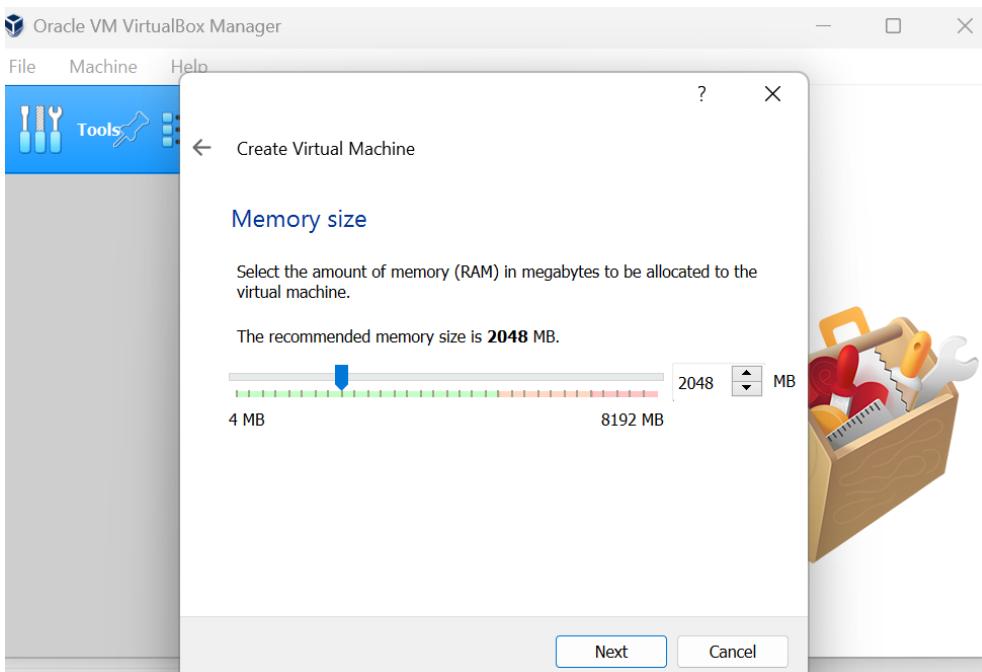
## RADIUS project

### RADIUS server on Windows Server 2012 & 2016:

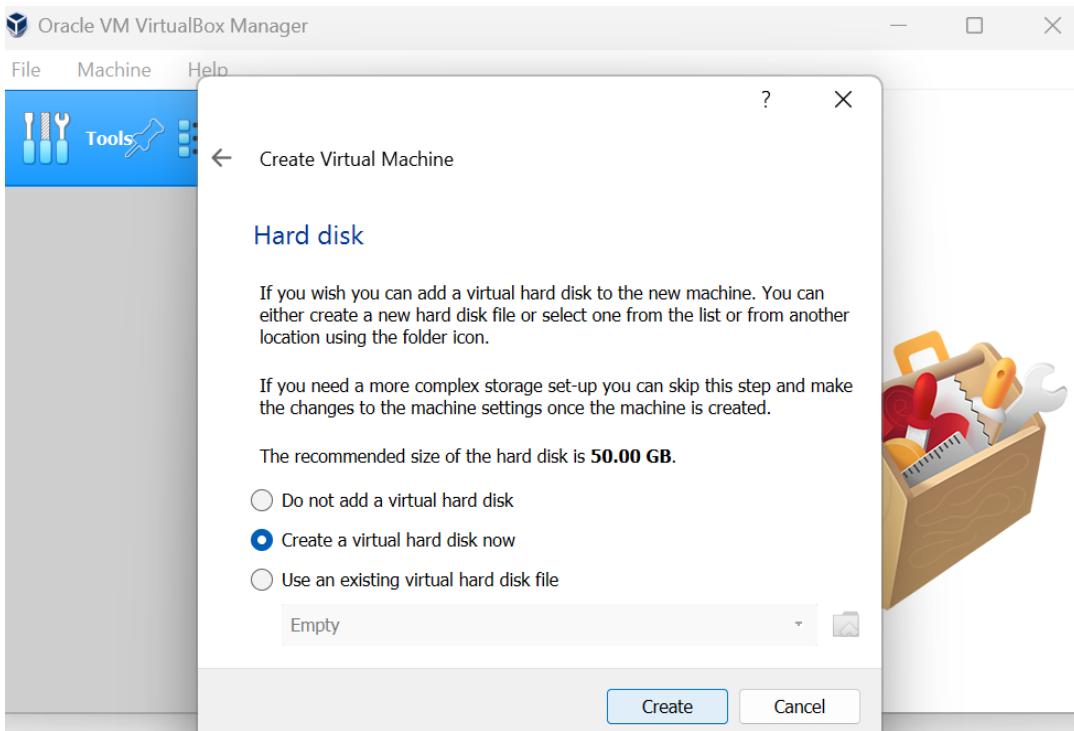
Download Oracle's VirtualBox and open after install is Finished.



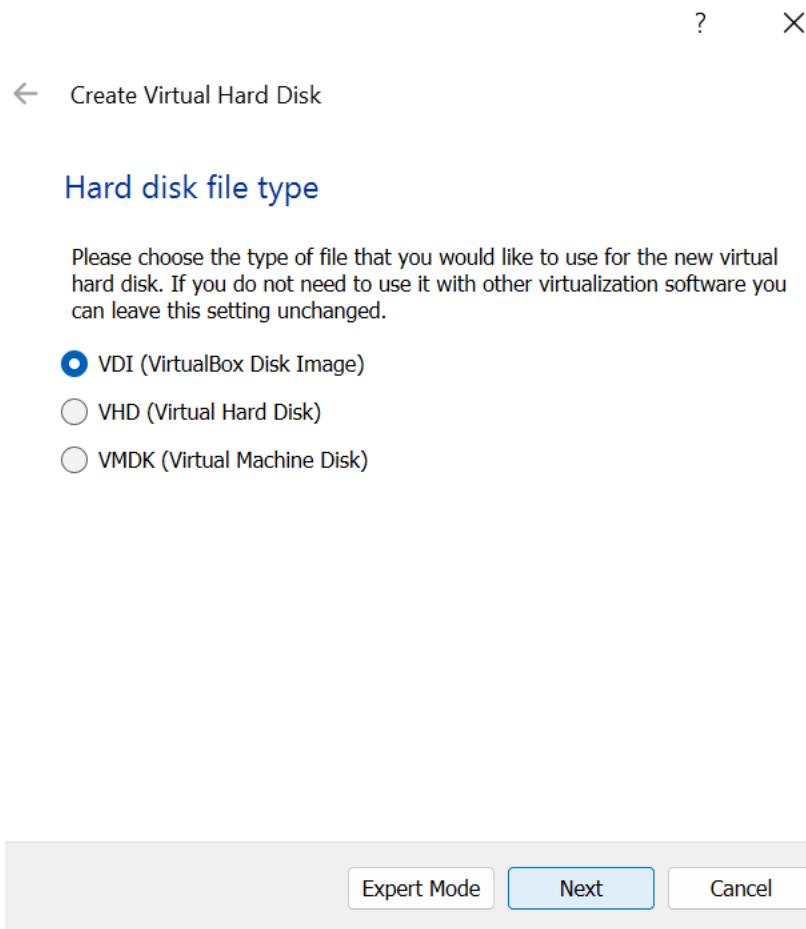
Click "New" to create a new Virtual Machine or VM, and click "Next".



Make VM at least 2048 MB of RAM memory or more, and click "Next".



Click on “Create a virtual hard disk”, and click “Next”.



Select “VDI (VirtualBox Disk Image)”, and click “Next”.



← Create Virtual Hard Disk

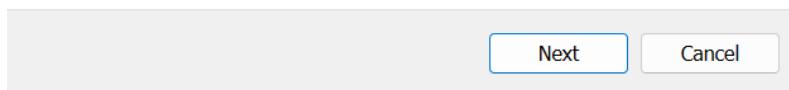
## Storage on physical hard disk

Please choose whether the new virtual hard disk file should grow as it is used (dynamically allocated) or if it should be created at its maximum size (fixed size).

A **dynamically allocated** hard disk file will only use space on your physical hard disk as it fills up (up to a maximum **fixed size**), although it will not shrink again automatically when space on it is freed.

A **fixed size** hard disk file may take longer to create on some systems but is often faster to use.

- Dynamically allocated  
 Fixed size



select "Dynamically allocated" and click "Next".



← Create Virtual Hard Disk

## File location and size

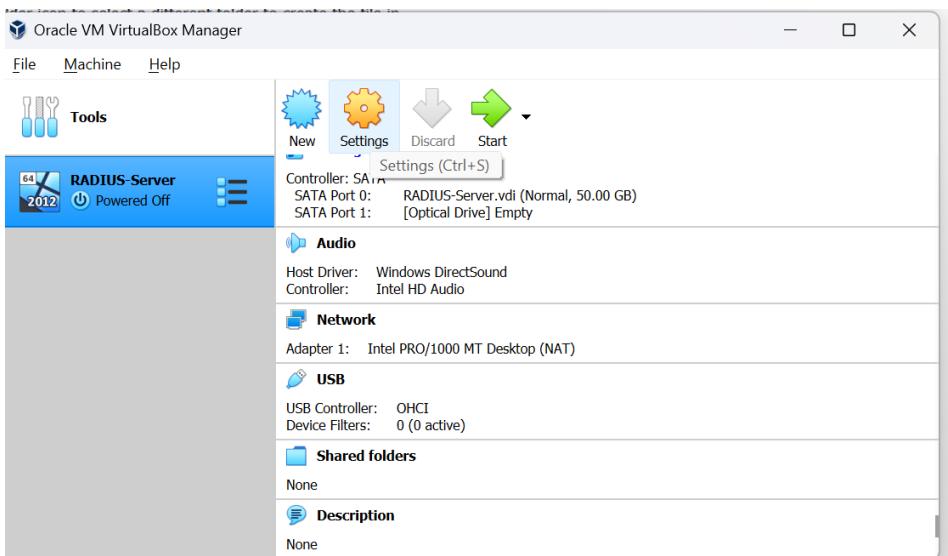
Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

C:\Users\13152\VirtualBox VMs\RADIUS-Server\RADIUS-Server.vdi

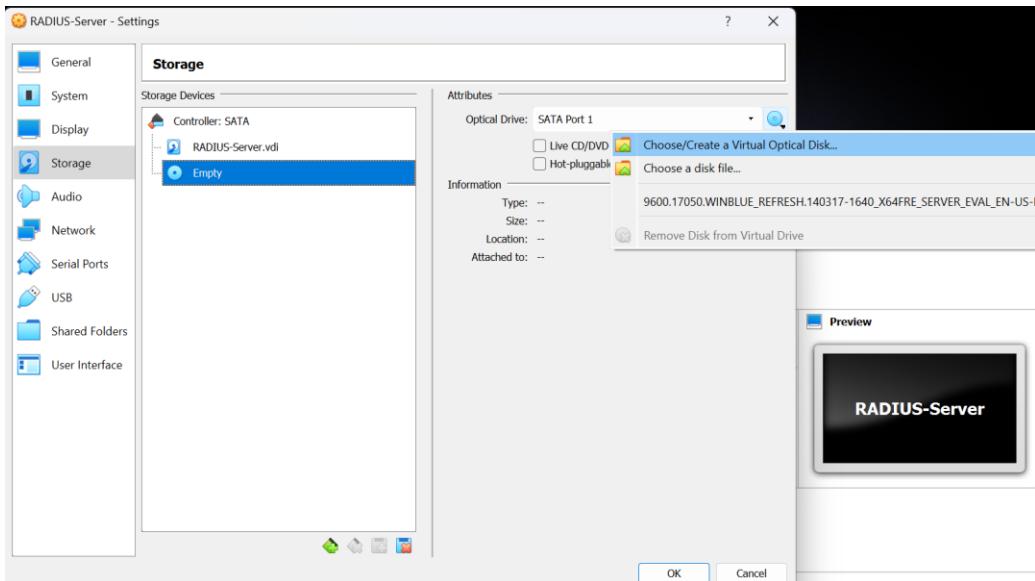
Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.



Choose file location and then make sure size it the recommended 50 GB minimum.

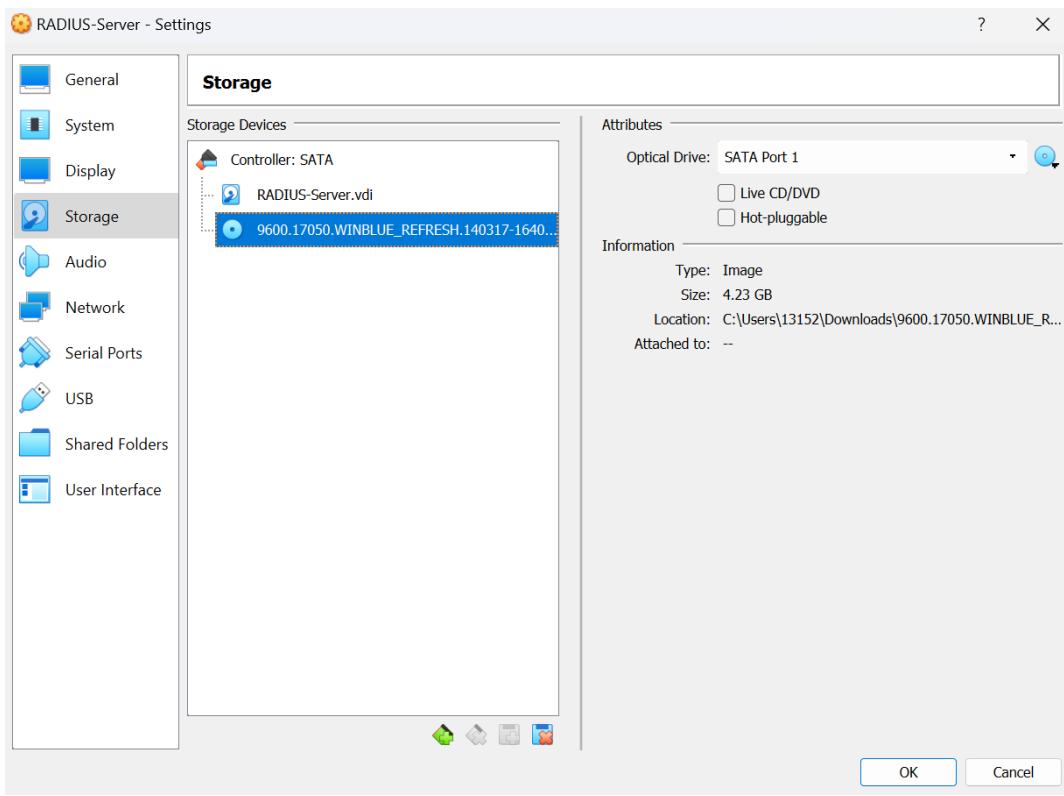


Click on “Settings” while on Windows Server VM.



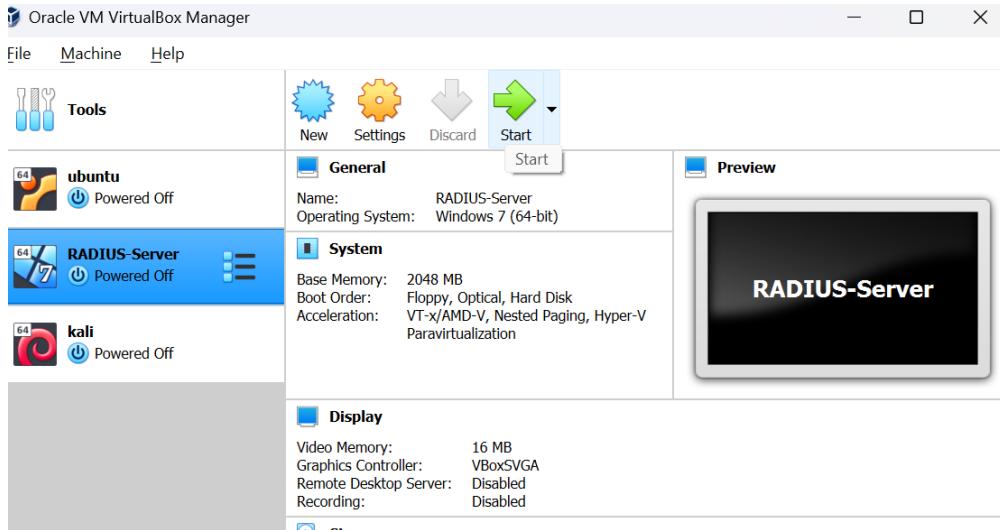
Go to “Storage” on the left side column and click under “Attributes” next to “Optical Drive”.

Select “Choose/Create a Virtual Optical Disk”.

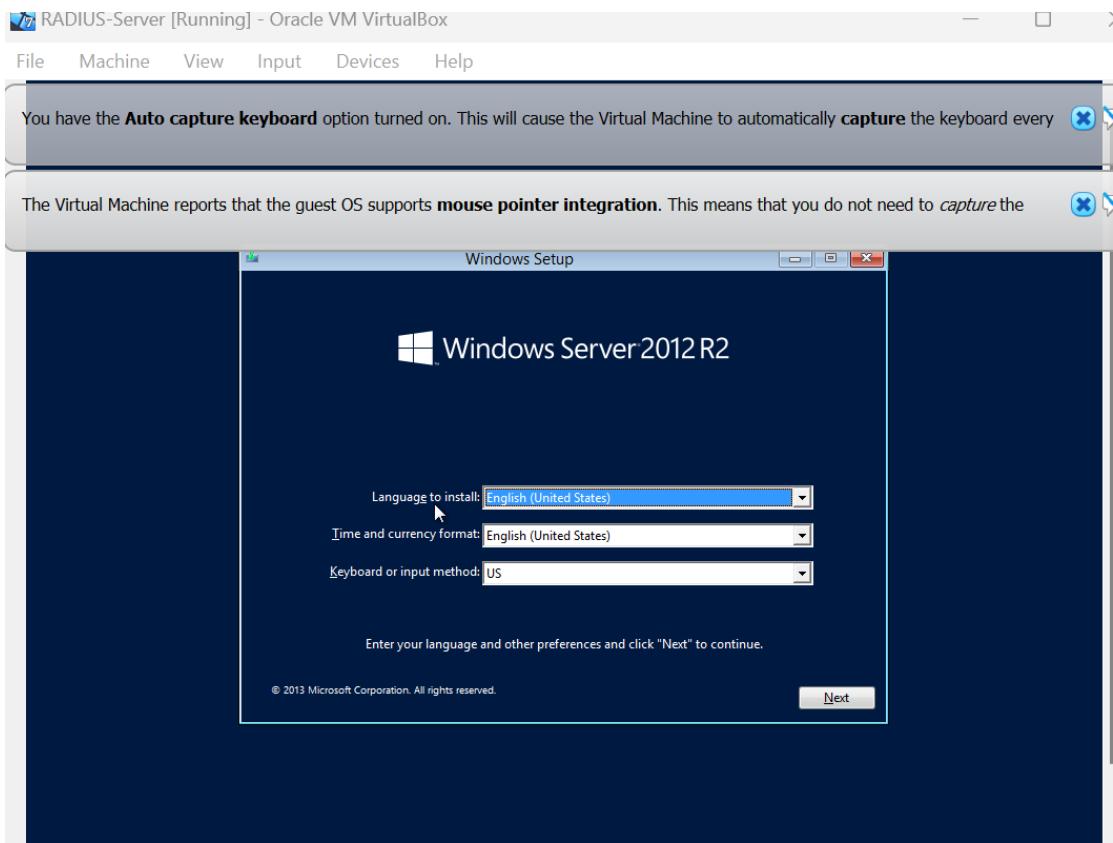


Under “Controller: SATA” is the hard drive for windows 2012 server. (that will be running RADIUS)

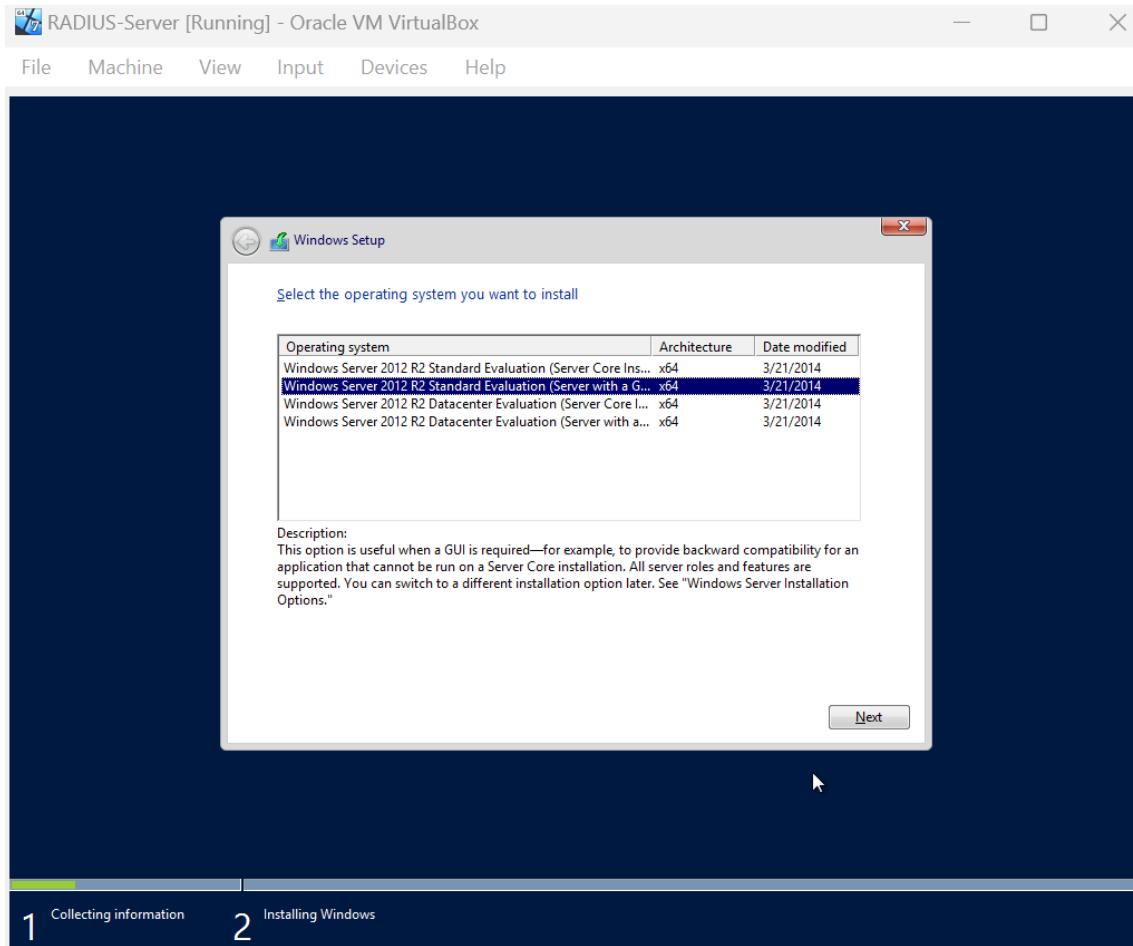
Click on “OK”.



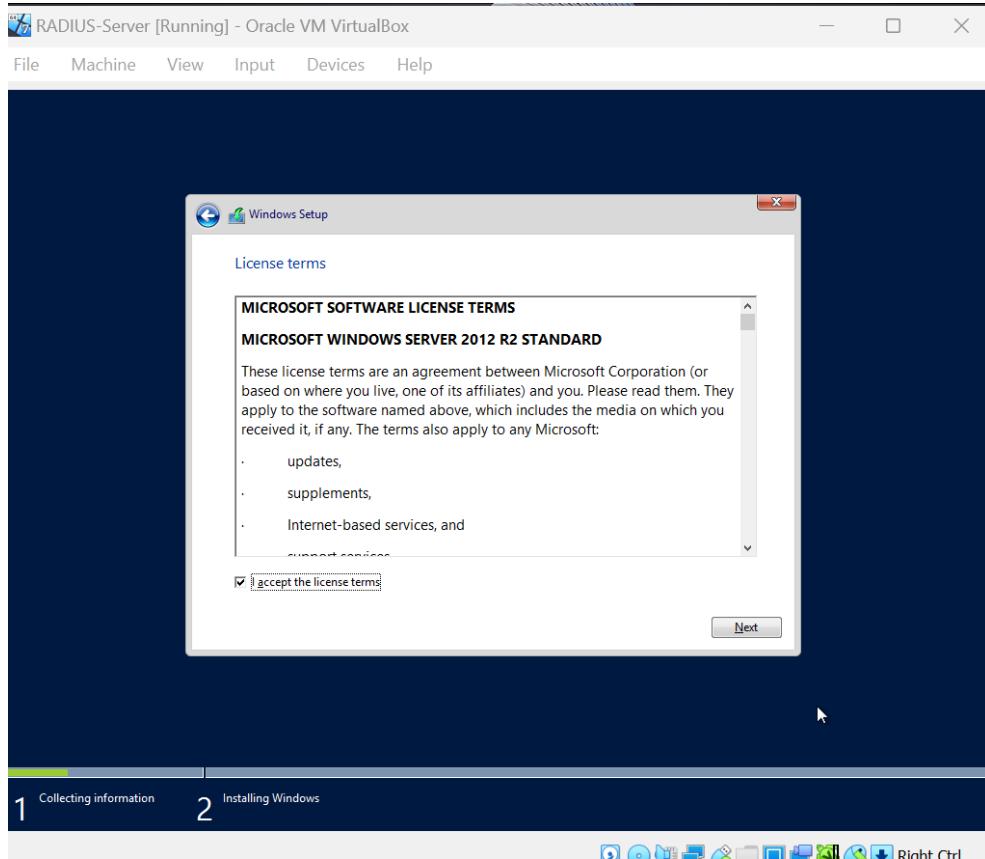
Click on “Start” which is the green right arrow.



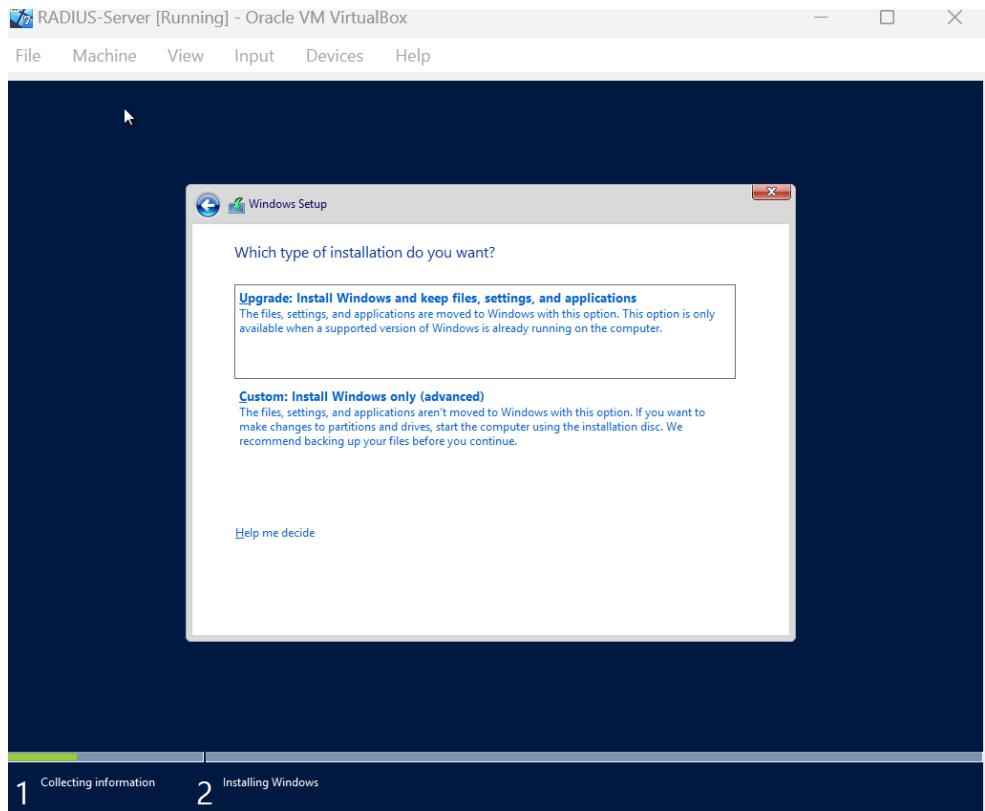
Select language and click “Next”.



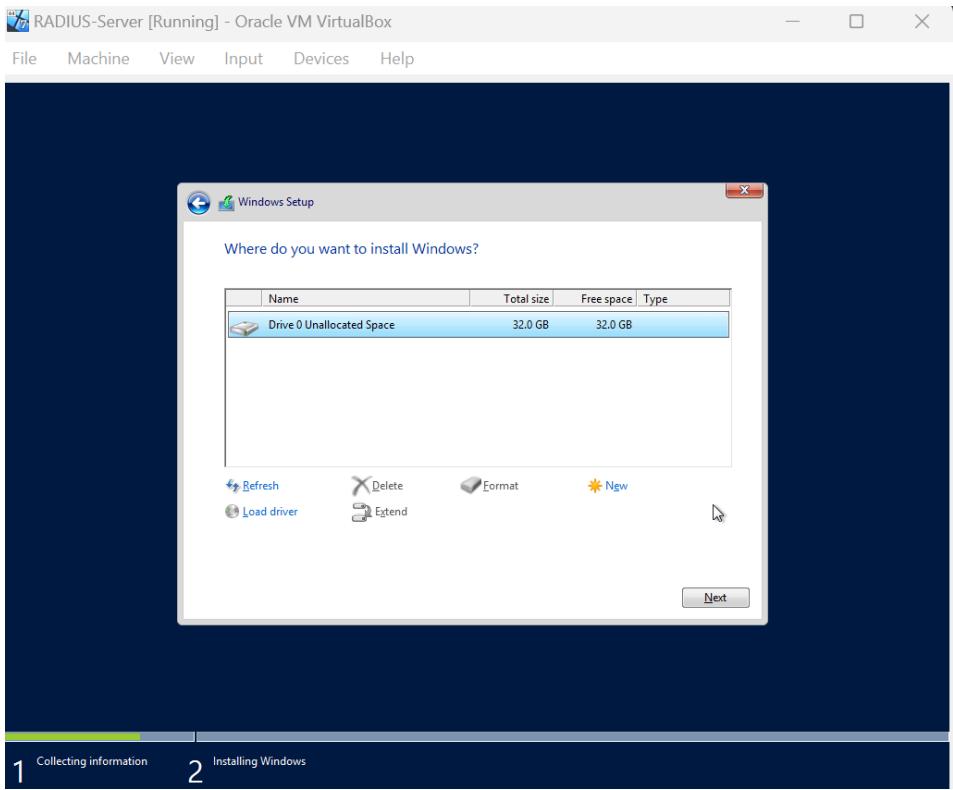
Choose the second option which is the Windows Server 2012 “with a GUI” and click “Next”.



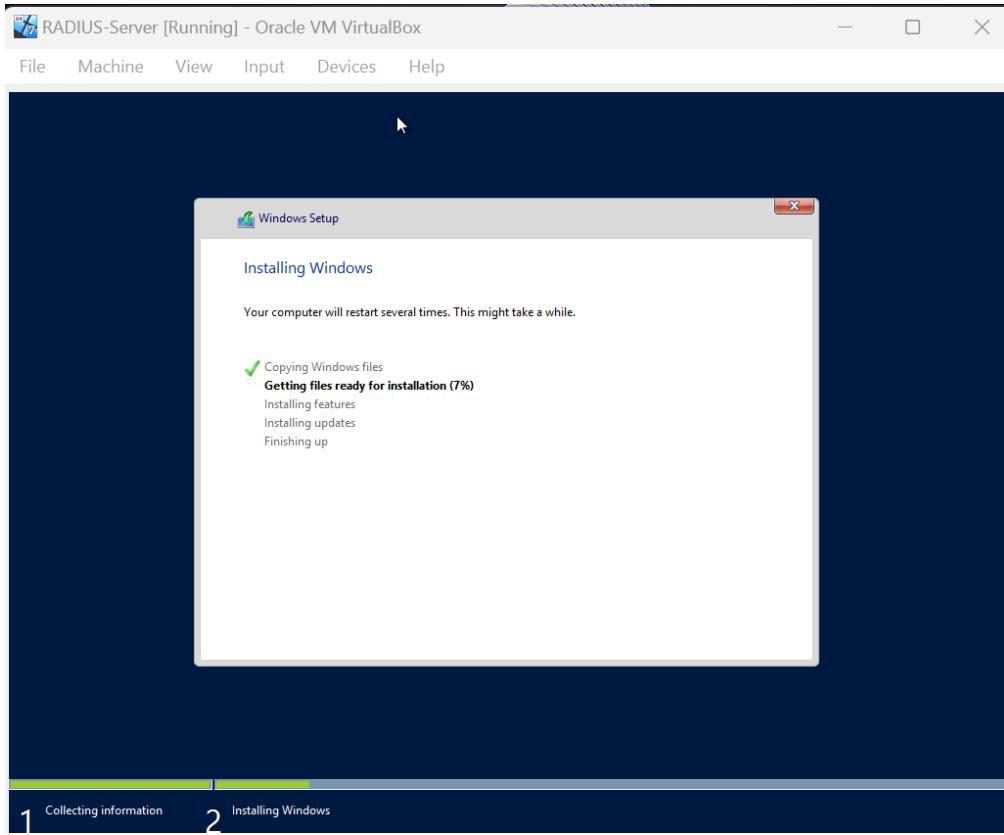
Check in “I accept the license terms” and click “Next”.

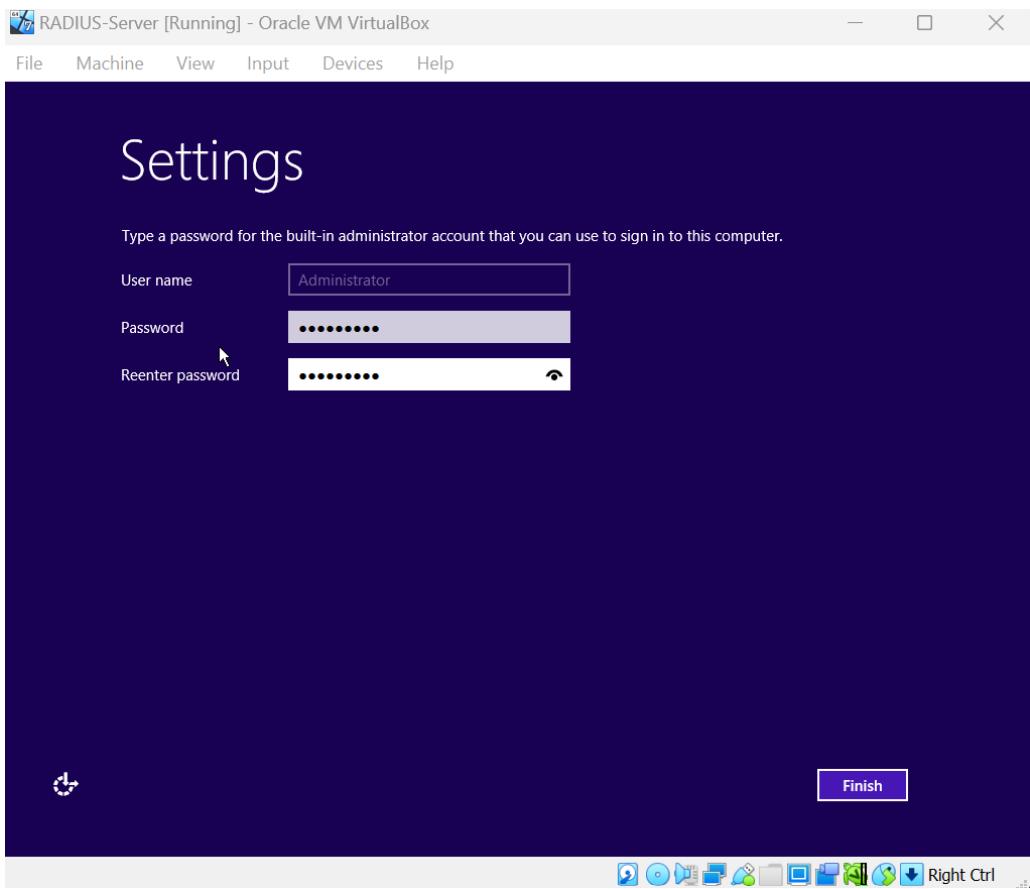


Choose/click “Upgrade Install Windows and keep files, settings, and applications”.



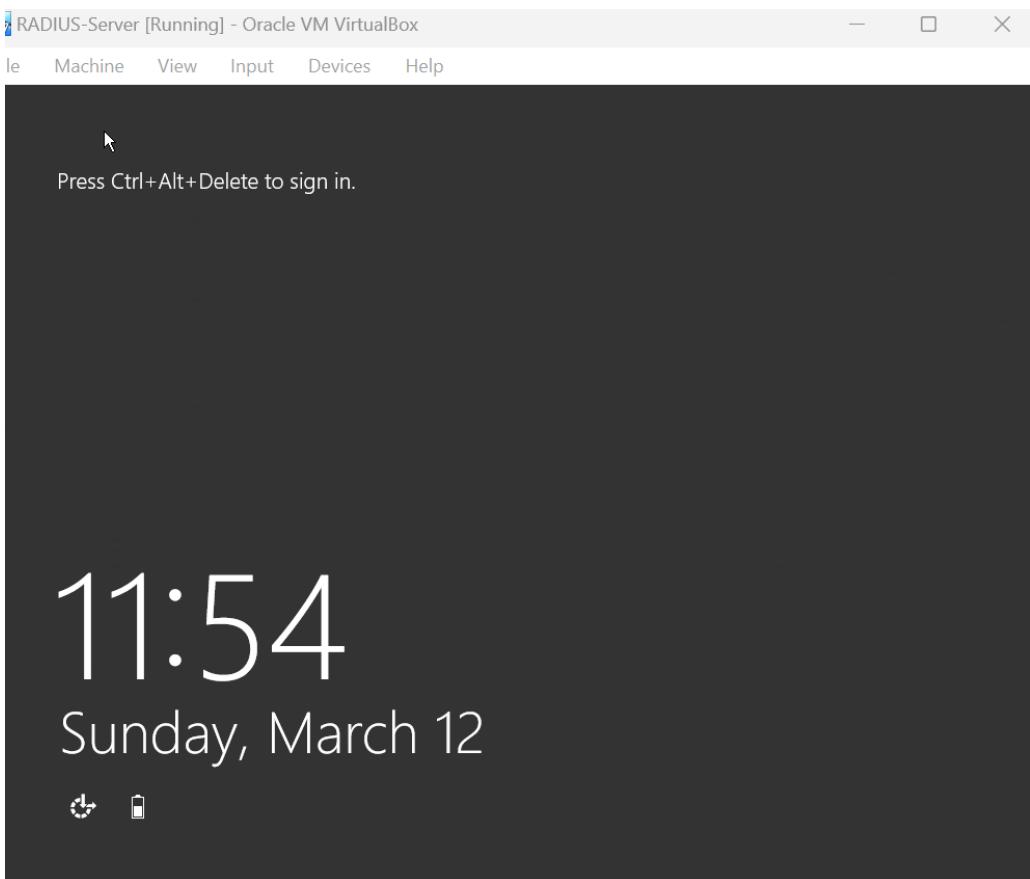
It will now automatically partition after clicking “Next”.



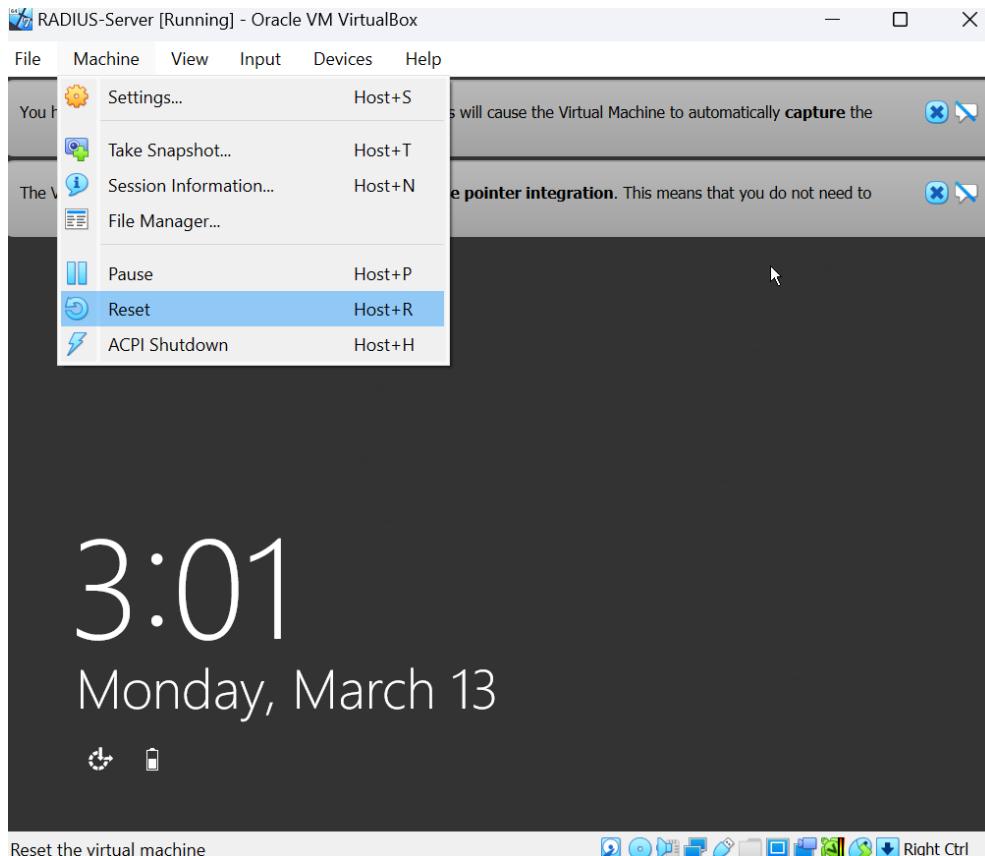


Create an admin password and click “Finish”.

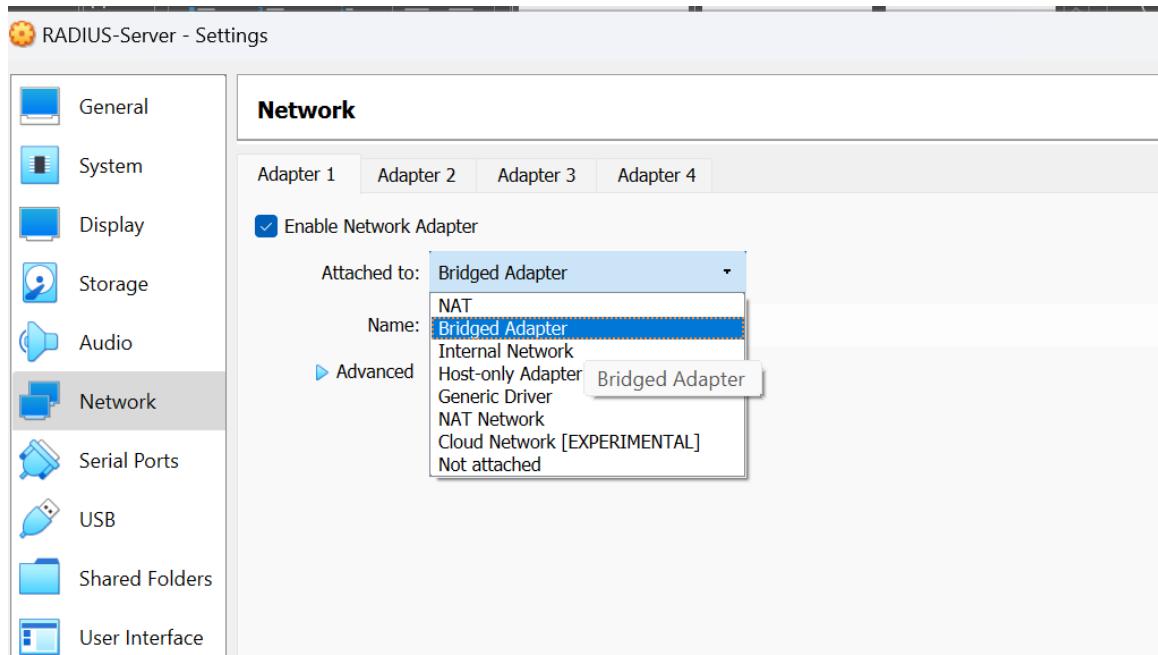
Restart VM.



Press ctrl + alt + delete buttons.

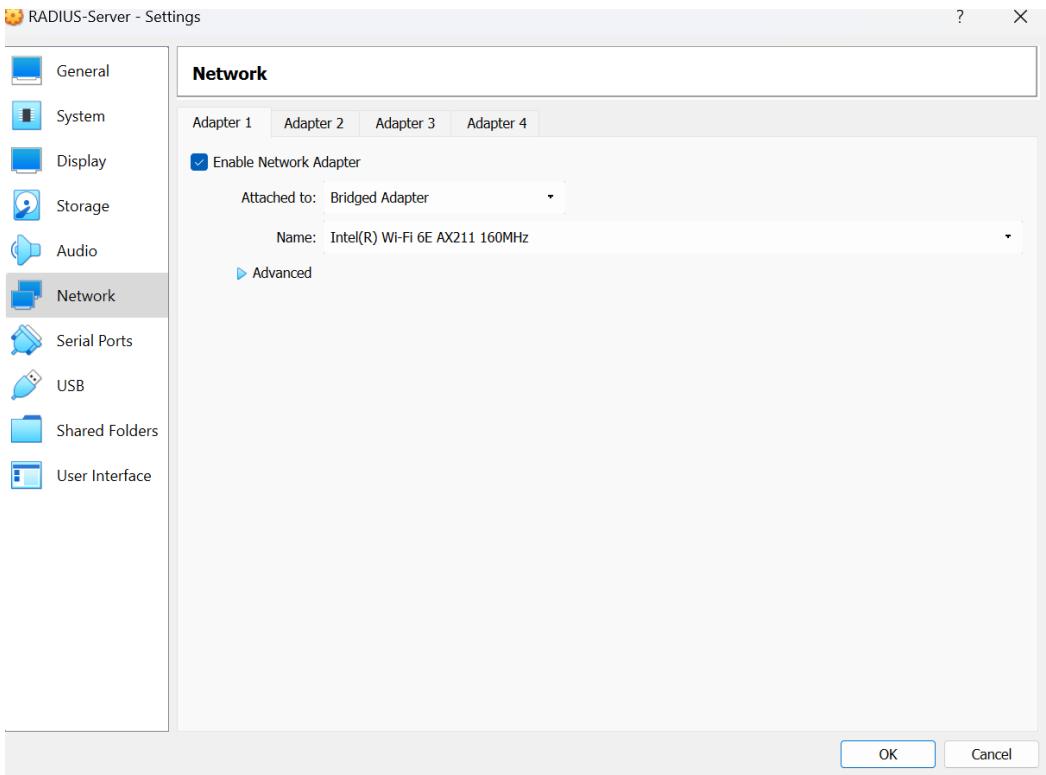


Go to “Machine” and click on “Reset”.



