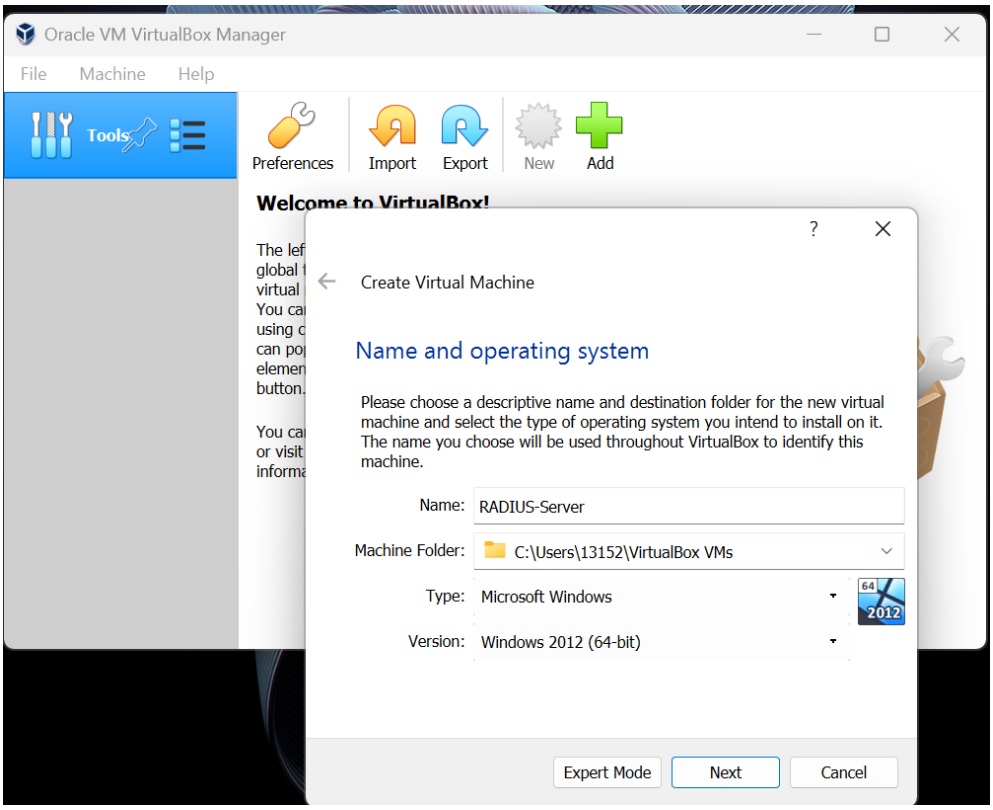
Justin Linder

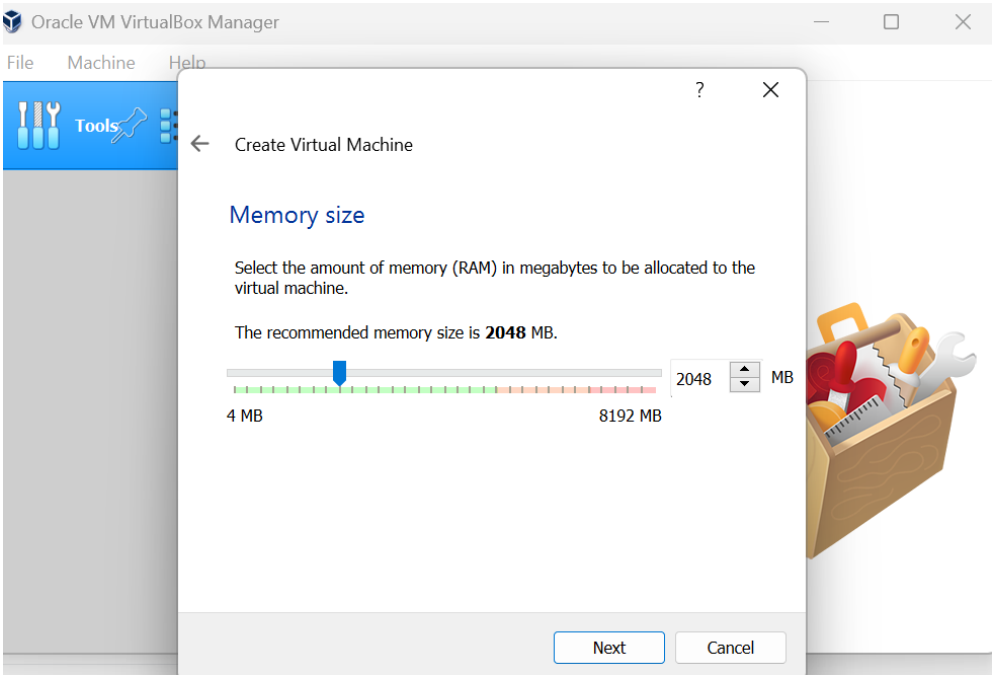
RADIUS project

RADIUS server on Window's Server 2012 & 2016:

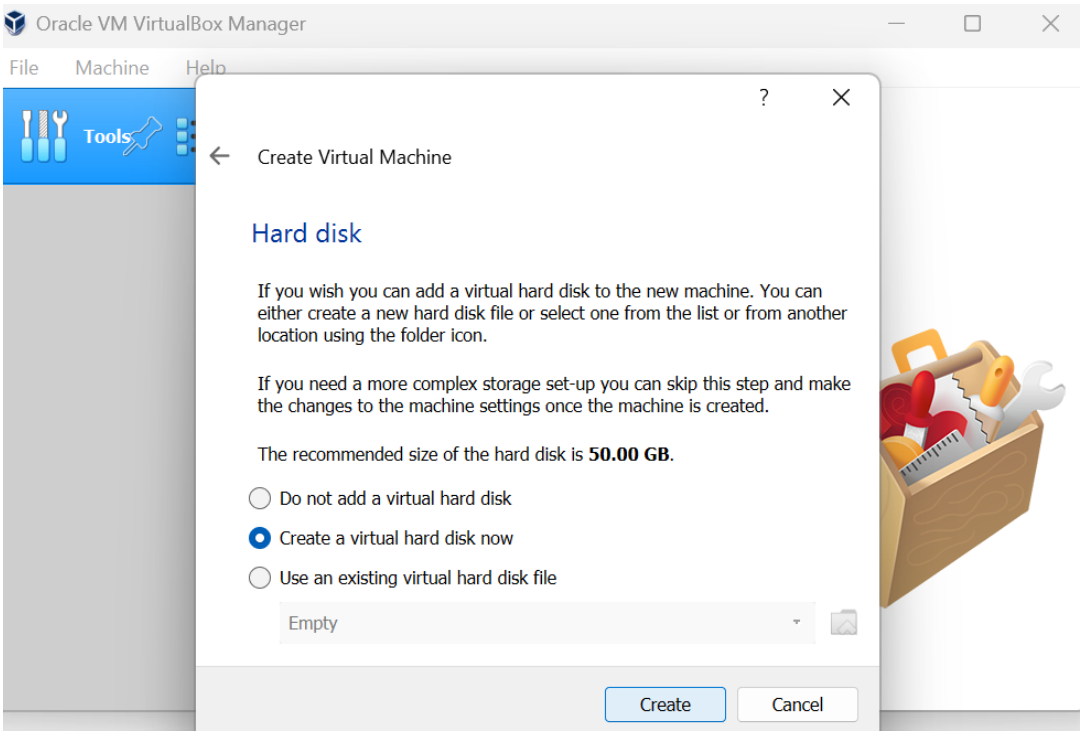
Download Oracle's VirtualBox and open after install is Finished.



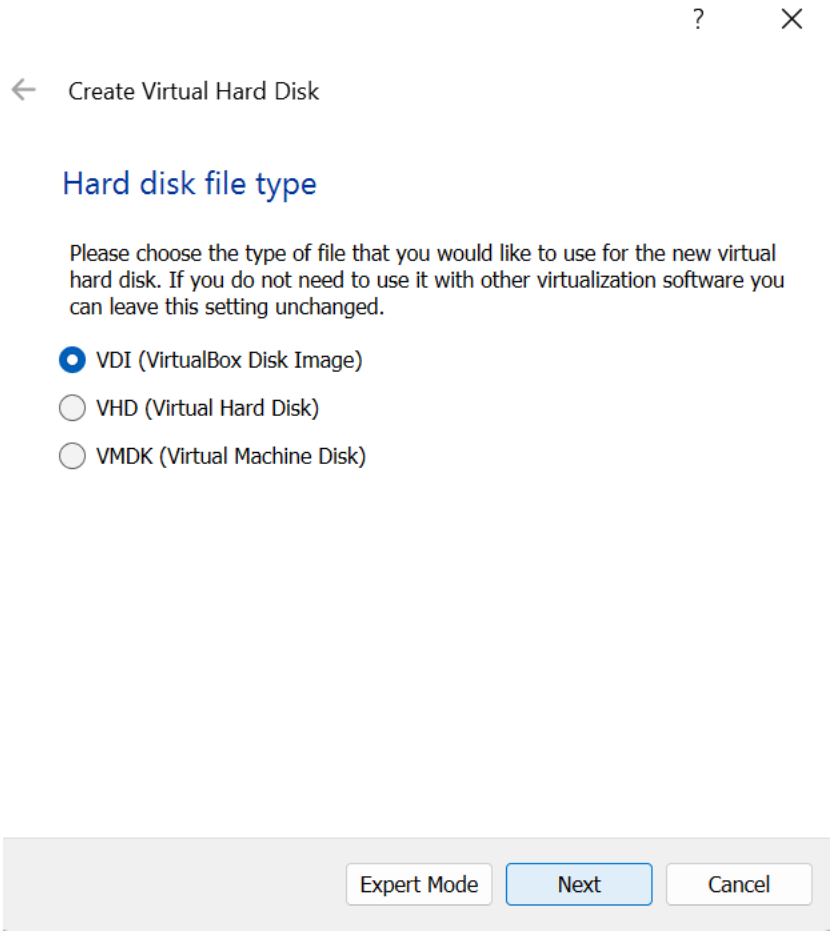
Click "New" to create a new Virtual Machine or VM, and click "Next".