Click on “Settings” again and go to “Network” on left side of the column.

Click on Adapter 1 next to “Attached to” and select “Bridged Adapter”.



Click on “OK”.

A screenshot of an Oracle VM VirtualBox window titled 'RADIUS-Server [Running] - Oracle VM VirtualBox'. Inside, there is a blue-tinted 'Administrator: Windows PowerShell' window. The PowerShell session shows the following command and output:

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

Windows IP Configuration

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . . .
Link-local IPv6 Address . . . . . : fe80::c84d:d2bf:7f5c:2ba0%12
IPv4 Address . . . . . : 192.168.1.35
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

Tunnel adapter isatap.{1C8F9589-5AE9-410C-98A8-C8A71C8E896A}:

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

PS C:\Users\Administrator> S\_

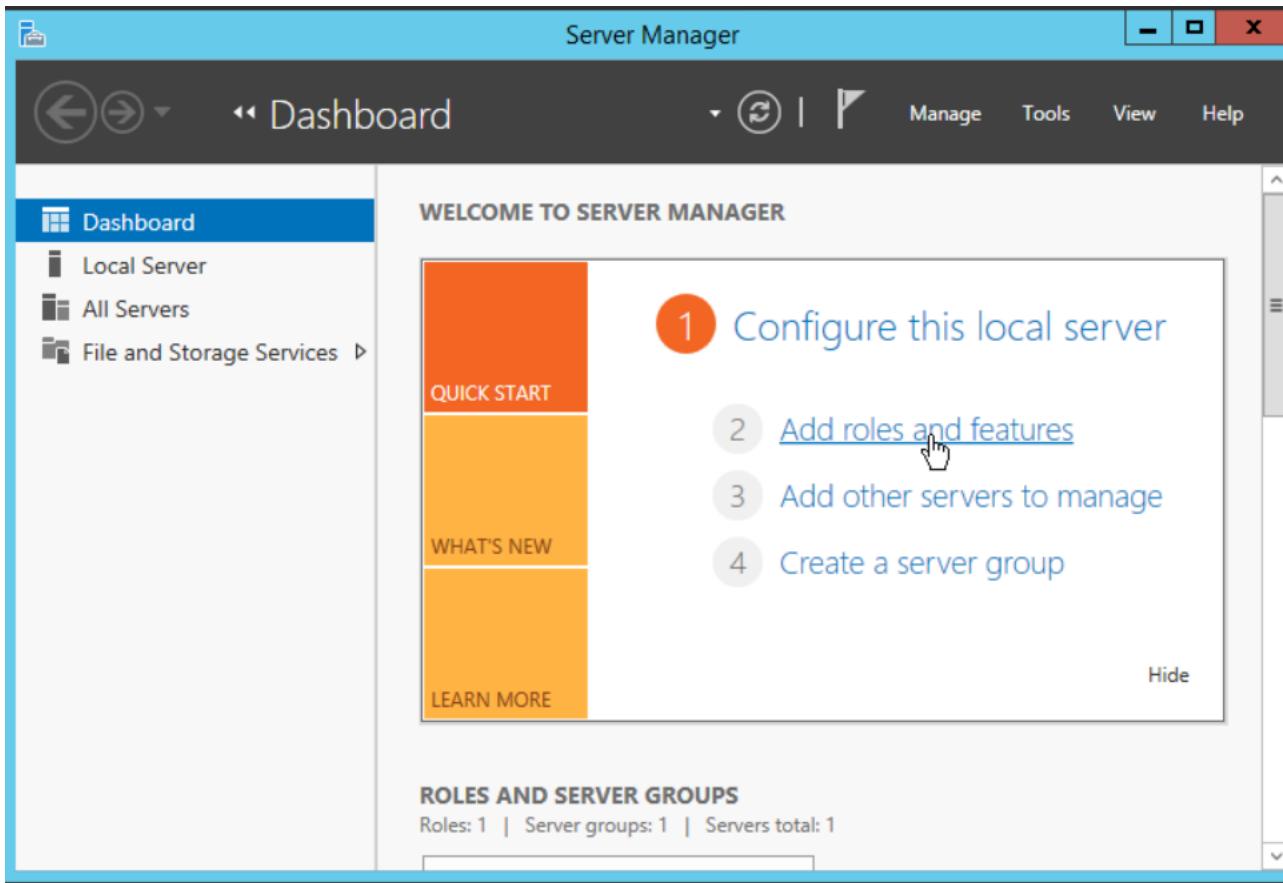
The cursor is positioned at the end of the command line.

Go to Windows PowerShell.

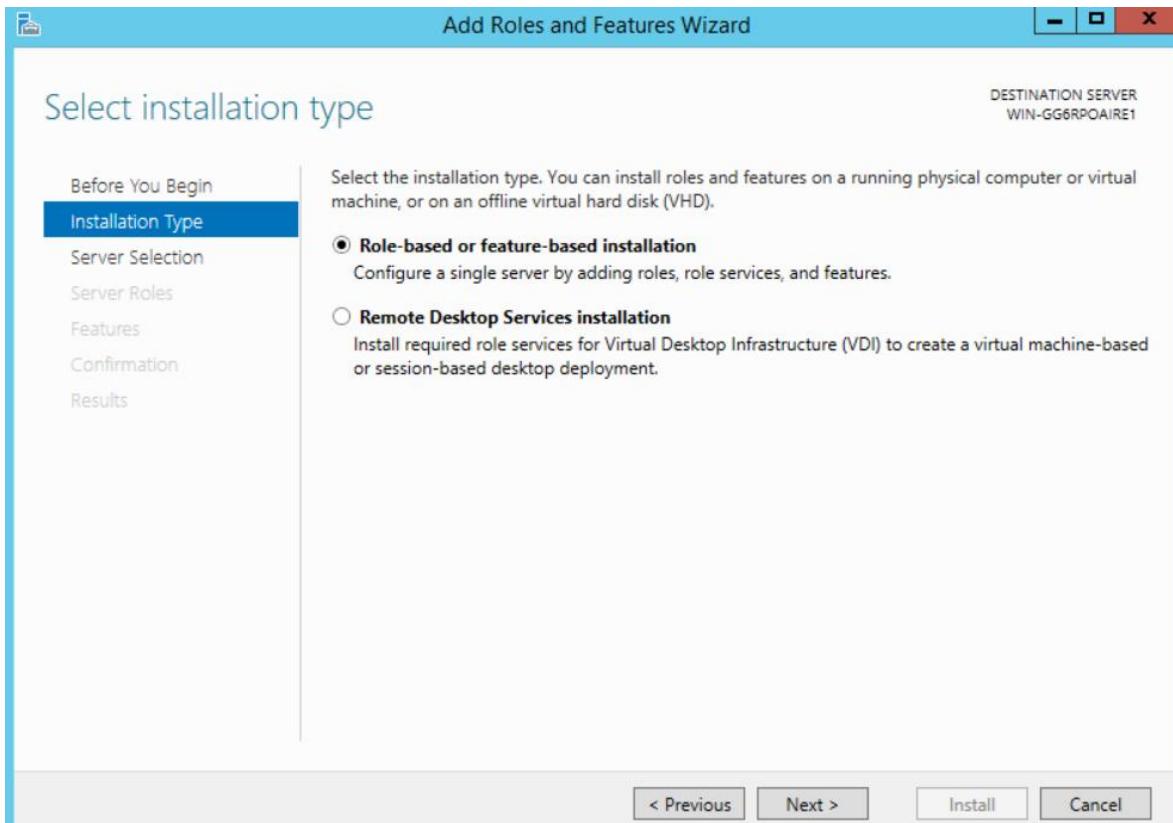
Type in “ipconfig” command.

IPV4 address for Window’s Server, Subnet Mask, and Default Gateway are shown.

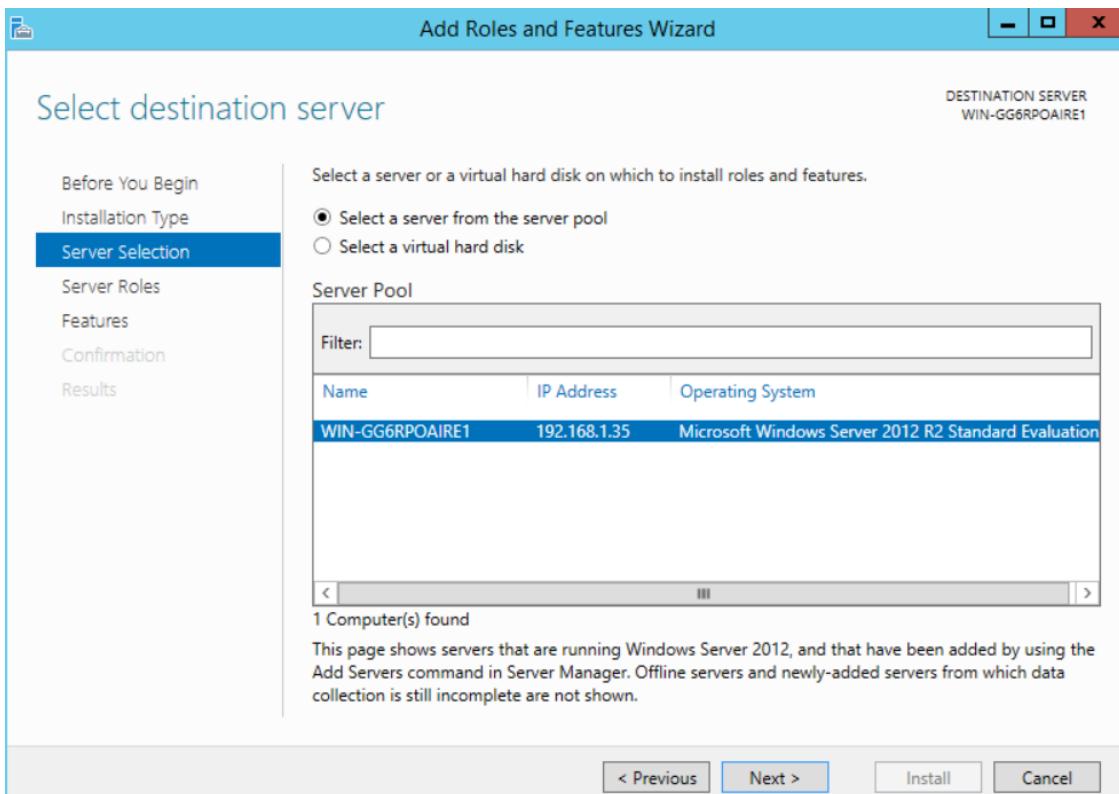
This is IP address for Windows Server through bridged adapter.



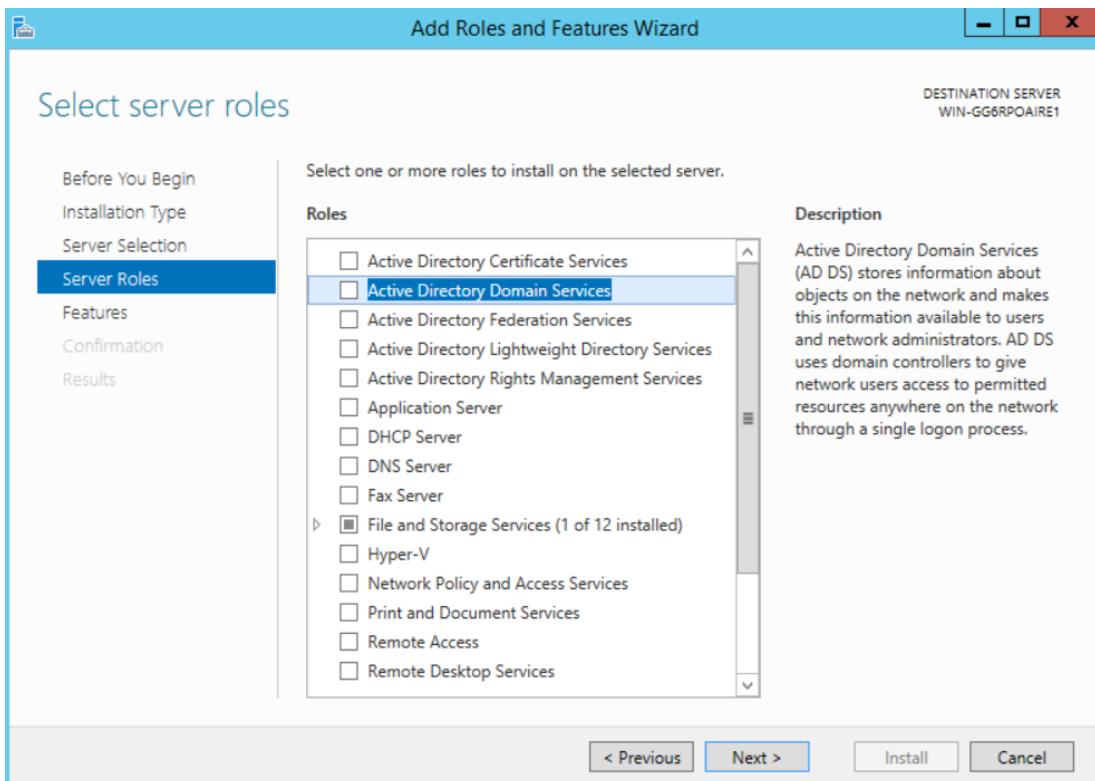
In Windows Server manager click “Add roles and features”.



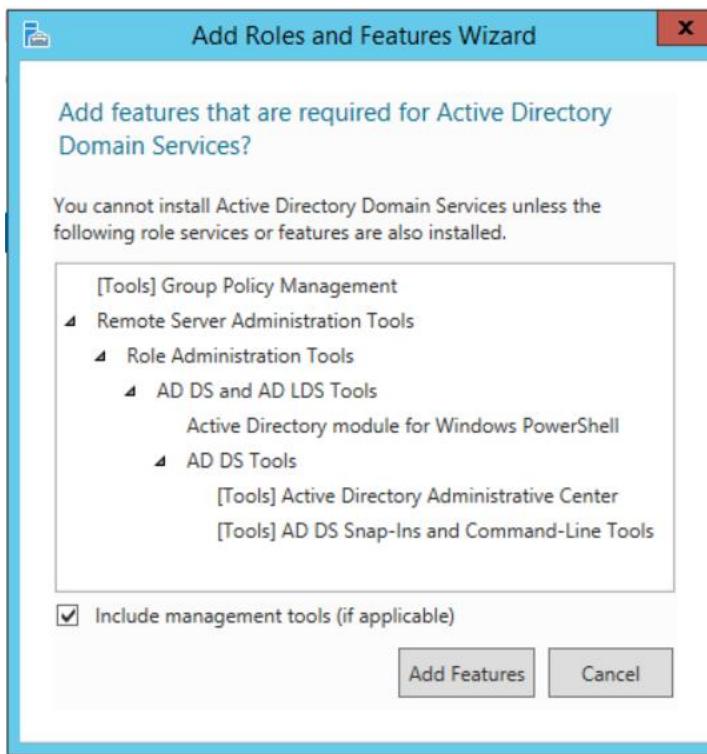
On left column select “Installation Type” and then make sure you select “Role-based or feature-based installation and click “Next”.



Choose "Select a server from the server pool" and click "Next".

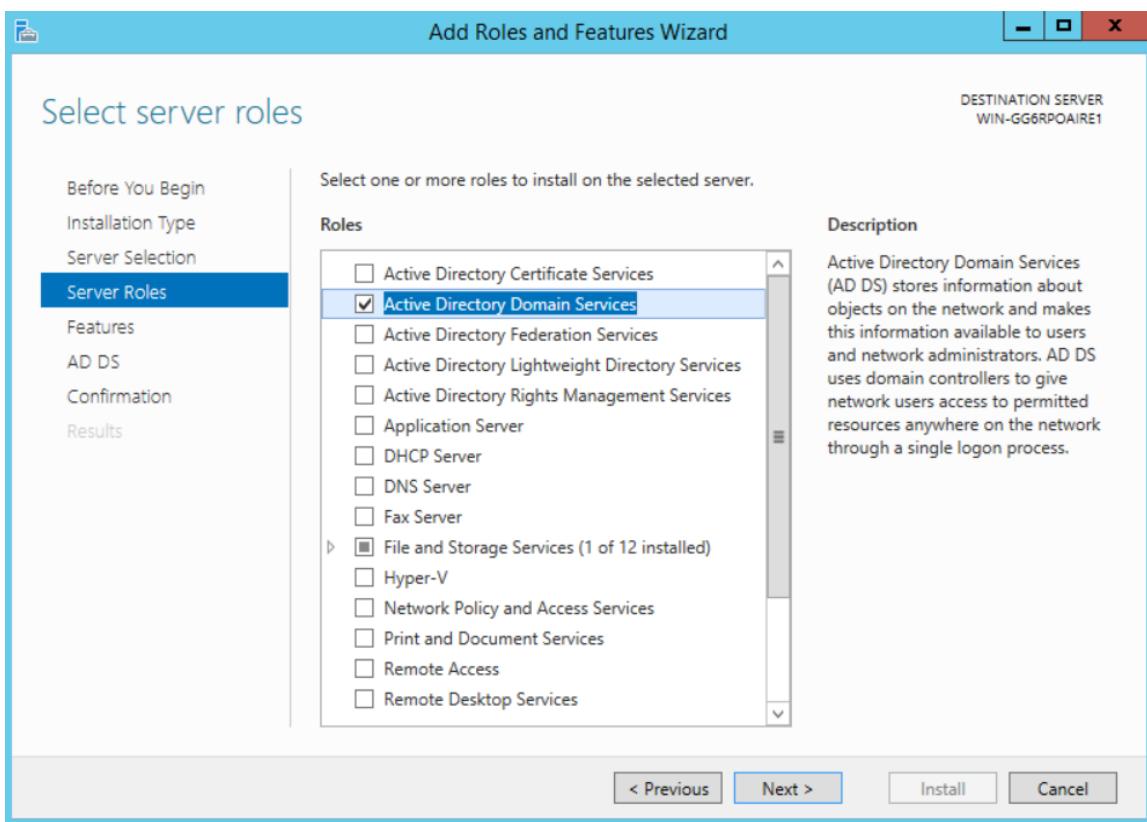


Now choose the roles "Active Directory Domain Services".

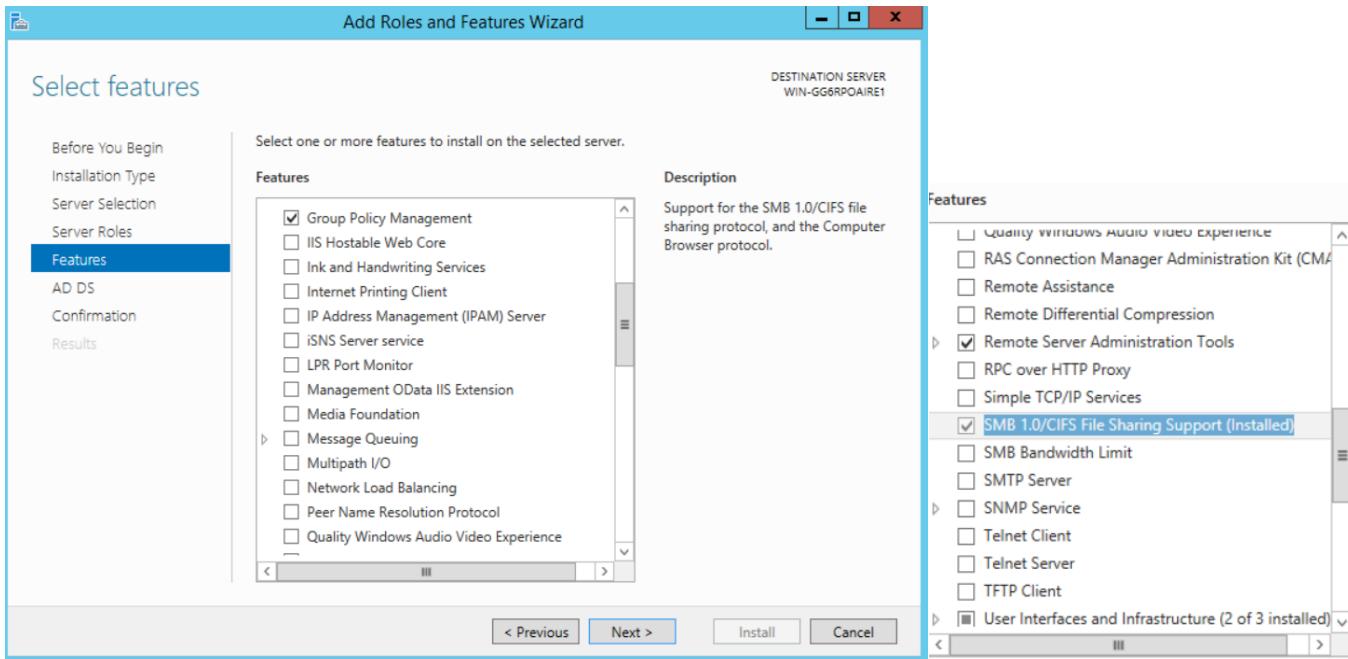


Then, a pop-up will appear so click on “Add Features” at the bottom.

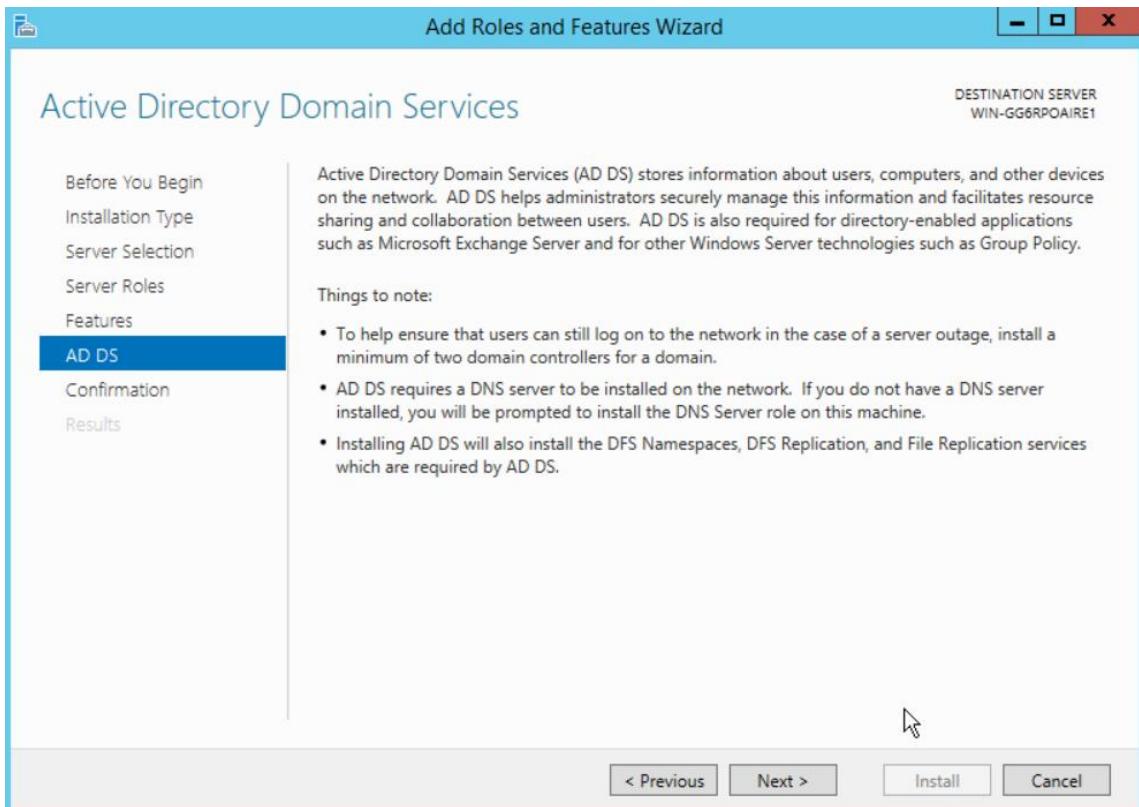
Keep “Include management tools (if applicable)” checked.



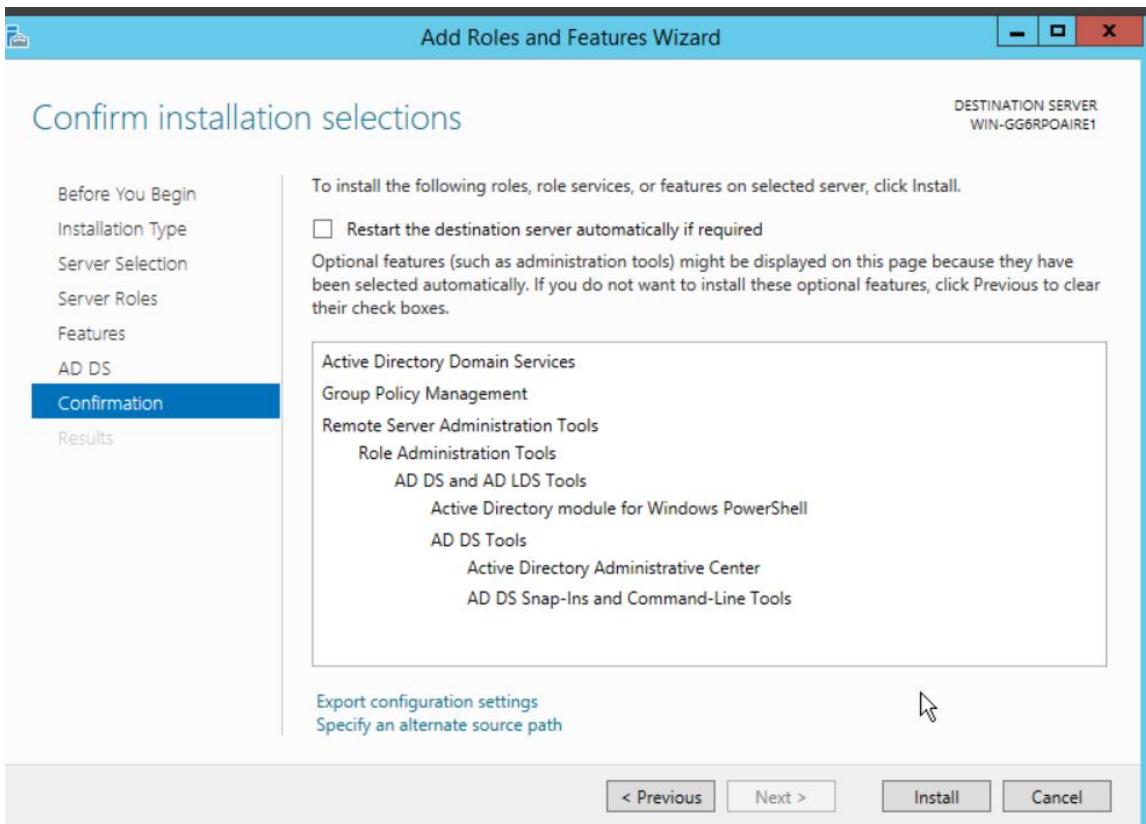
Now “Active Directory Domain Services” will be checked in, click “Next”.



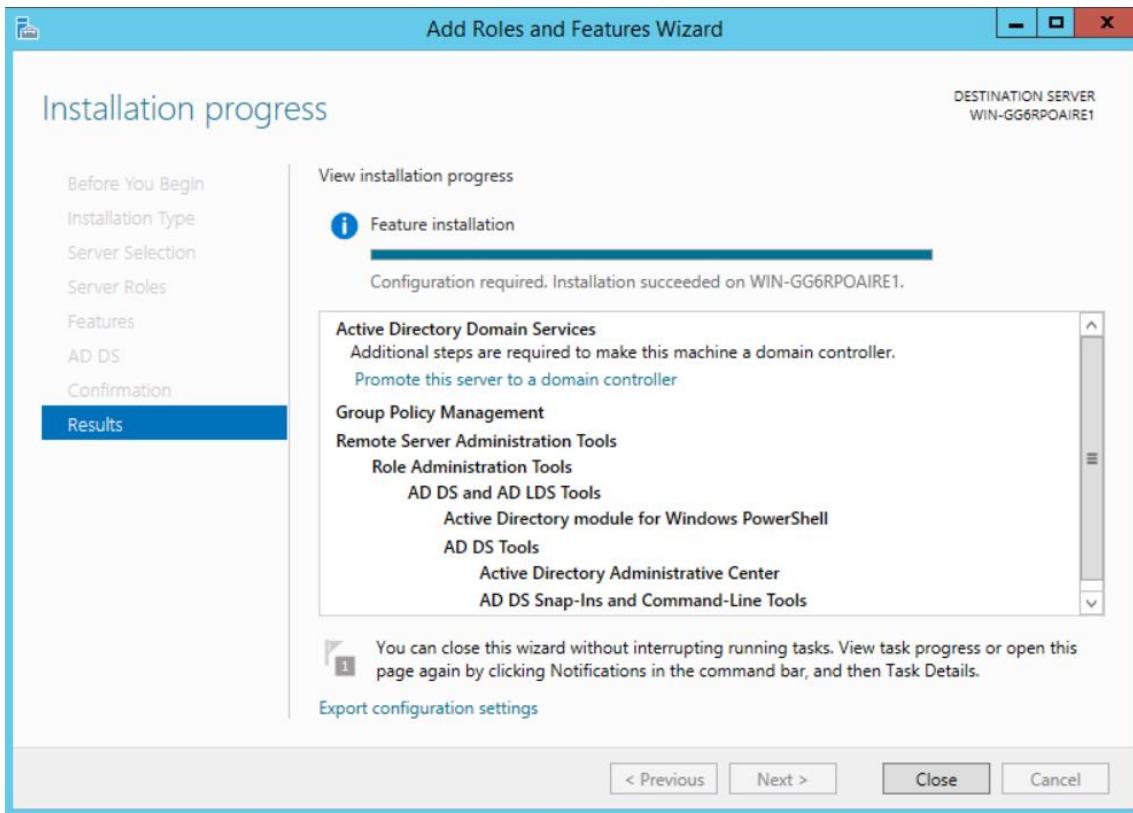
Keep “Group Policy Management” and “Remote Serve Administration Tools” checked, which should automatically be by default. Click “Next”.



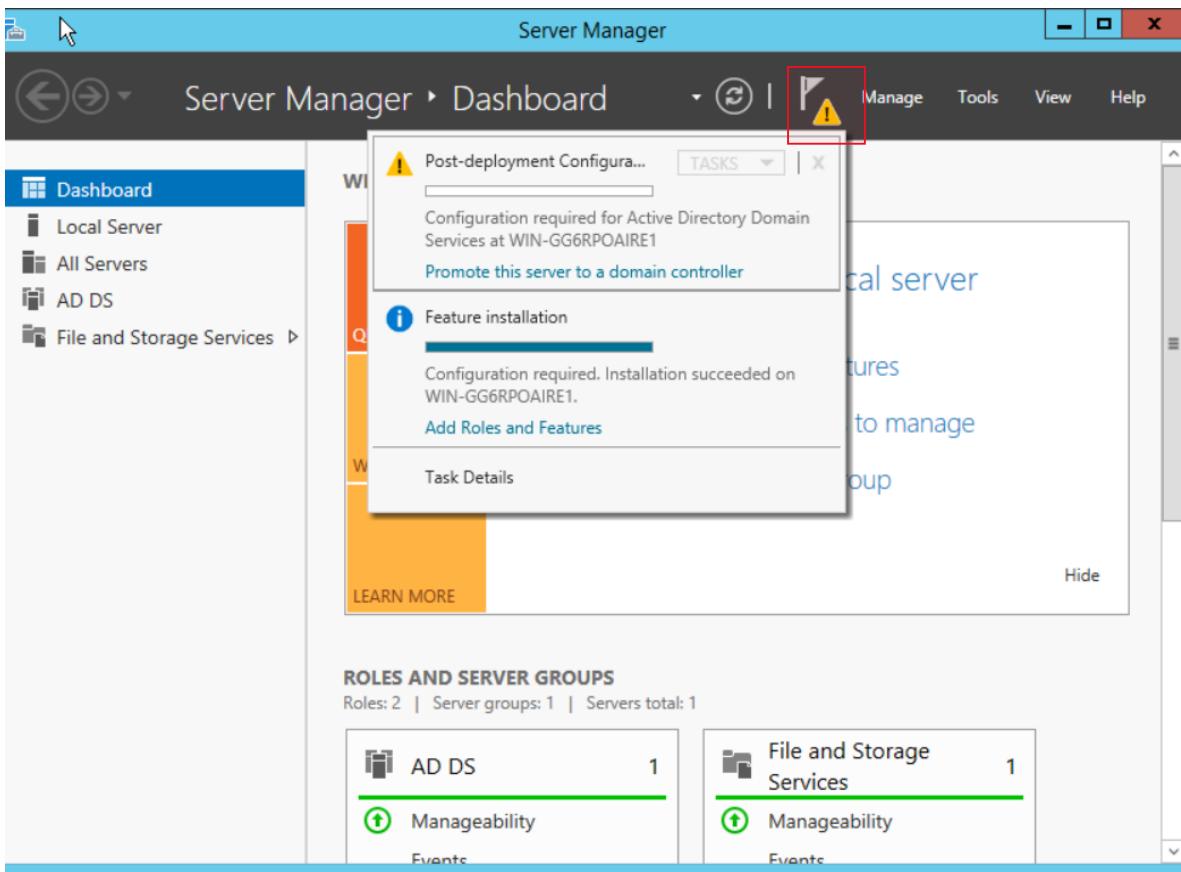
Click “Next” again.



Click "Install" to have every feature installed that was selected before.

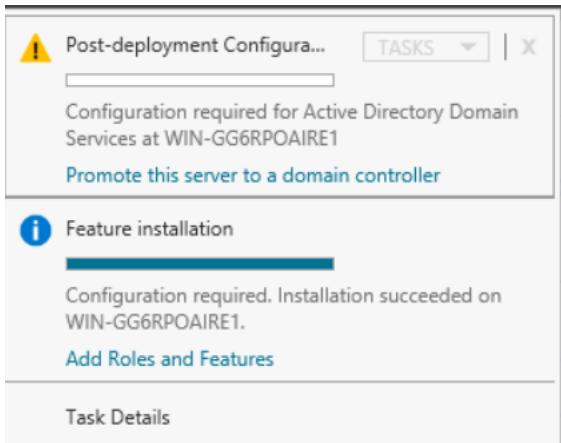


After all features were installed successfully and click "Close" so you can apply configuration as reminded above.



In the red box above there is a yellow triangle with an explanation point next to a flag. Click on that.

This is the notifications, and the “configuration required” message for AD or Active Directory is needed.



Click “Promote this server to domain controller”.

Active Directory Domain Services Configuration Wizard

TARGET SERVER  
WIN-GG6RPOAIRE1

## Deployment Configuration

Deployment Configuration

- Domain Controller Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select the deployment operation

Add a domain controller to an existing domain

Add a new domain to an existing forest

Add a new forest

Specify the domain information for this operation

Root domain name:

More about deployment configurations

< Previous Next > Install Cancel

Choose the 3<sup>rd</sup> option or “Add a new forest”.

Then, in the red box type in your “Root domain name” and click “Next”.

Active Directory Domain Services Configuration Wizard

TARGET SERVER  
WIN-GG6RPOAIRE1

## Deployment Configuration

Deployment Configuration

- Domain Controller Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select the deployment operation

Add a domain controller to an existing domain

Add a new domain to an existing forest

Add a new forest

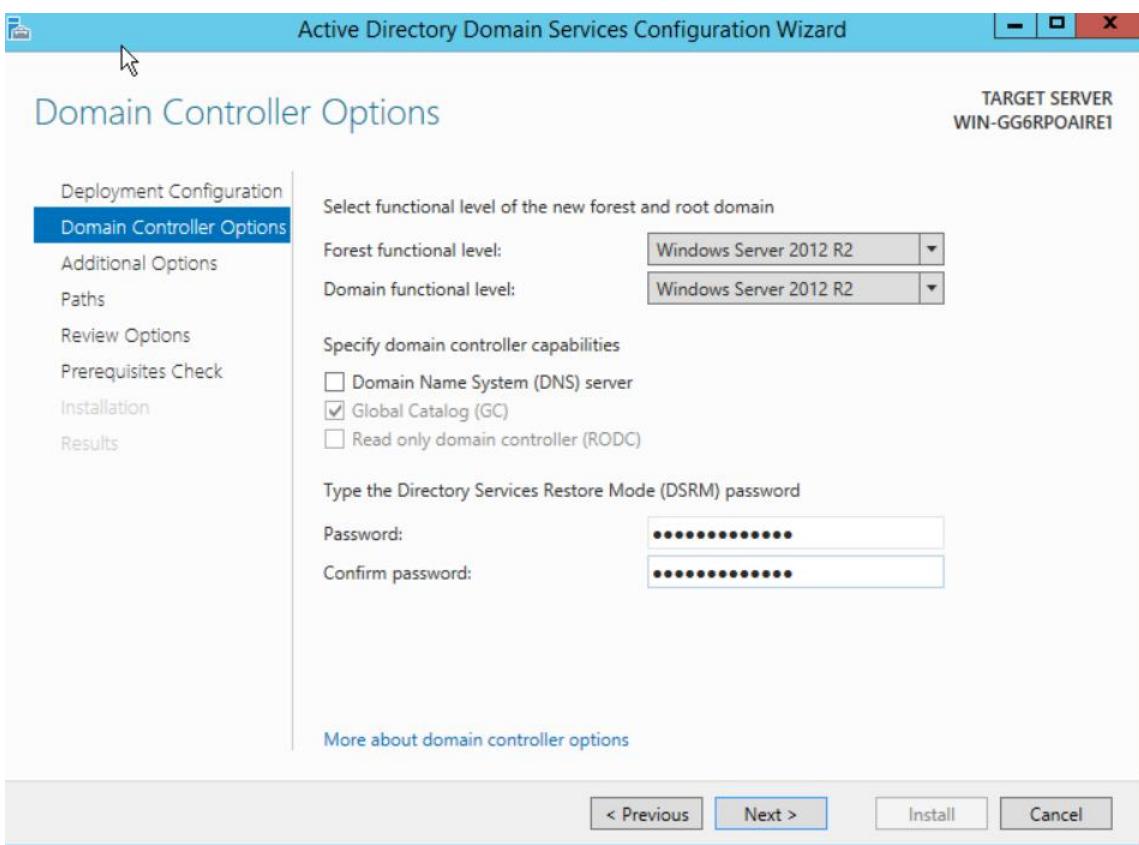
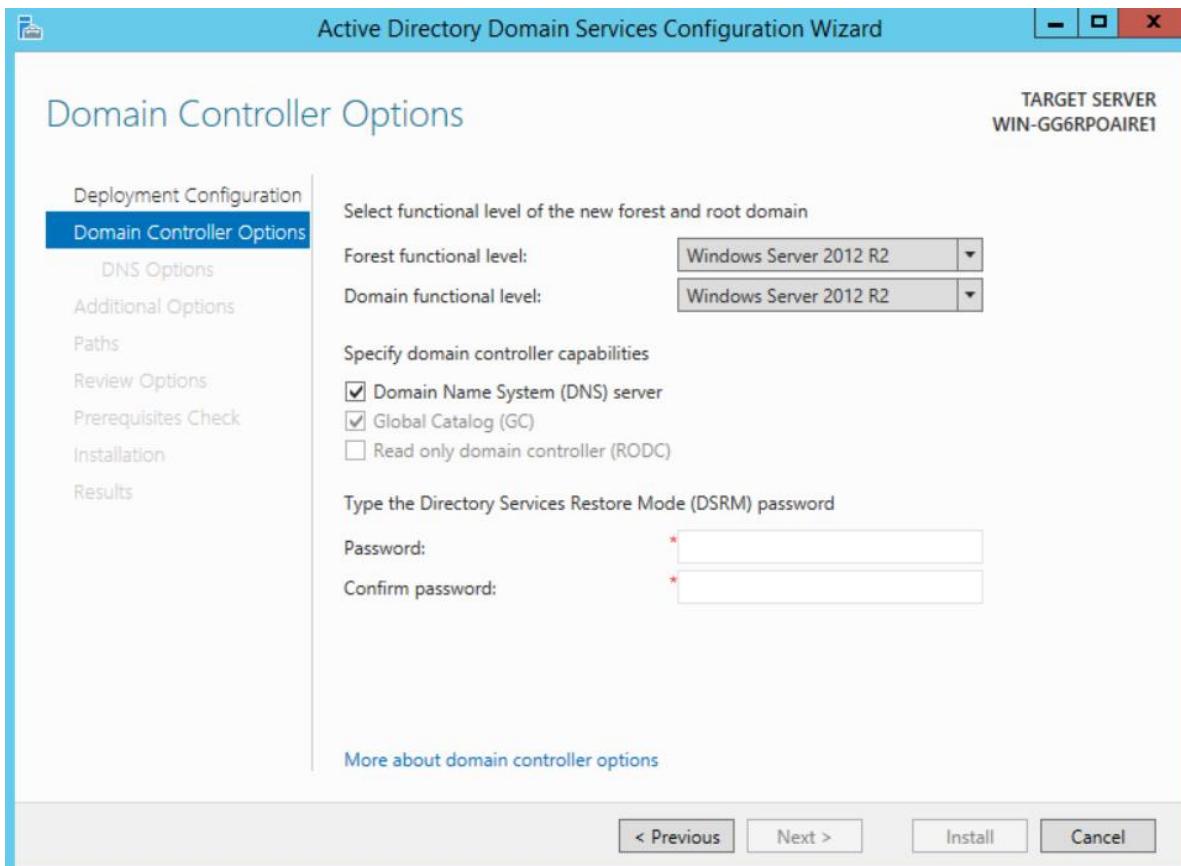
Specify the domain information for this operation

Root domain name:

More about deployment configurations

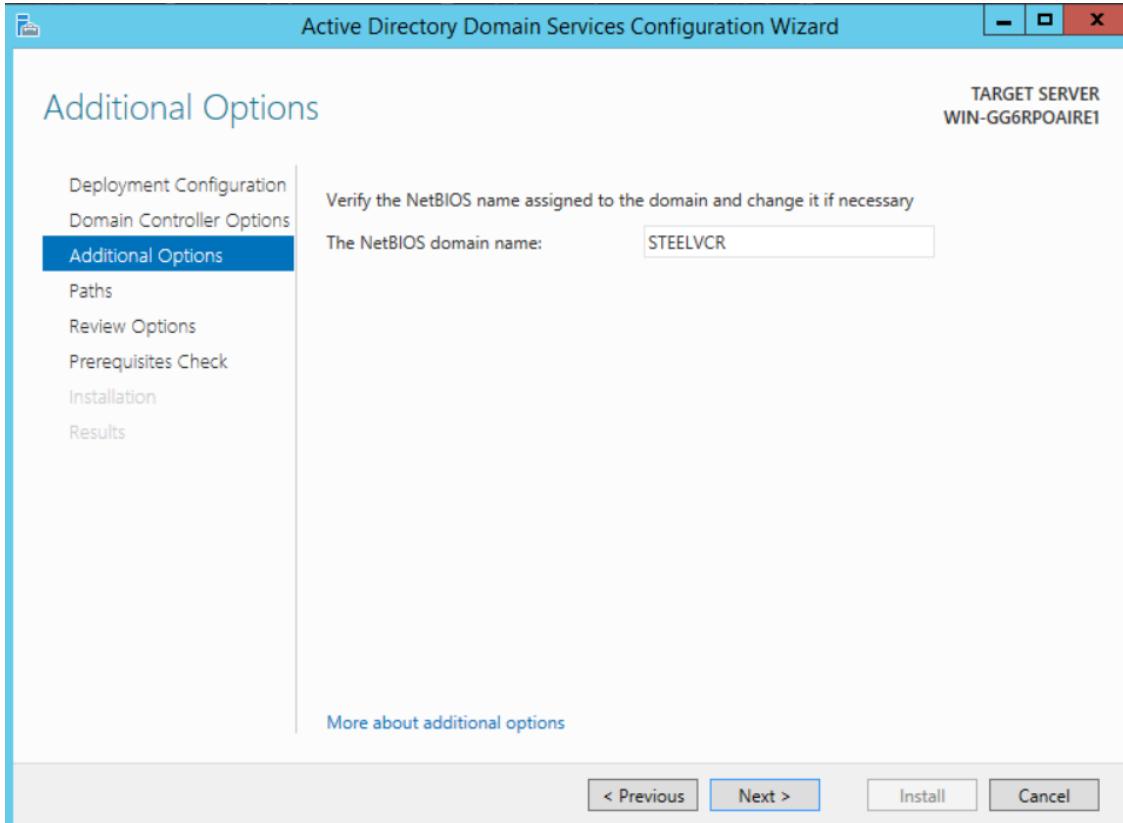
< Previous Next > Install Cancel

After typing root domain name click “Next”.

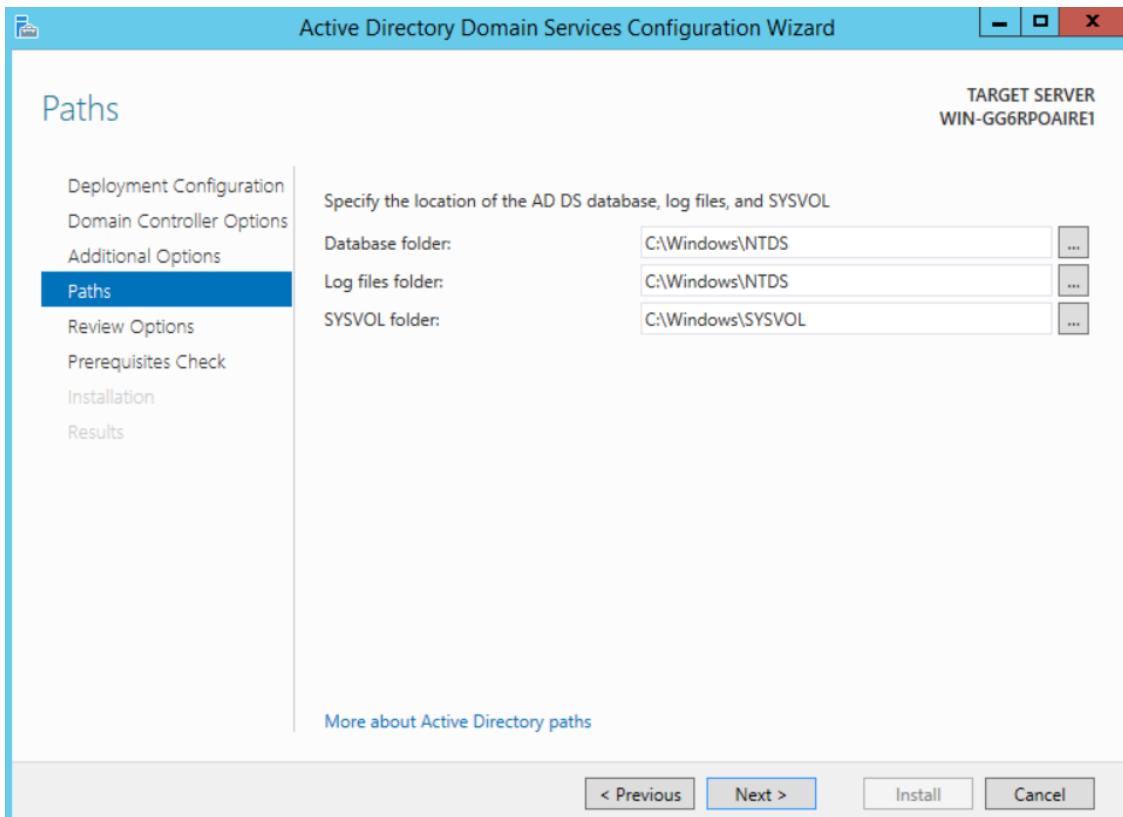


Take off the checkmark on first checkbox that read “Domain Name System (DNS) server”.

Then, create your Active Directory “DSRM” password and click “Next” when done.

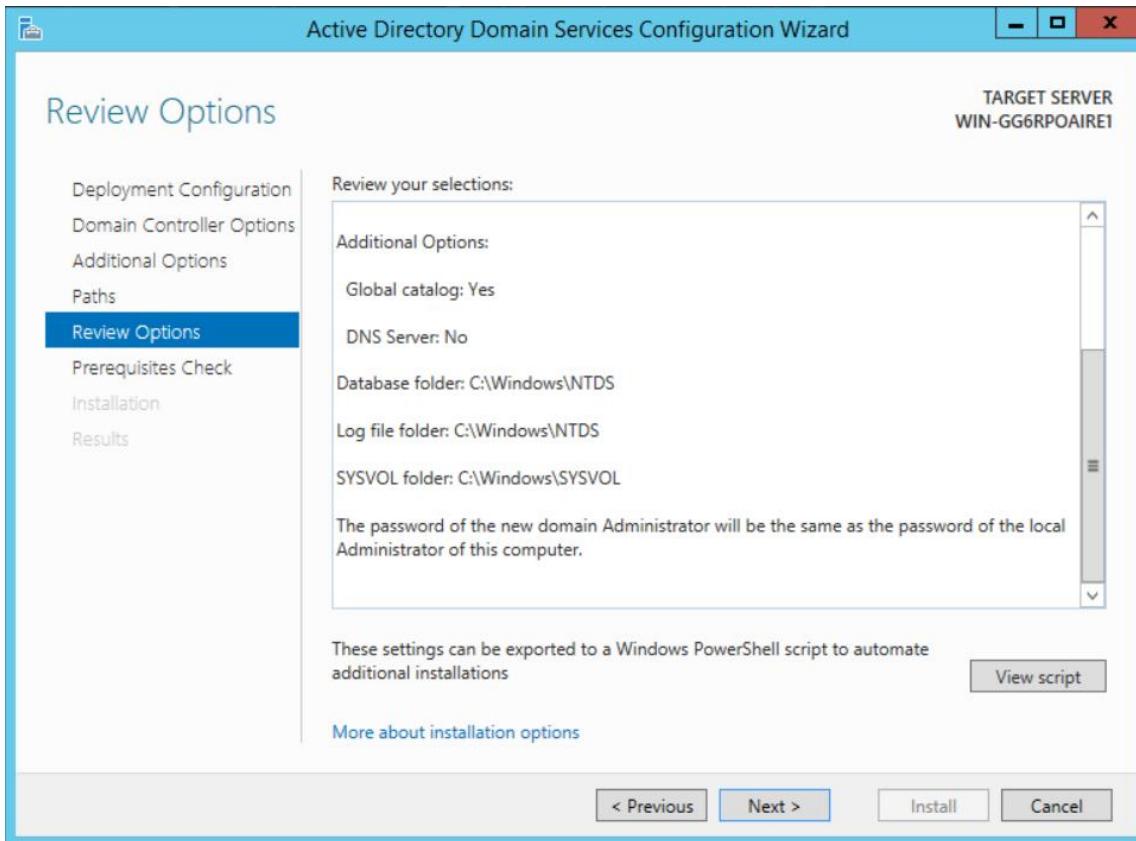


Keep or change NetBIOS domain name (addition option for Domain Controller), and click “Next”.

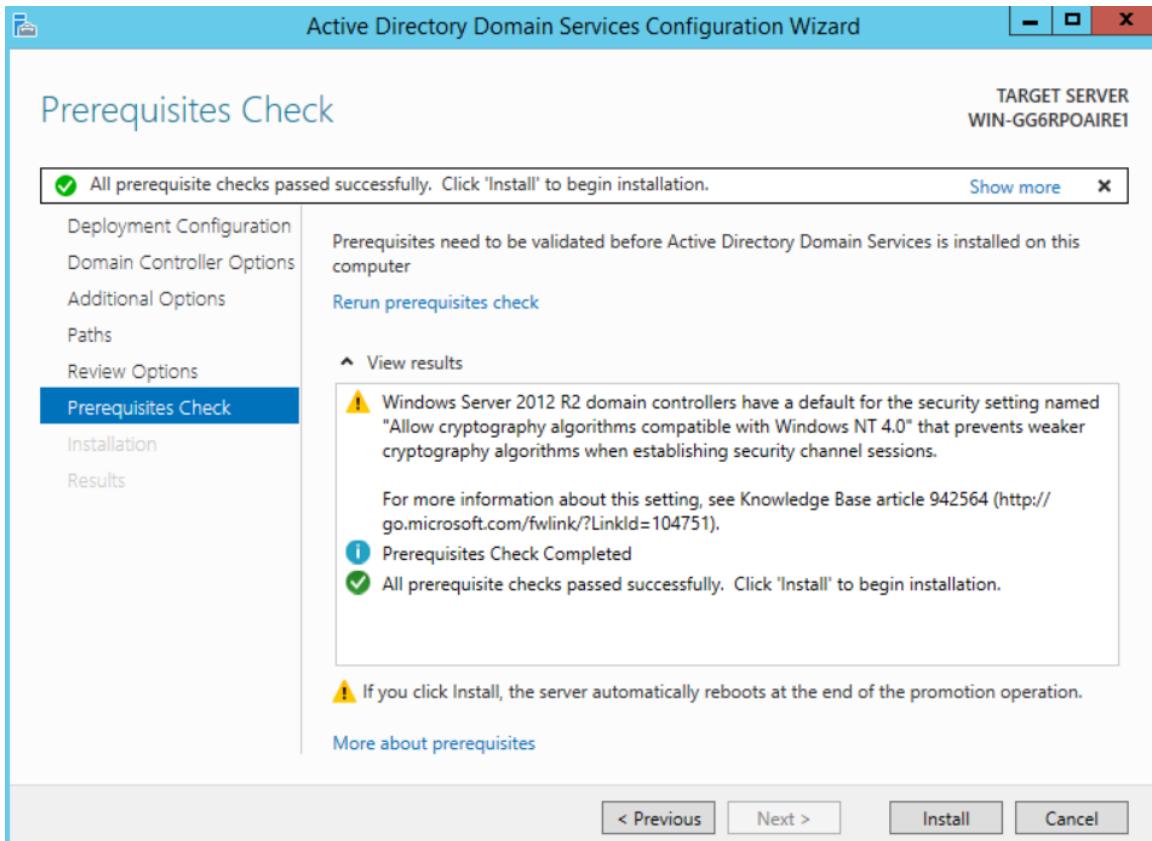


The paths are shown automatically and can be edited.

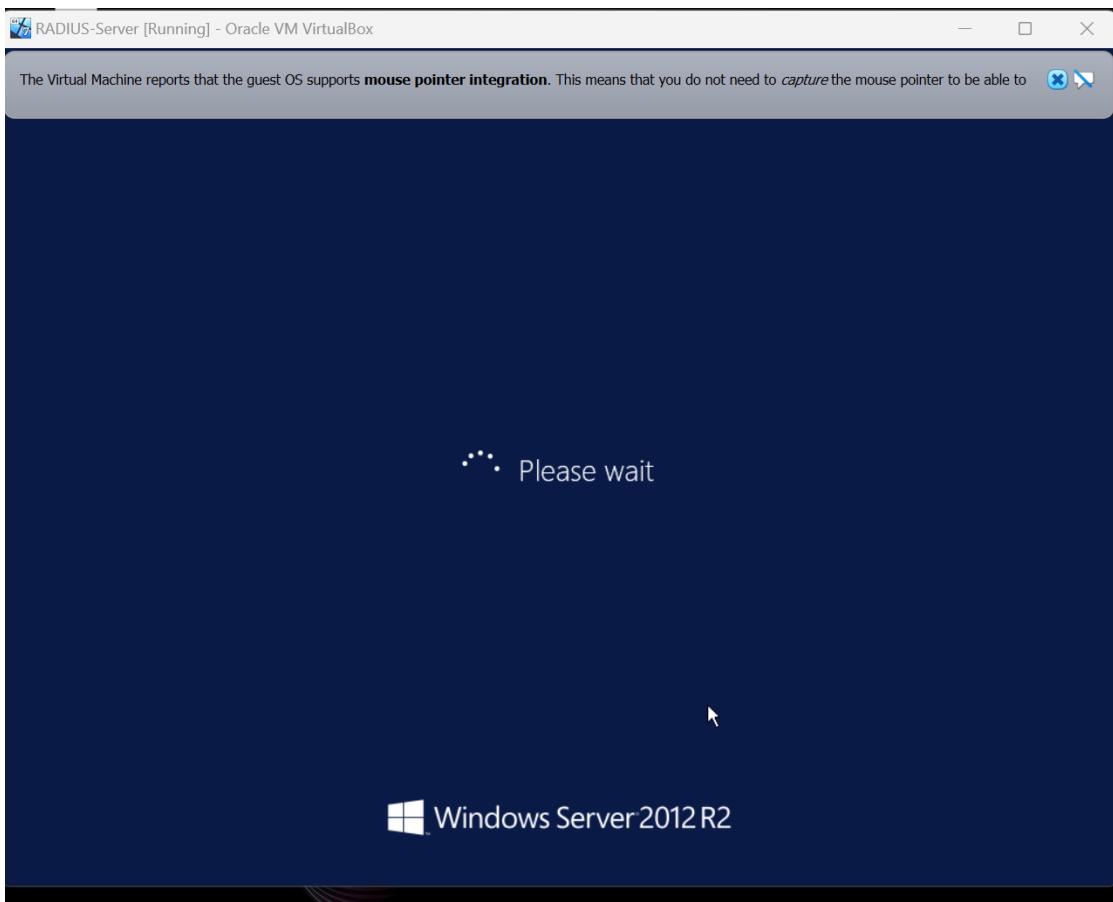
These paths are for Active Directory “database, log files, and SYSVOL” directories/folders. Click “Next”.



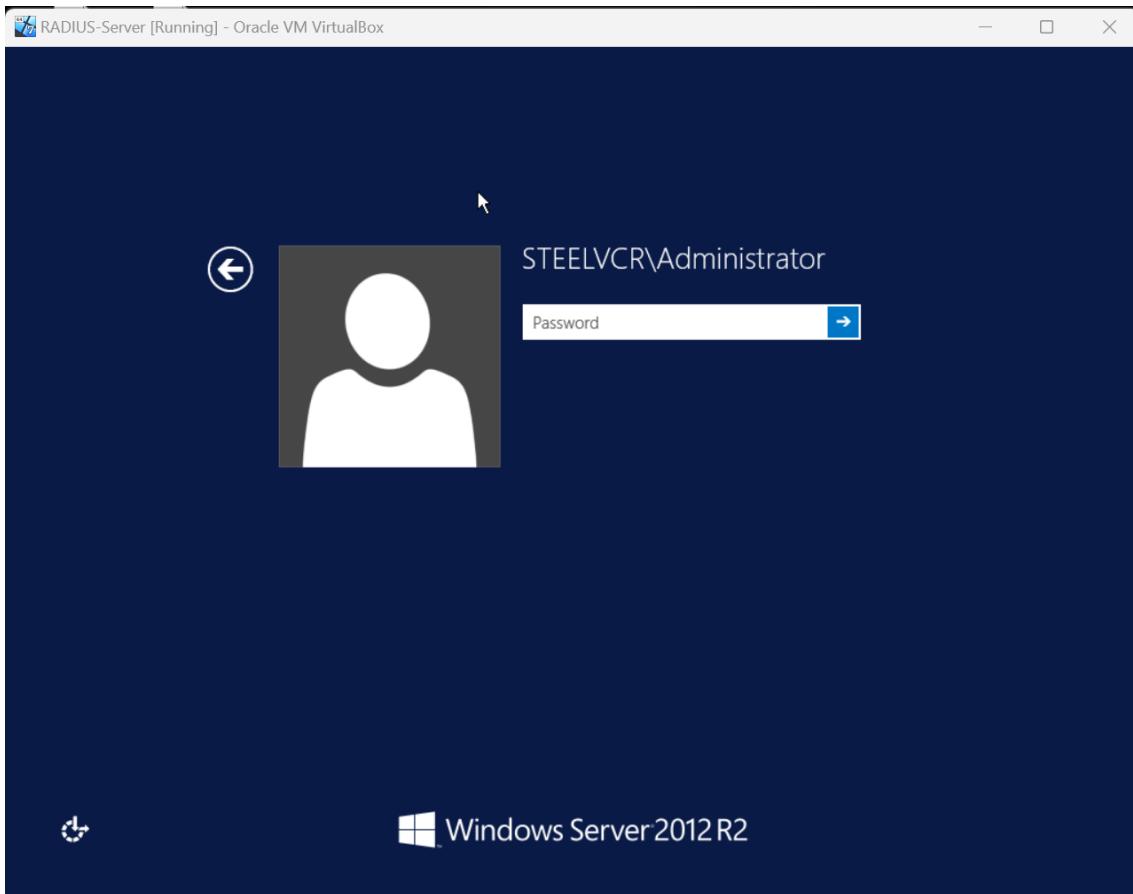
Check to make sure everything is right and click “Next”.



After prerequisite check is successful, click “Install”.

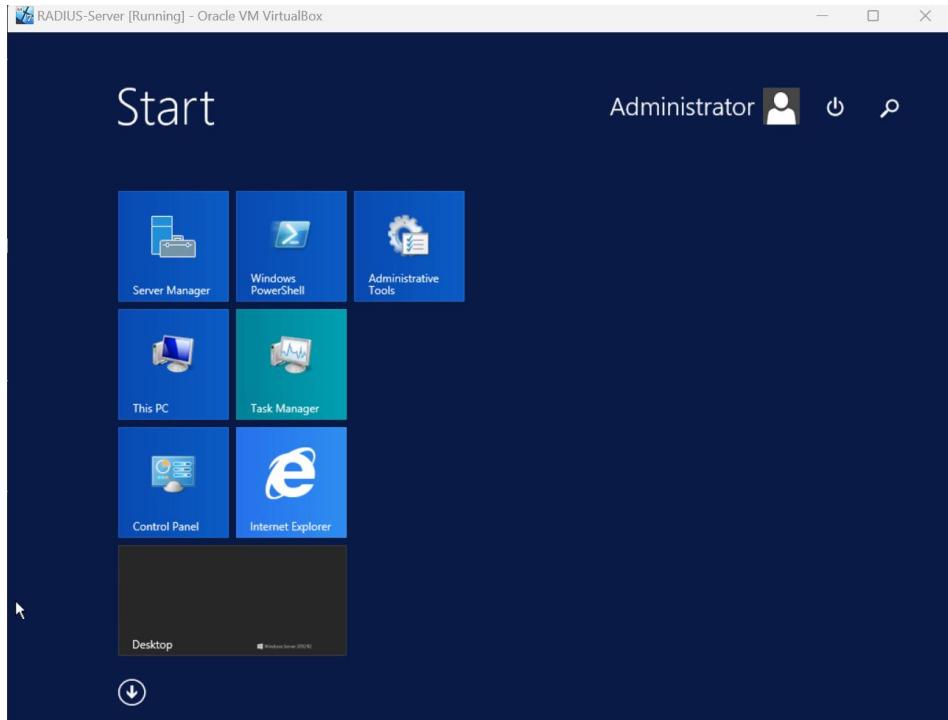


Wait 10 minutes or maybe longer depending on your connection.

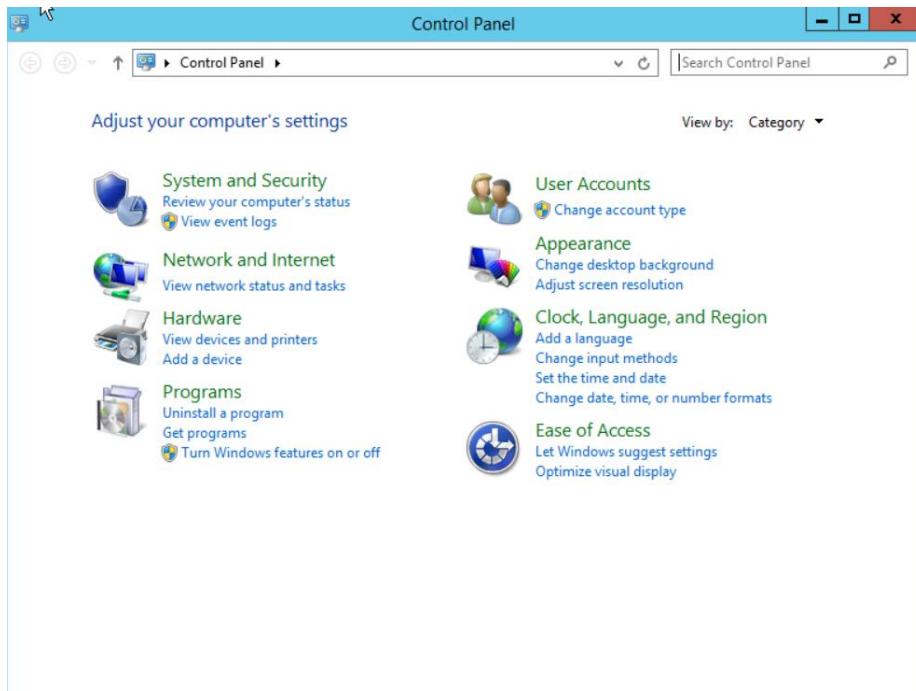


Login again.

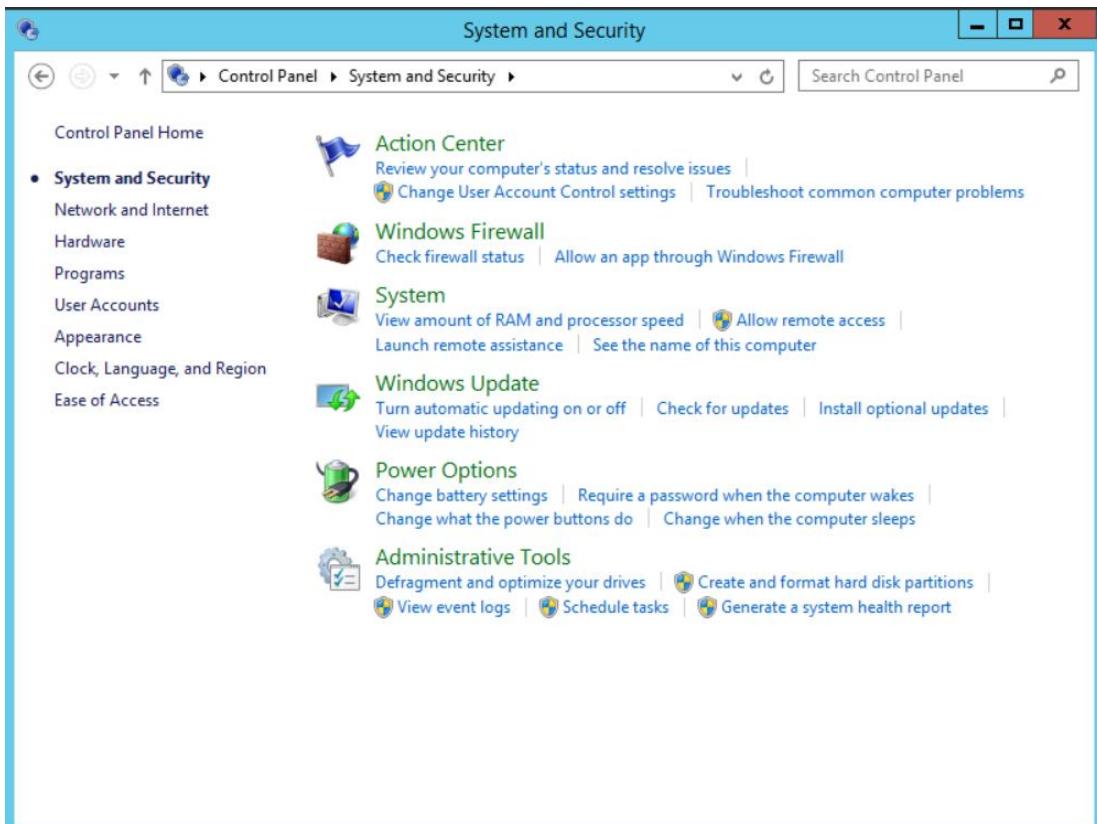
(Might get a pop up about password expiring in 5 days, ignore that for now)



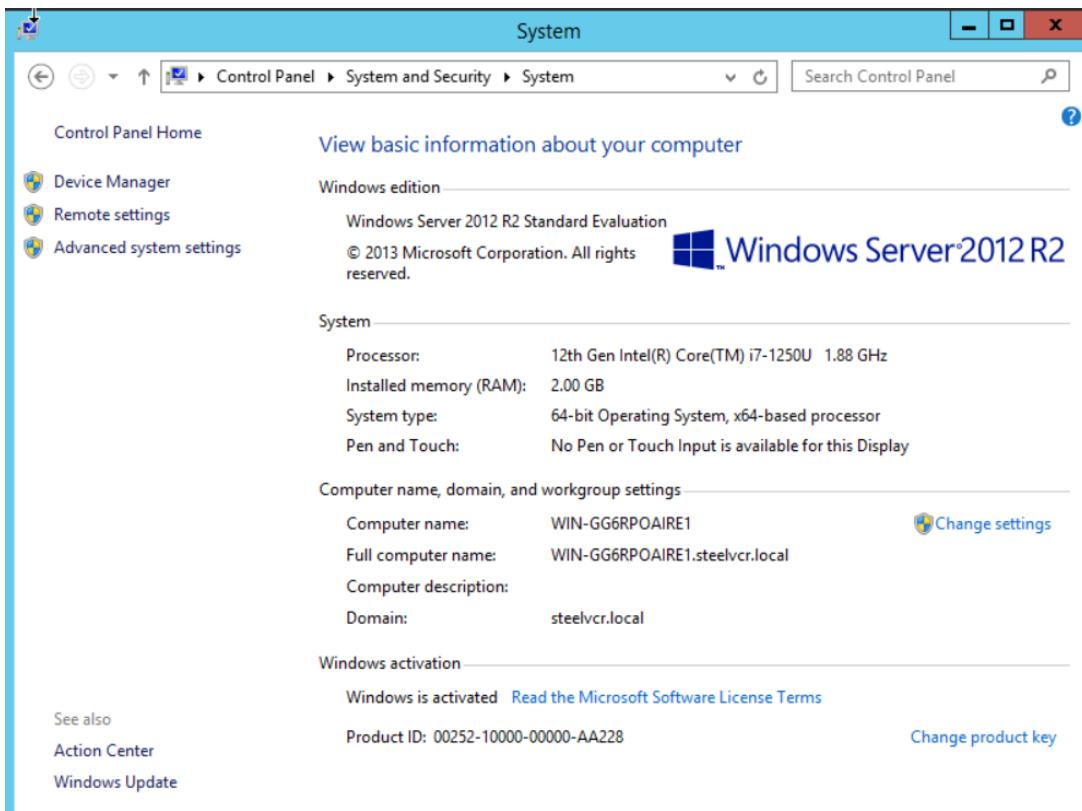
Go to Control Panel on the Start Menu.



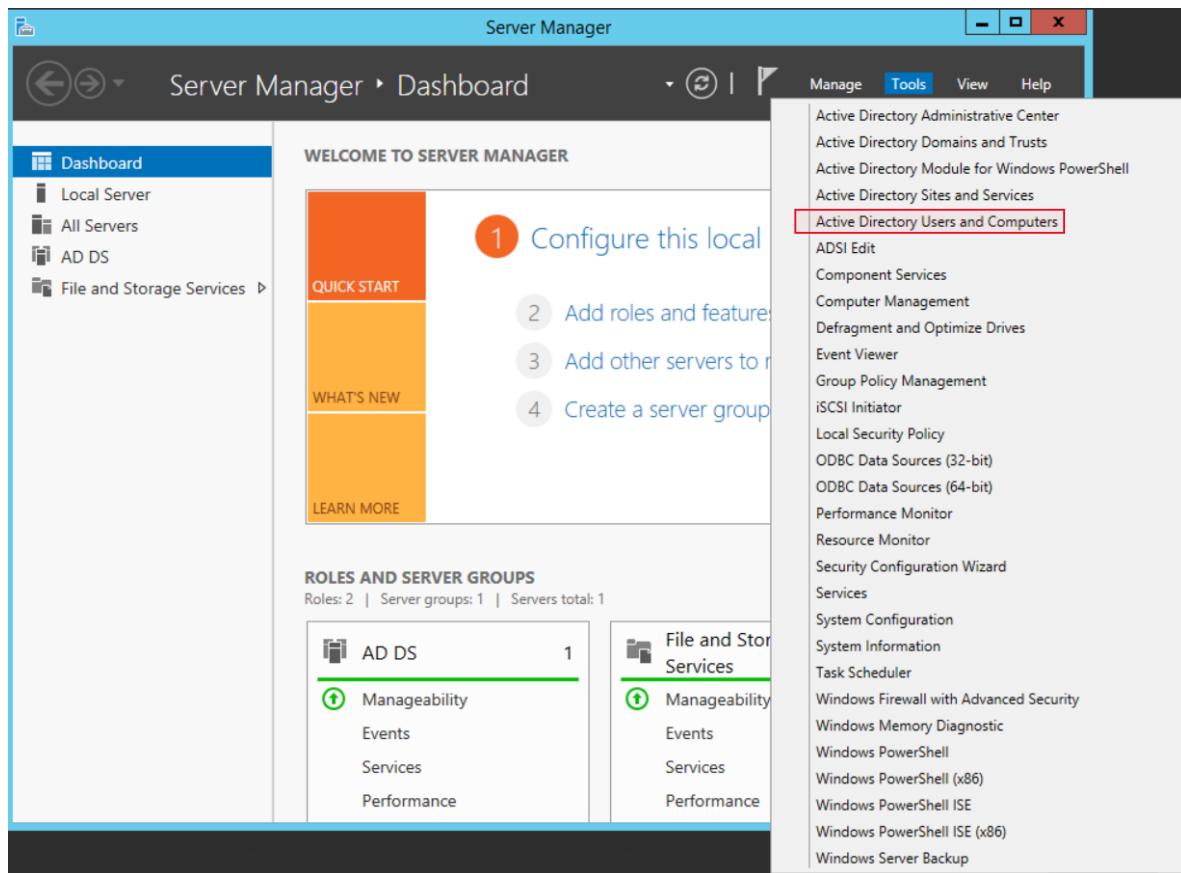
In the Control Panel go to "System and Security".



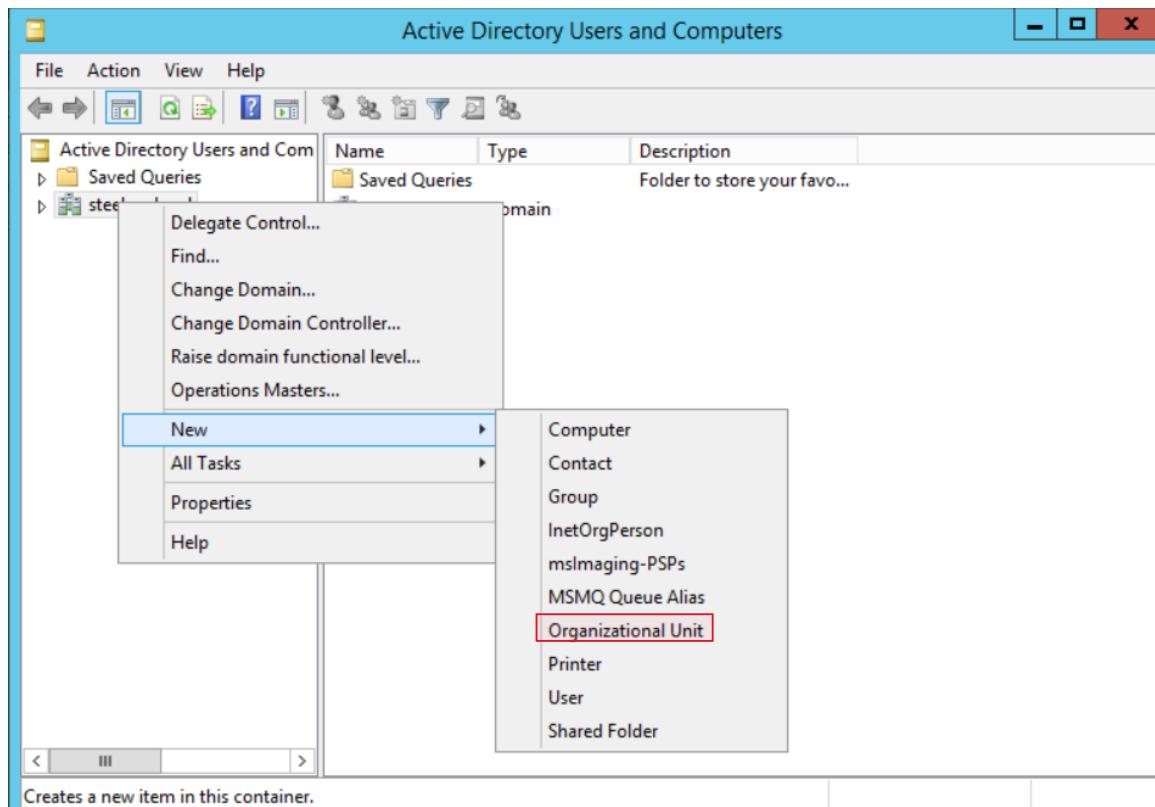
Go to "System".



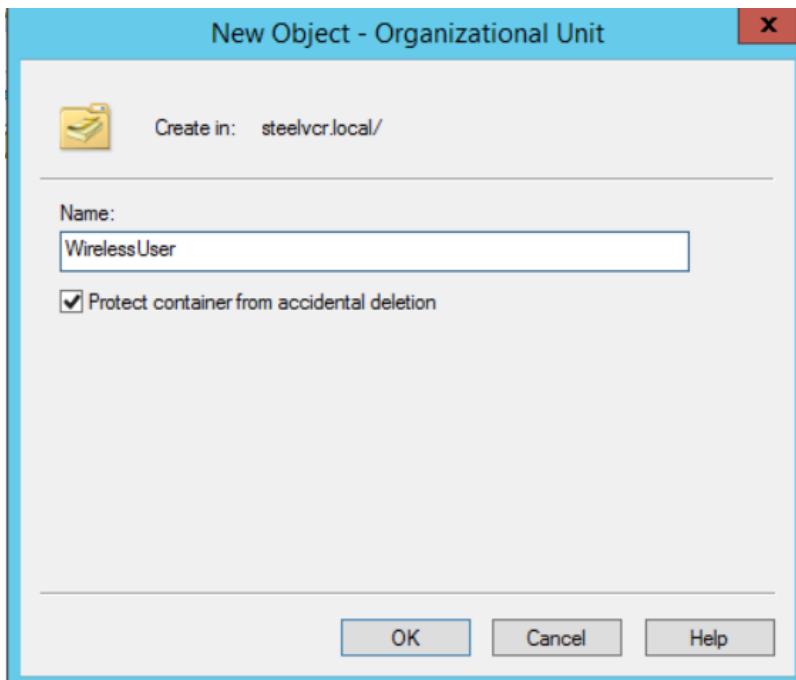
In the System there is information regarding O.S. and more.



Click on “Tools” in the upper right-hand corner and select “Active Directory Users and Computers”.



Right-click on your root domain name and select "New", and then click on "Organizational Unit".



Now create a new object for OU or **organizational unit** keep “Protect container from accidental deletion” checked. Click “Ok” when done.

This **object** will be located within the directory of root domain user.

Active Directory Users and Computers

File Action View Help

Active Directory Users and Computers

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...
WirelessUser	Organizational...	

The new organizational unit has been created.

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com

Saved Queries

ste

Delegate Control...

Find...

Change Domain...

Change Domain Controller...

Raise domain functional level...

Operations Masters...

New

All Tasks

View

Refresh

Export List...

Properties

Help

Name Type Description

Builtin builtinDomain

Container Default container for up...

Organizational... Default container for do...

Container Default container for sec...

Container Default container for ma...

Container Default container for up...

Organizational...

Computer

Contact

Group

InetOrgPerson

msImaging-PSPs

MSMQ Queue Alias

Organizational Unit

Printer

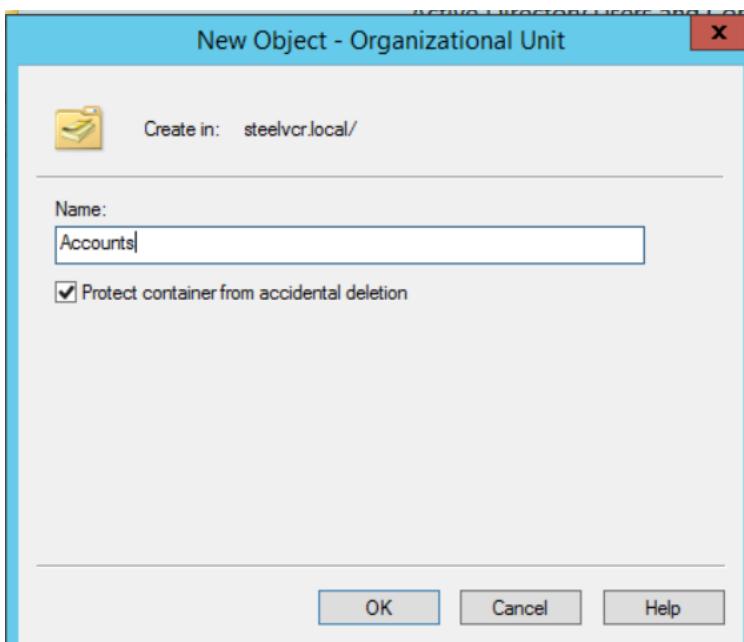
User

Shared Folder

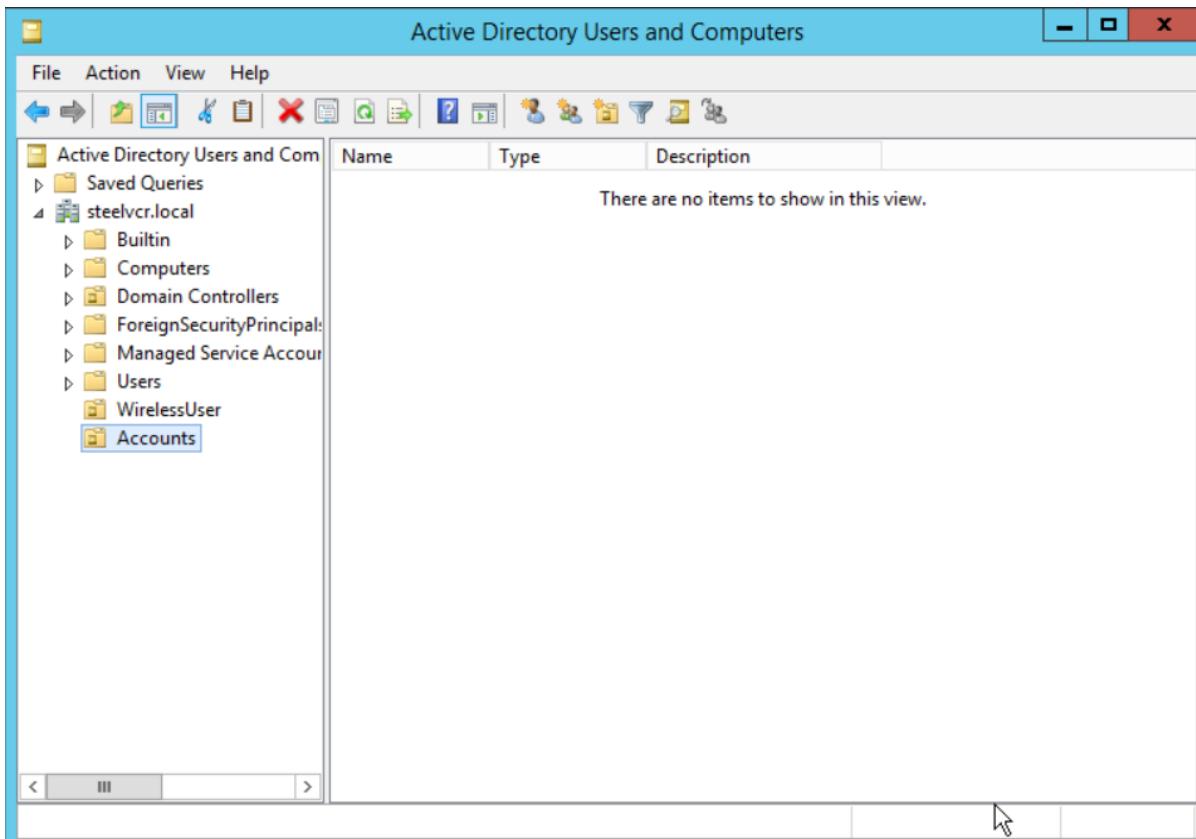
Creates a new item in this container.

This screenshot shows the 'Active Directory Users and Computers' snap-in in Windows Server. A context menu is open over an empty container, with 'New' selected. A secondary dropdown menu lists various object types: Computer, Contact, Group, InetOrgPerson, msImaging-PSPs, MSMQ Queue Alias, Organizational Unit, Printer, User, and Shared Folder. The 'Organizational Unit' option is highlighted. At the bottom of the main window, a status bar says 'Creates a new item in this container.'

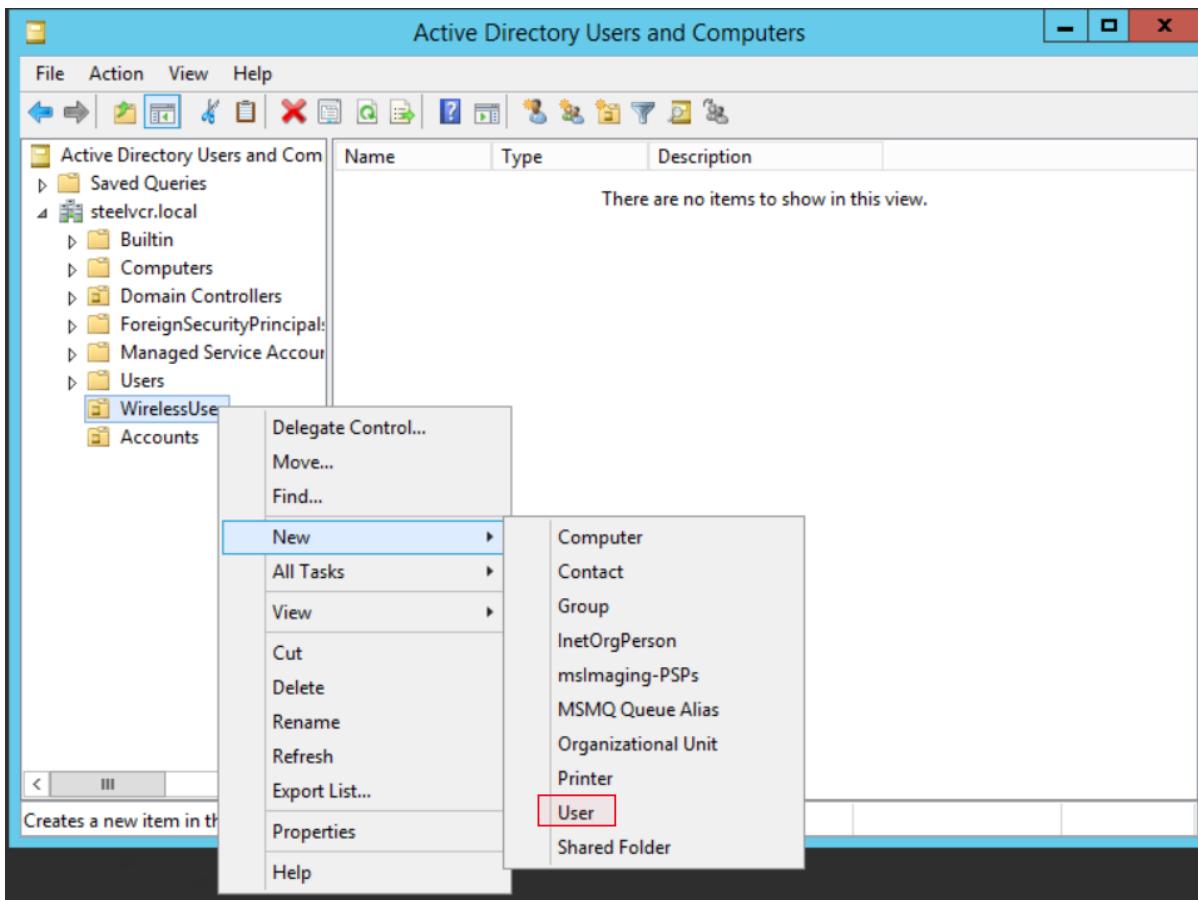
Do the same thing again to create another Organizational Unit.



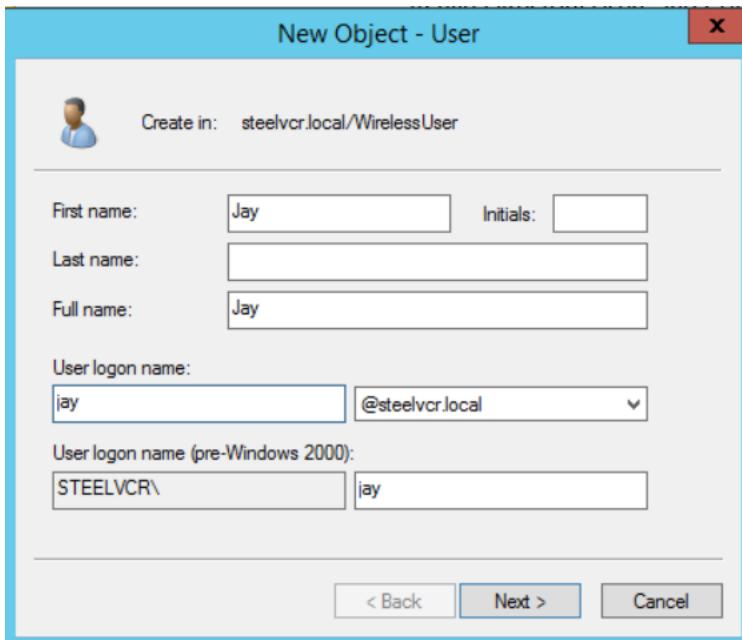
Add the new object which is another organizational unit and click "Ok".



Both object/folders will be there now within “steelvcr.local” directory/folder.

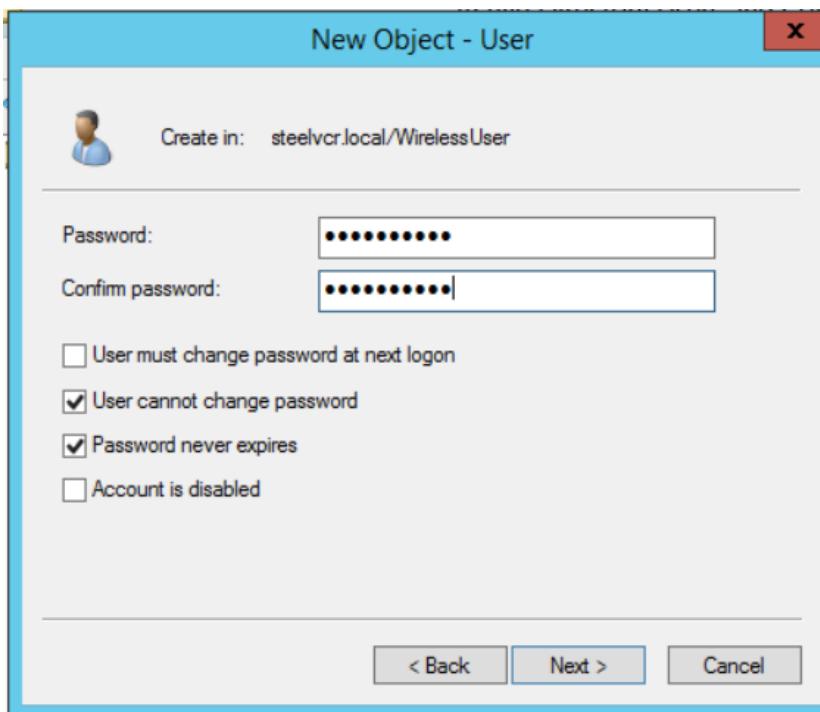


Right-click on first newly created object/folder and go to “New” and then click on “User”.



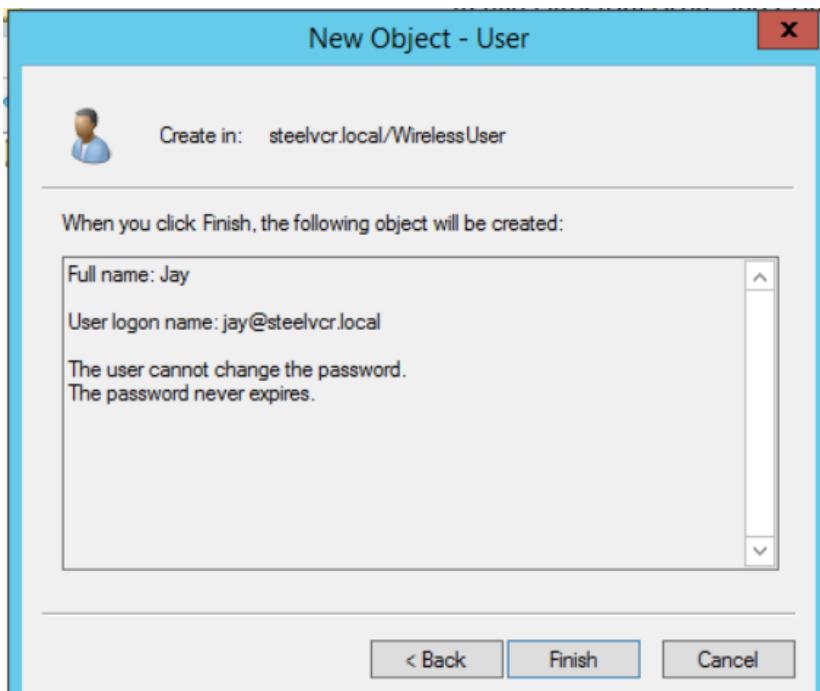
Enter a first name (optional last name) and the “User logon name” can be same as your name @ the root domain name.