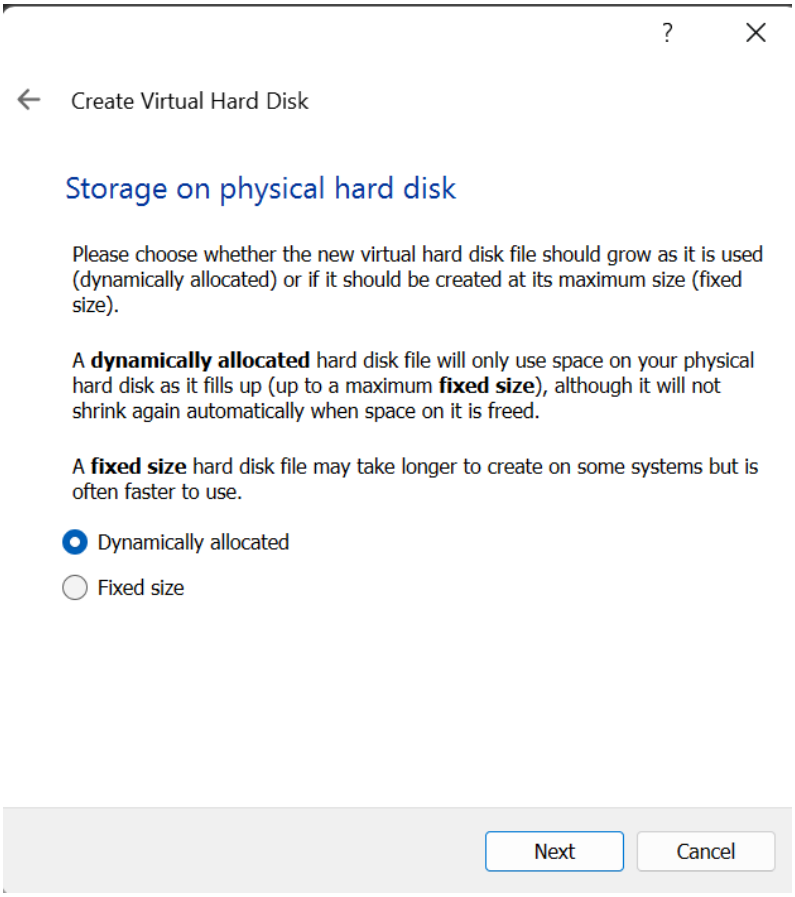
Make VM at least 2048 MB of RAM memory or more, and click "Next".