Click “Next”.

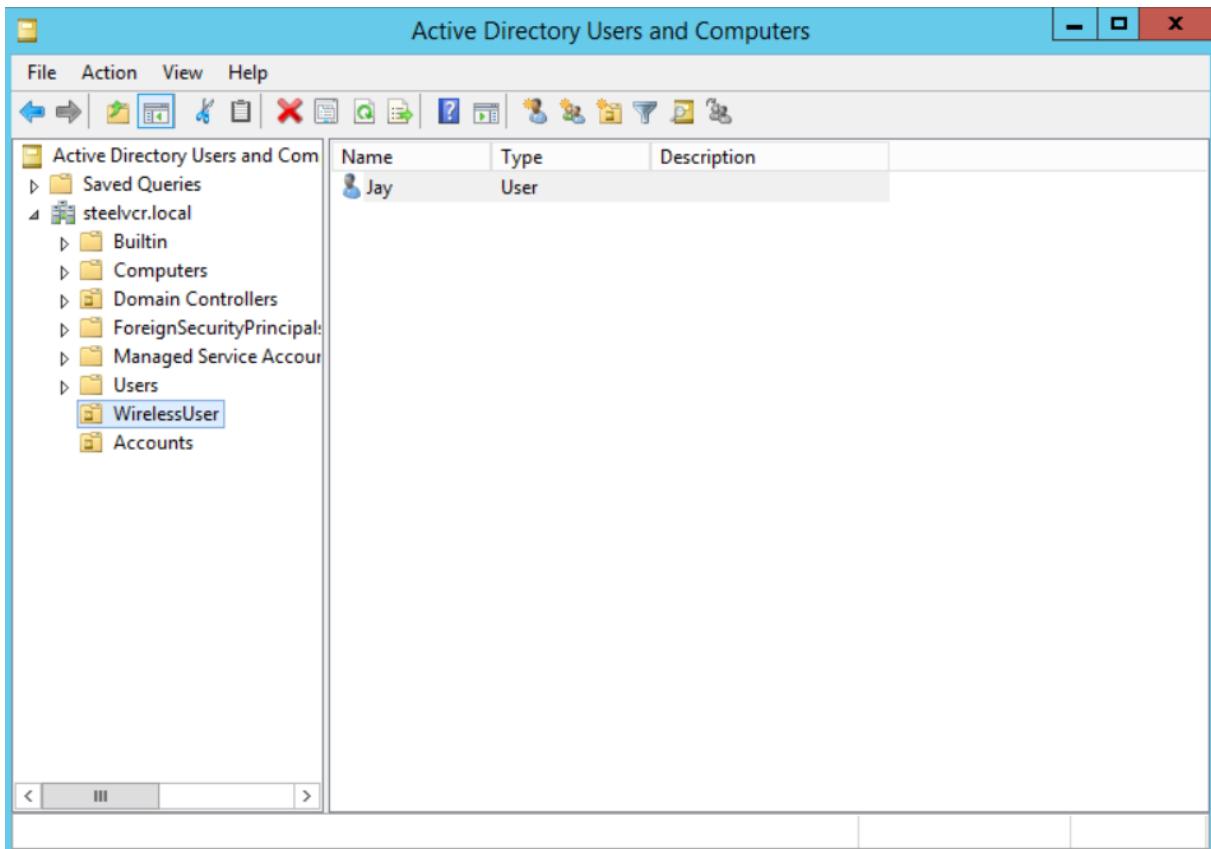


Uncheck the “User must change password at next logon” and keep “Account is disable” unchecked.

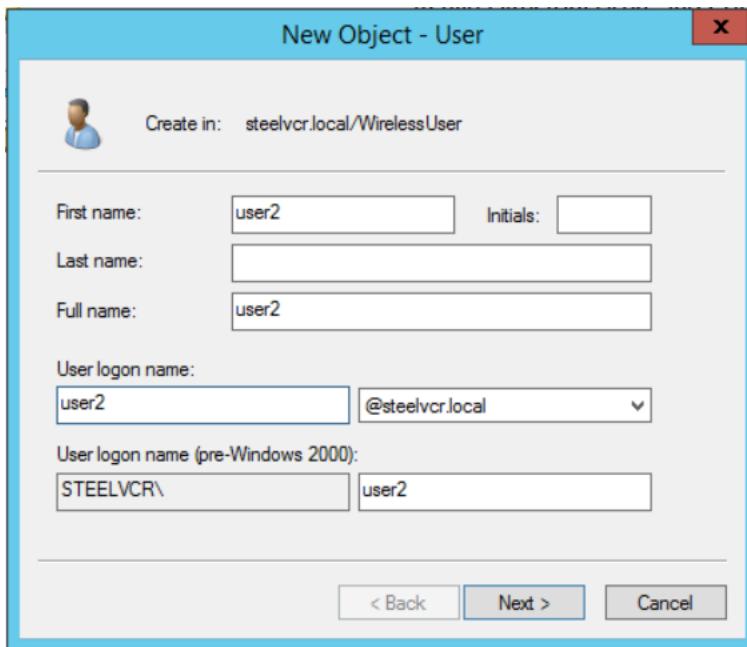
Check in the “User cannot change password” and the “Password never expires” checkboxes.



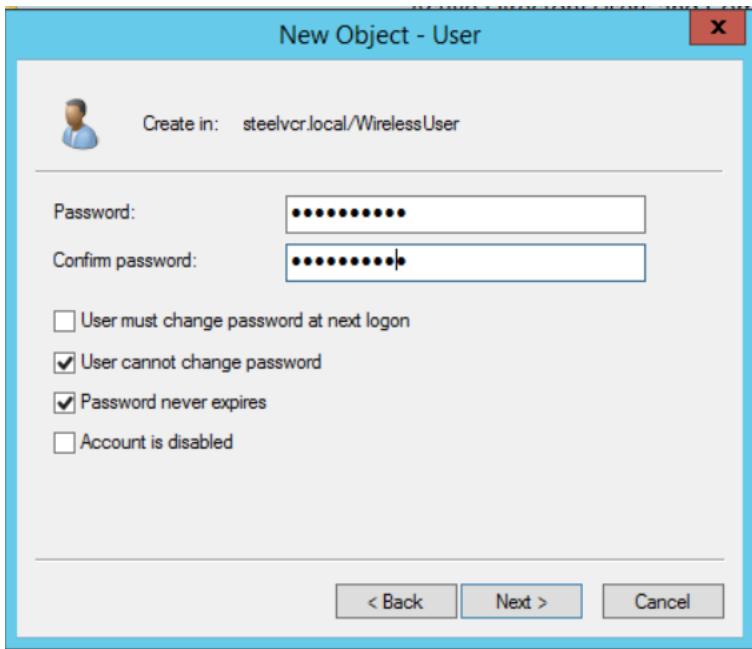
Click “Finish” after user is created.



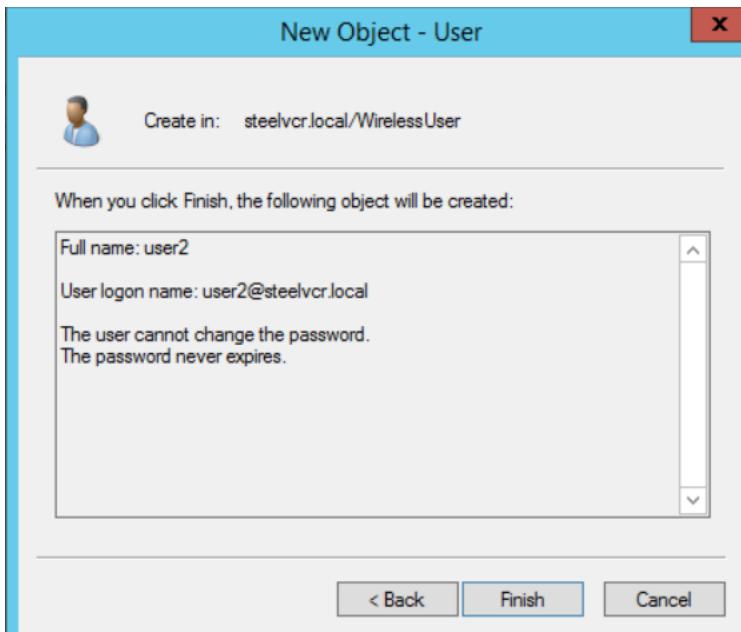
The new user "Jay" is now displayed under that folder.



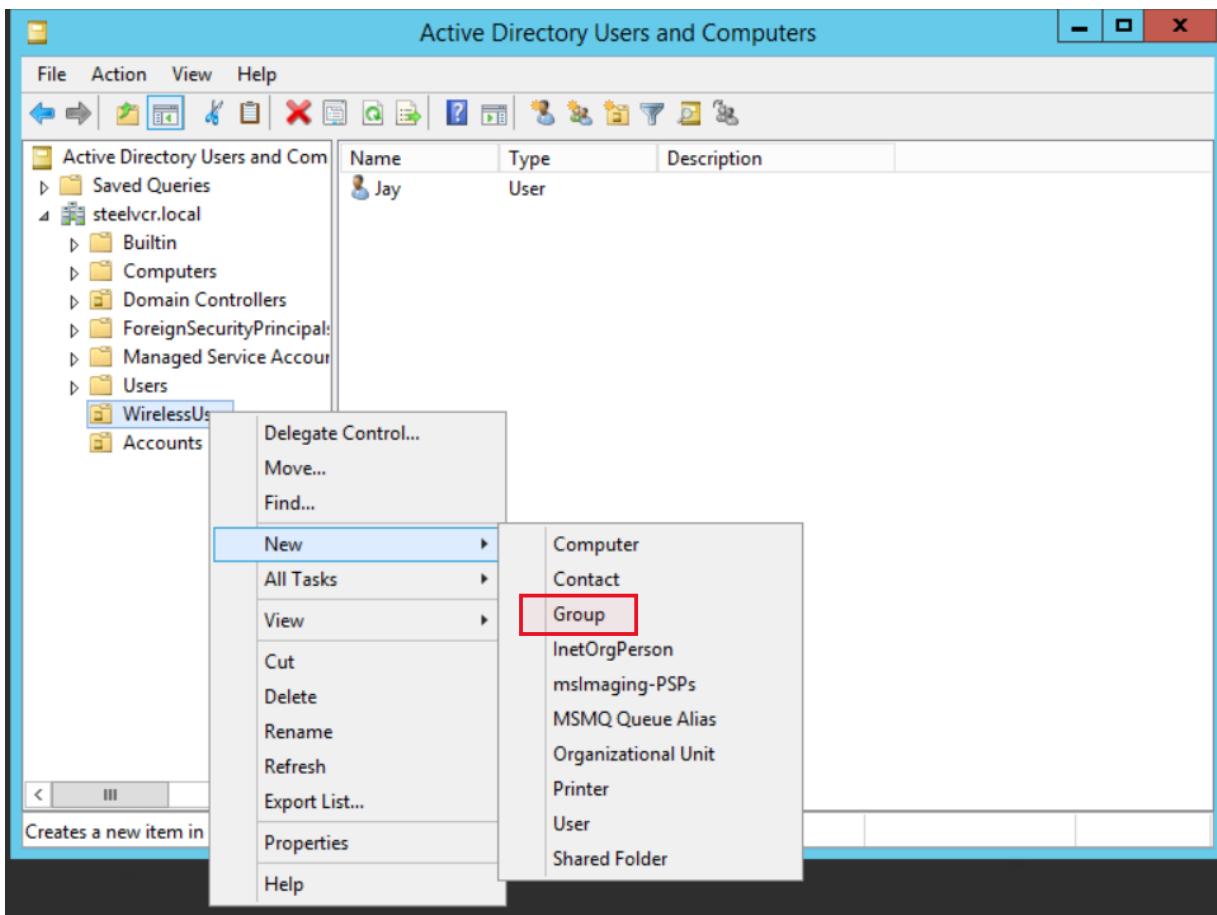
Can create a second user or however many users you want in that same organizational unit.



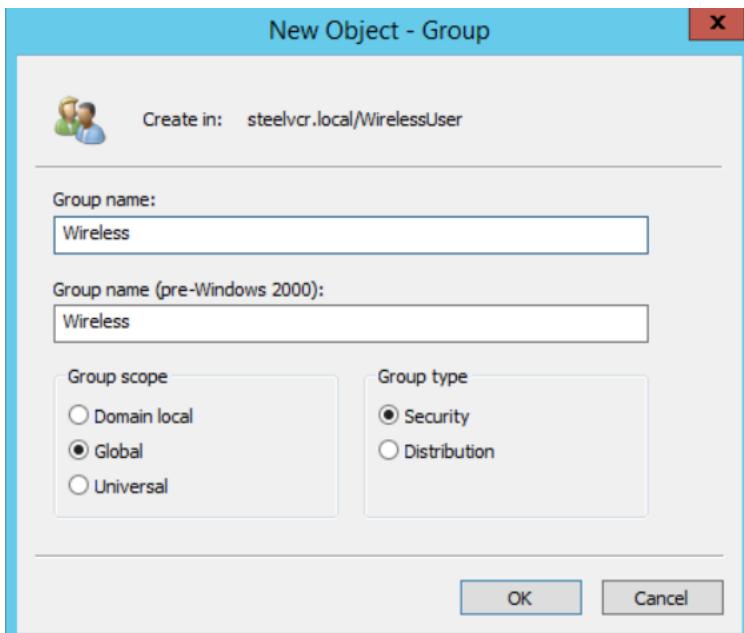
Do same checkboxes as before.



Click "Finish" for second user.

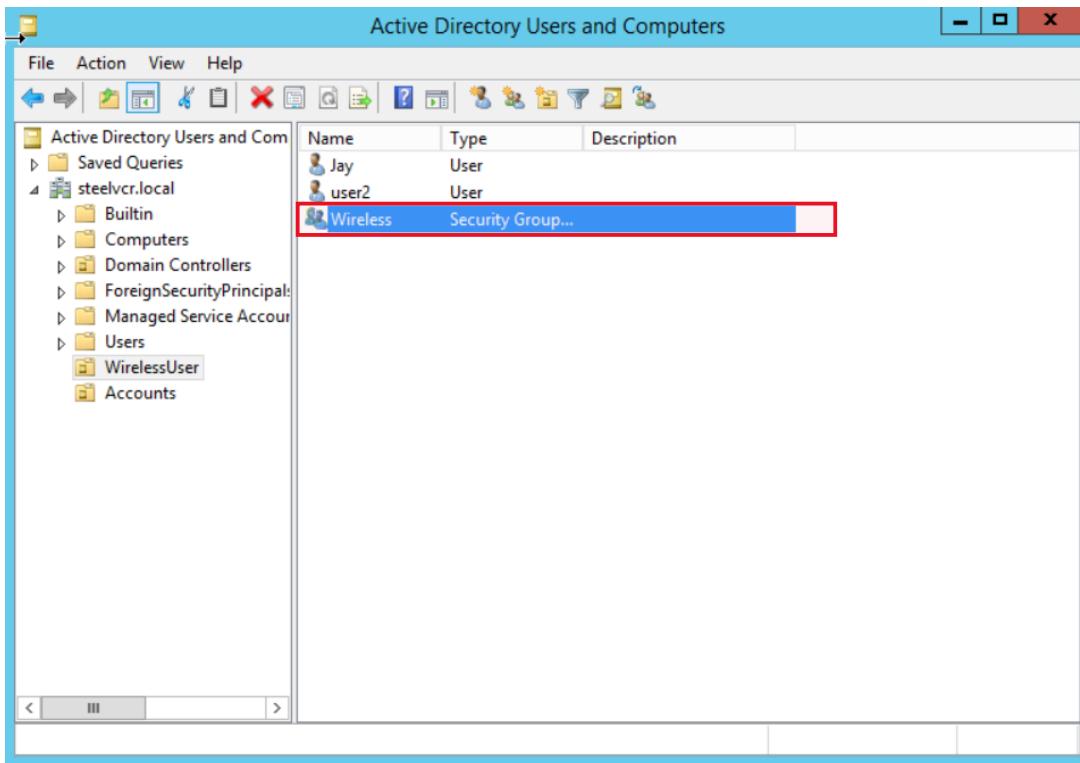


Right-click on that first organizational unit again, but this time select “New” and then “Group” to create a new group.

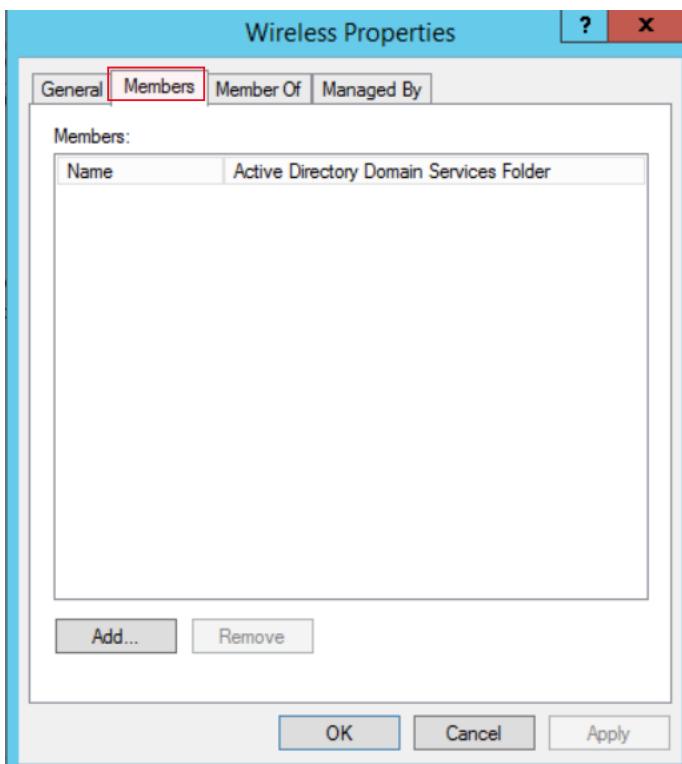


Type in a group name.

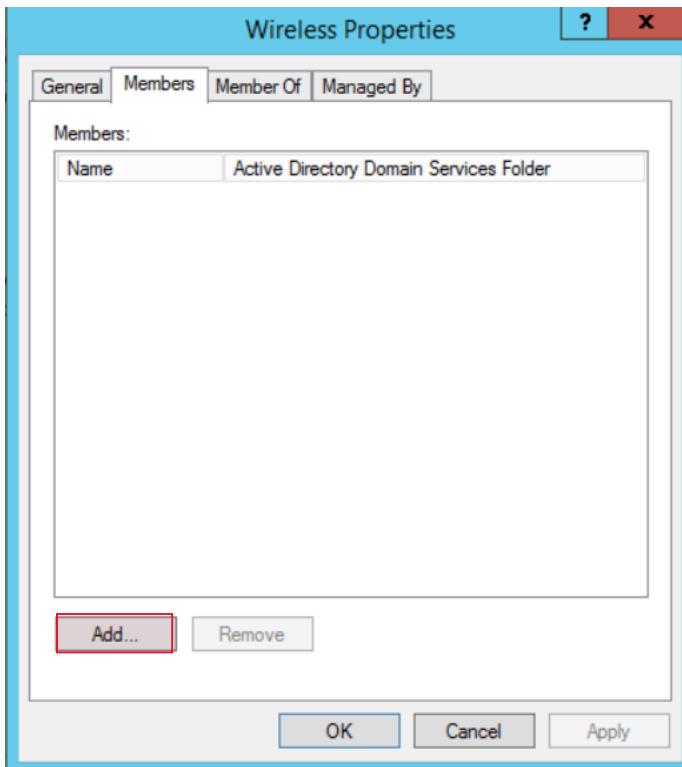
Keep “Group scope” as “Global”, and keep “Group type” as “Security”.



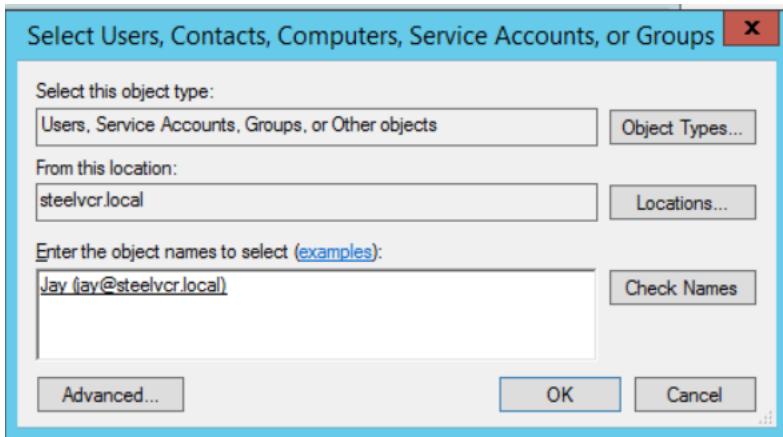
After the group has been added to the organizational unit, double-click on that newly created group within your first OU/organizational unit.



Click on "Members".

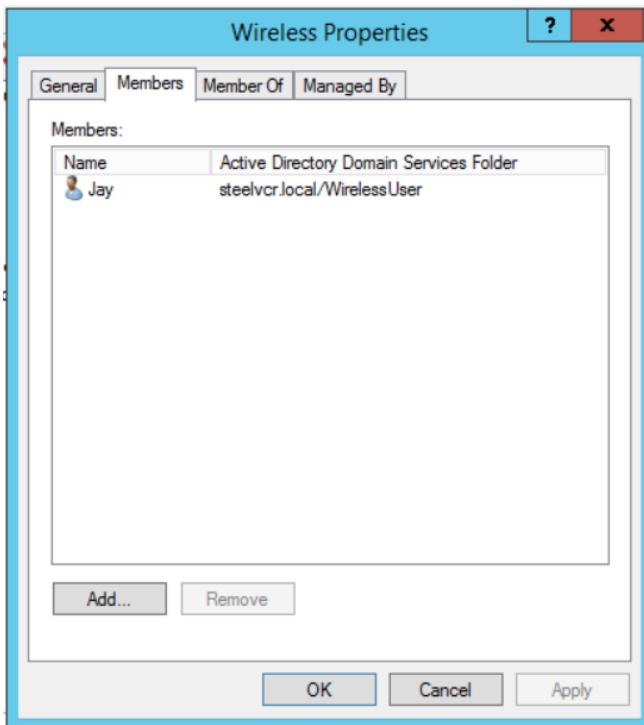


Click on "Add".

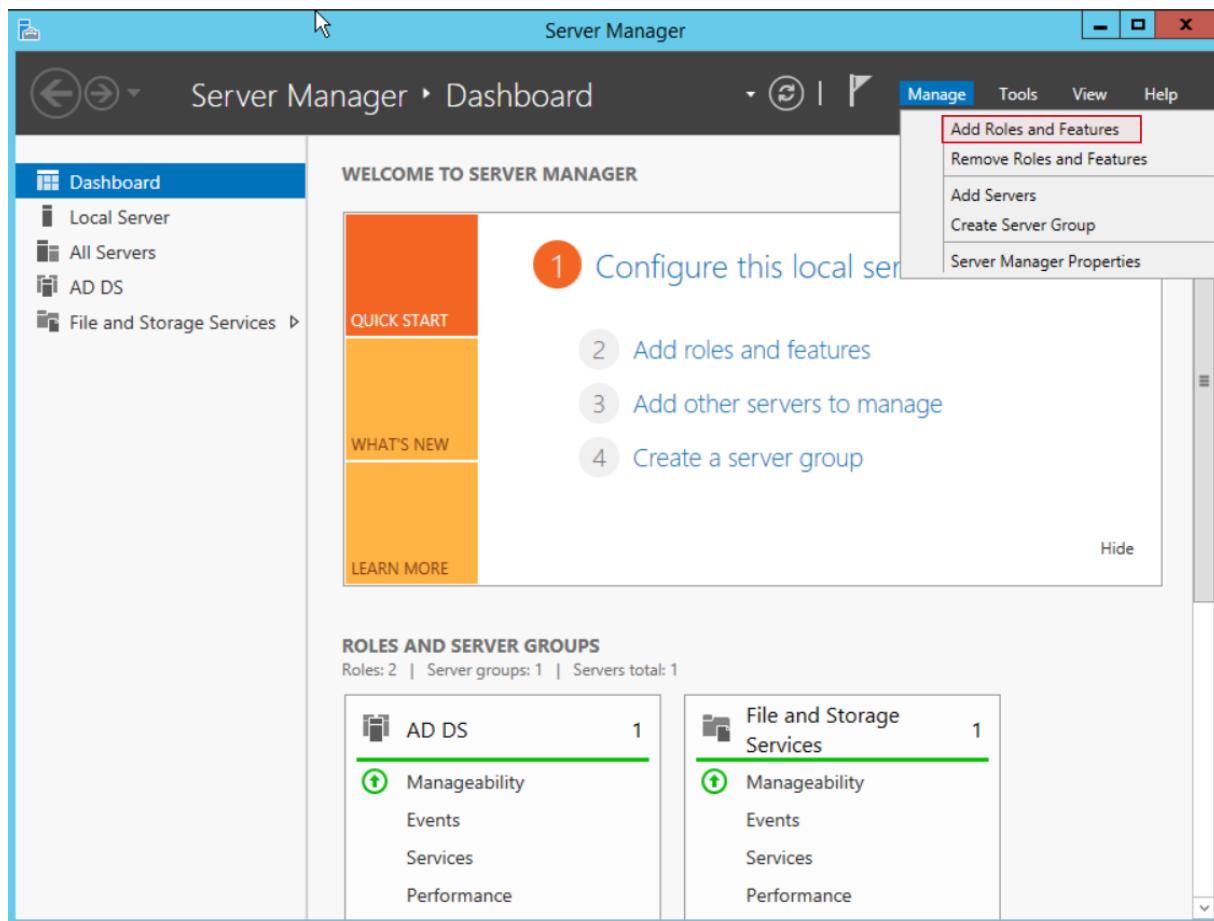


At the bottom under "Enter the object names to select", enter your object name or enter beginning of it and then click "Check Names" on the right-hand side.

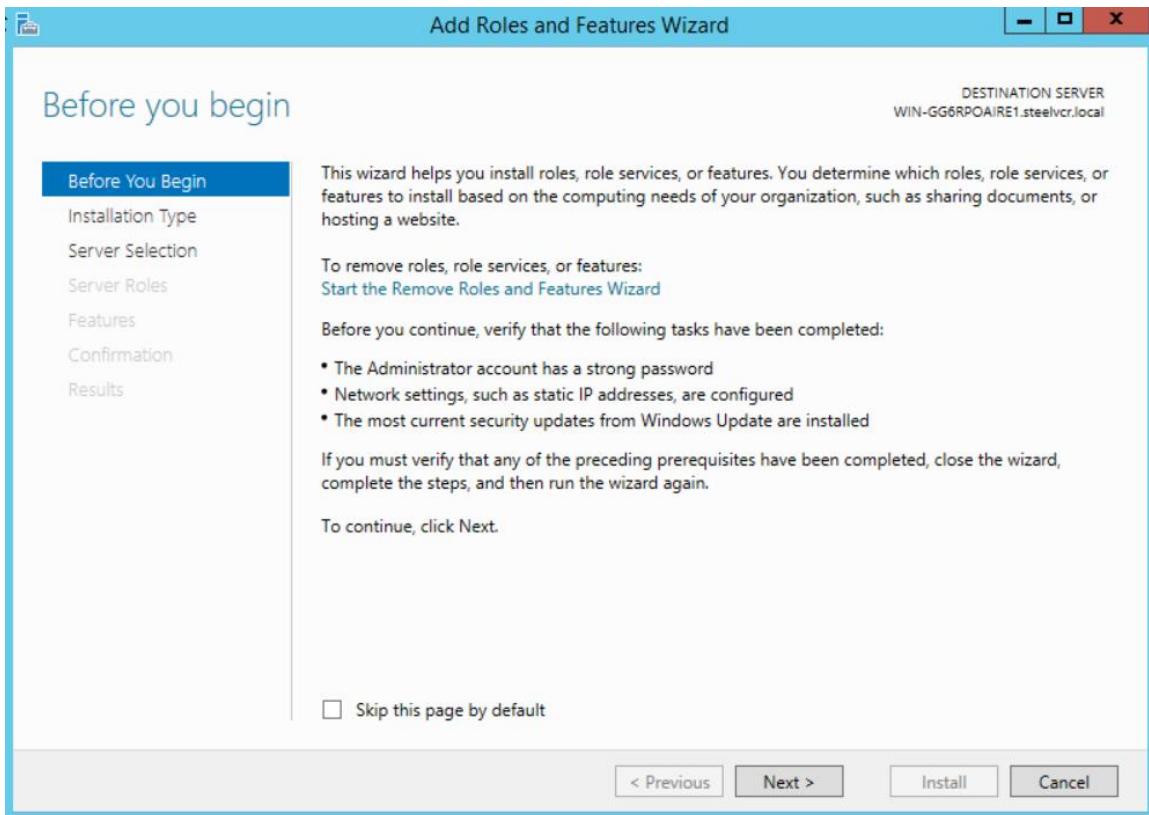
Click "OK" when finished.



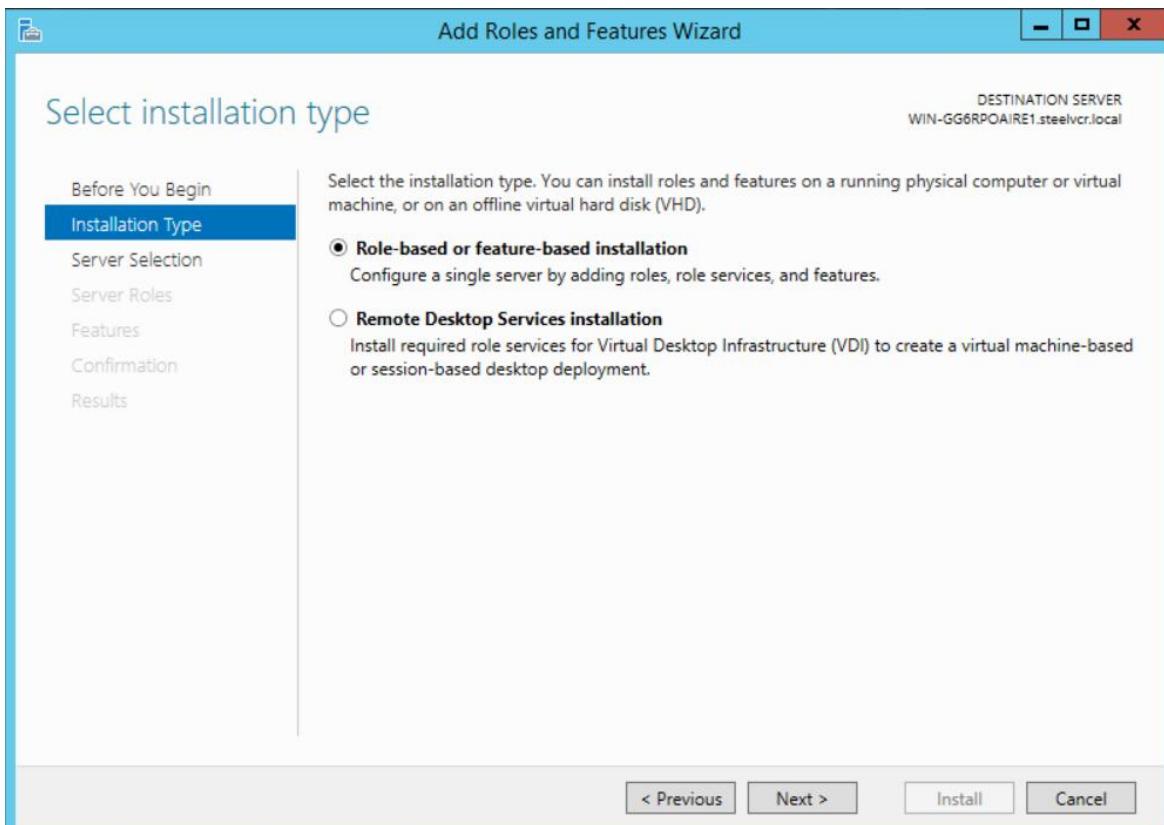
Click on "Apply" and then click on "OK".



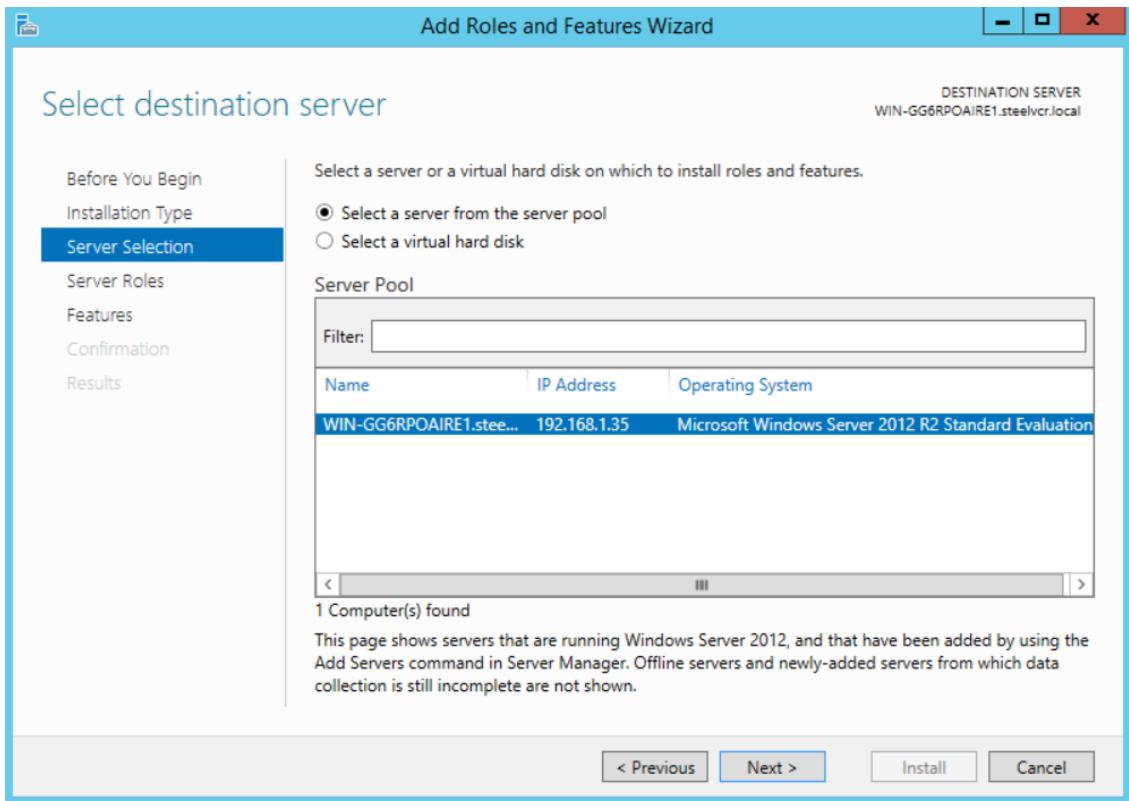
In upper right-hand corner click on "Manage" and then click on "Add Roles and Features".



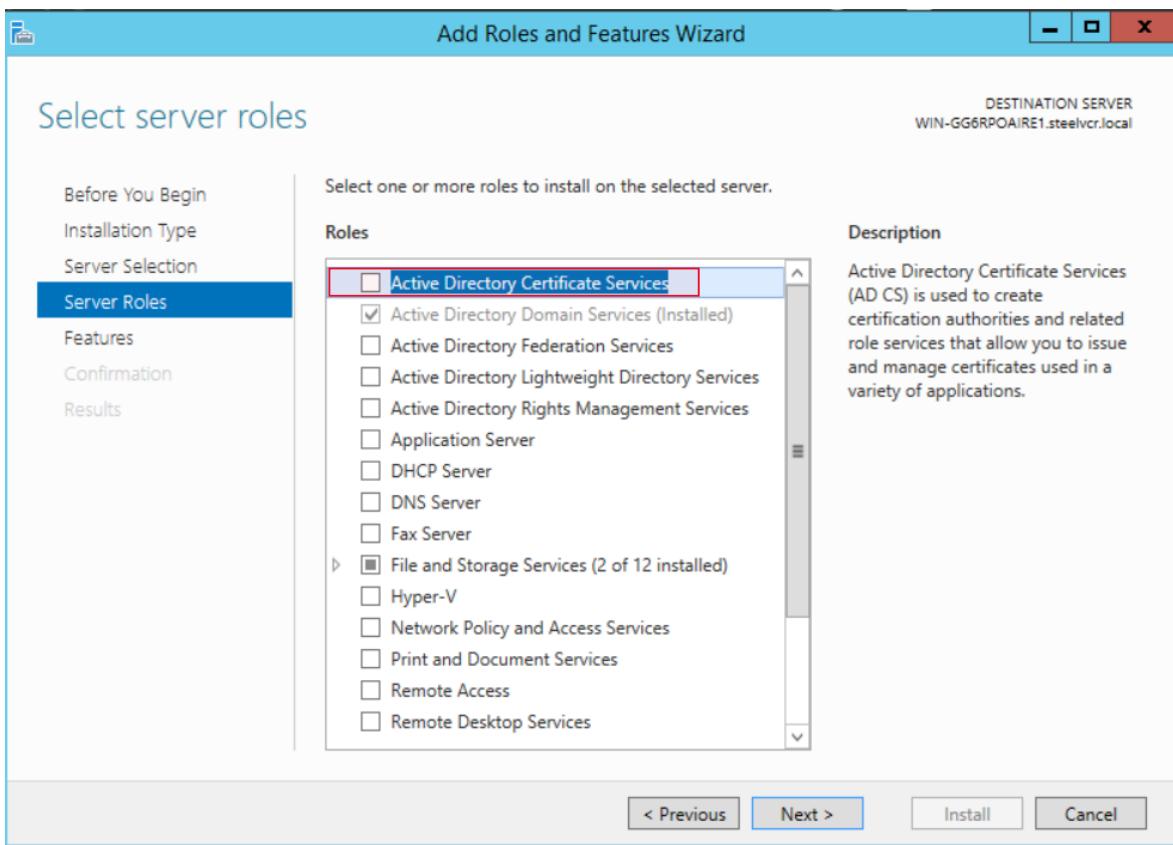
Click on “Next” after reading.



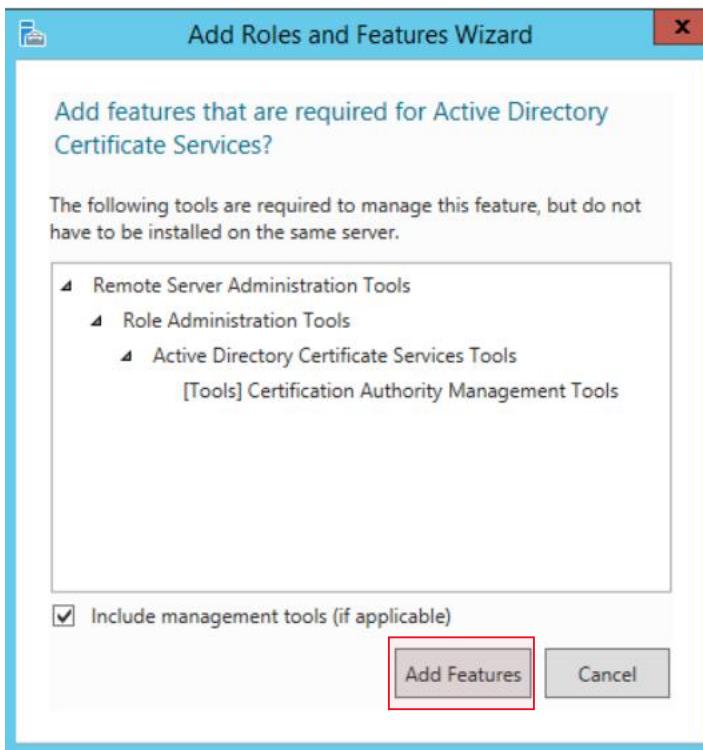
Select “Role-based or feature based installation” and click “Next”.



Click on the “Select a server from the server pool”, choose server, and then click “Next”.

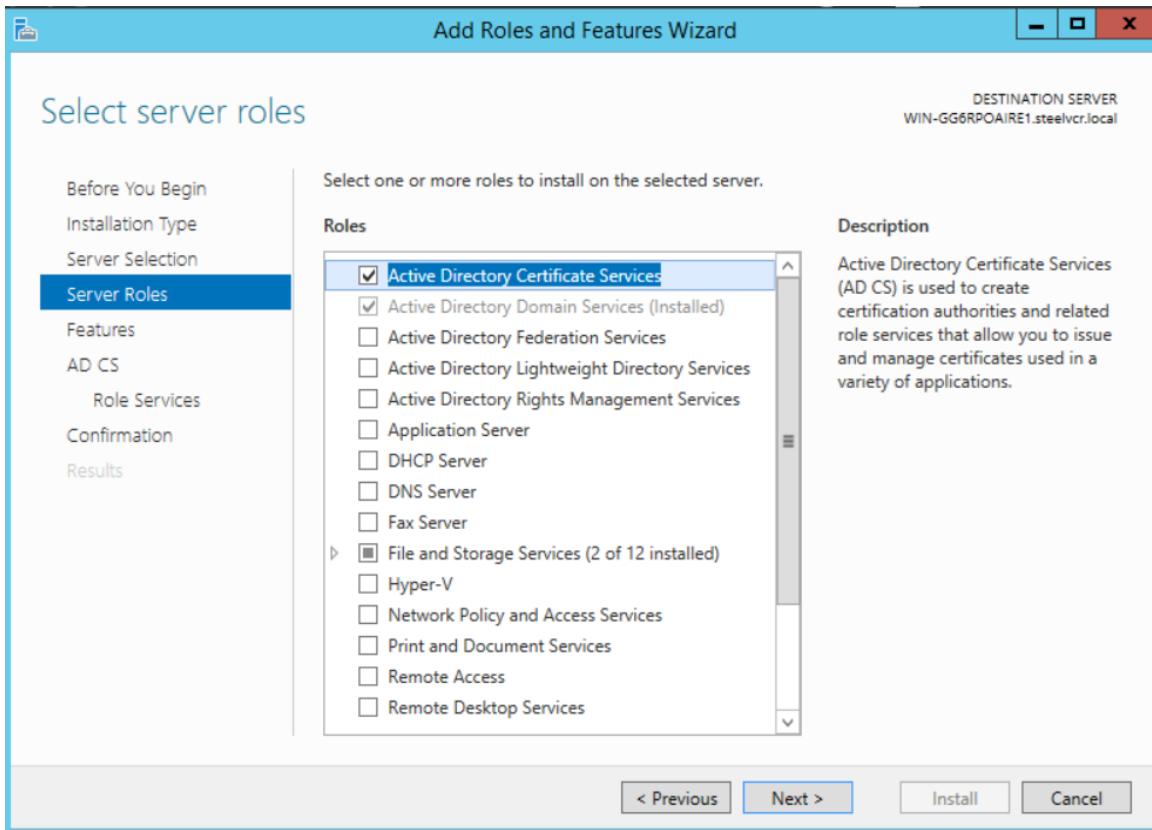


Click on “Active Directory Certificate Services” checkbox.

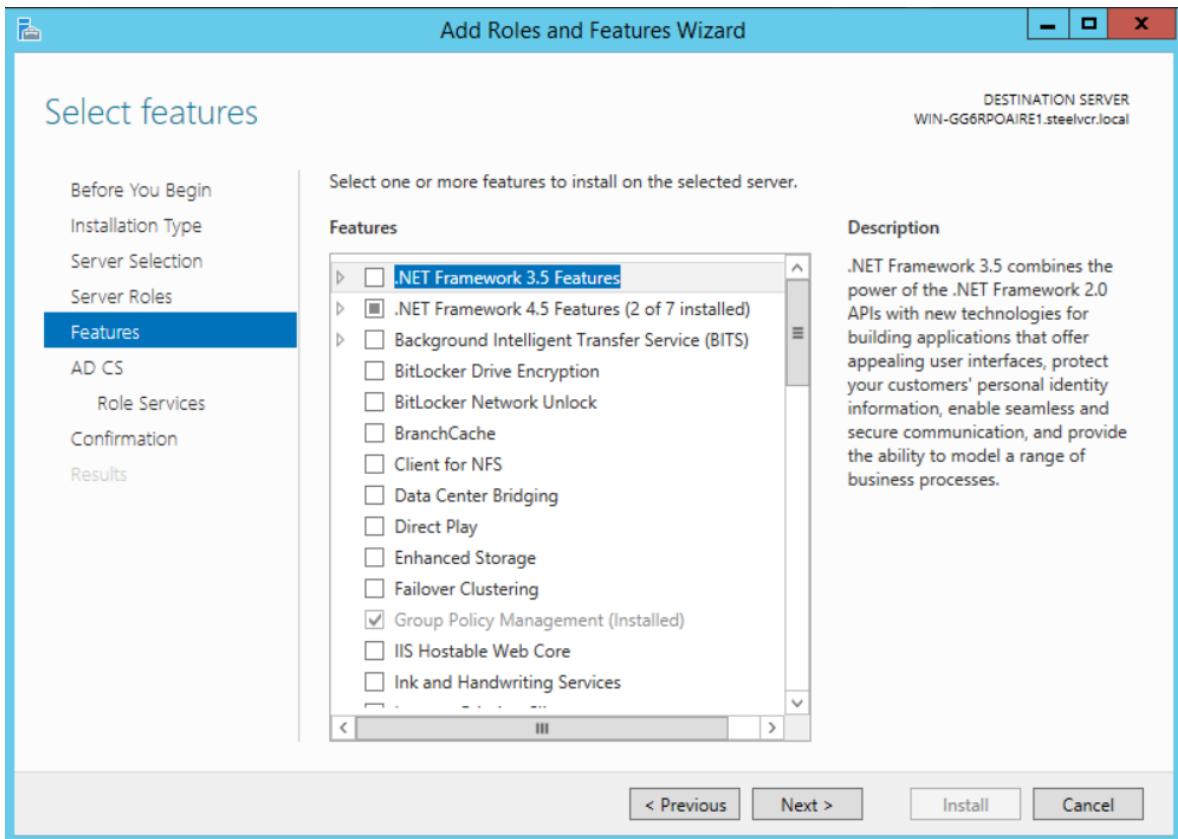


Click on “Add Features”.

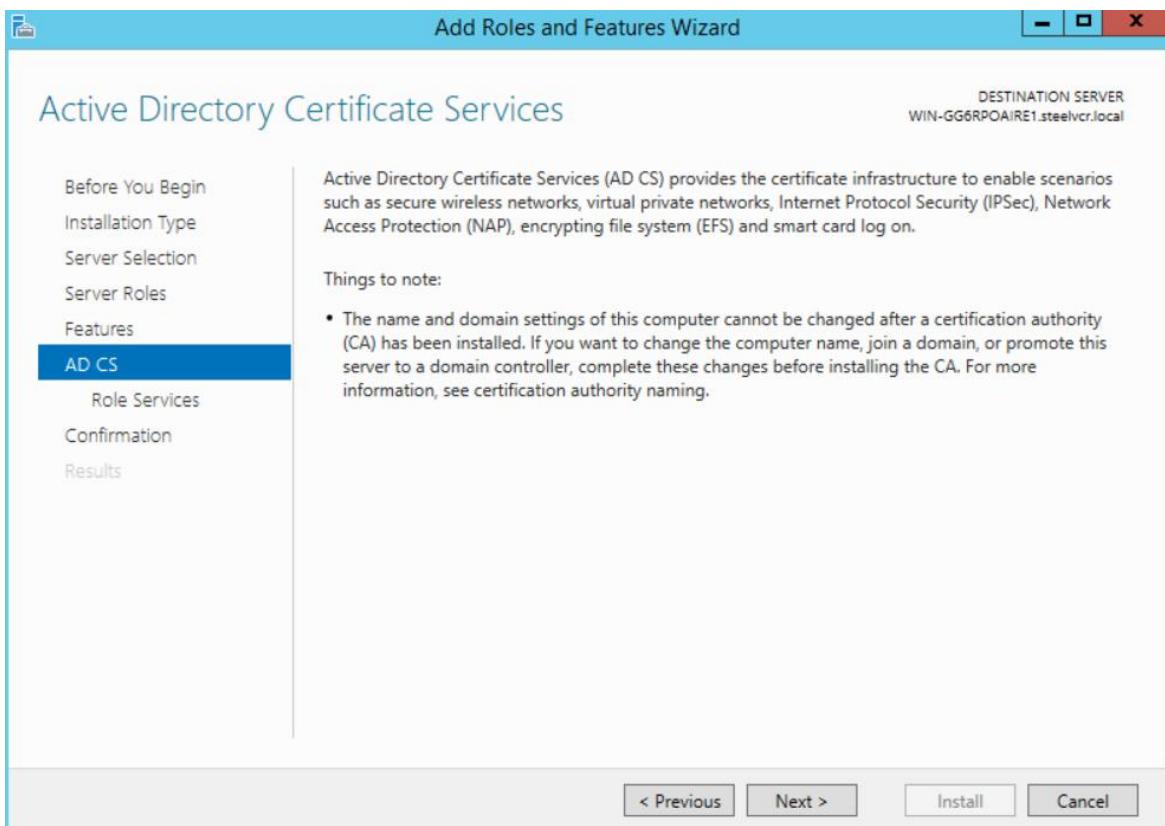
Keep “Include management tool (if applicable)” box checked.



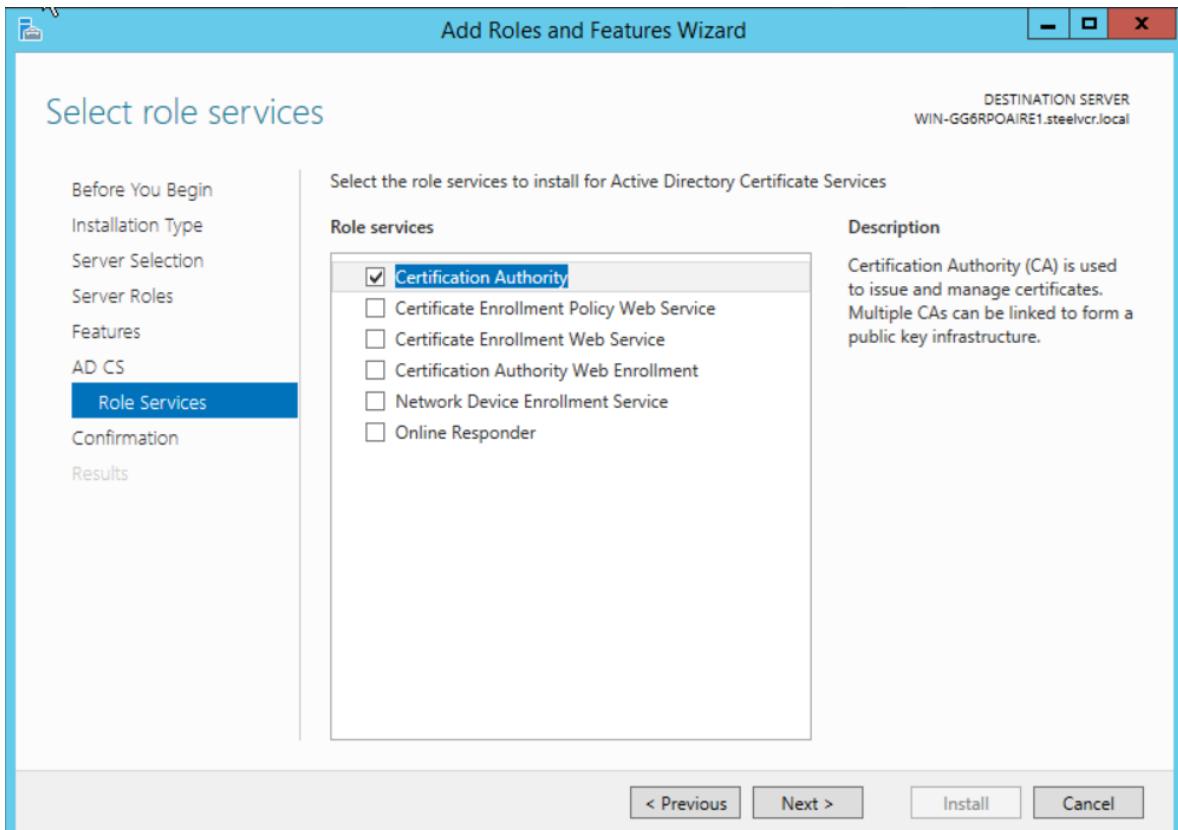
Click “Next”.



Click "Next" without changing anything.

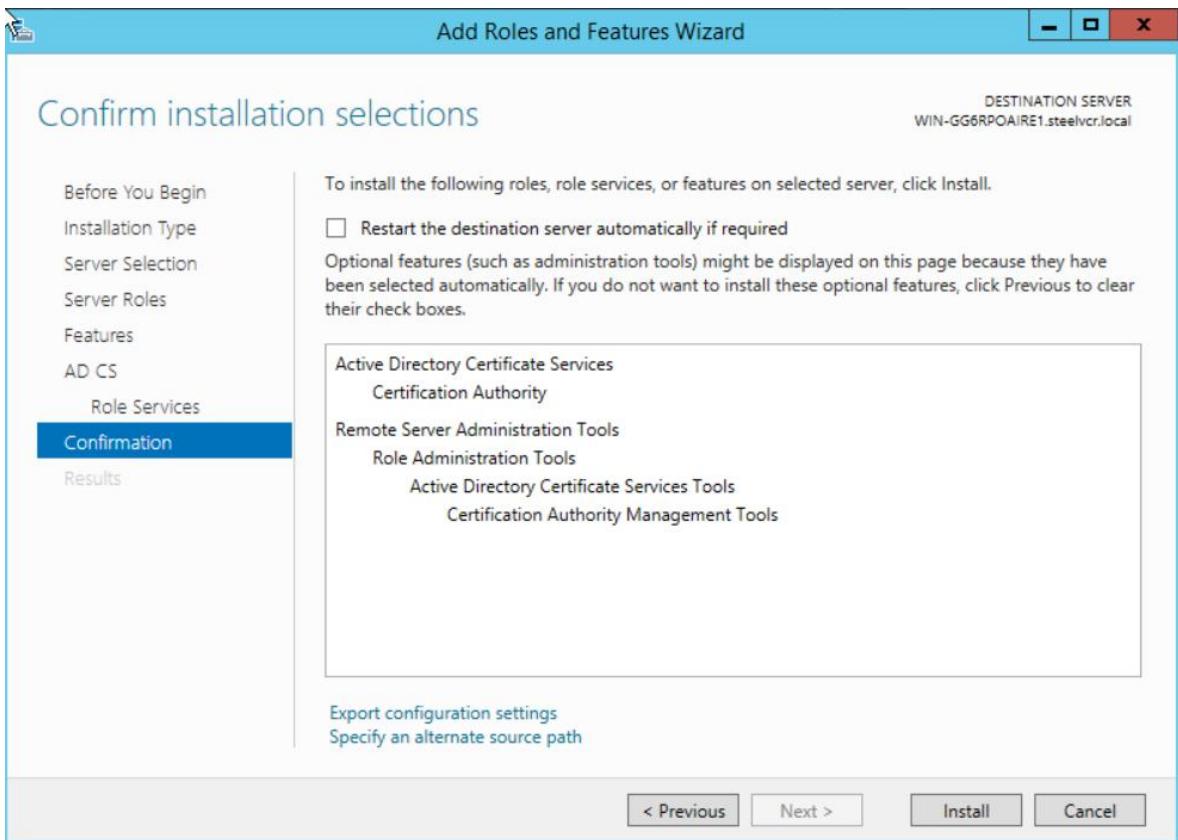


click "Next" again.

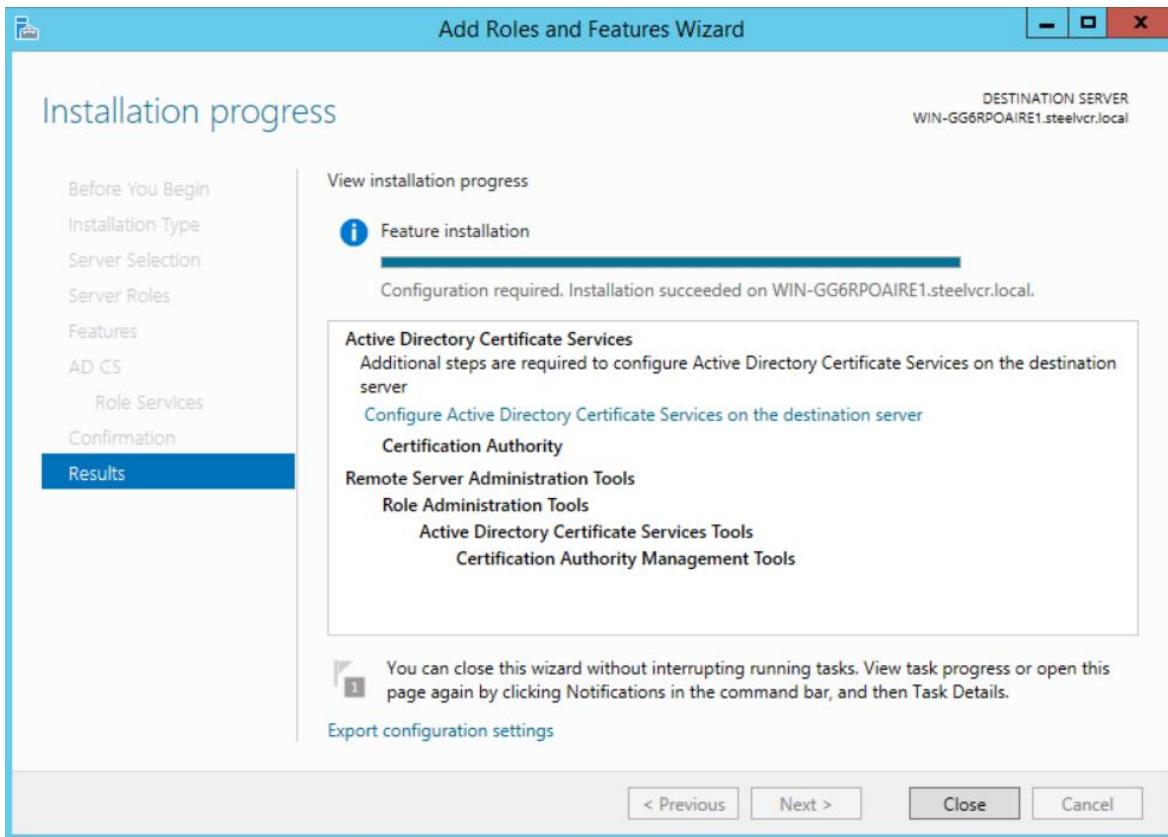


Keep "Certificate Authority" checked for issuing/managing certificates.

Leave everything else unchecked.

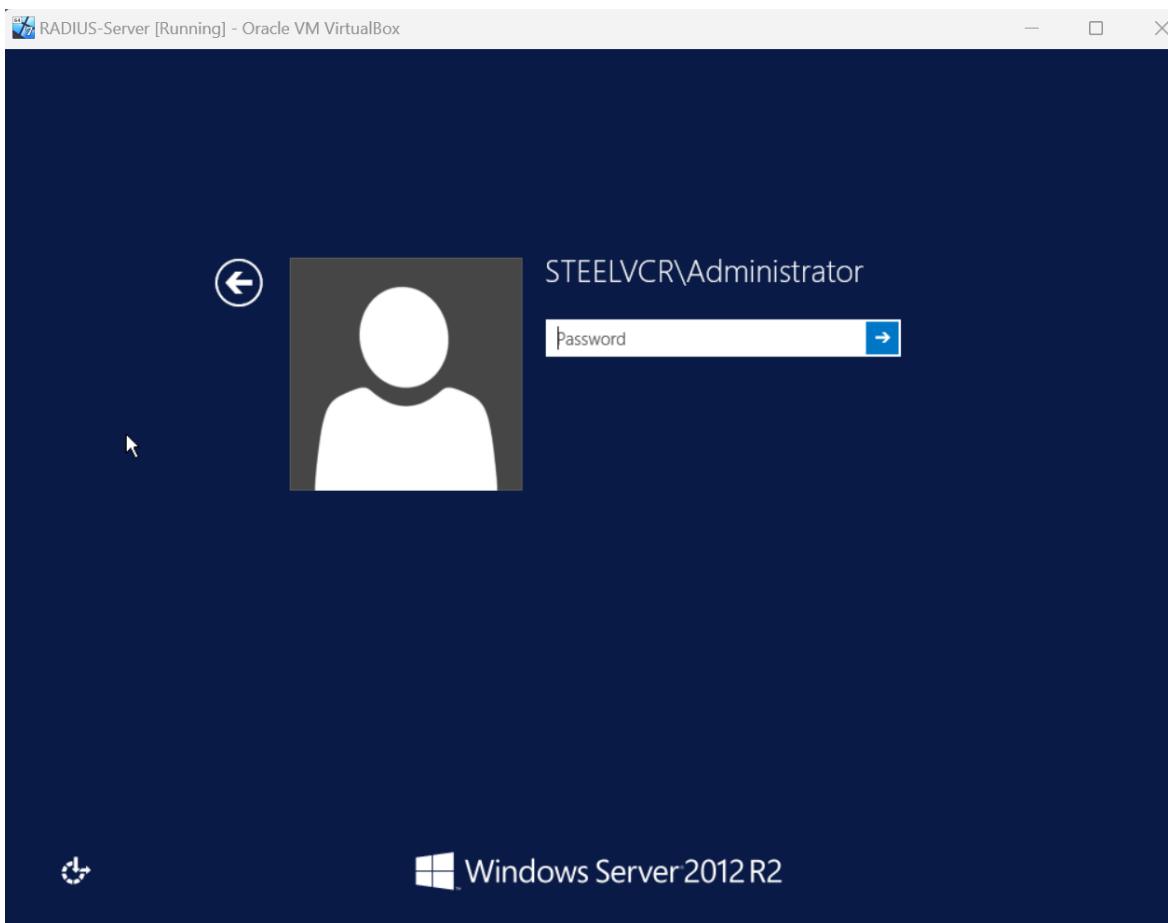


Click "Install" and leave the Restart box unchecked.

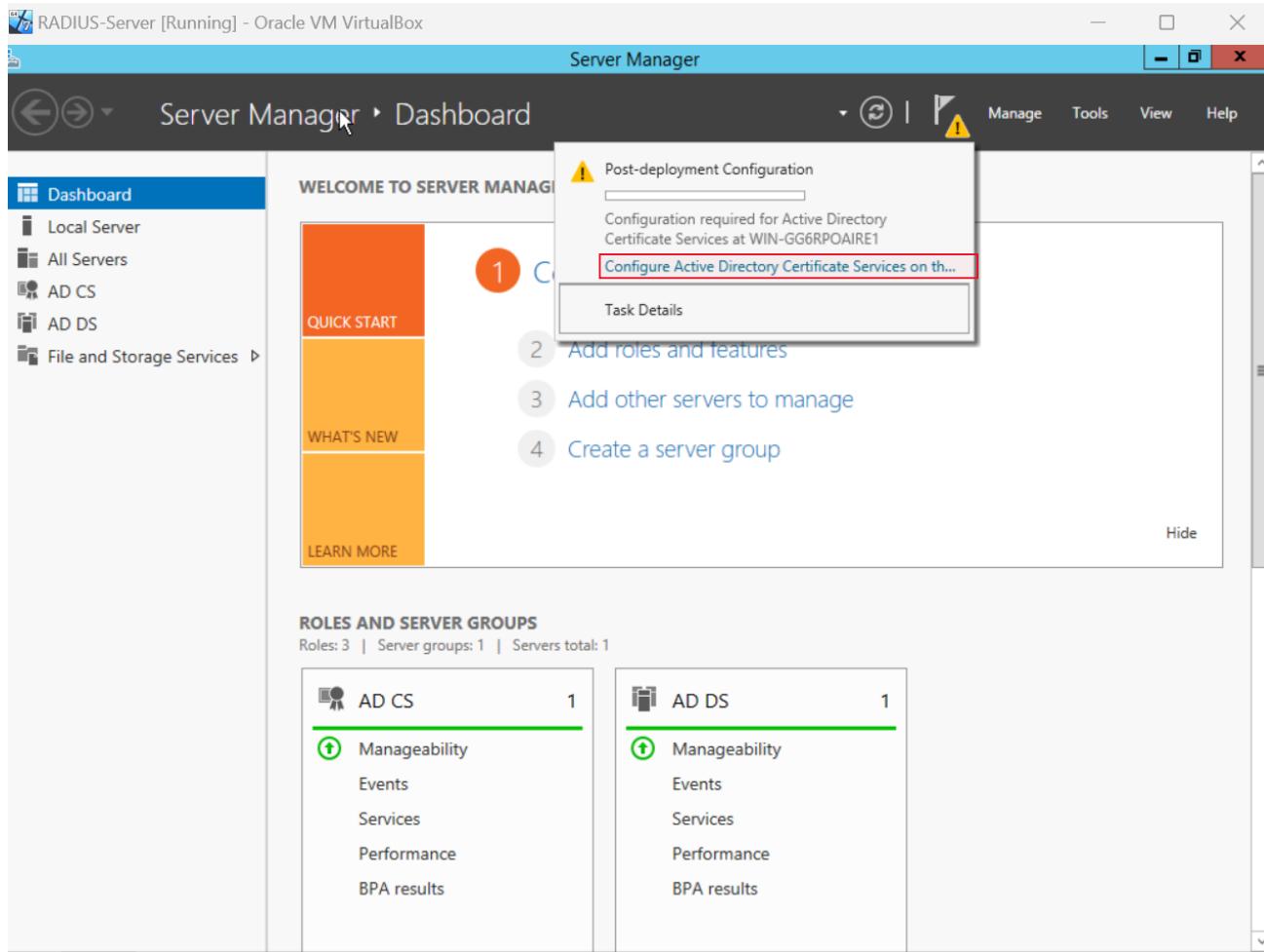


After install if successful click the “Close” button.

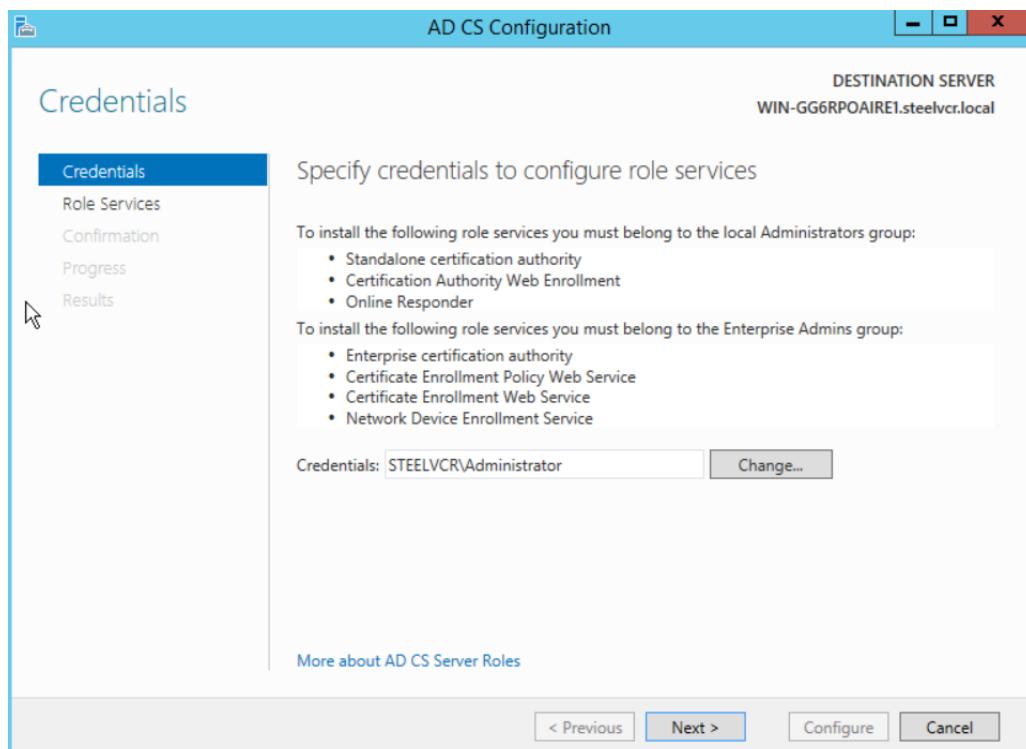
Do a manual reboot if one is not done automatically after this step.



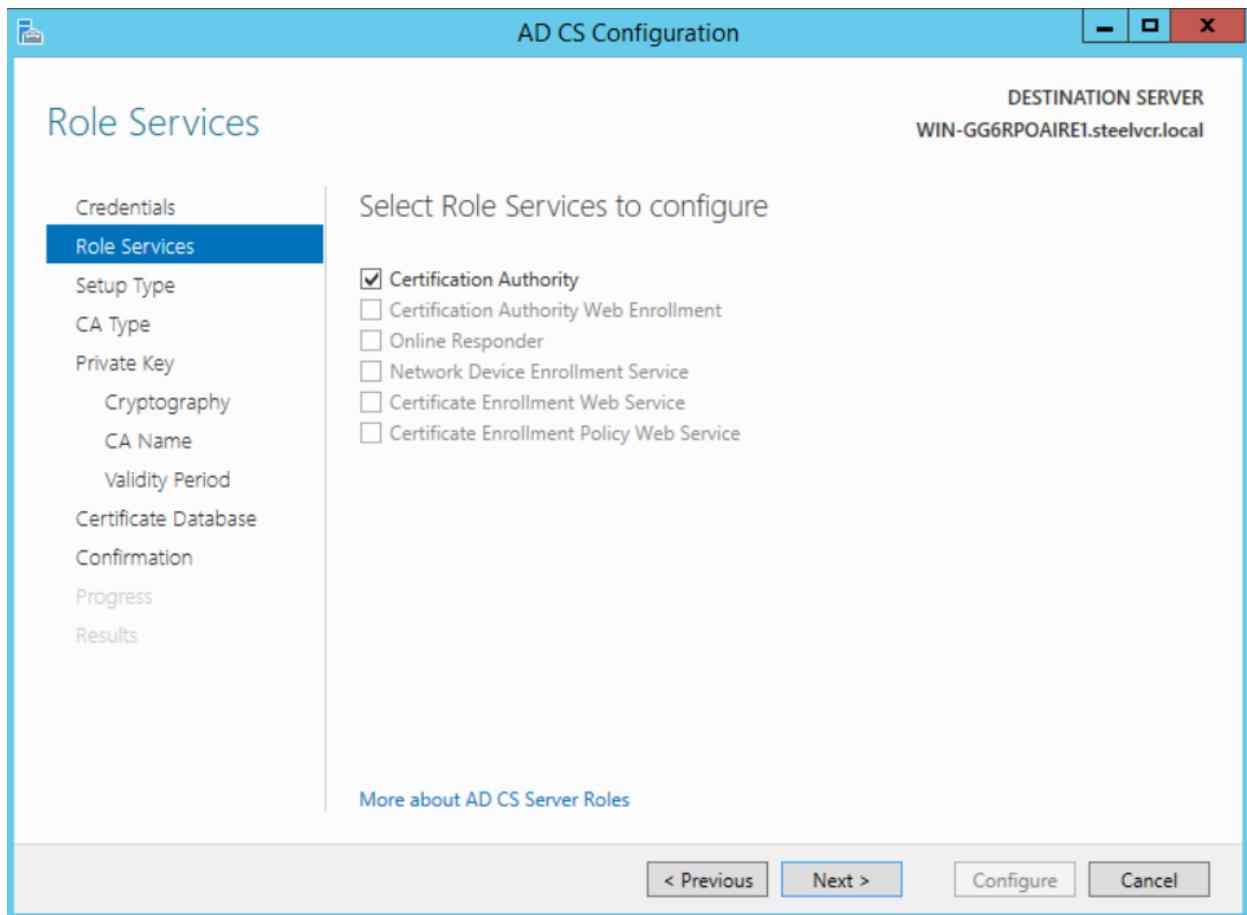
Log back in.



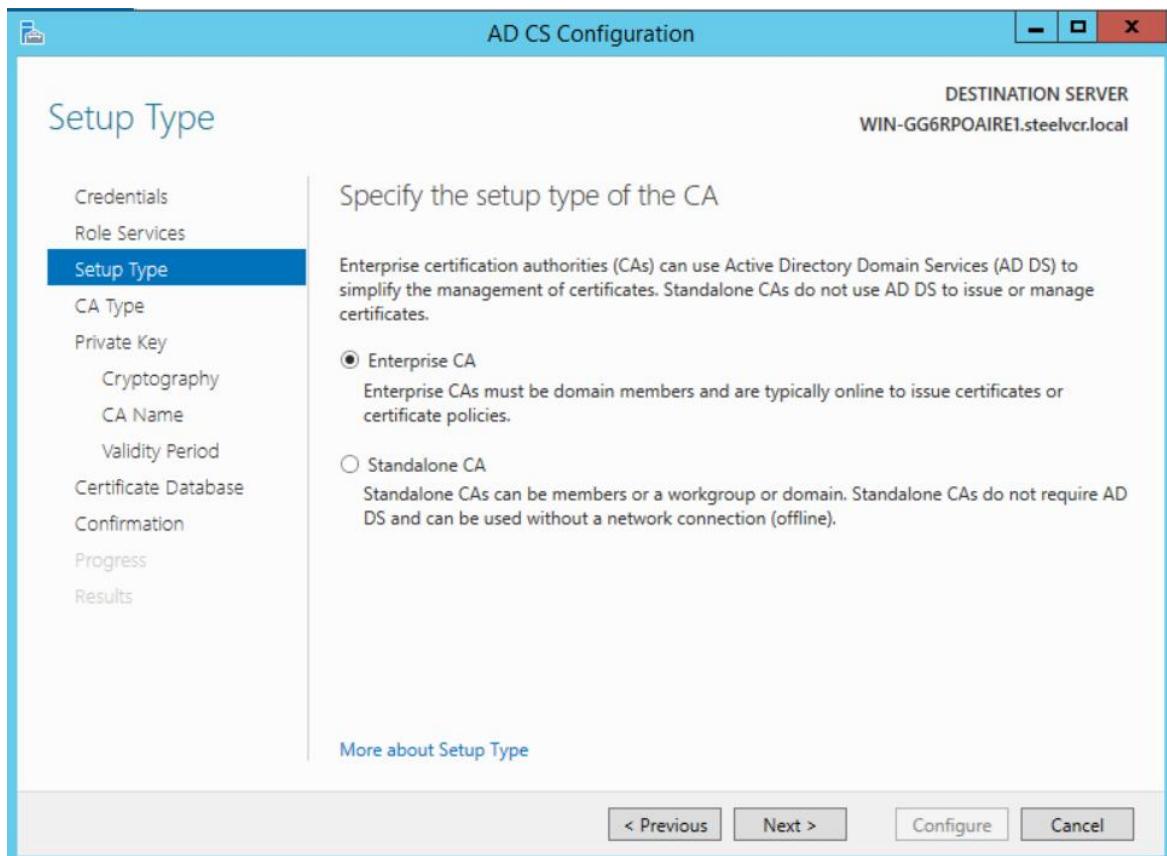
Click on notifications or the flag with yellow triangle and under “Post-deployment Configuration” click on “Configure Active Directory Certificate services on the destination server”.



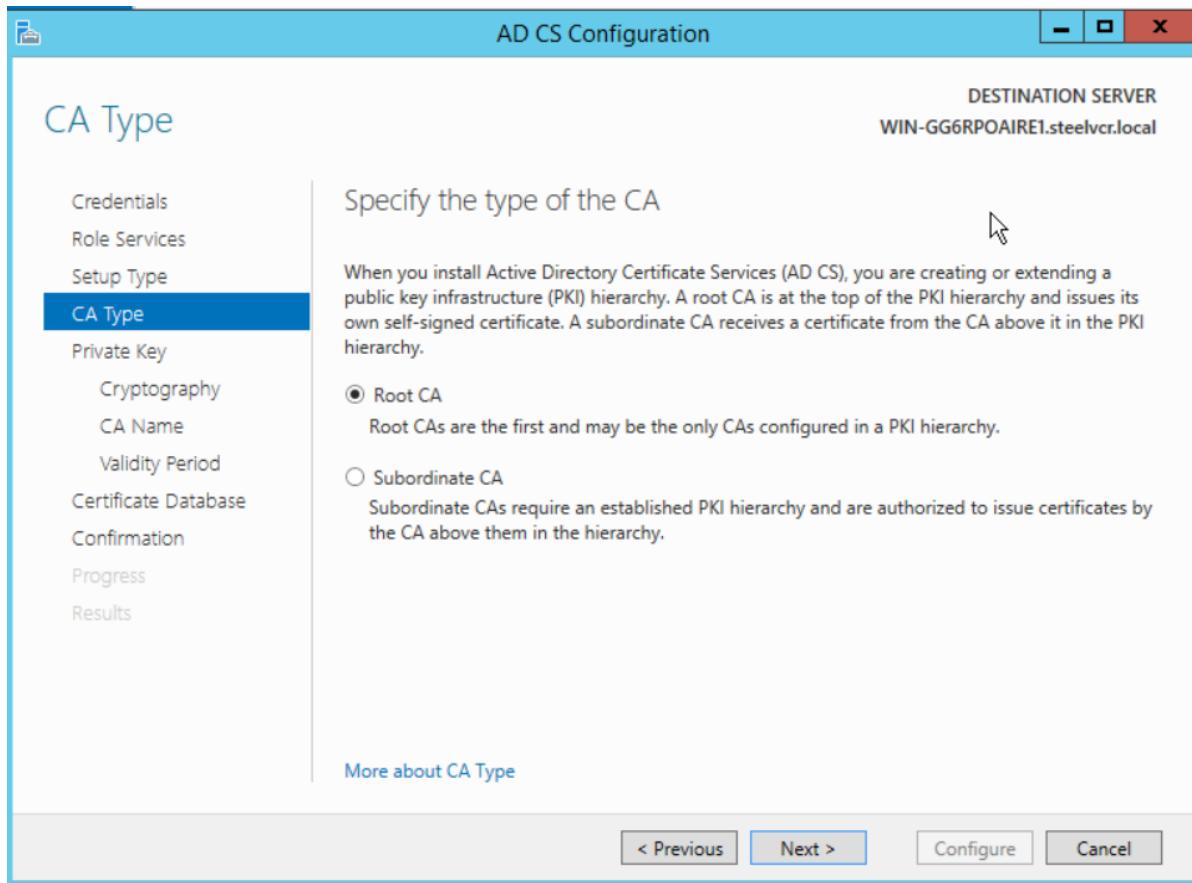
Click “Next” after credentials are confirmed.



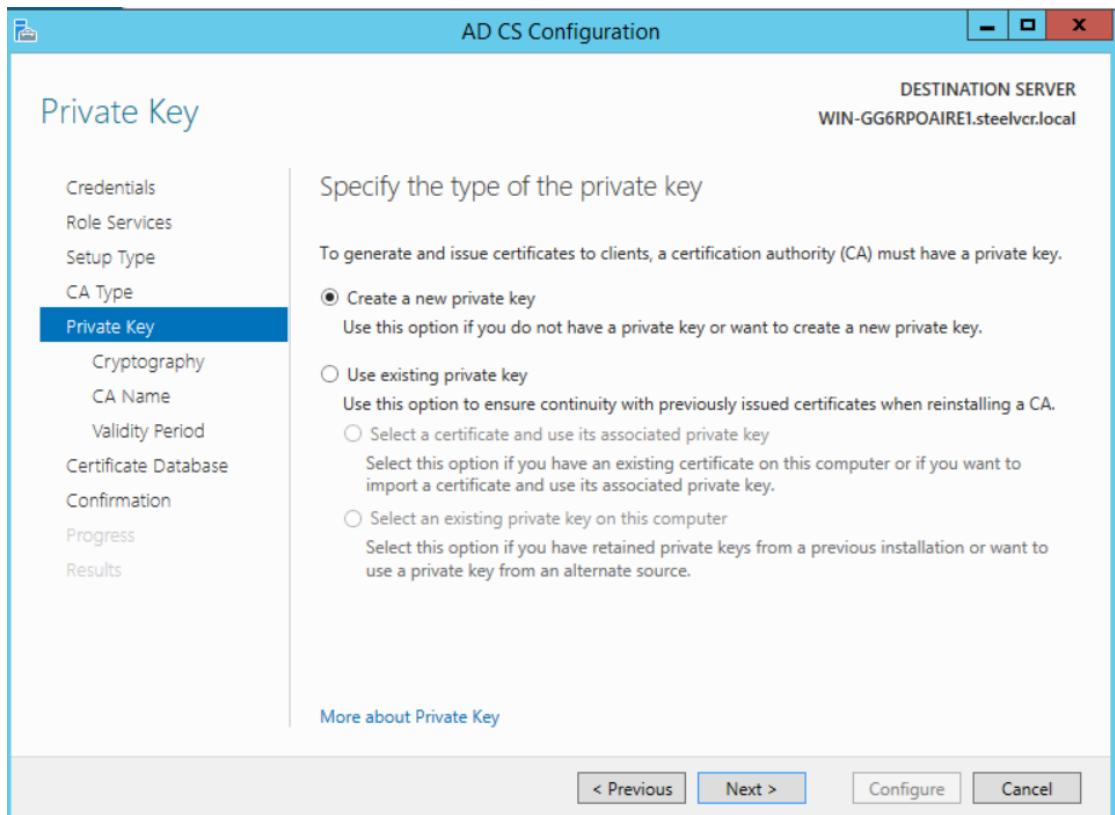
Click in the checkbox “Certificate Authority” as a role service to be configured, and click “Next”.



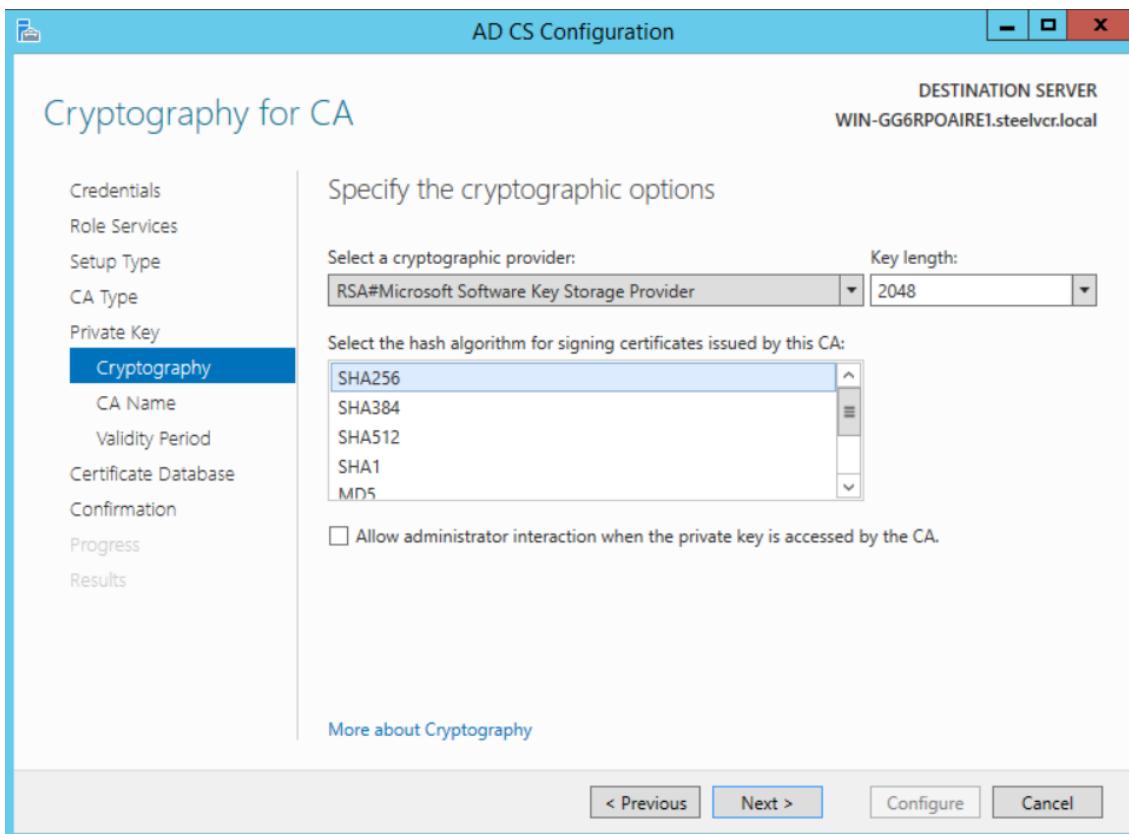
Keep “Enterprise CA” selected and click “Next”. Enterprise CA will issue certificates and their policies.



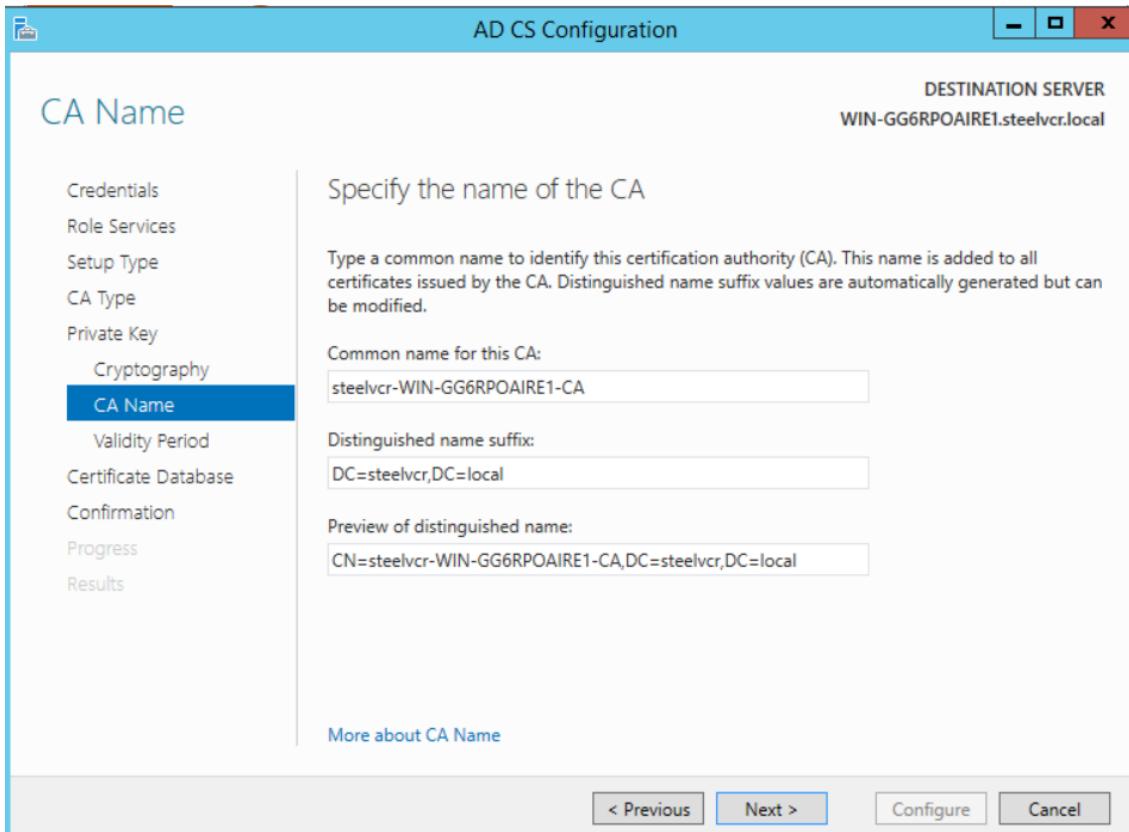
Keep “Root CA” selected so they are at top of PKI hierarchy.



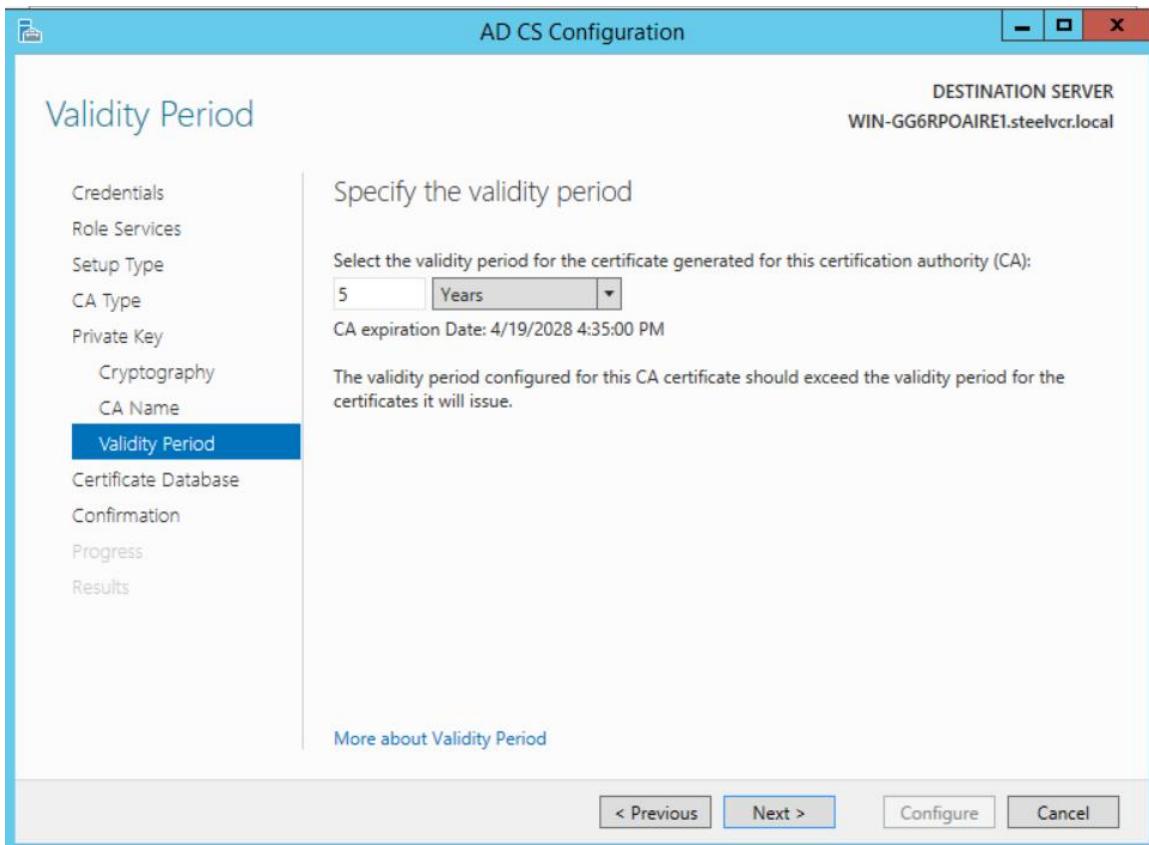
Select “Create a new private key” so a private key is created and click “Next”.



Keep “RSA#Microsoft Software Key Storage Provider” selected for crypto provider and select “SHA256” as hash algorithm for signing certificates.

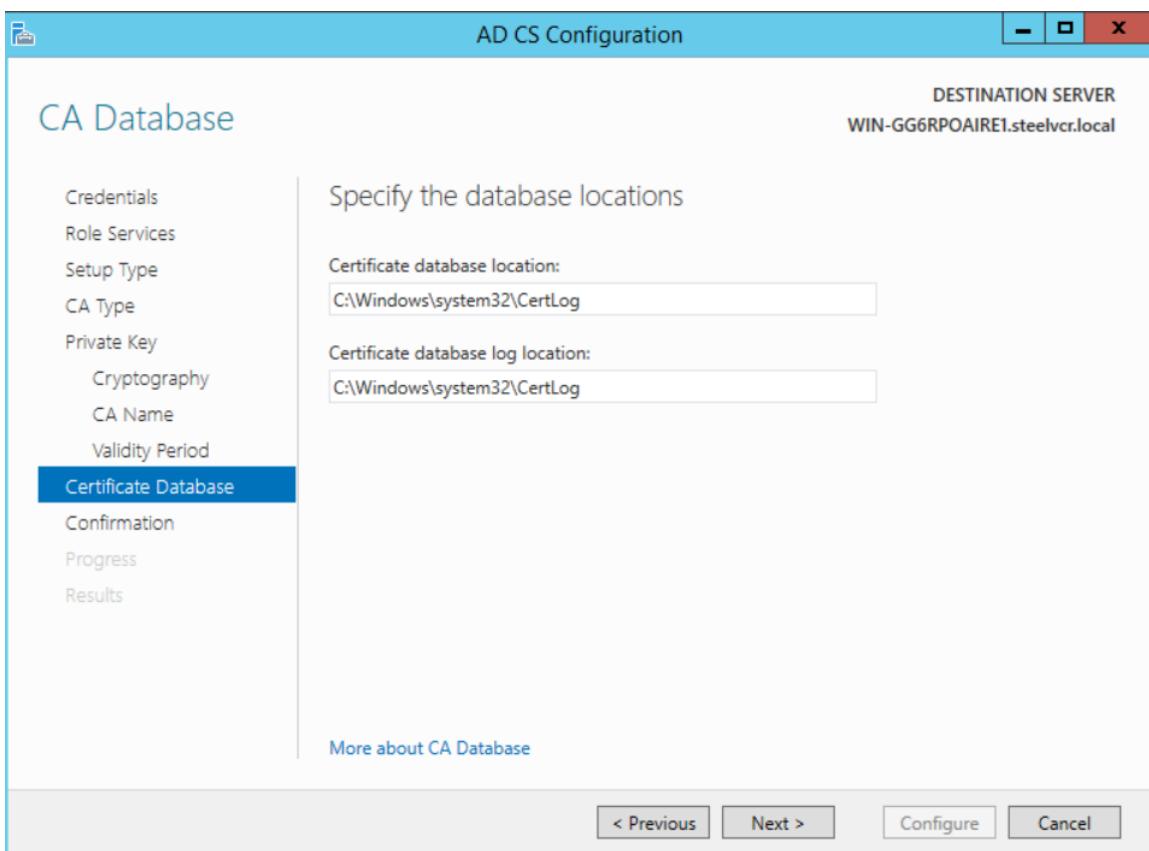


The “Common name for this CA”, “Distinguished name suffix”, and “Preview of distinguished name” should be filled in automatically. Click “Next”.