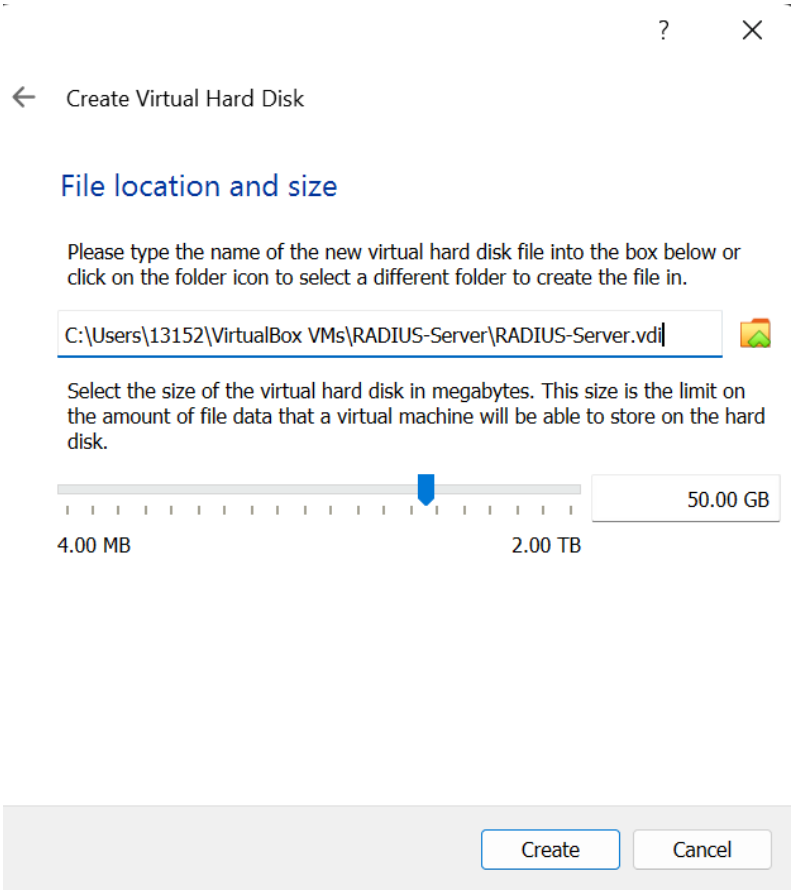
Click on “Create a virtual hard disk”, and click “Next”.



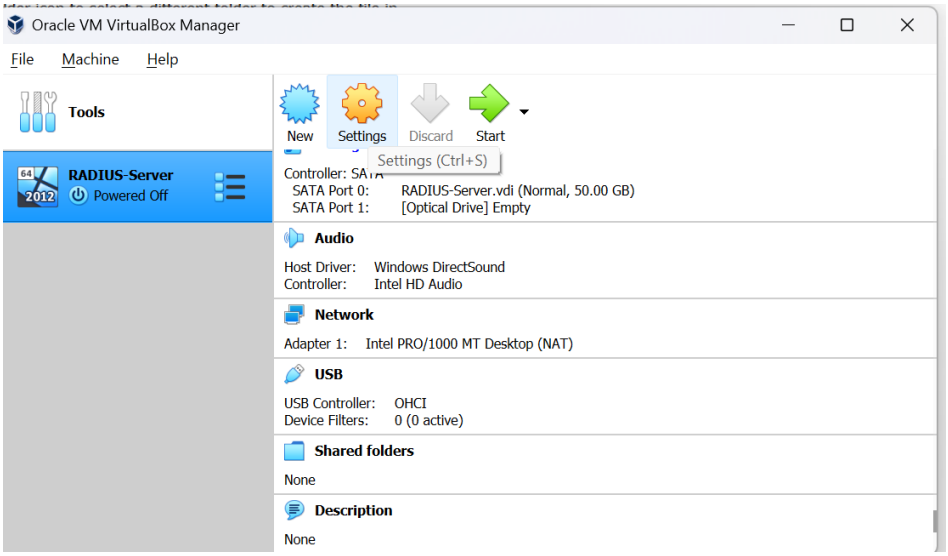
Select “VDI (VirtualBox Disk Image)”, and click “Next”.



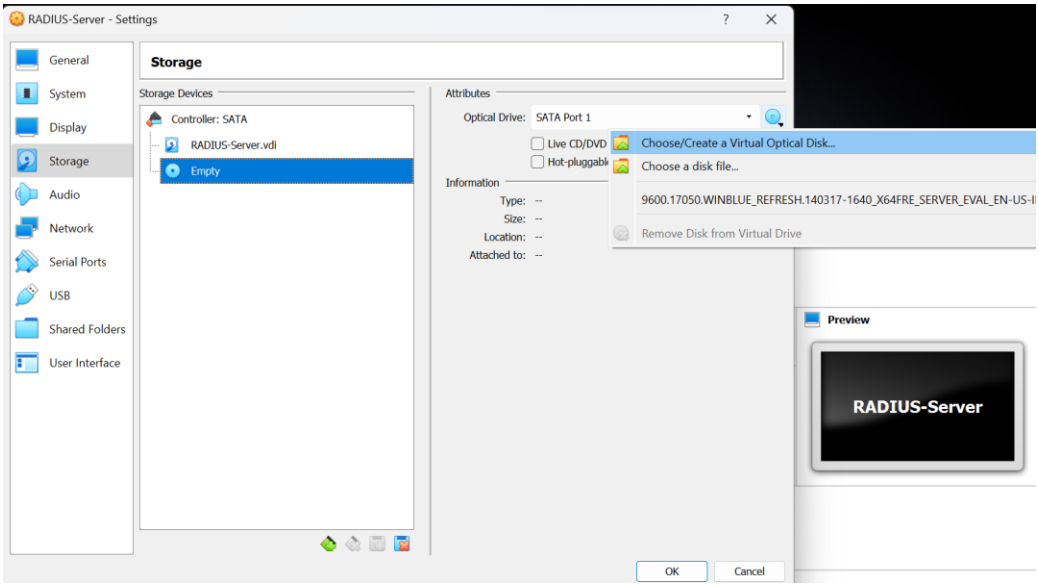
select "Dynamically allocated" and click “Next”.