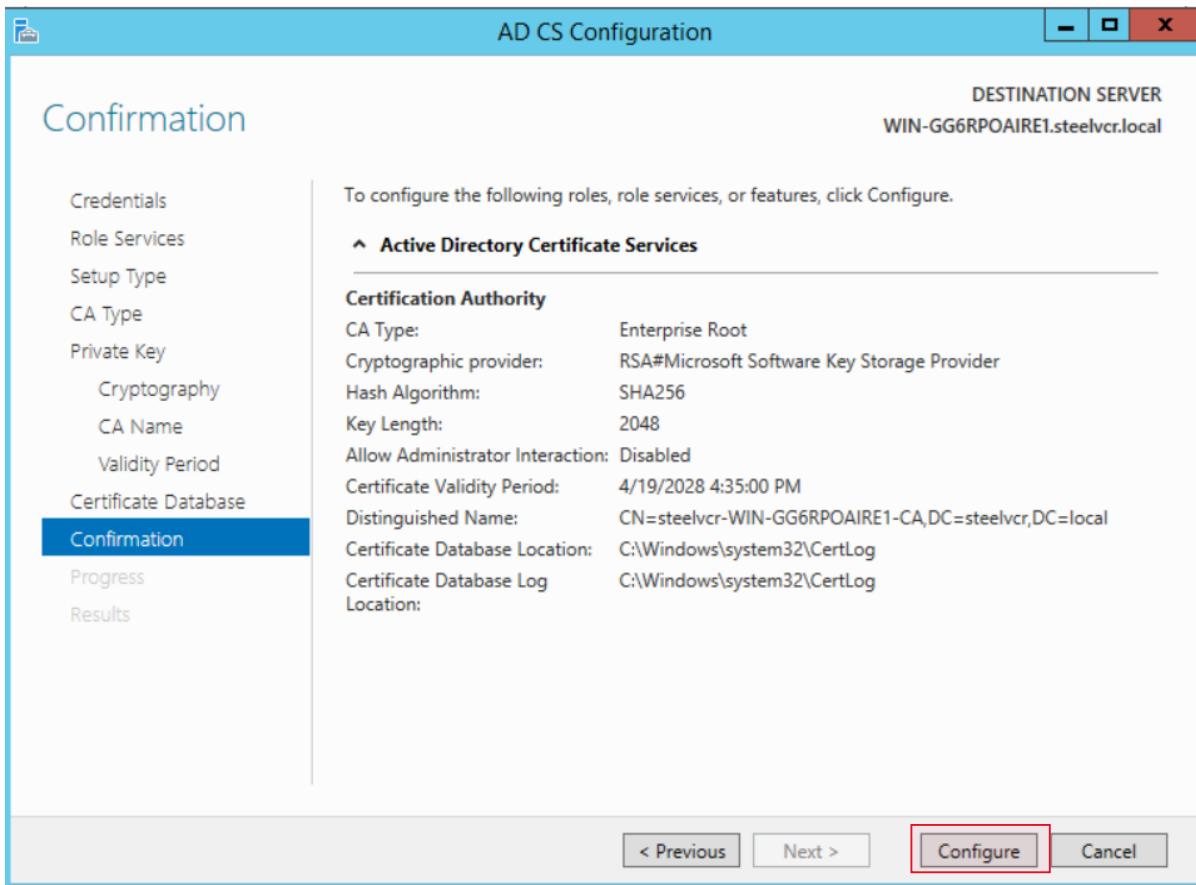


Keep or change validity period and click “Next”.

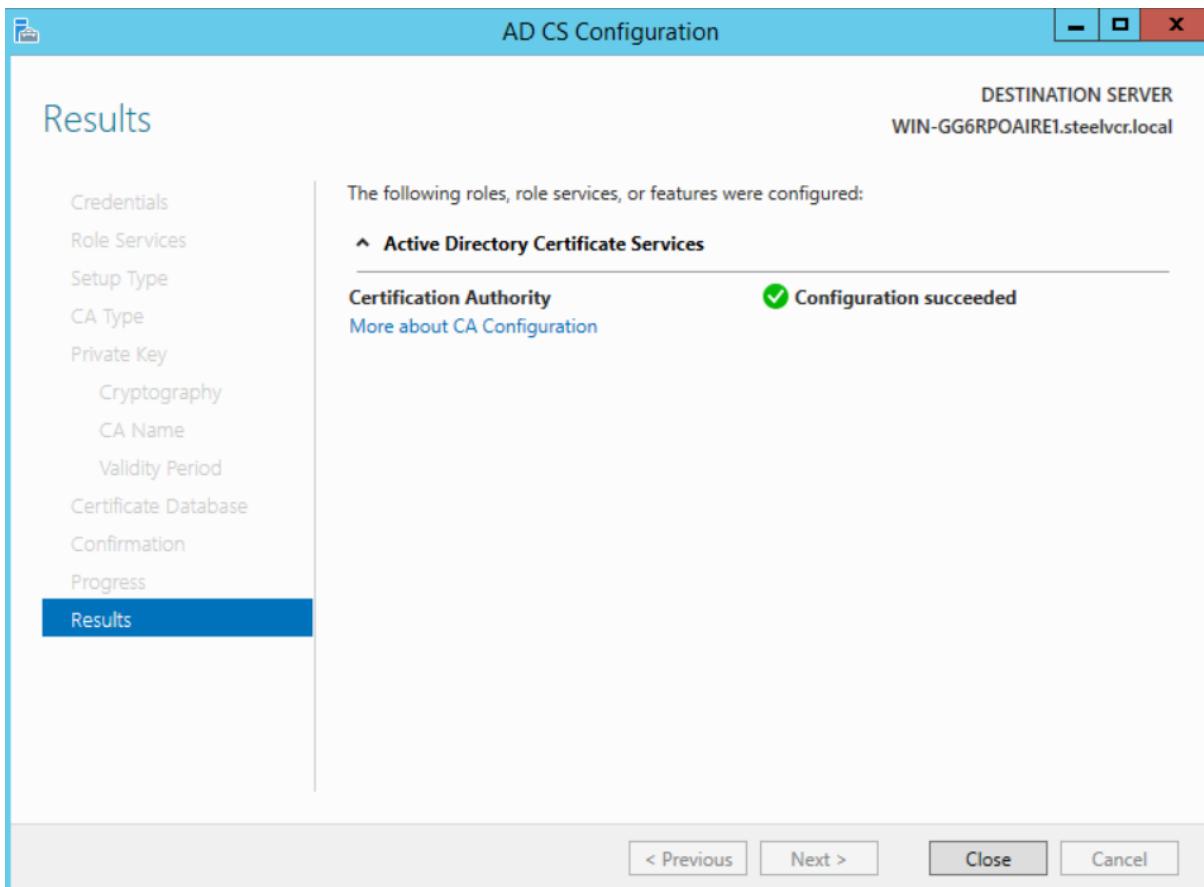
Can change “years” to “days”, “weeks”, or “months”.



Keep the locations for certificate database and log database. Click “Next”.



Review everything and click "Configure".



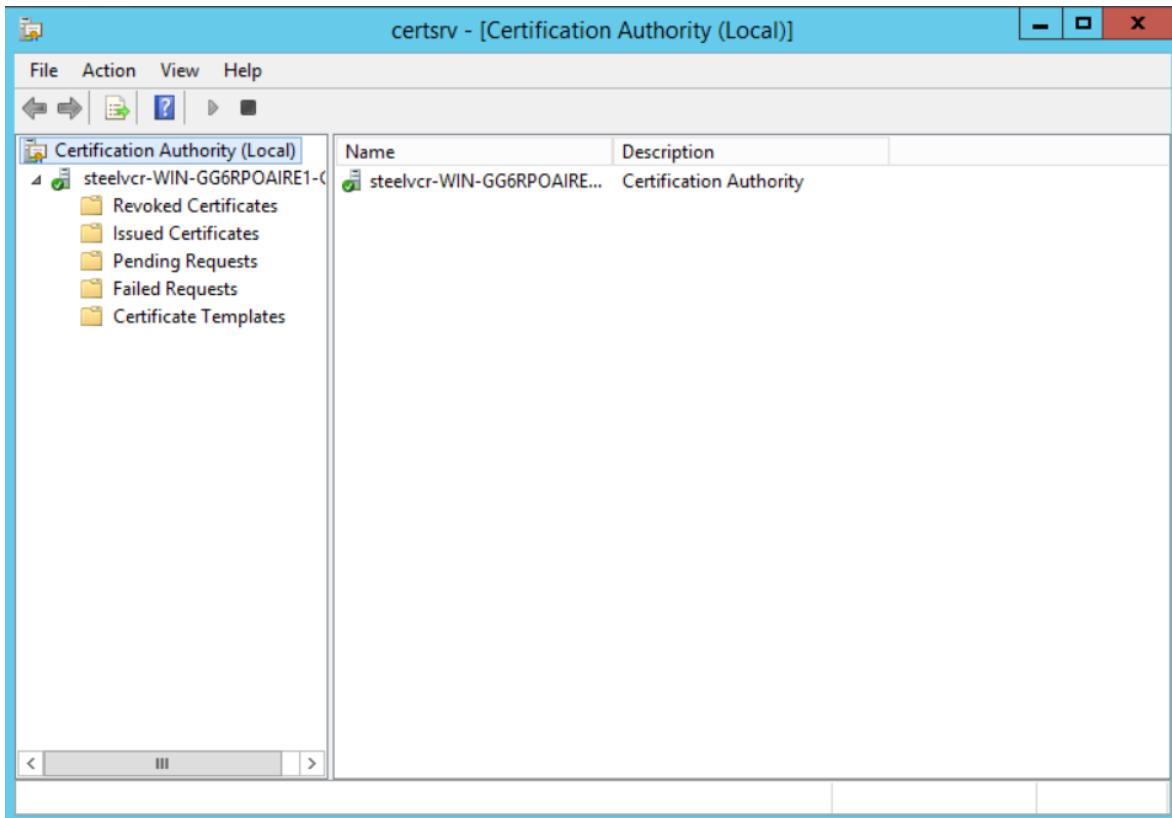
After a successful configuration click on "Close".

The screenshot shows the Windows Server Manager interface. On the left, a navigation pane lists several options: Dashboard, Local Server, All Servers, **AD CS** (which is selected and highlighted in blue), AD DS, and File and Storage Services. The main content area is divided into two sections: 'SERVERS' and 'EVENTS'.  
**Servers:** A table titled 'All servers | 1 total' shows one entry: WIN-GG6RPOAIRE1, 192.168.1.35, Online - Performance counters not started. The table has columns: Server Name, IPv4 Address, Manageability, Last Update, and Windows Activation.  
**Events:** A table titled 'All events | 1 total' shows one entry: WIN-GG6RPOAIRE1, ID 103, Warning, Microsoft-Windows-CertificationAuthority, Application, Date and Time 4/19/2023 5:05:50 PM. The table has columns: Server Name, ID, Severity, Source, Log, and Date and Time.

In Server Manager click on “AD DS” on left-hand side.

This screenshot is similar to the previous one, but the 'Tools' menu in the top right corner is now open. The 'Certification Authority' option is highlighted with a red box. Other visible items in the 'Tools' menu include: Active Directory Domains and Trusts, Active Directory Module for Windows PowerShell, Active Directory Sites and Services, Active Directory Users and Computers, ADSI Edit, Component Services, Computer Management, Defragment and Optimize Drives, Event Viewer, Group Policy Management, iSCSI Initiator, Local Security Policy, ODBC Data Sources (32-bit), ODBC Data Sources (64-bit), Performance Monitor, Resource Monitor, Security Configuration Wizard, Services, System Configuration, System Information, Task Scheduler, Windows Firewall with Advanced Security, Windows Memory Diagnostic, Windows PowerShell, Windows PowerShell (x86), Windows PowerShell ISE, and Windows PowerShell ISE (x86).

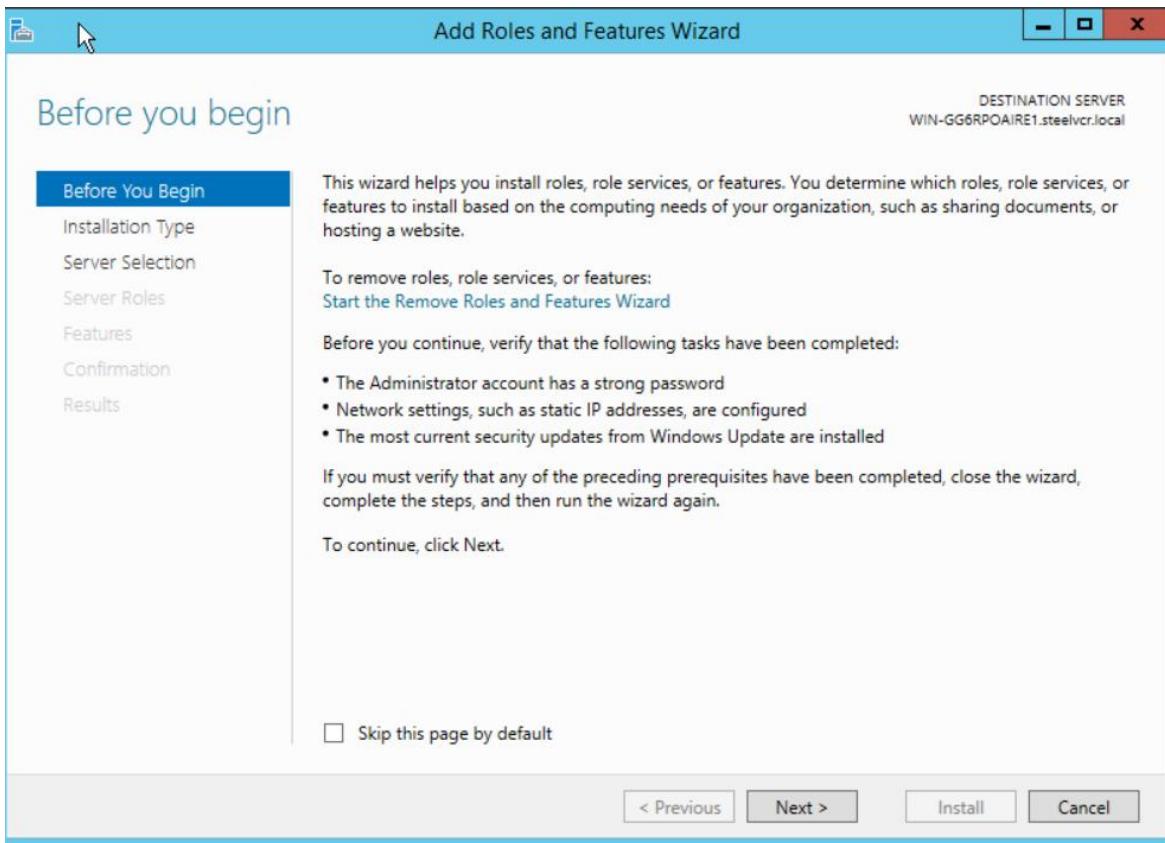
While in “AD CS” (left side column), Click on “Tools” in upper right-hand corner and then click on “Certificate Authority”.



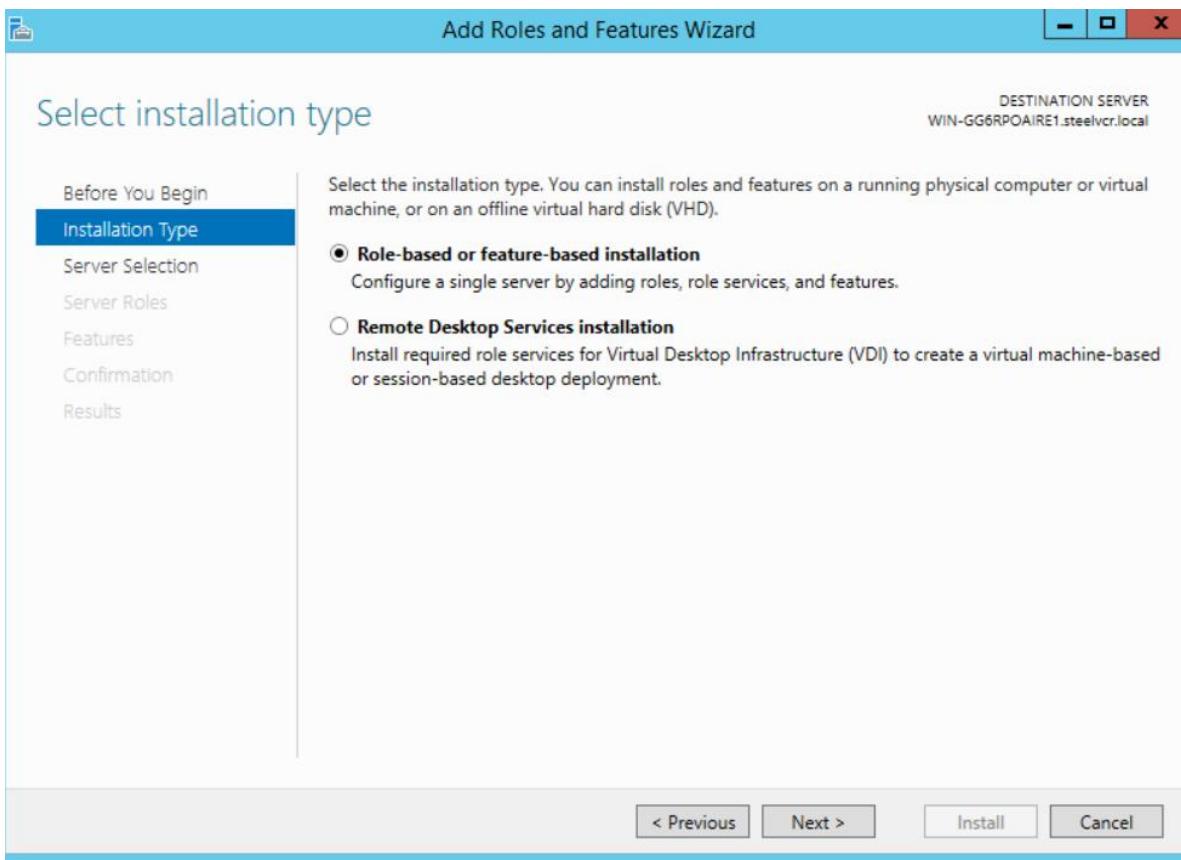
This is the CA/certificate authority that we just installed. Exit out of this.

The screenshot shows the Windows Server Manager window titled "Server Manager". The left navigation pane has "AD CS" selected. The main area shows the "Servers" section with one server listed: "WIN-GG6RPOAIRE1". The top ribbon bar has "Manage" selected. A context menu is open over the server entry, with the "Add Roles and Features" option highlighted with a red box.

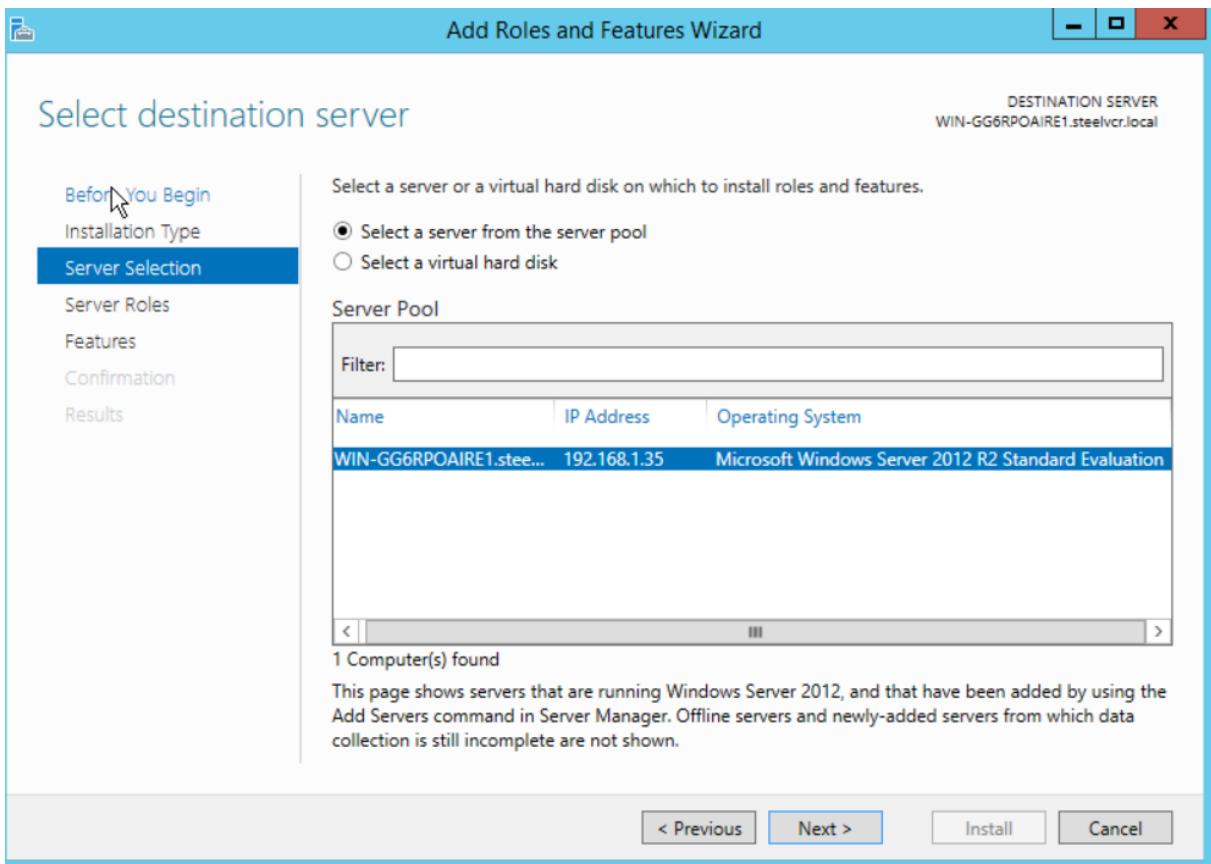
In "AD CS" go to "Manage" in top right corner and click on "Add Roles and Features".



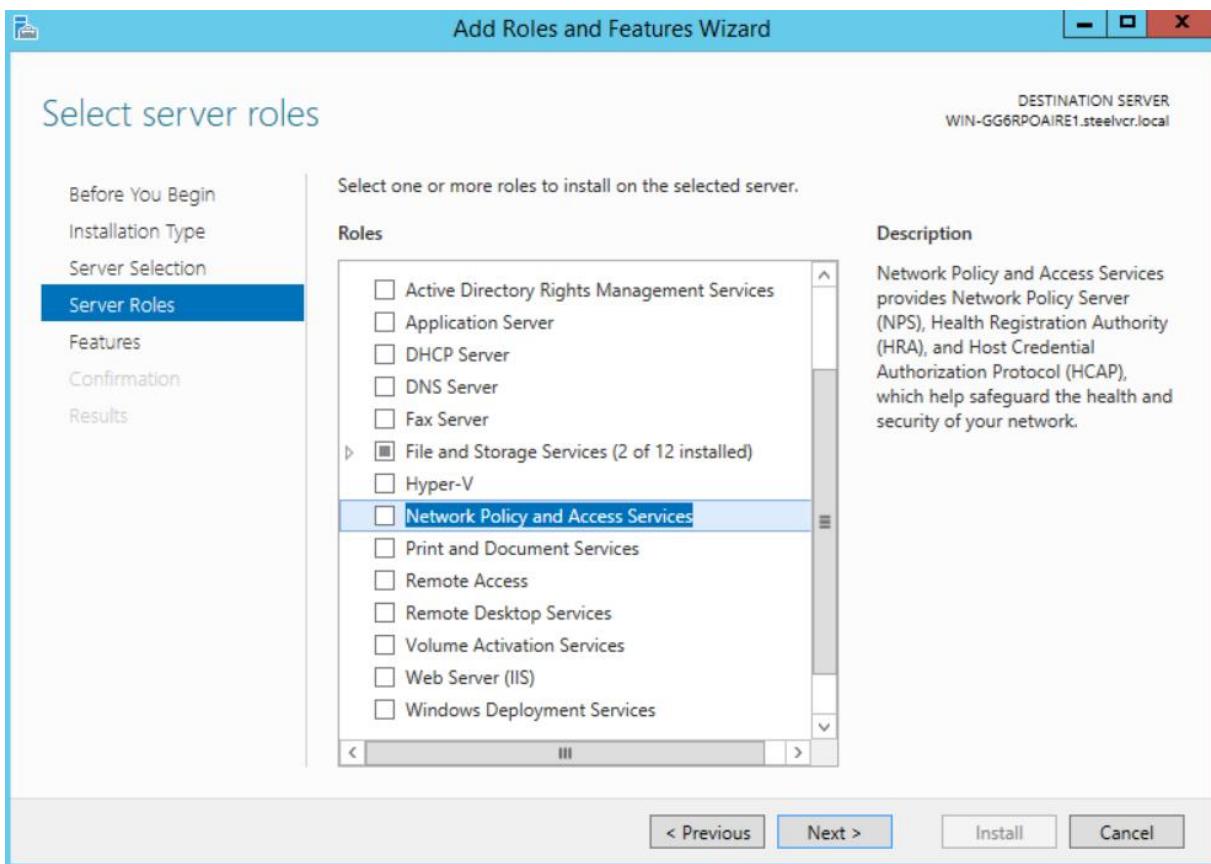
Read and click "Next".



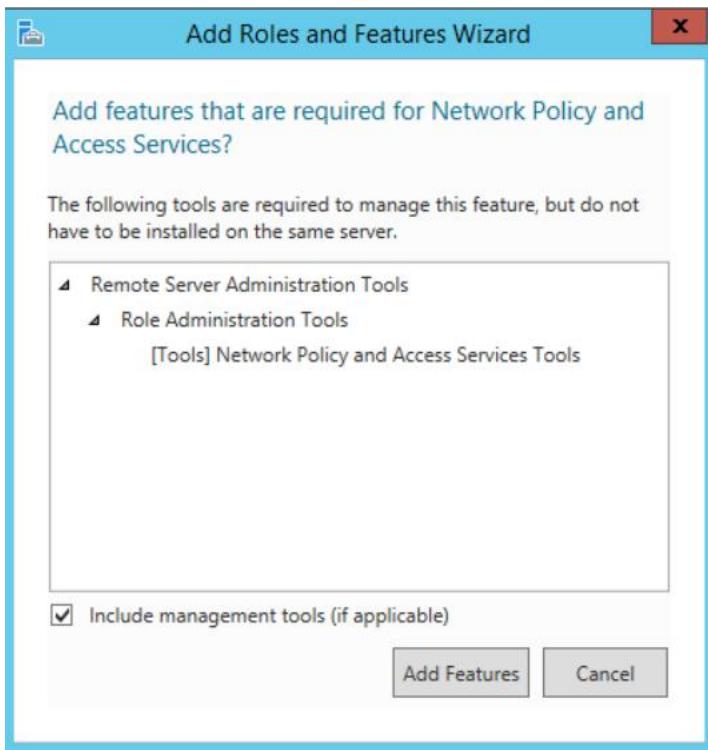
Keep "Role-based or feature-based installations" selected.



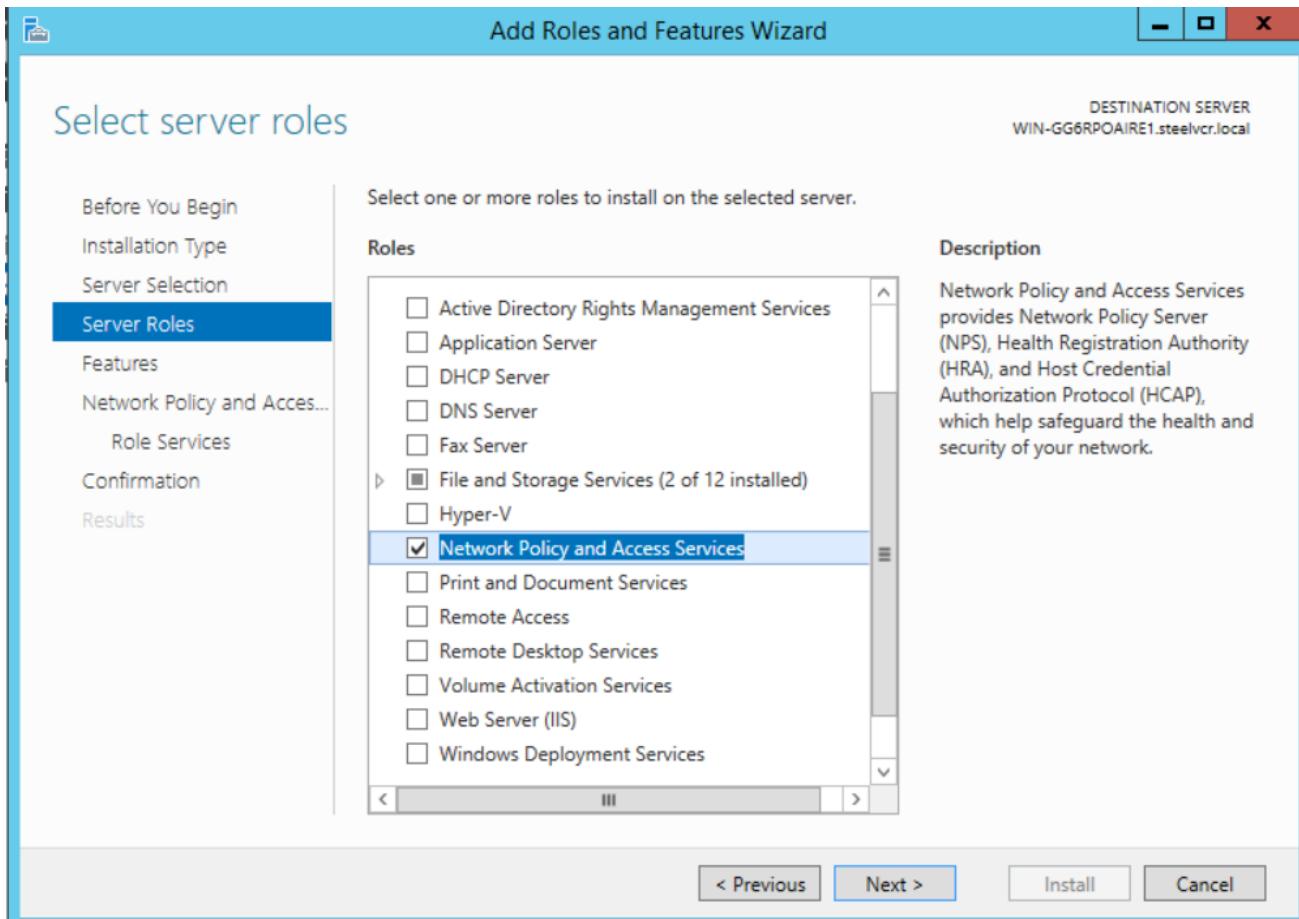
Keep server selected and click "Next".



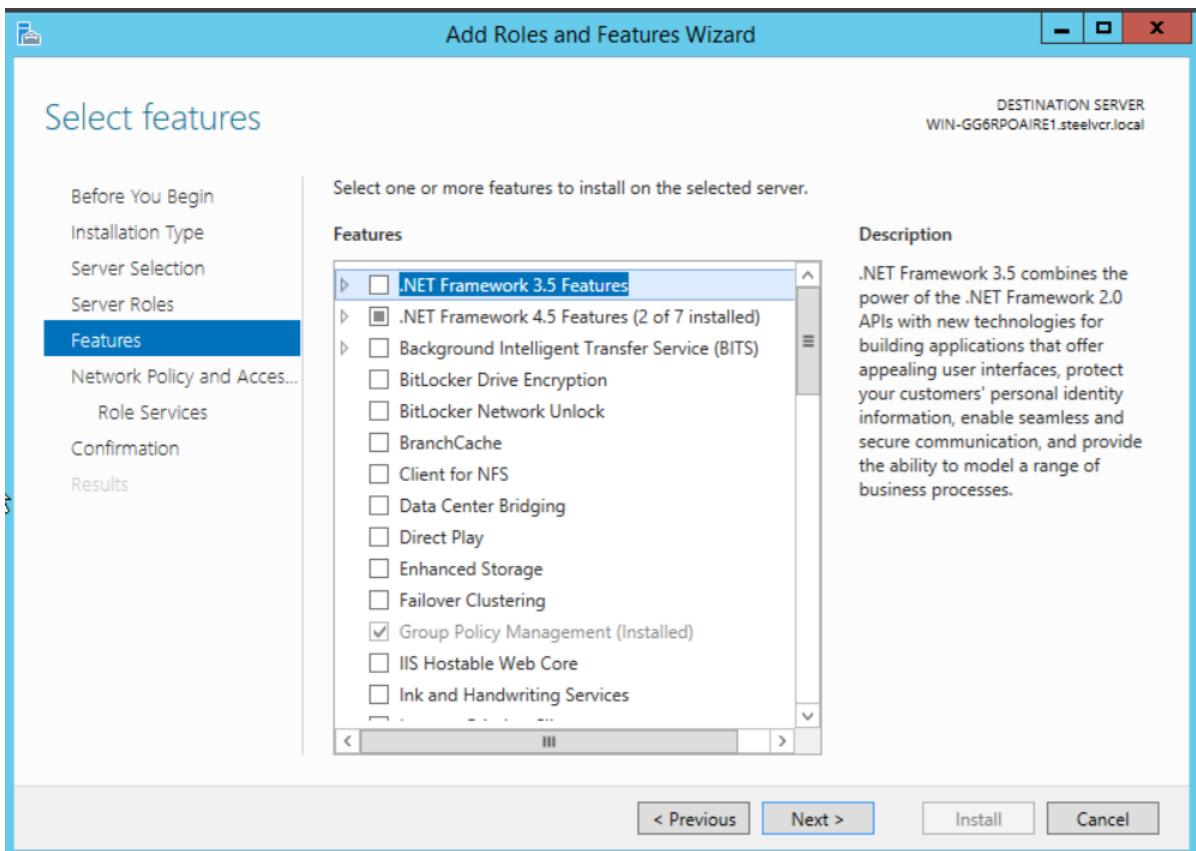
Click on checkbox for "Network Policy and Access Services".



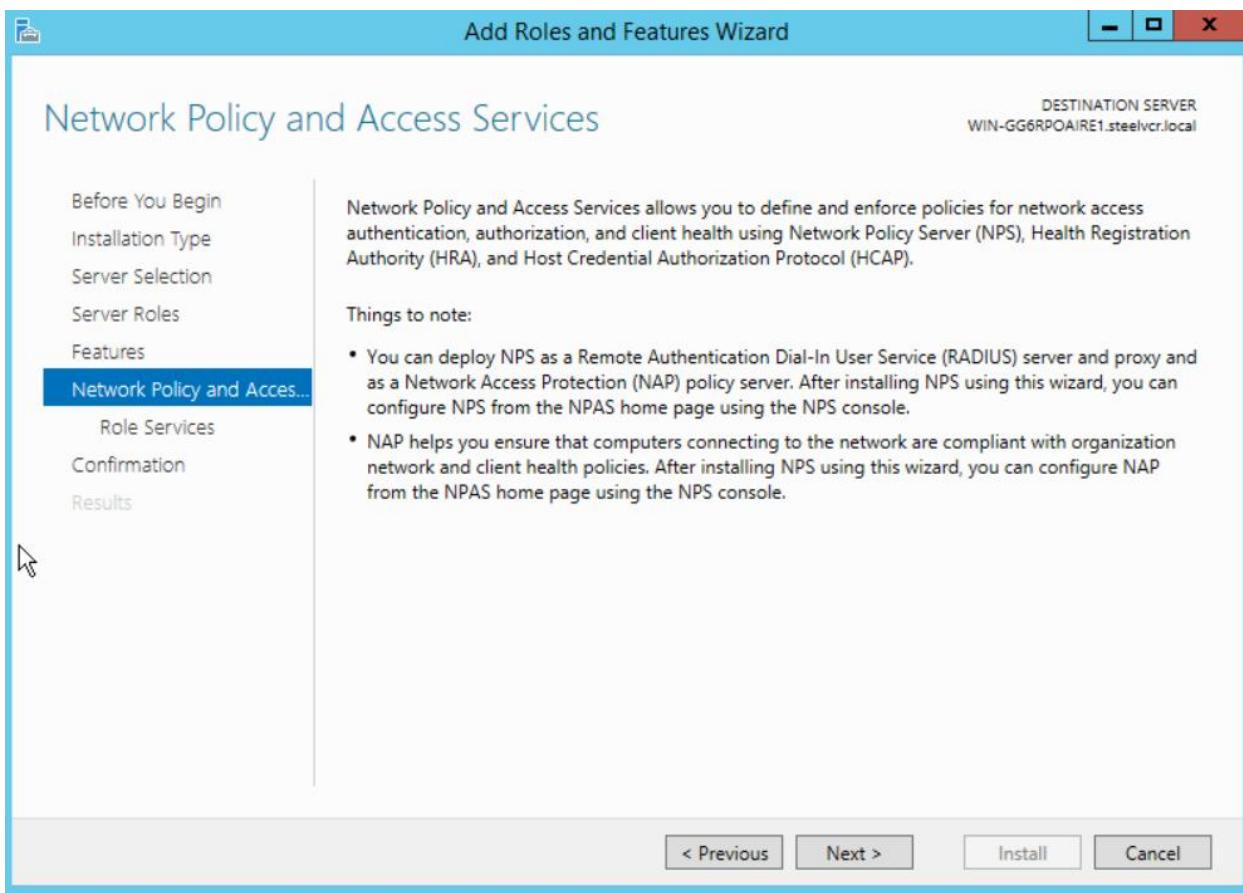
Click on “Add Features”. (This feature is for network security/protection)



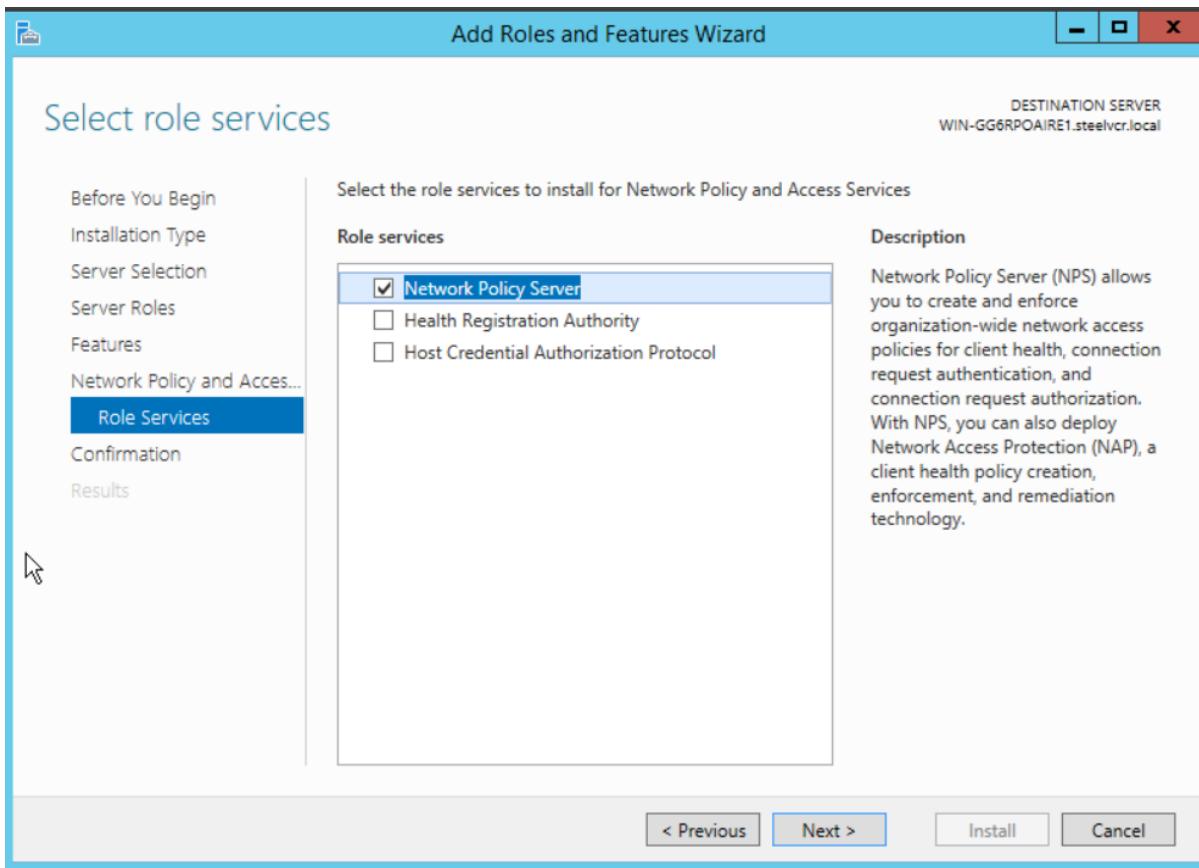
Click “Next”.



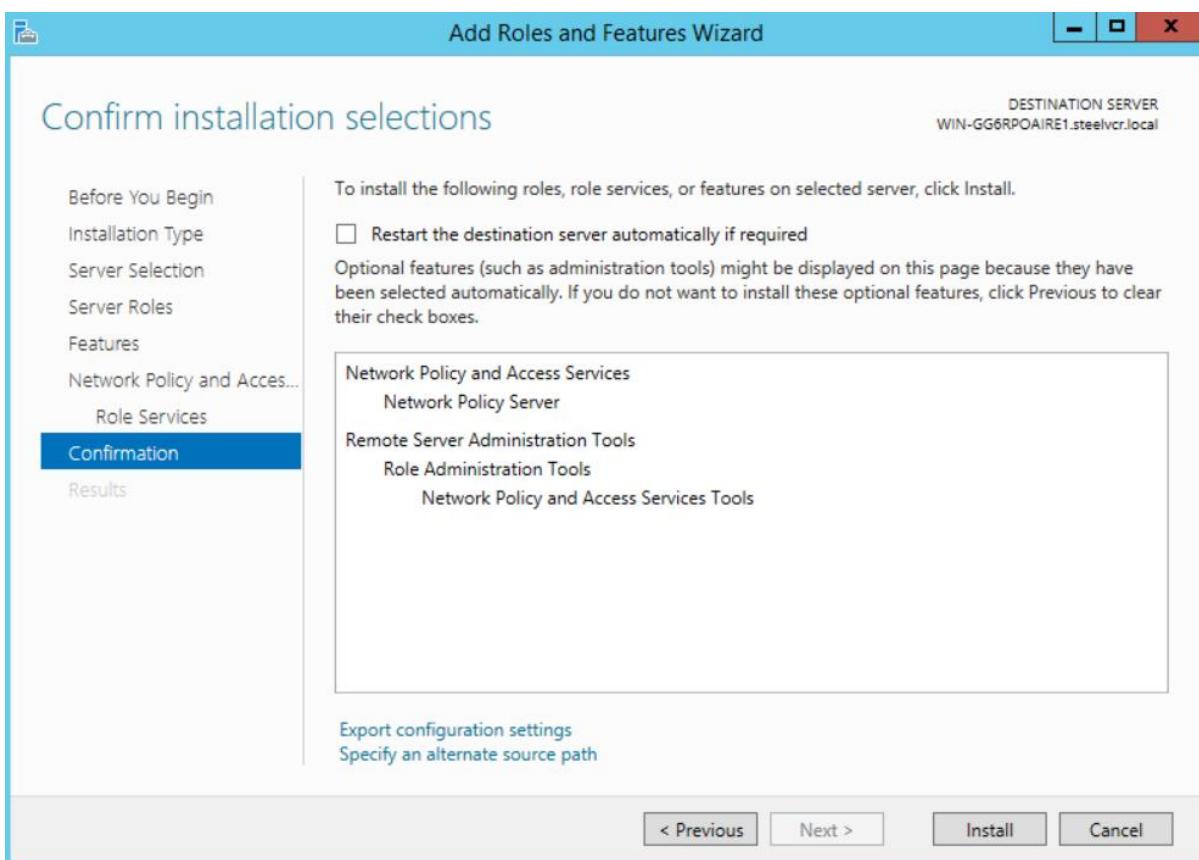
Don't check anything here and click "Next".