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

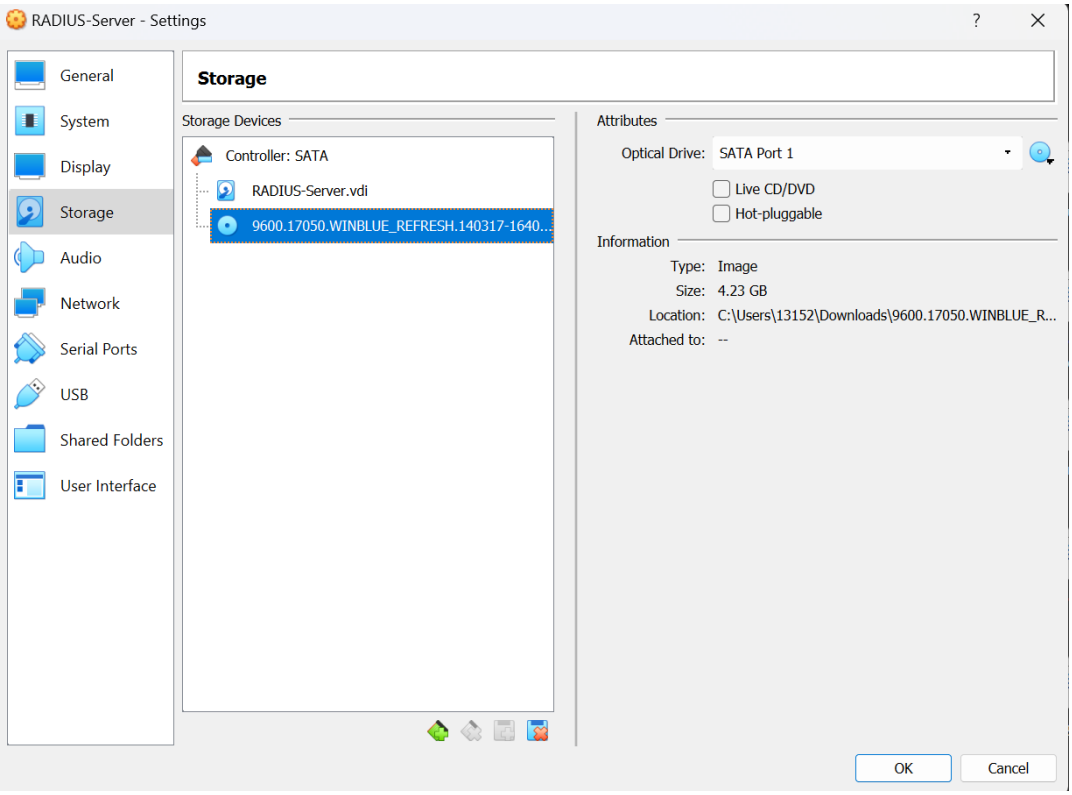


Click on “Settings” while on Windows Server VM.