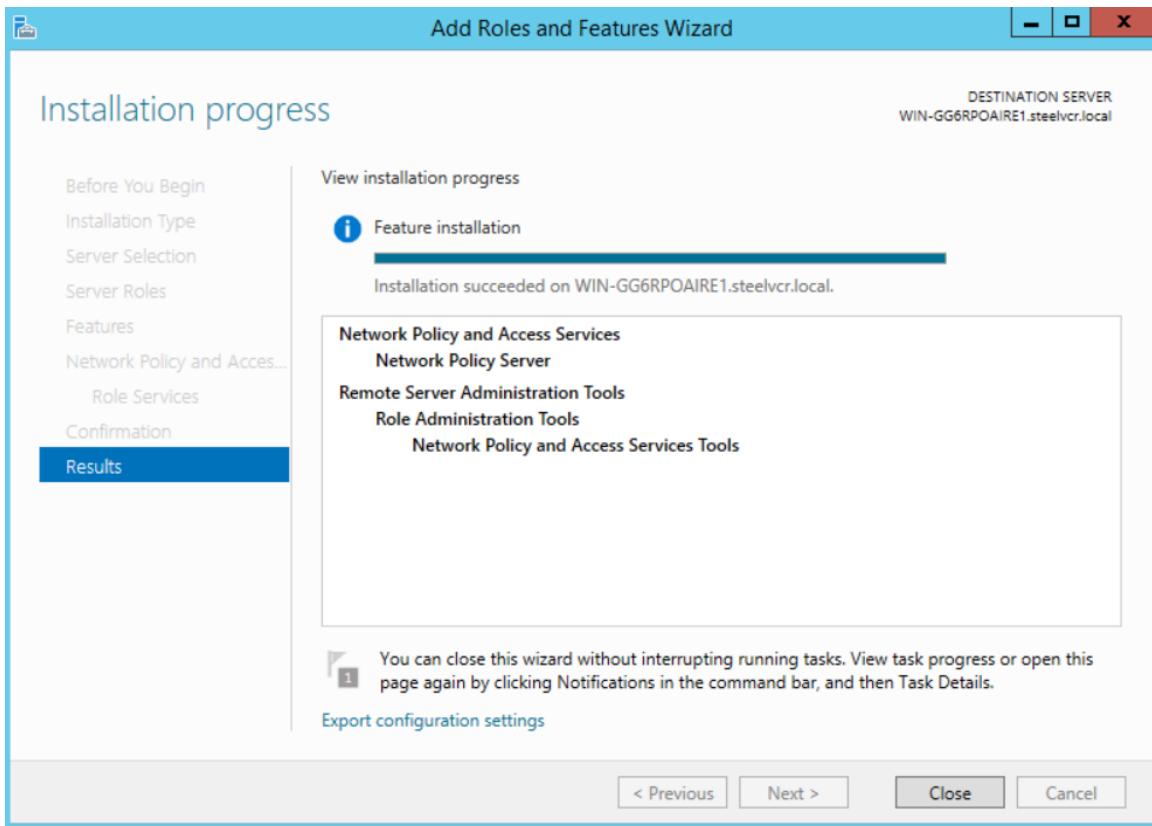
Read and click "Next".



Keep "Network Policy Server" and click "Next".



Click "Install".



After successful installation click "Close".

Server Manager

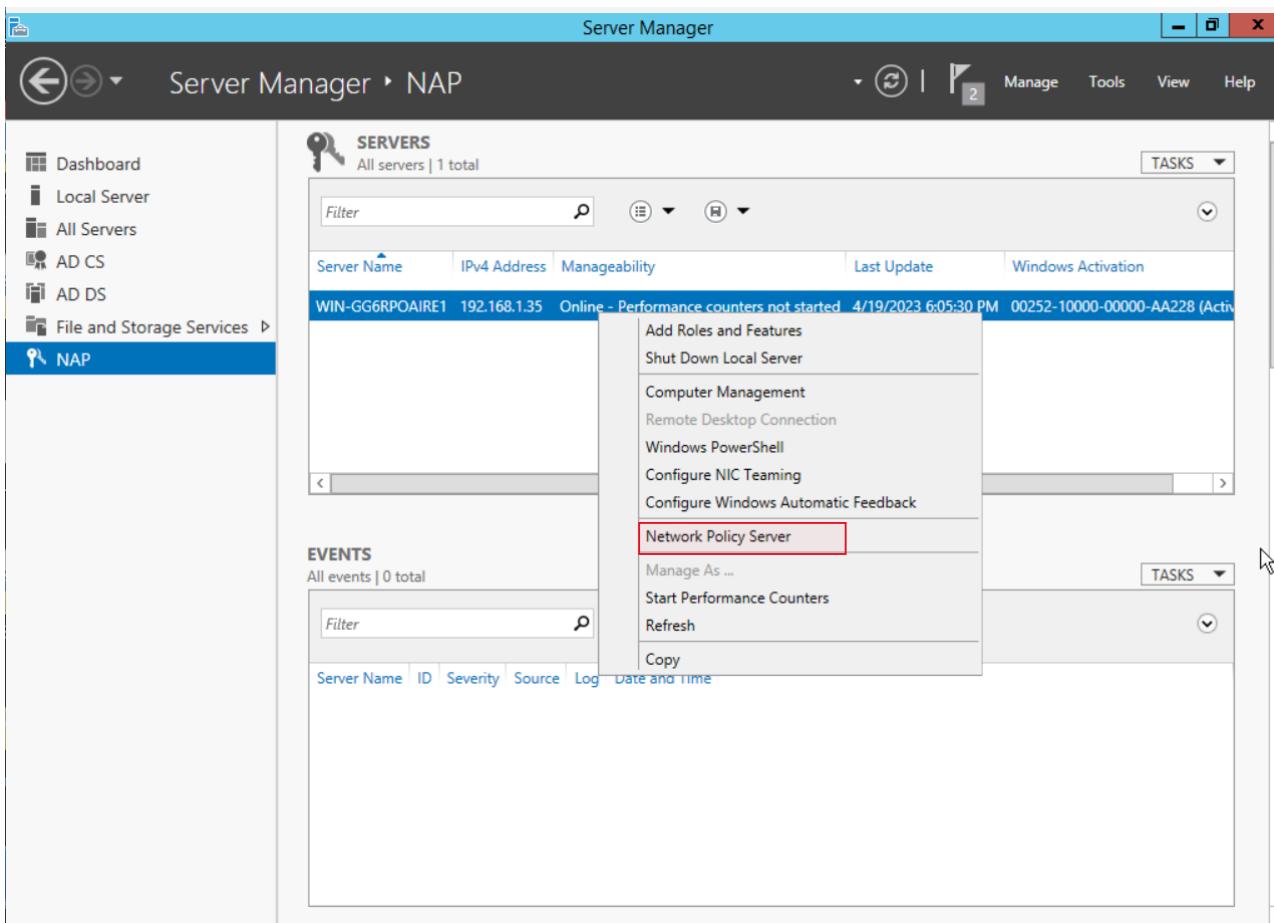
SERVERS  
All servers | 1 total

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WIN-GG6RPOAIRE1	192.168.1.35	Online - Performance counters not started	4/19/2023 6:05:30 PM	00252-10000-00000-AA228 (Activ)

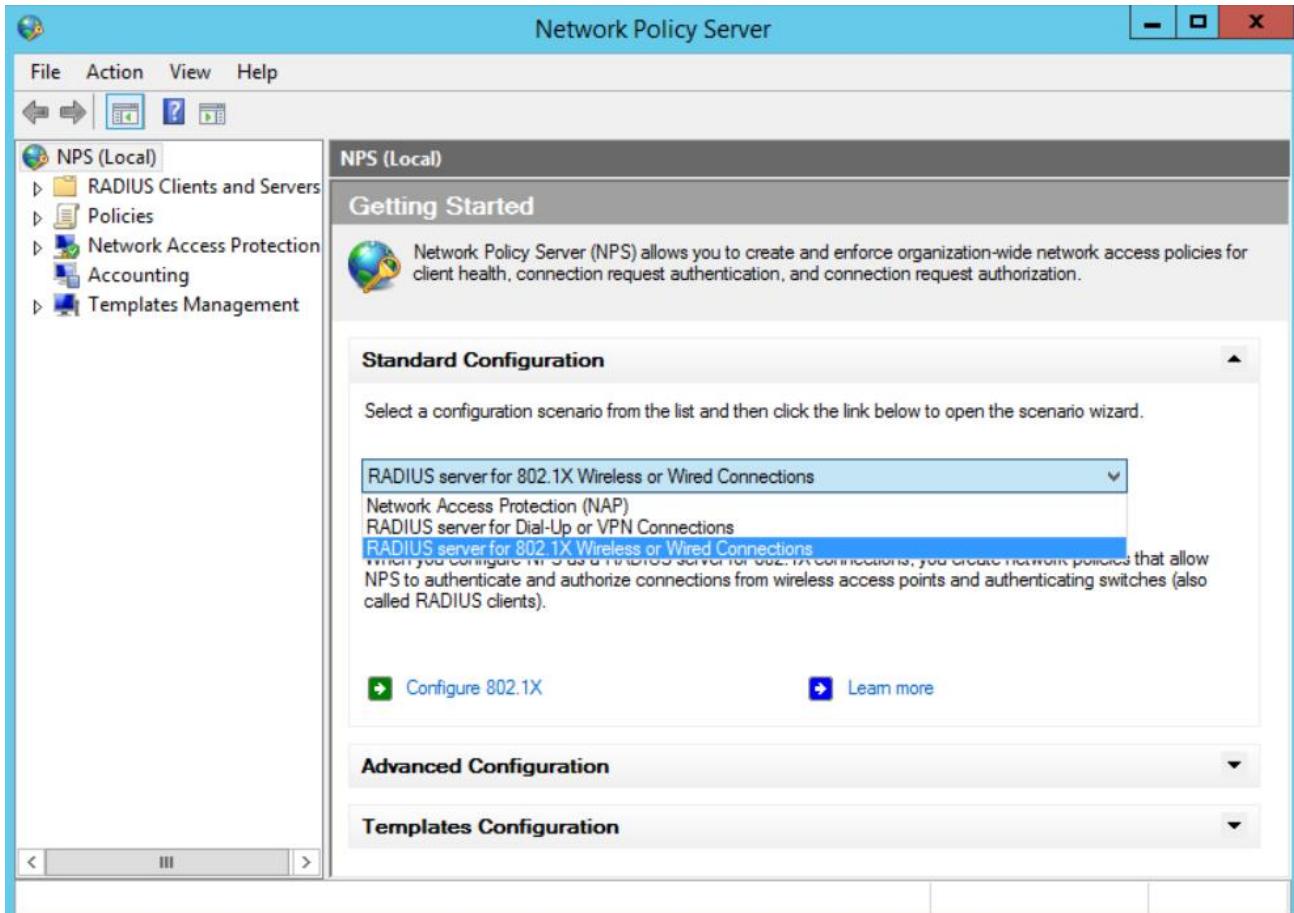
EVENTS  
All events | 0 total

Server Name	ID	Severity	Source	Log	Date and Time

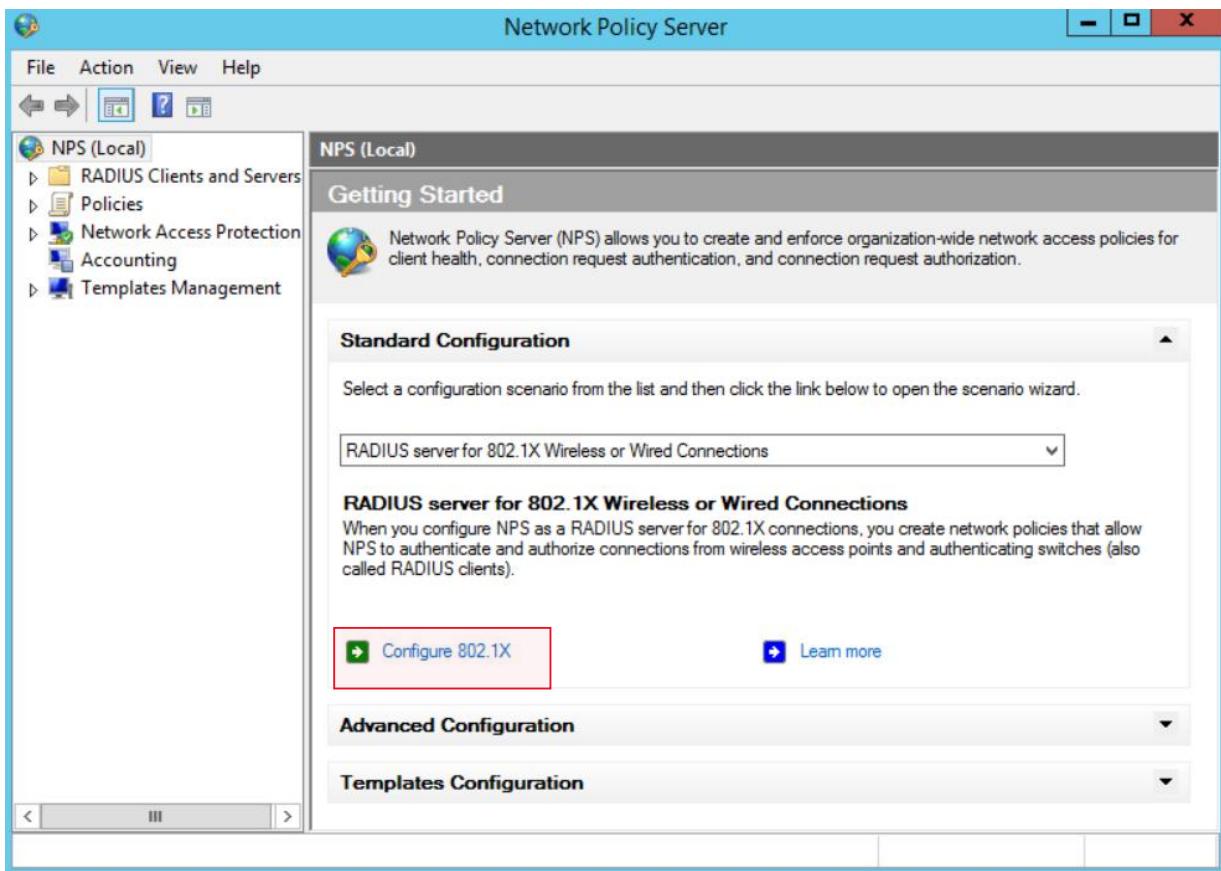
On left side column click on "NAP" (Windows Server 2012). This could be "NPAS" on Windows Server 2016.



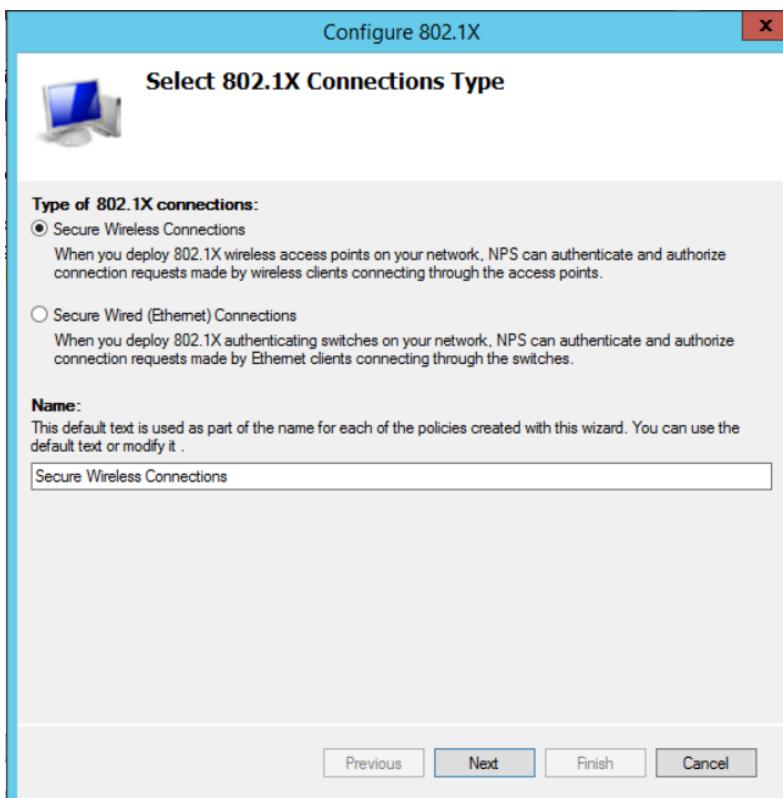
Right-click on Server in “NAP” and click on “Network Policy Server”.



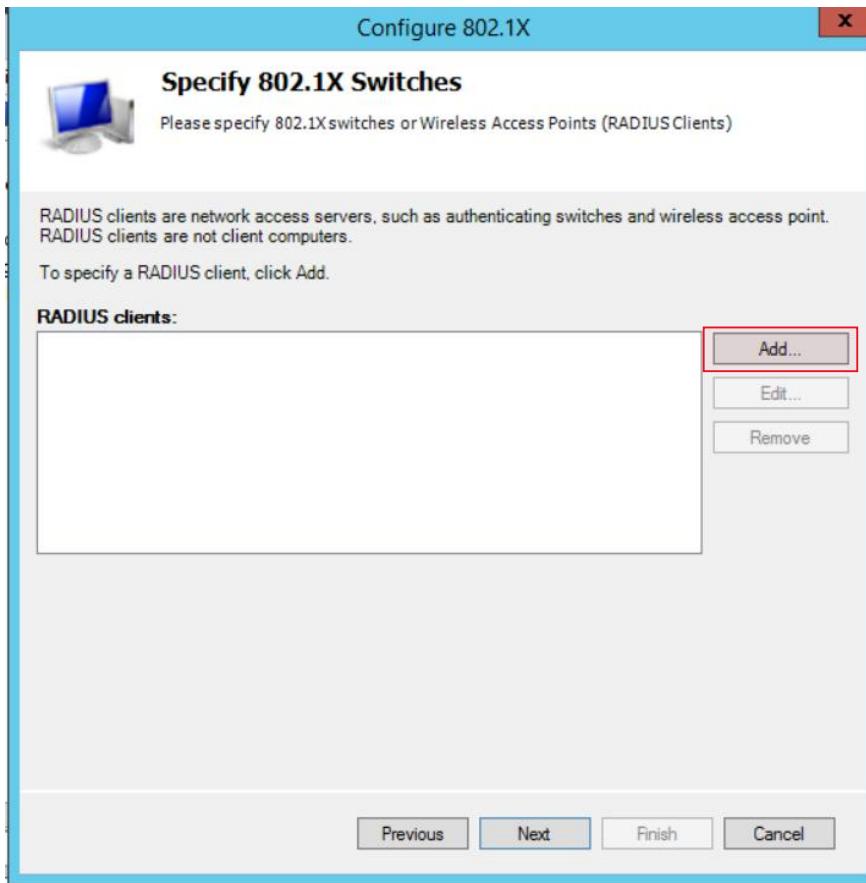
Click under “Standard Configuration” on “NPS (Local)” and select “RADIUS server for 802.1X Wireless or Wired Connections”.



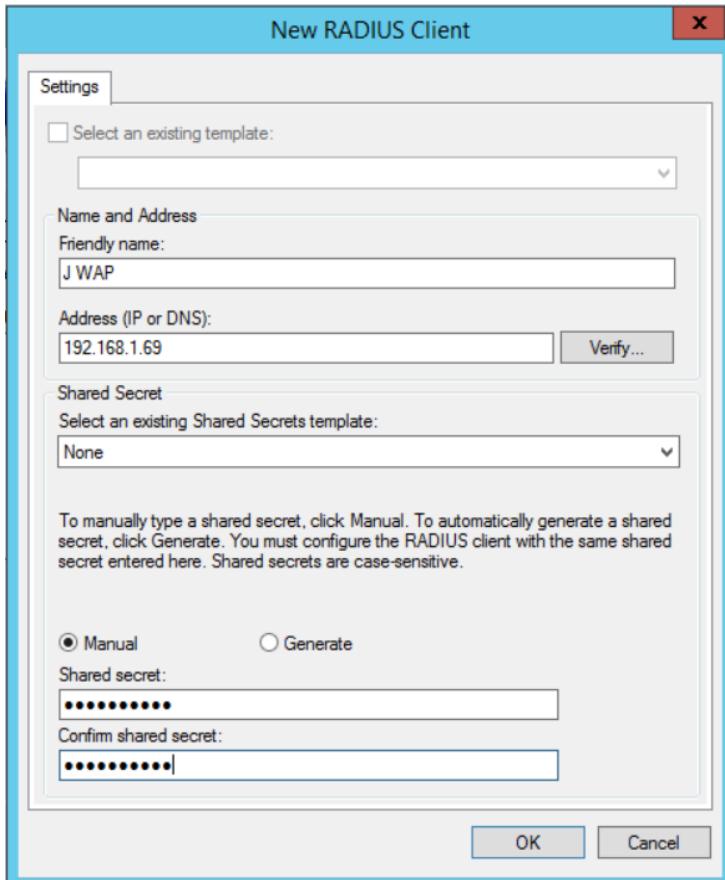
Then click on “Configure 802.1X”.



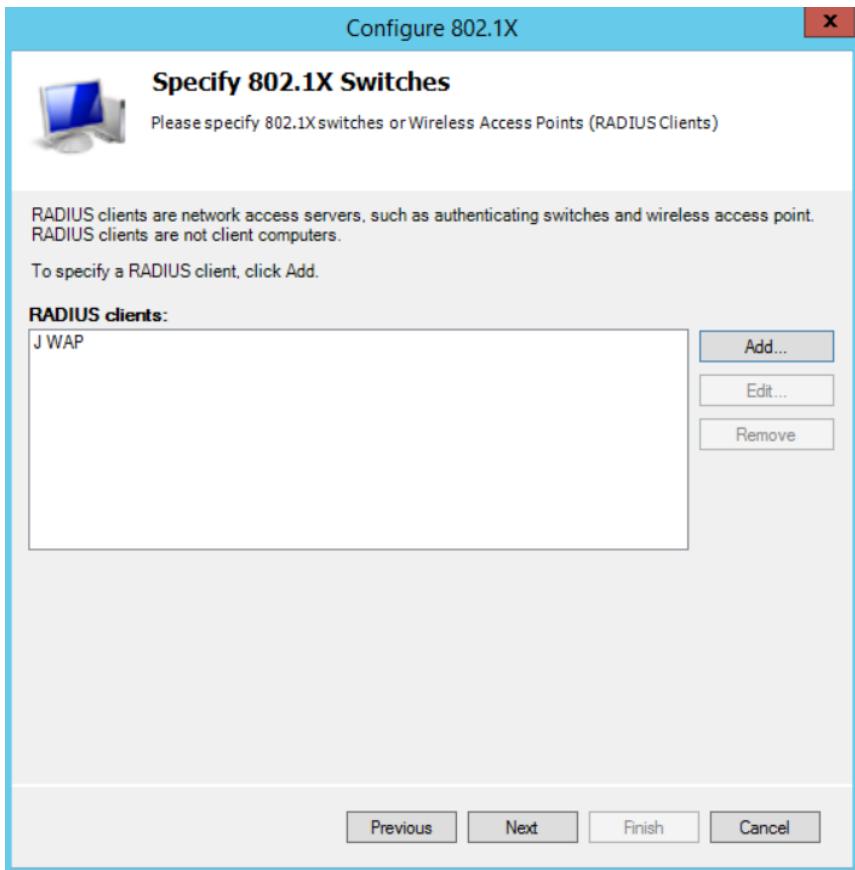
Choose/click on “Secure Wireless Connections” and click “Next”. (Name should fill in automatically)



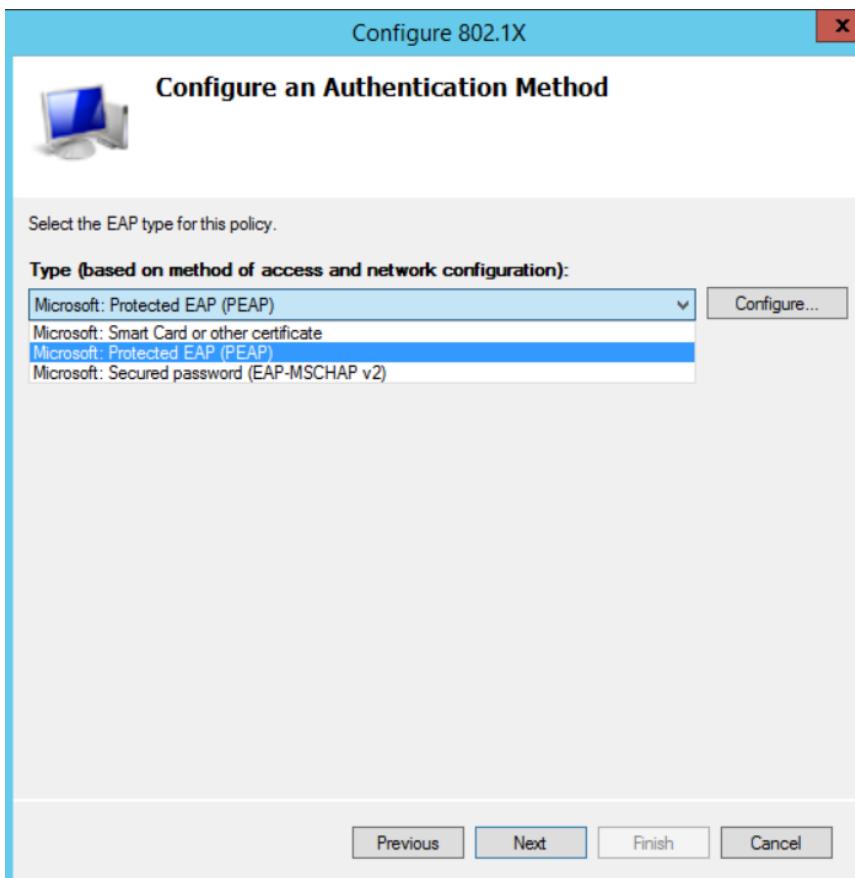
Click on "Add" to add RADIUS clients.



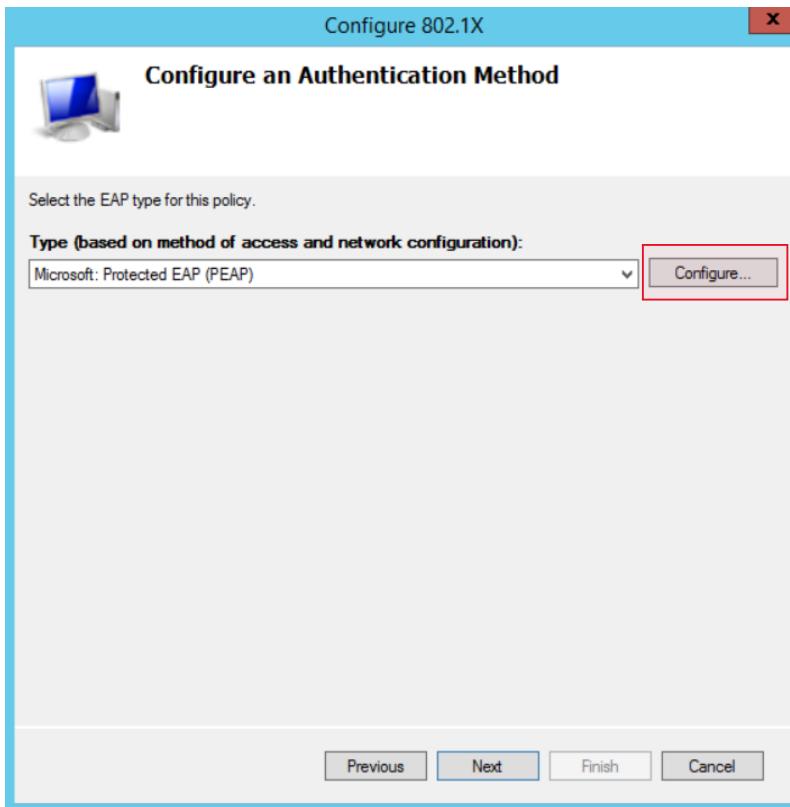
Enter a name and IP address for RADIUS client, create a secret password, and click "OK".



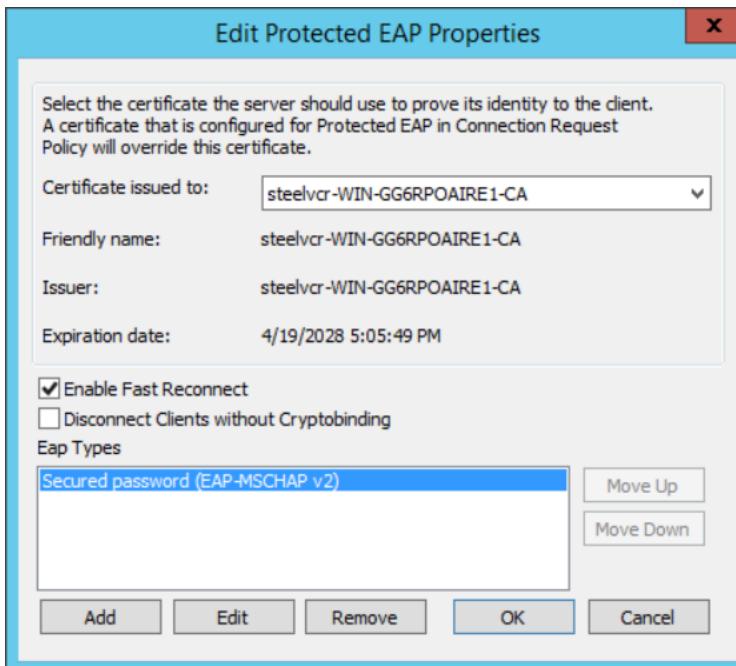
Then click "Next".



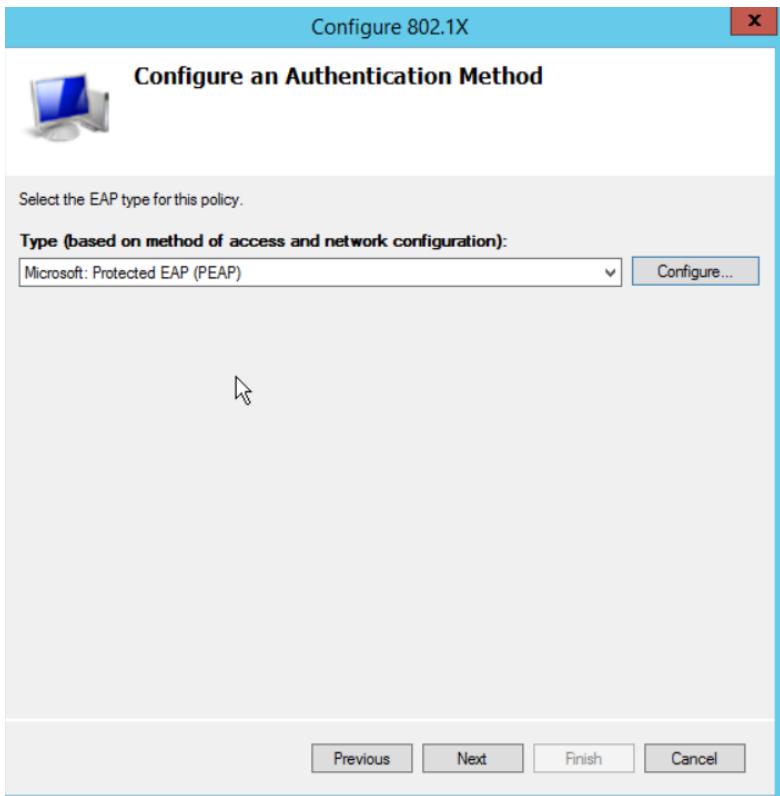
For Type select the option "Microsoft: Protected EAP (**PEAP**)".



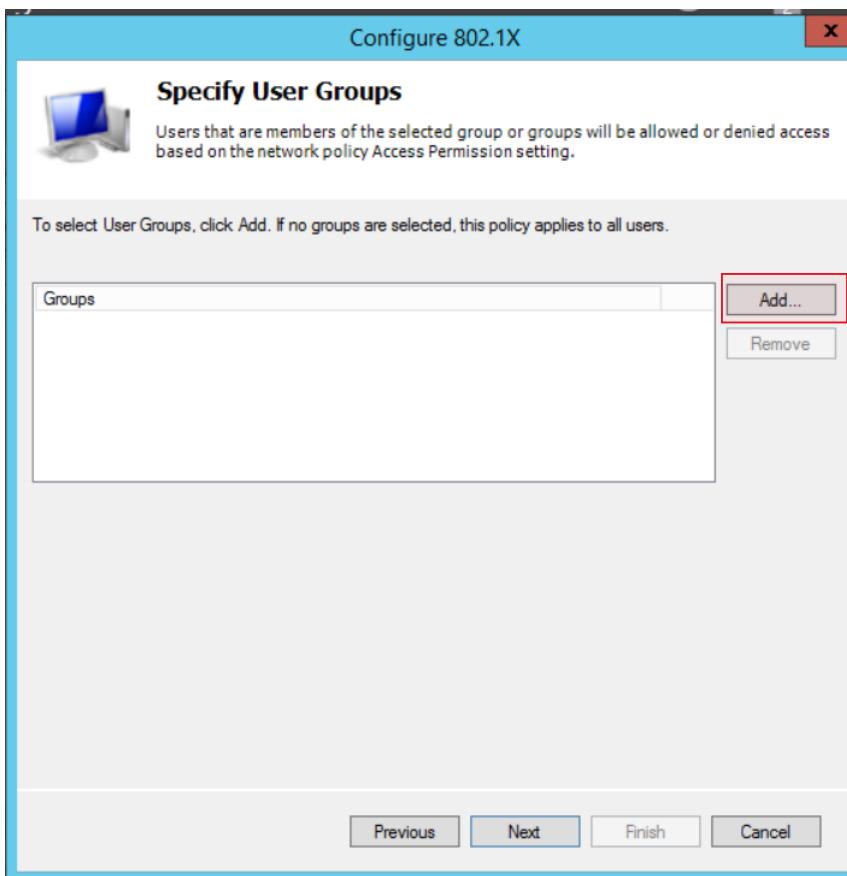
Click on “Configure...”



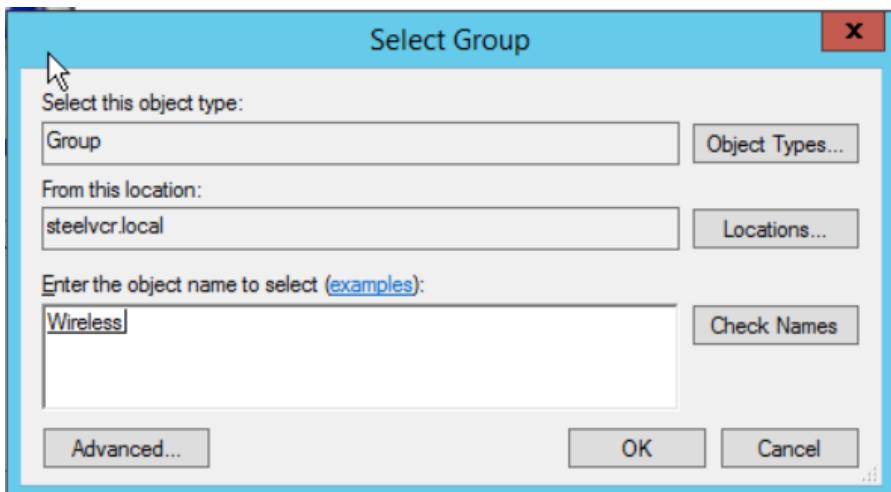
Click “OK” and everything here should appear automatically.



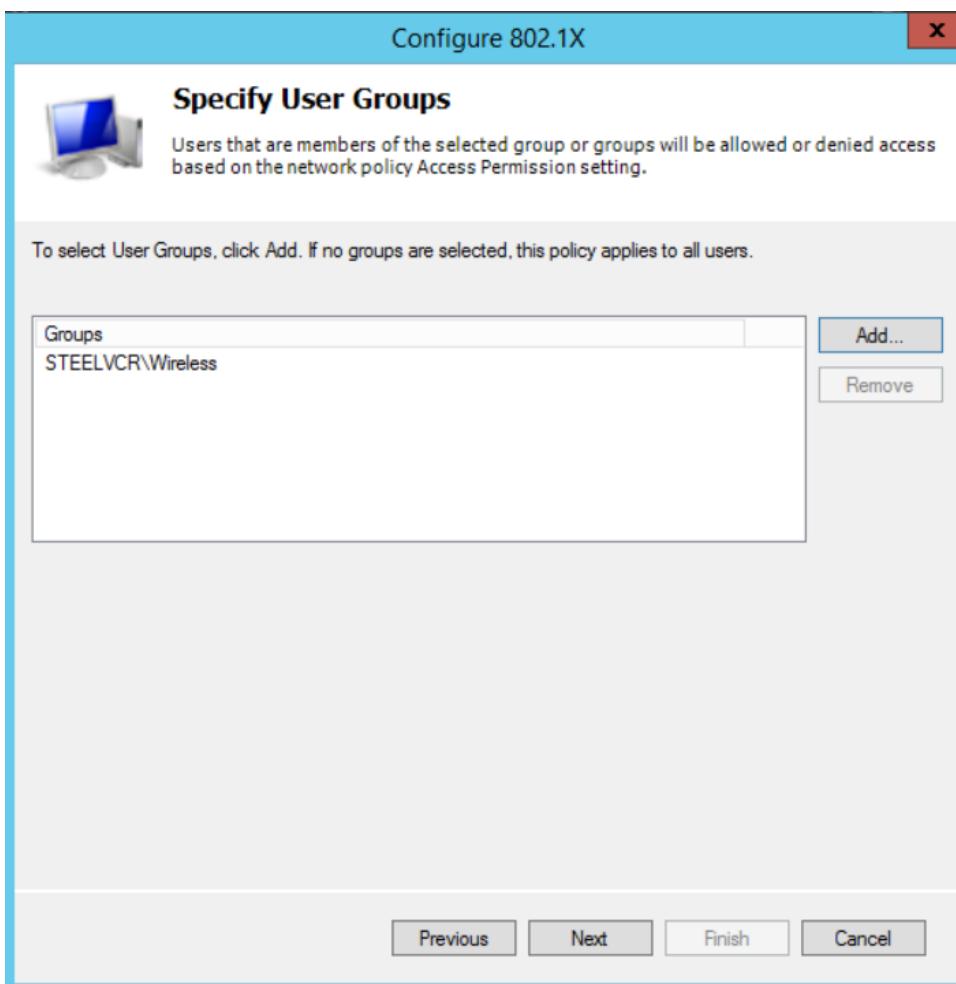
Click "Next".



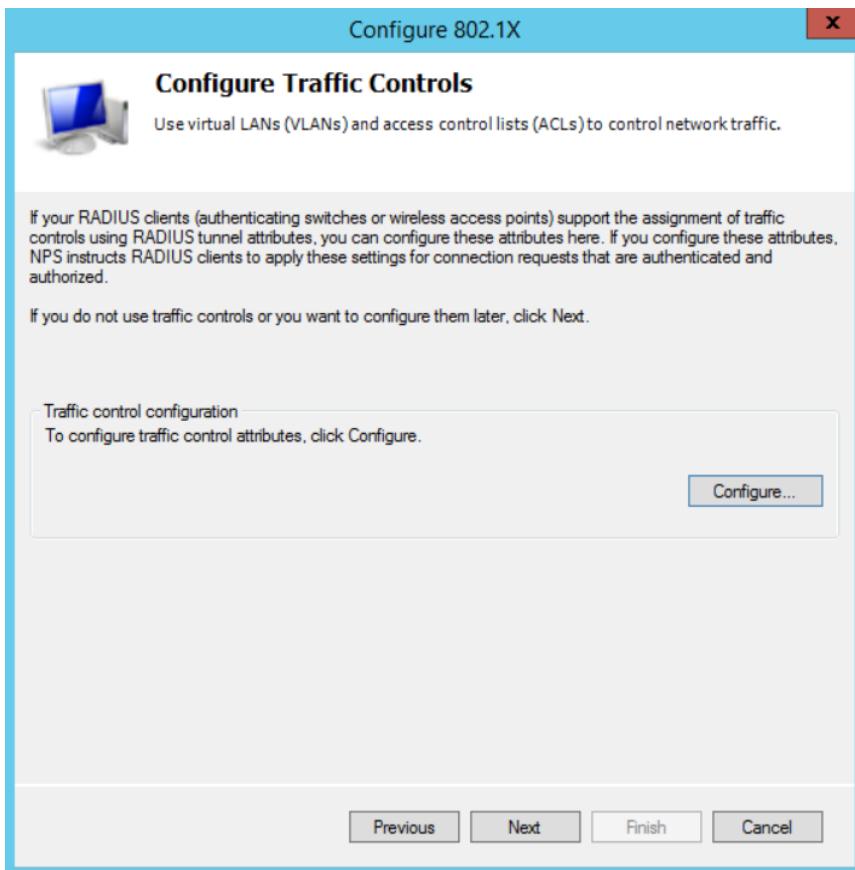
Click on "Add" to add groups.



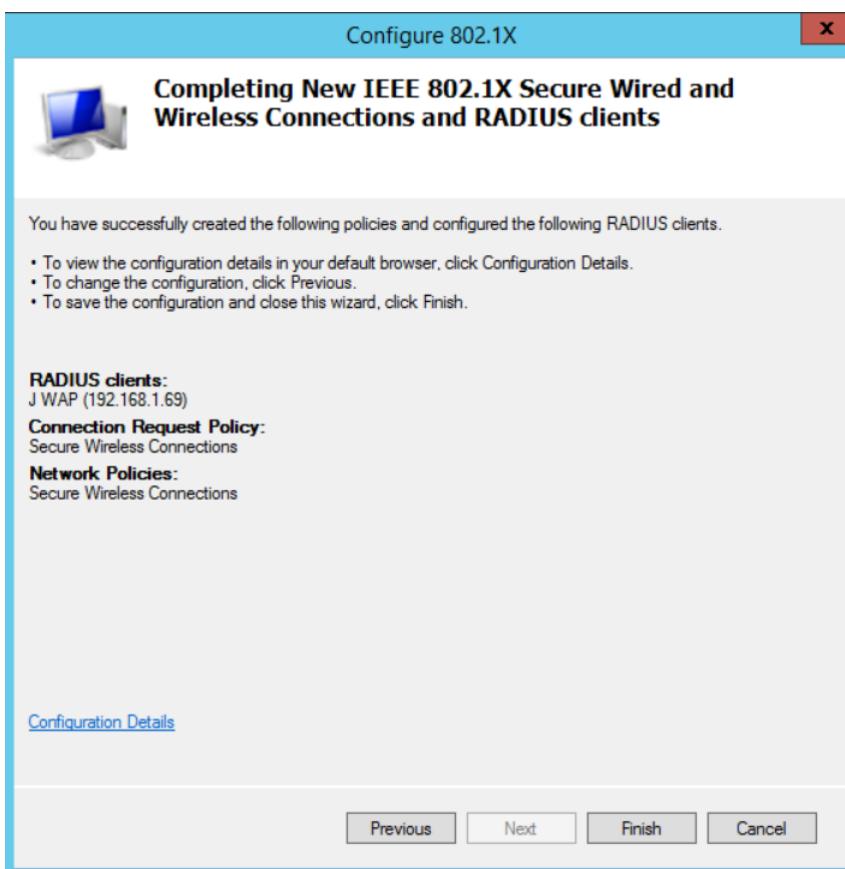
Type in beginning of group/object and click “Check Names” and then click “OK”.



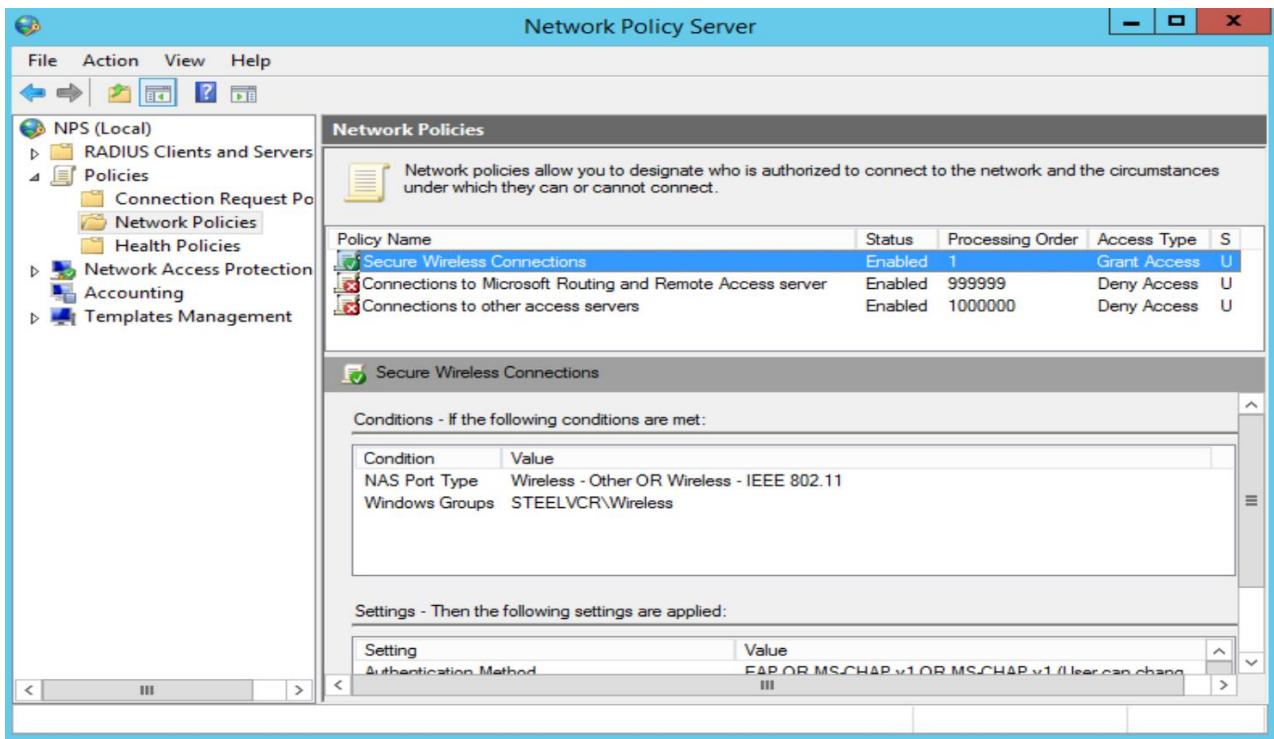
Click “Next”.