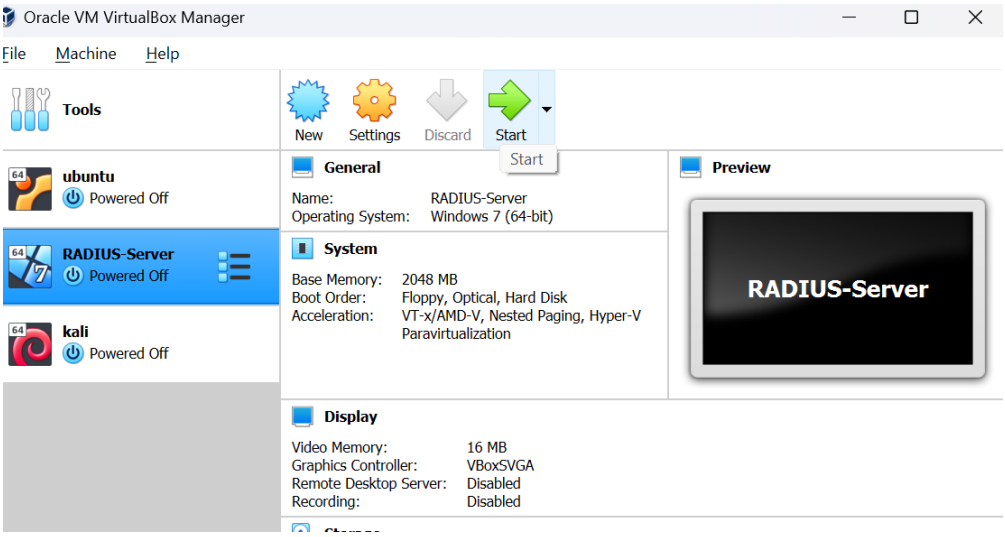
Go to “Storage” on the left side column and click under “Attributes” next to “Optical Drive”.

Select “Choose/Create a Virtual Optical Disk”.

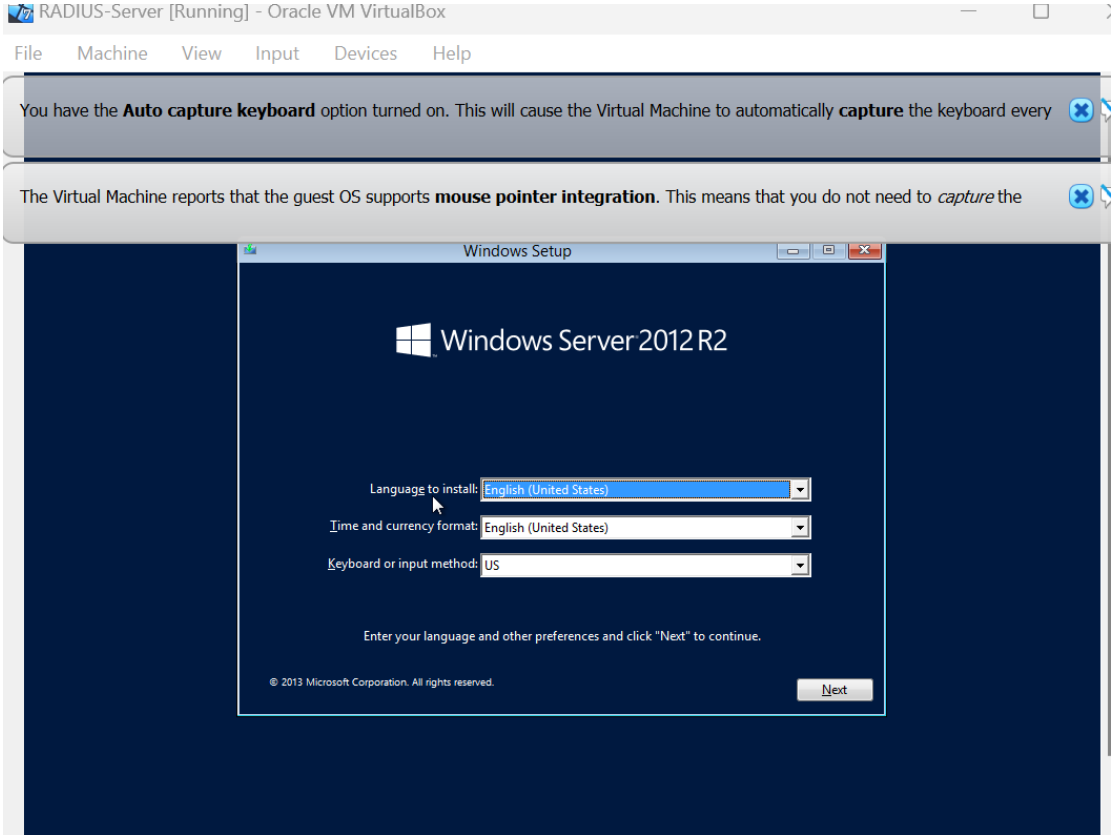


Under “Controller: SATA” is the hard drive for windows 2012 server. (that will be running RADIUS)

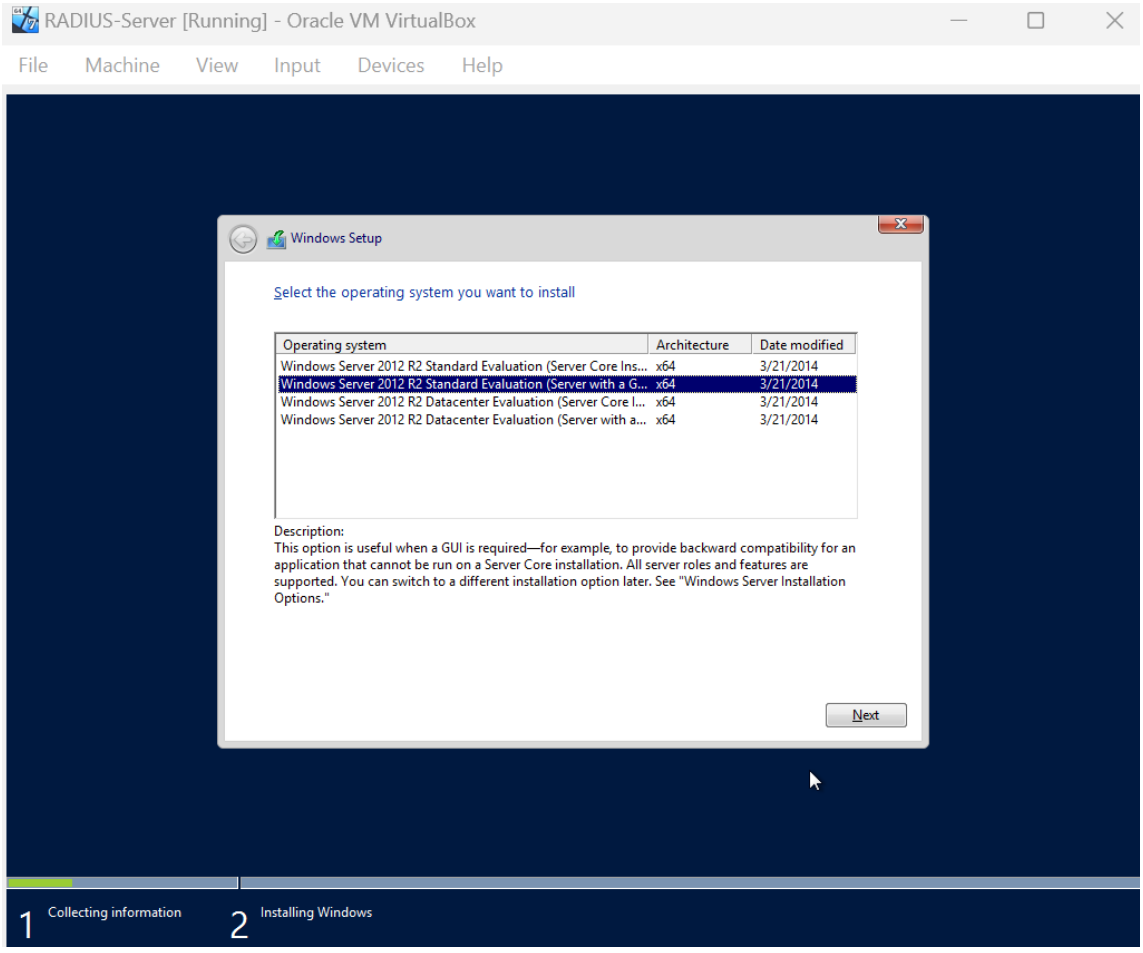
Click on “OK”.