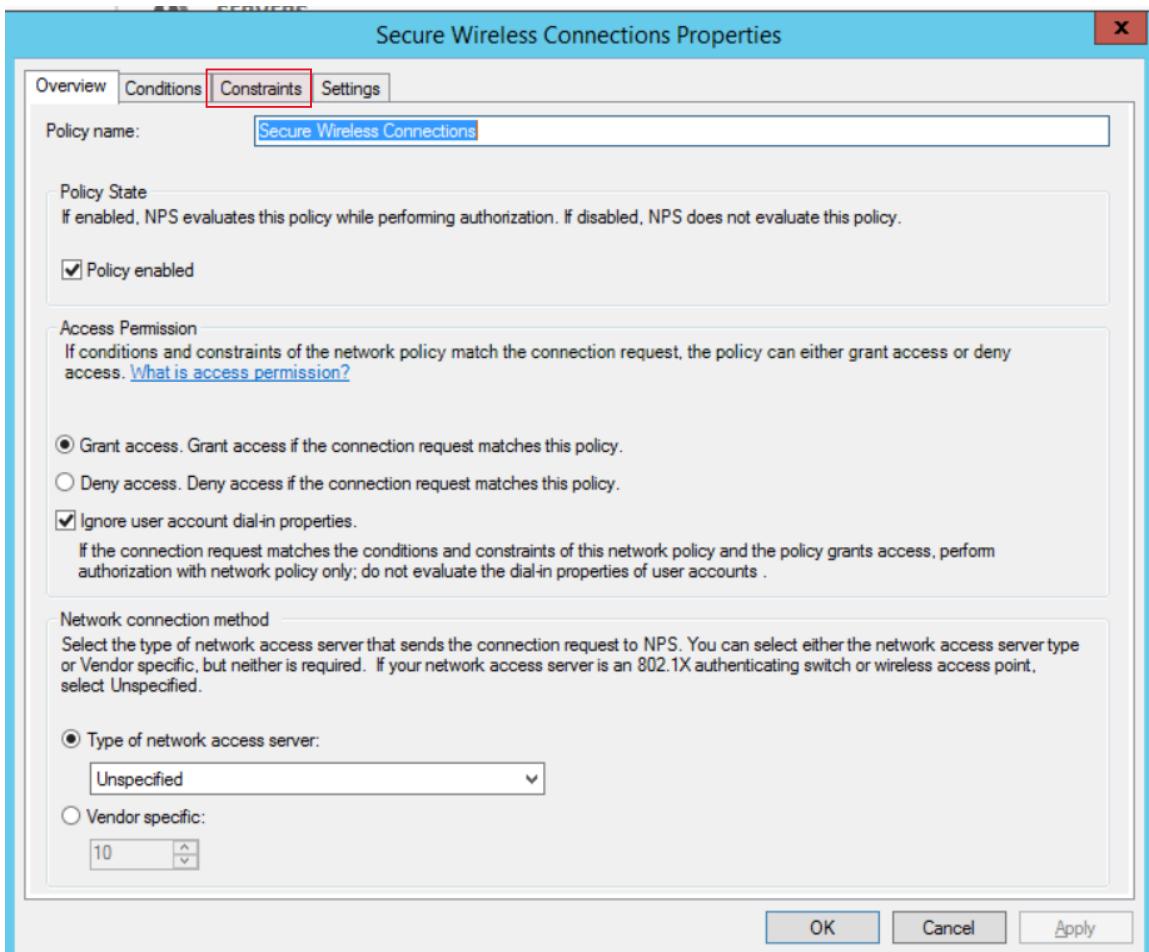
Don't have to configure traffic control attributes so click "Next".



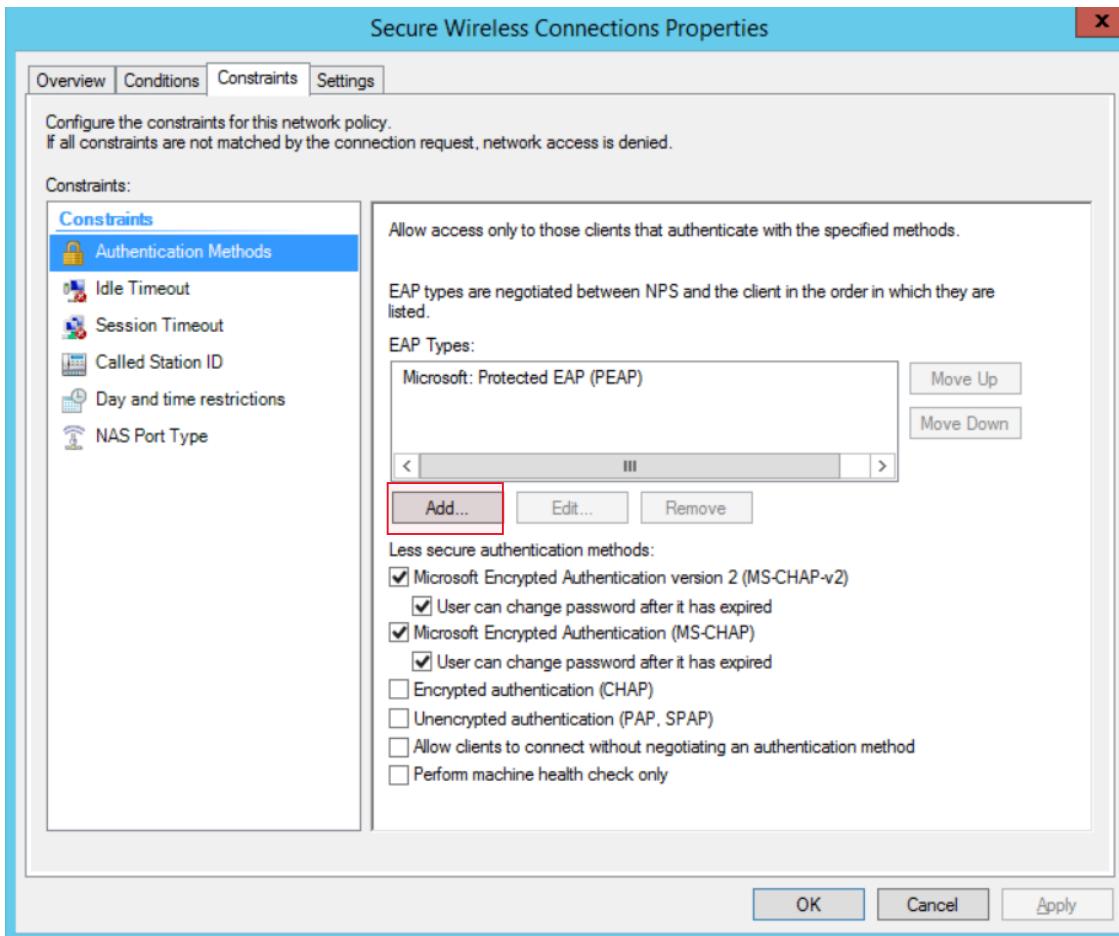
Click "Finish".



Then click on “Policies” (left side column) and under that click on “Network Policies” and then double click on “Secure Wireless Connections”.

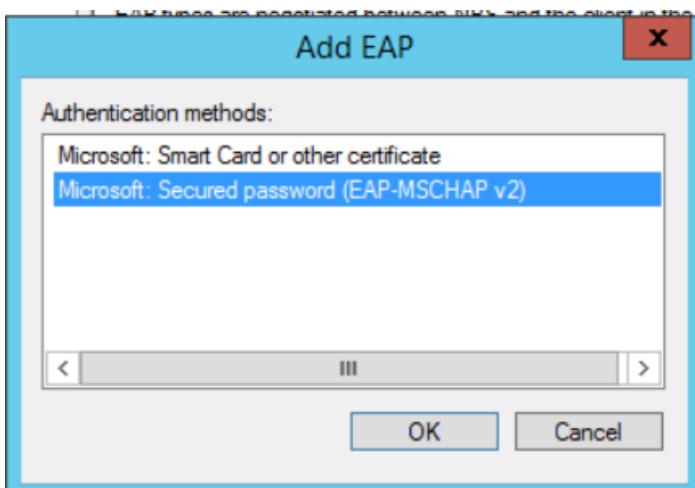


Click on “Constraints”.

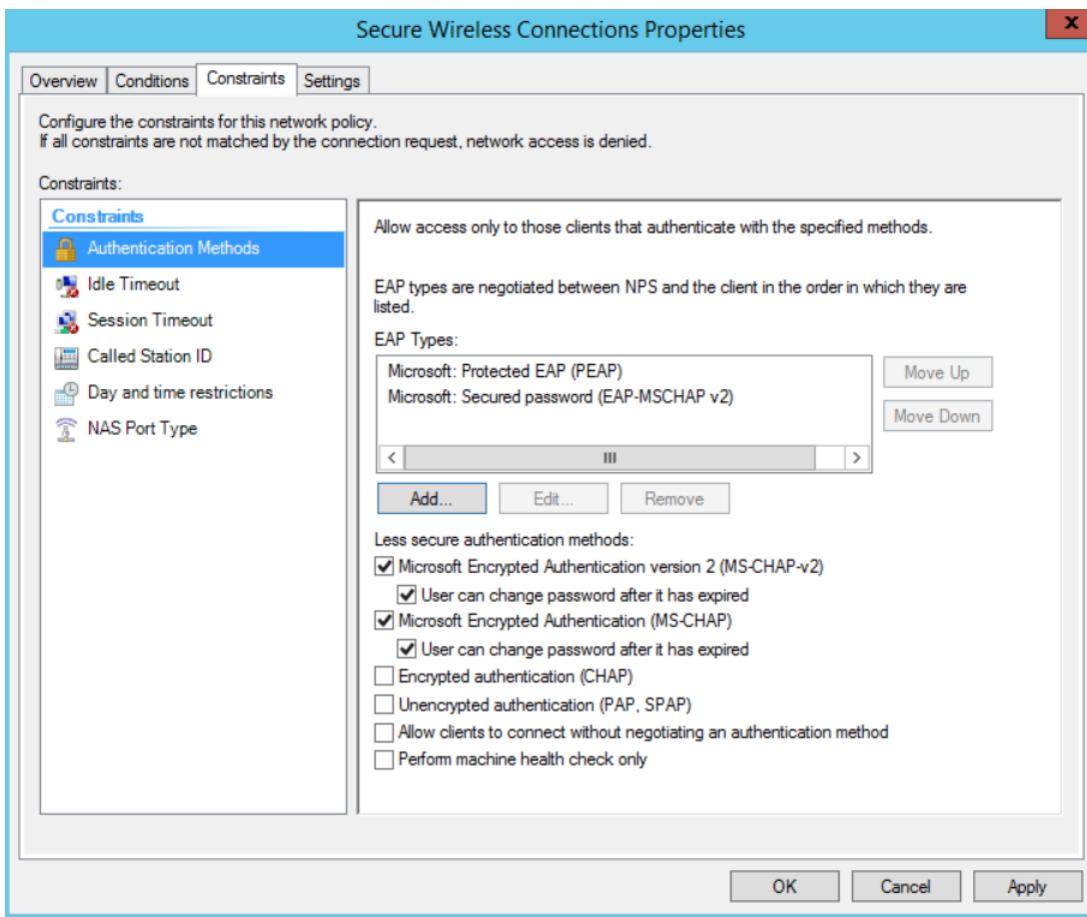


Keep every checked that is checked in automatically as shown above.

Then, click the on “Add...” to add EAP types.



Click “Microsoft: Secured password (EAP-MSCHAP v2)” and then click “OK”.



The new EAP type has been added.

Now click on “Apply” so everything gets saved/applied, and then click “OK”.

tp-link

Quick Setup Basic Advanced English Logout Reboot

Status Network Operation Mode Wireless

Wireless Settings 2.4GHz | 5GHz

SSID will be displayed), and your wireless device will automatically switch connection to the Wi-Fi band that provides the fastest speed.

Wireless Settings

Sharing Network

Enable Wireless Radio  TP-Link\_3C3C Hide SSID

Security: WPA/WPA2-Enterprise

Version: Auto WPA WPA2

Encryption: Auto TKIP AES

RADIUS Server IP: 192.168.1.35

RADIUS Port: 1812

RADIUS Password: cyber2022#

Mode: 802.11b/g/n mixed

Channel Width: Auto

Channel: Auto

Transmit Power: Low Middle High

Save

Physical plug-in access point to computer the RADIUS server is on.

Make sure you are using correct SSID for access point that will be the radius client.

For “Security” change it to “WPA/WPA-2-Enterprise” mode so we can use RADIUS.

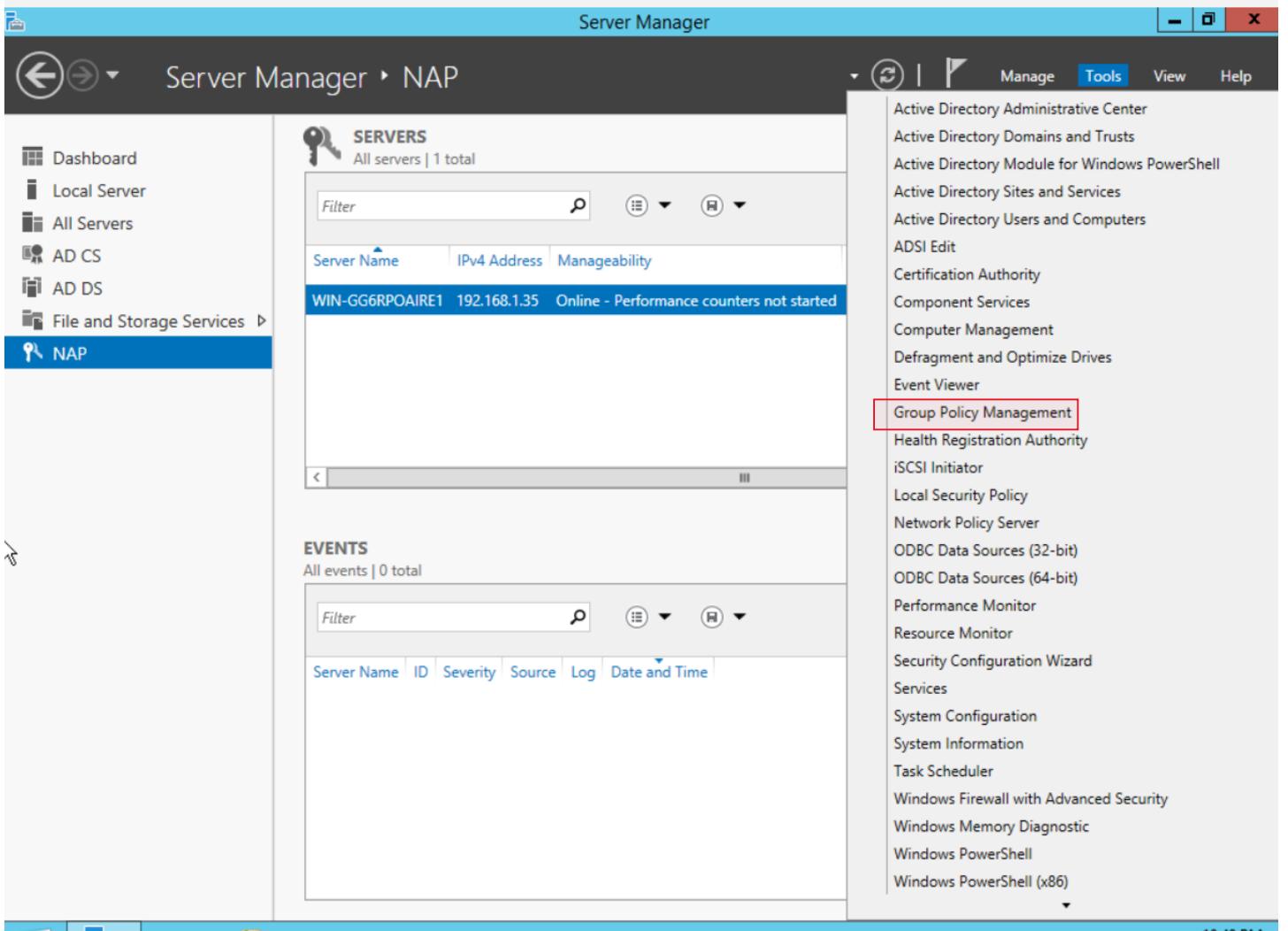
Then, enter in the IP address of RADIUS server located on Windows Server.

Type in the secret code/password for the “RADIUS Passwords”.

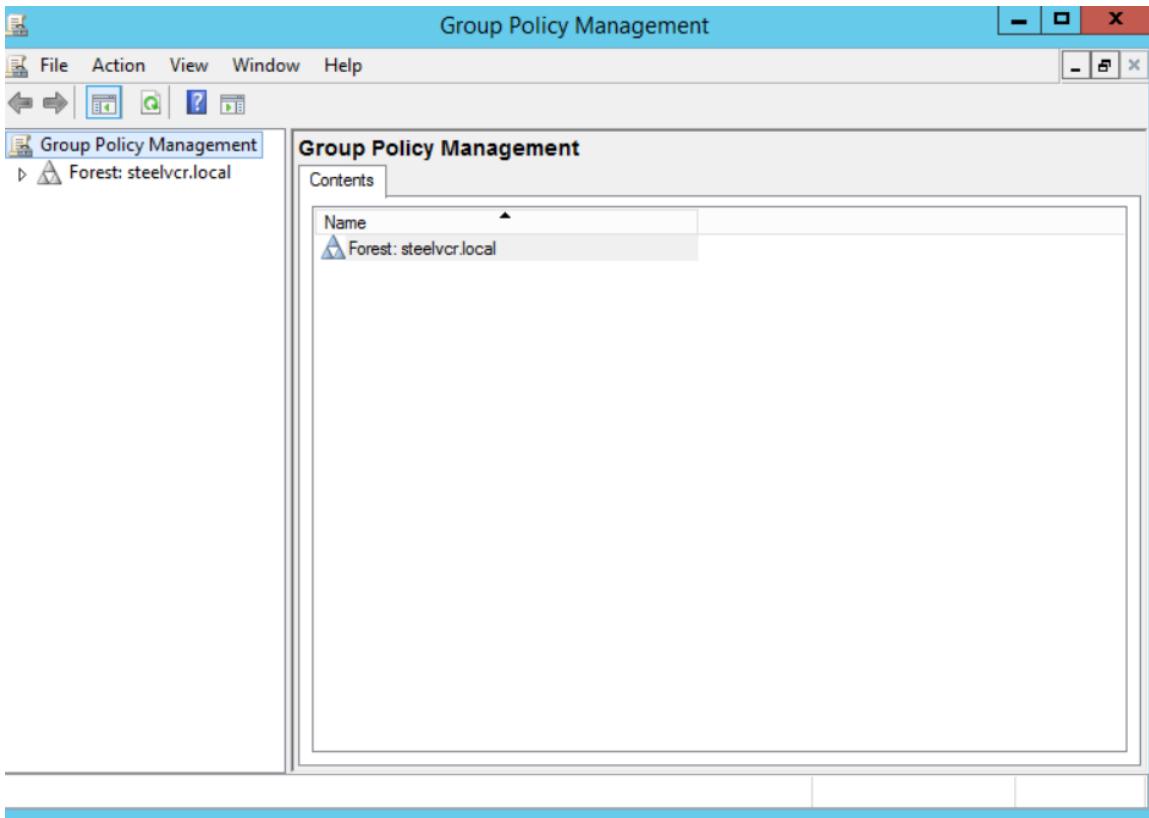
Click save, reboot, and logout.

Unplug access point, reconnect to internet, and log back into RADIUS server while leaving access point powered on wirelessly.

NOTE: make sure you are on same network (RADIUS client and server)



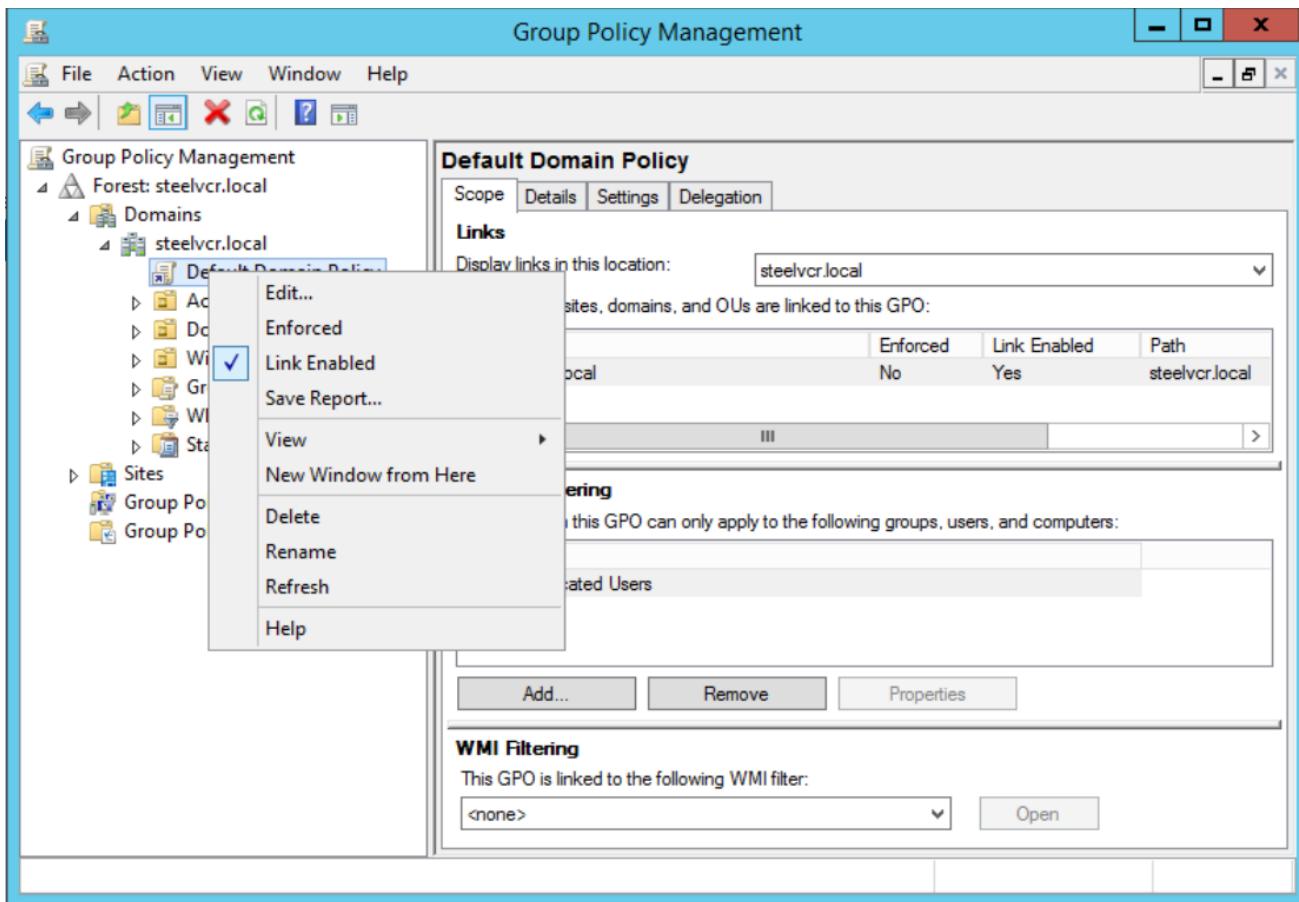
Within Server Manager click on “NAP”, then click “Tool” at the top right menu and select “Group Policy Management”.



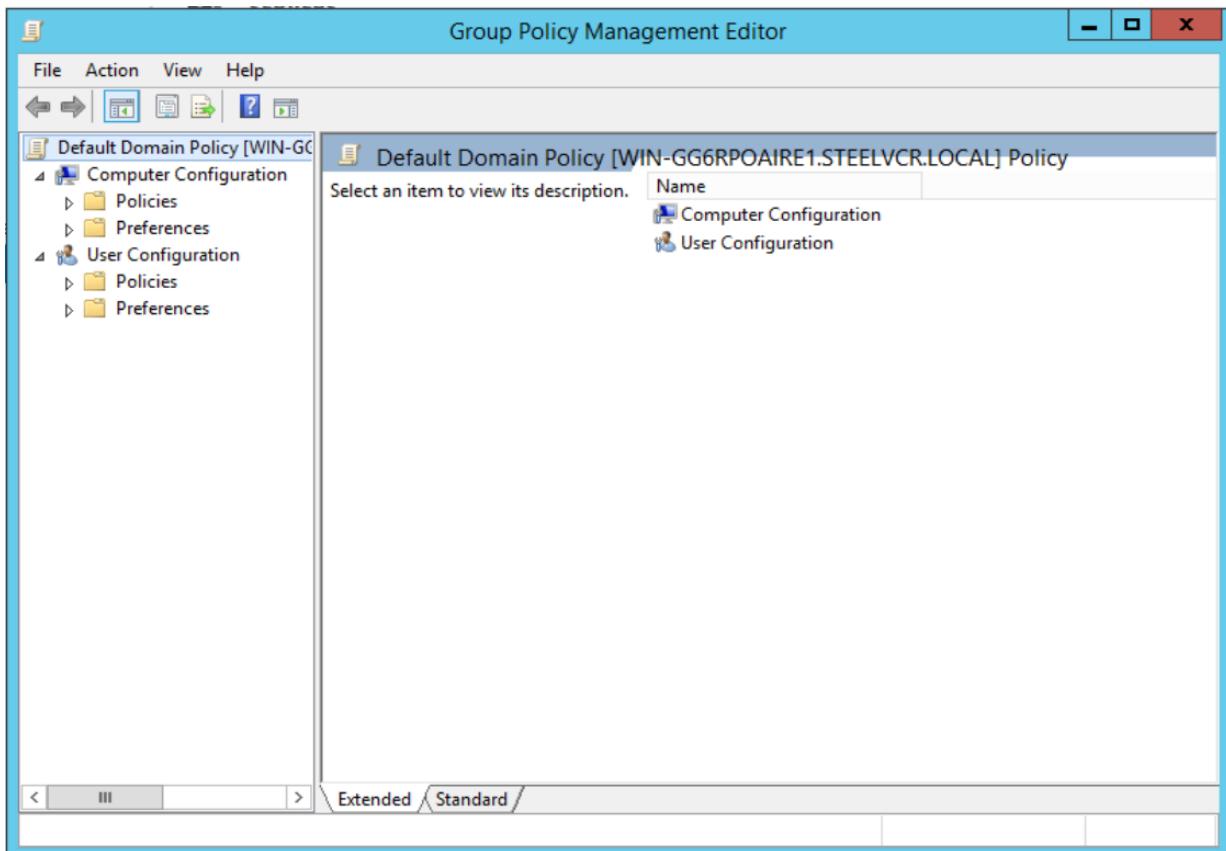
Click on first drop down “Forest:”

This screenshot shows the "Default Domain Policy" details for the "steelvcr.local" domain. The left navigation pane shows the hierarchy: Group Policy Management &gt; Forest: steelvcr.local &gt; Domains &gt; steelvcr.local &gt; Default Domain Policy. The main pane displays the "Default Domain Policy" settings. The "Scope" tab is selected. It shows the linked GPOs: "steelvcr.local" (Location: steelvcr.local, Enforced: No, Link Enabled: Yes, Path: steelvcr.local). The "Security Filtering" section lists "Authenticated Users" as the target group. The "WMI Filtering" section indicates no WMI filter is applied.

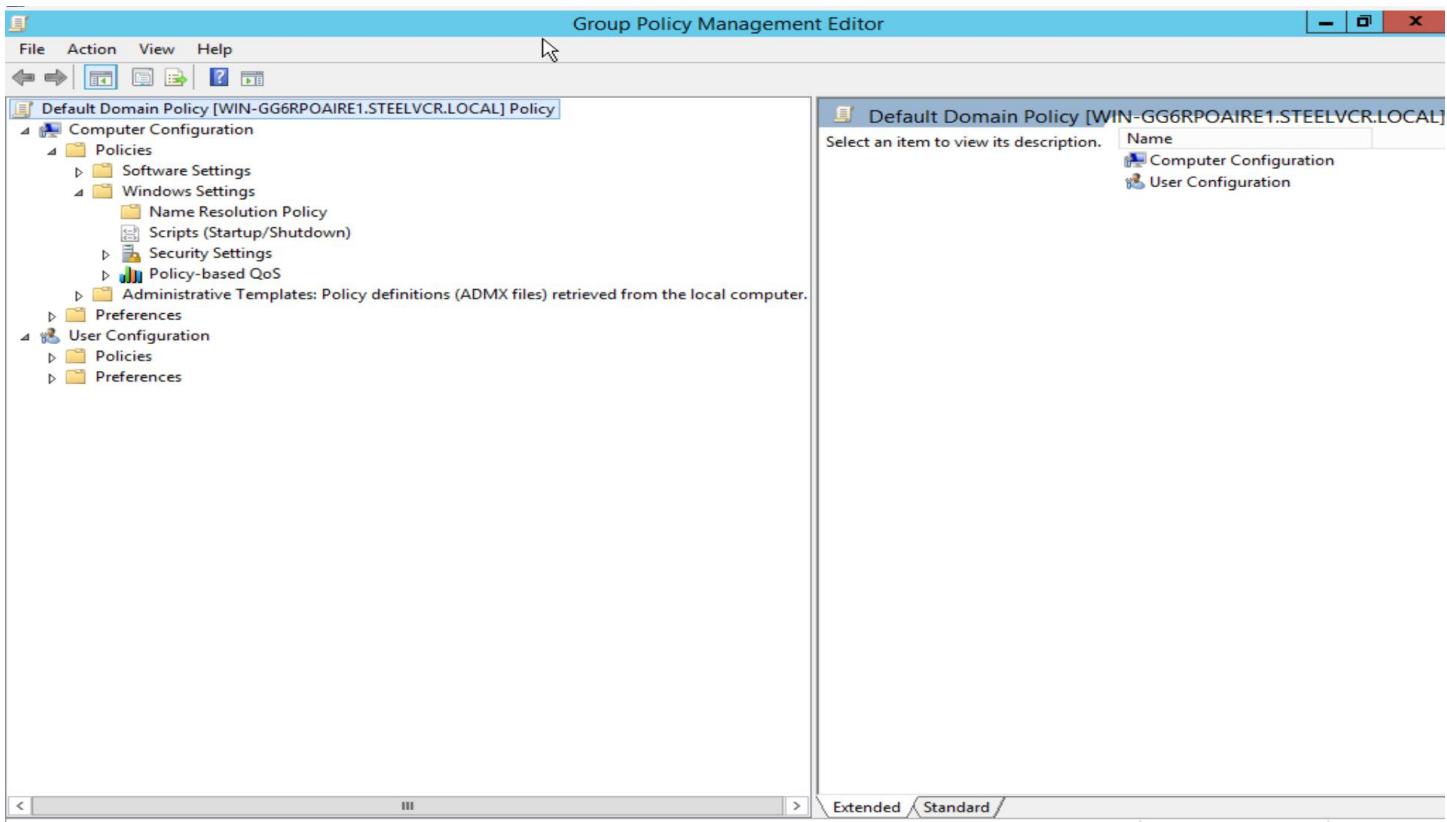
Click on “Domains” dropdown menu, then click your root domain name “steelvcr.local”, and then click on “Default Domain Policy”.



Right-click on “Default Domain Policy” and select “Edit”.



Click on “Policies”.



Click on “Windows Settings” and then click “Security Settings”.

Group Policy Management Editor

File Action View Help

Default Domain Policy [WIN-GG6RPOAIRE1.STEELVCR.LOCAL] Policy

Computer Configuration

- Policies
  - Software Settings
  - Windows Settings
    - Name Resolution Policy
    - Scripts (Startup/Shutdown)
    - Security Settings
      - Account Policies
      - Local Policies
      - Event Log
      - Restricted Groups
      - System Services
      - Registry
      - File System
      - Wired Network (IEEE 802.3) Policies
      - Windows Firewall with Advanced Security
      - Network List Manager Policies
      - Wireless Network (IEEE 802.11) Policies
    - Public Key Policies
    - Software Restriction Policies
    - Network Access Protection
    - Application Control Policies
    - IP Security Policies on Active Directory (STEELVCR.LOCAL)
    - Advanced Audit Policy Configuration
    - Policy-based QoS
  - Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer.

User Configuration

  - Policies
  - Preferences

Click on “Wireless Network (IEEE 802.11) Policies”.

Group Policy Management Editor

File Action View Help

Default Domain Policy [WIN-GG6RPOAIRE1.STEELVCR.LOCAL] Policy

Computer Configuration

- Policies
  - Software Settings
  - Windows Settings
    - Name Resolution Policy
    - Scripts (Startup/Shutdown)
    - Security Settings
      - Account Policies
      - Local Policies
      - Event Log
      - Restricted Groups
      - System Services
      - Registry
      - File System
      - Wired Network (IEEE 802.3) Policies
      - Windows Firewall with Advanced Security
      - Network List Manager Policies
      - Wireless Network (IEEE 802.11) Policies
    - Public Key Policies
    - Software Restriction Policies
    - Network Access Protection
    - Application Control Policies
    - IP Security Policies on Active Directory
    - Advanced Audit Policy Configuration
    - Policy-based QoS
  - Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer.

User Configuration

  - Policies
  - Preferences

Create A New Wireless Network Policy for Windows Vista and Later Releases

Create A New Windows XP Policy

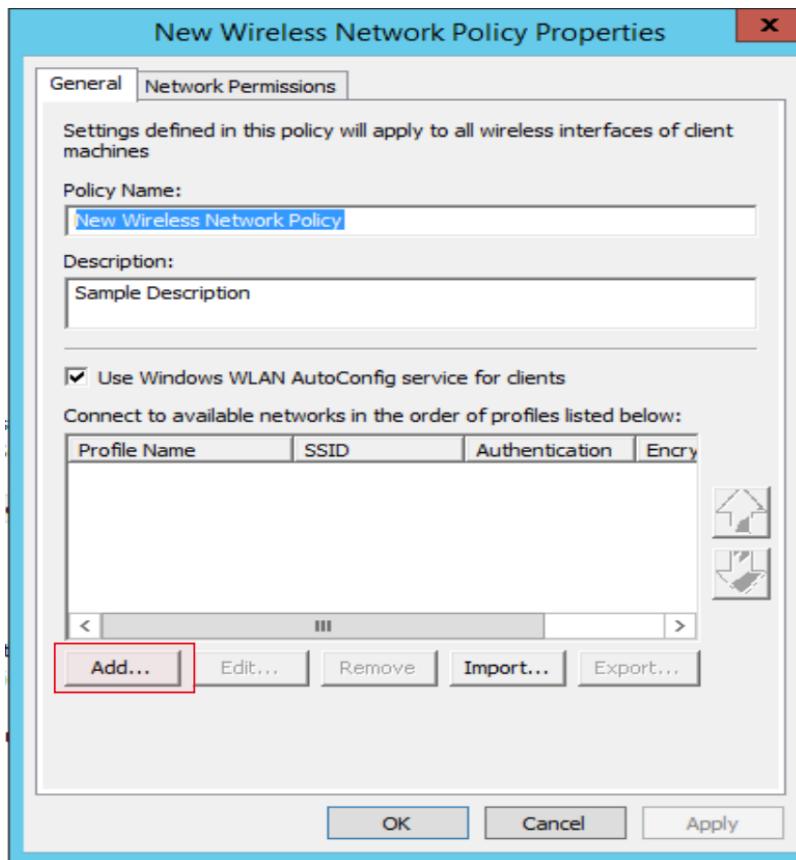
View

Refresh

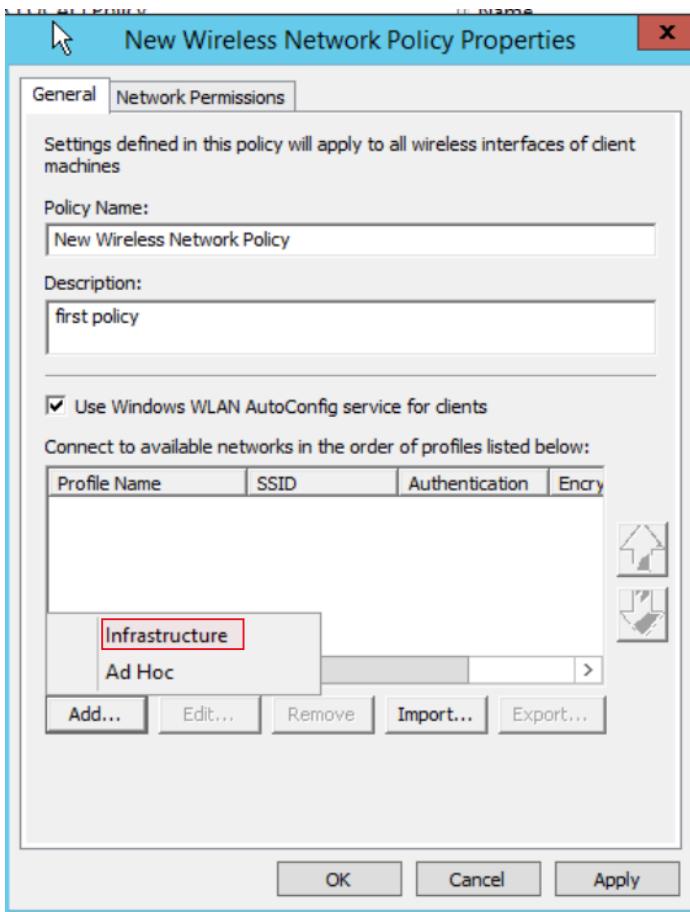
Export List...

Help

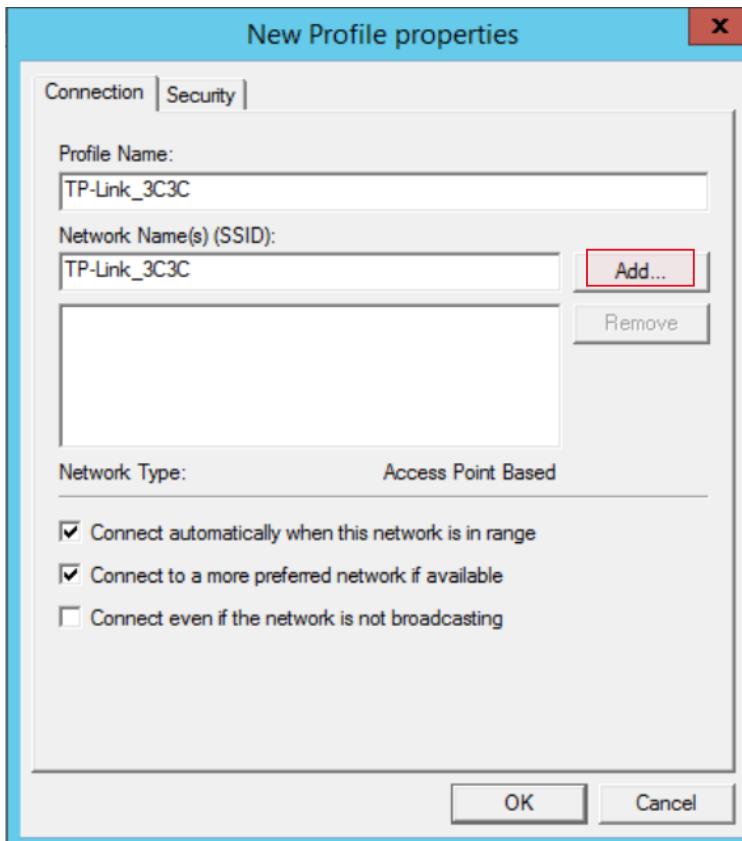
Right-click on that and select “Create a New Wireless Network Policy for Windows Vista and Later Releases”.



Click on "Add".



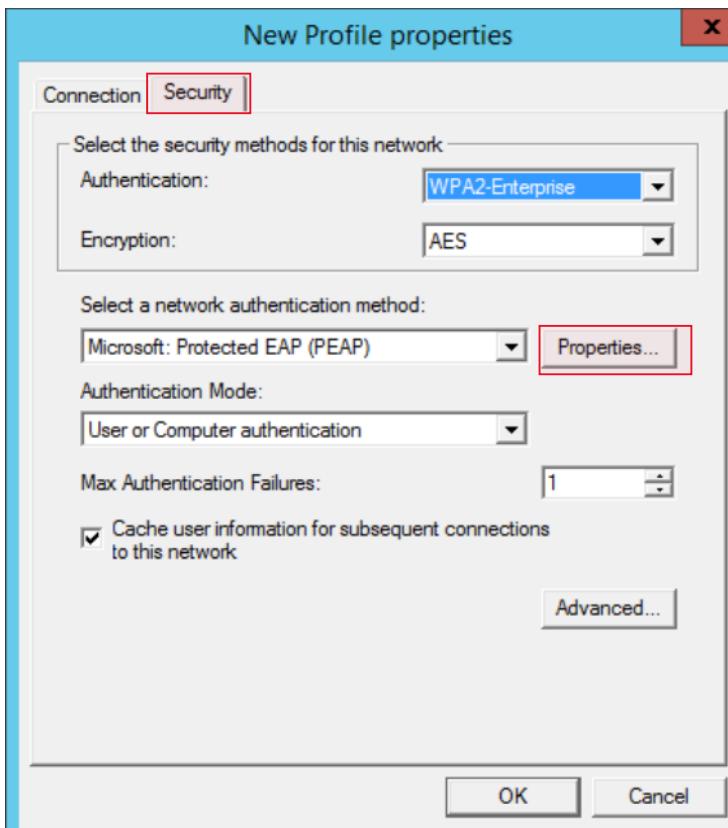
Click on "Infrastructure".



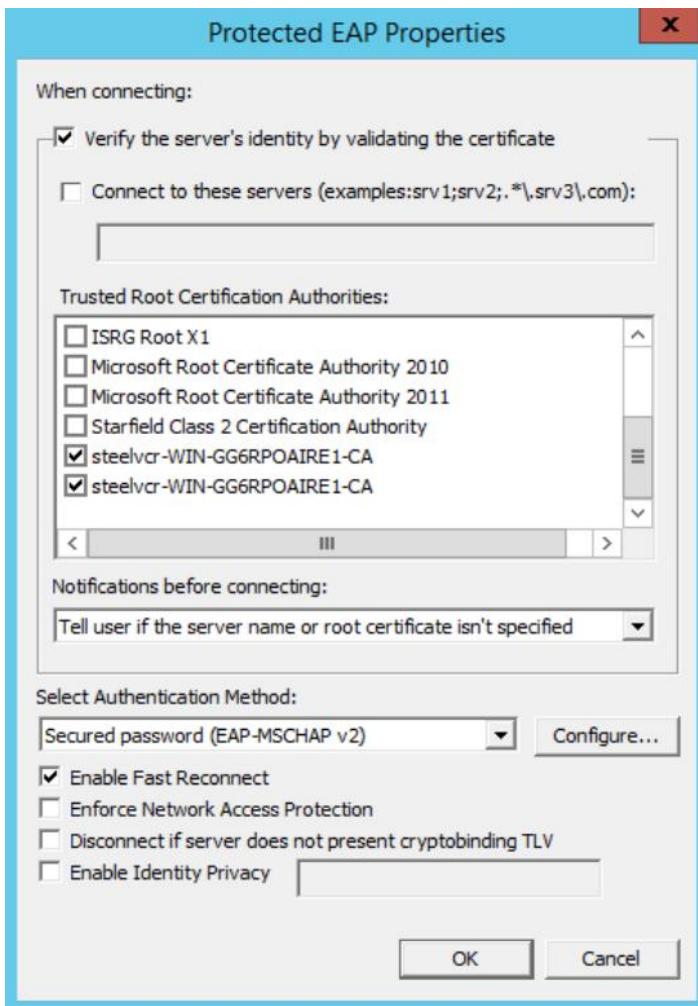
Type in profile name, and SSID for access point/RADIUS client then click “Add...”

Keep “Connect automatically when this network is in range” and “Connect to a more preferred network if available” checked.

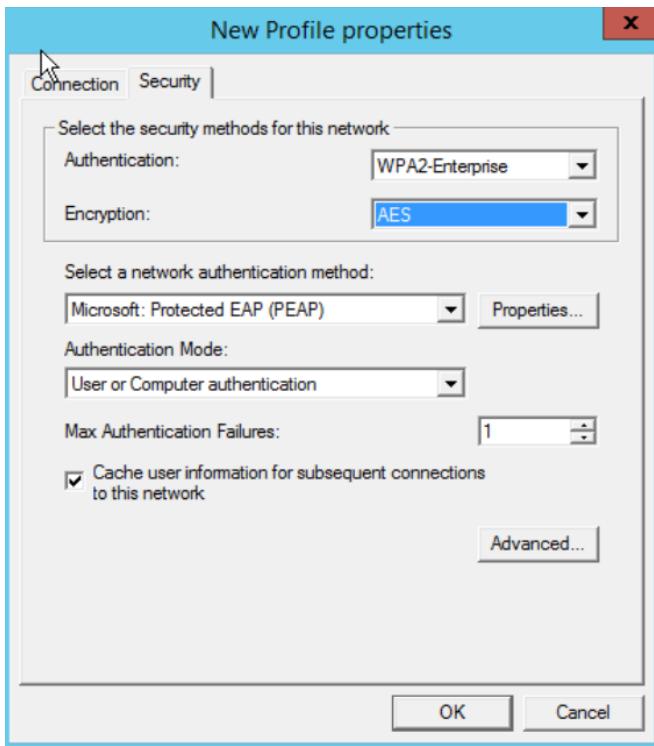
Click on “Security” at the top right.



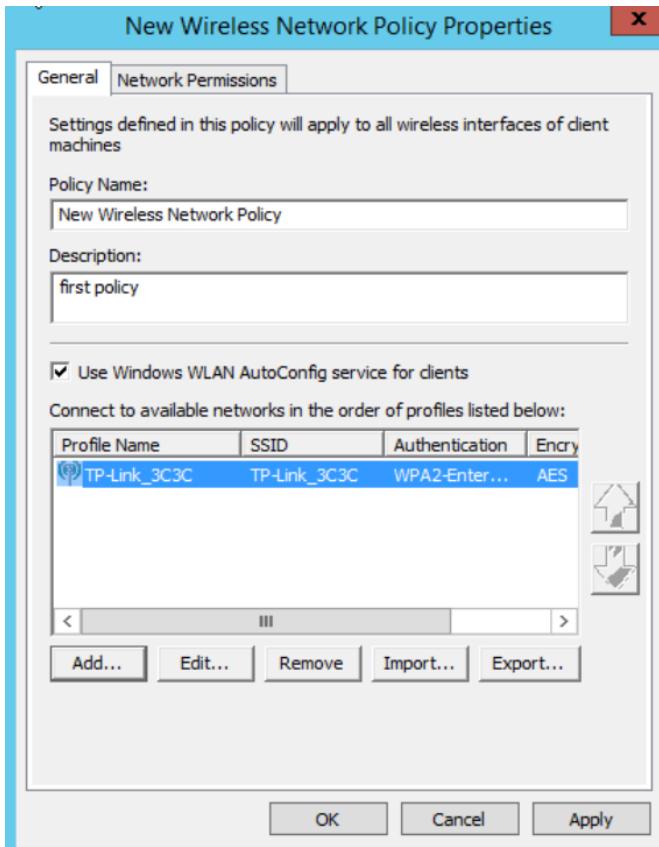
Click on “Properties”.



Underneath “Trusted Root Certification Authorities” look for your two server names. Make sure everything shown above is checked in. Click “OK”.



Click “OK”.



Click “Apply” and then “OK”.

Exit out of any opens tabs besides Server Manager.

The screenshot shows the Windows Server Manager interface. The left navigation pane is visible with options like Dashboard, Local Server, All Servers, AD CS, AD DS, File and Storage Services, and NAP. The NAP option is selected and highlighted in blue. The main content area is titled "Server Manager • NAP". Below this, there is a "SERVICES" section with a table showing one service: WIN-GG6RPOAIRE1 (Network Policy Server) with Service Name IAS, Status Running, and Start Type Automatic (Delayed Start). A red box highlights the "SERVICES" title. At the bottom, there is a "BEST PRACTICES ANALYZER" section.

Scroll down until you see “SERVICES”.

The screenshot shows the same Windows Server Manager interface as the previous one. The "SERVICES" section is visible, showing the IAS service. A right-click context menu is open over the IAS service row. The menu items are: Start Services, Stop Services, **Restart Services** (which is highlighted with a red box), Pause Services, Resume Services, and Copy. The "BEST PRACTICES ANALYZER" section is also present at the bottom.

Right-click on server and select “Restart Services”. Make sure the server is running and the access point is on.

Authentication from mobile device to RADIUS client/access point.