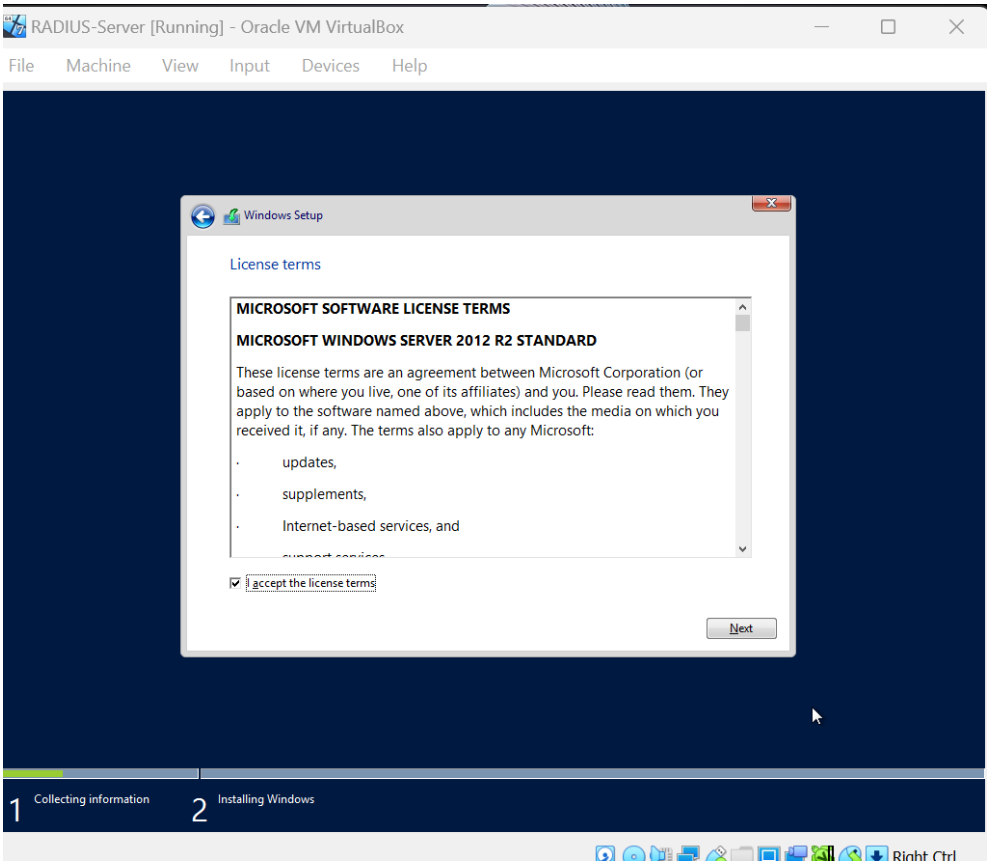
Click on “Start” which is the green right arrow.



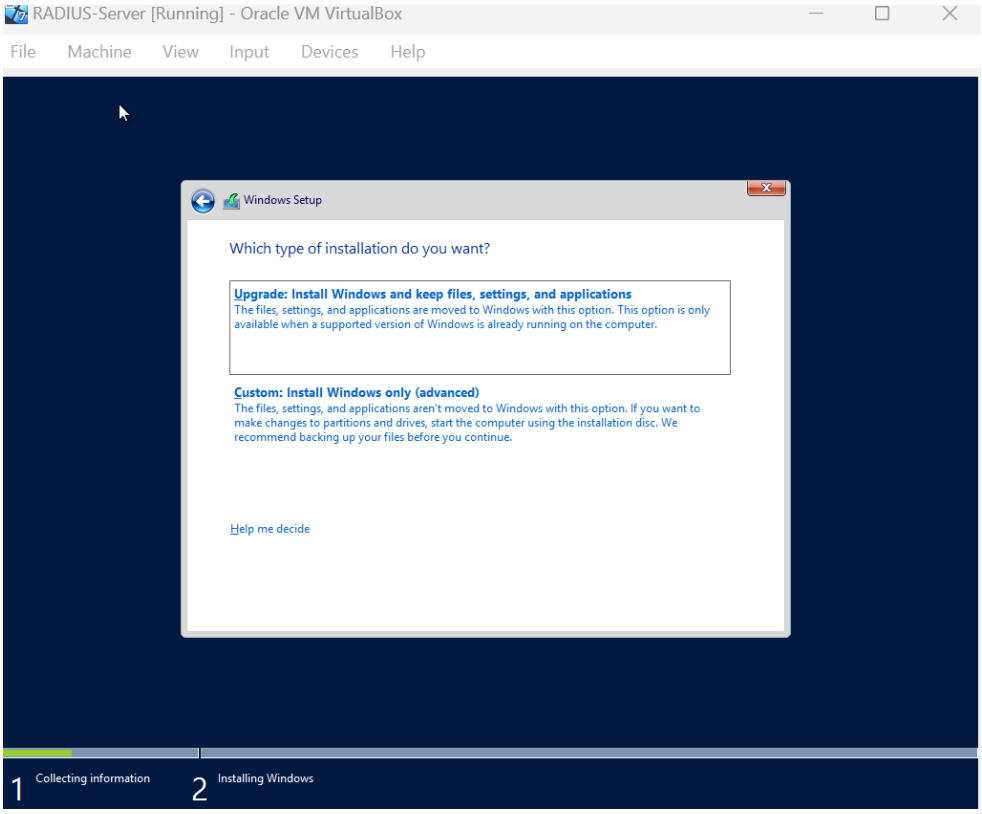
Select language and click “Next”.



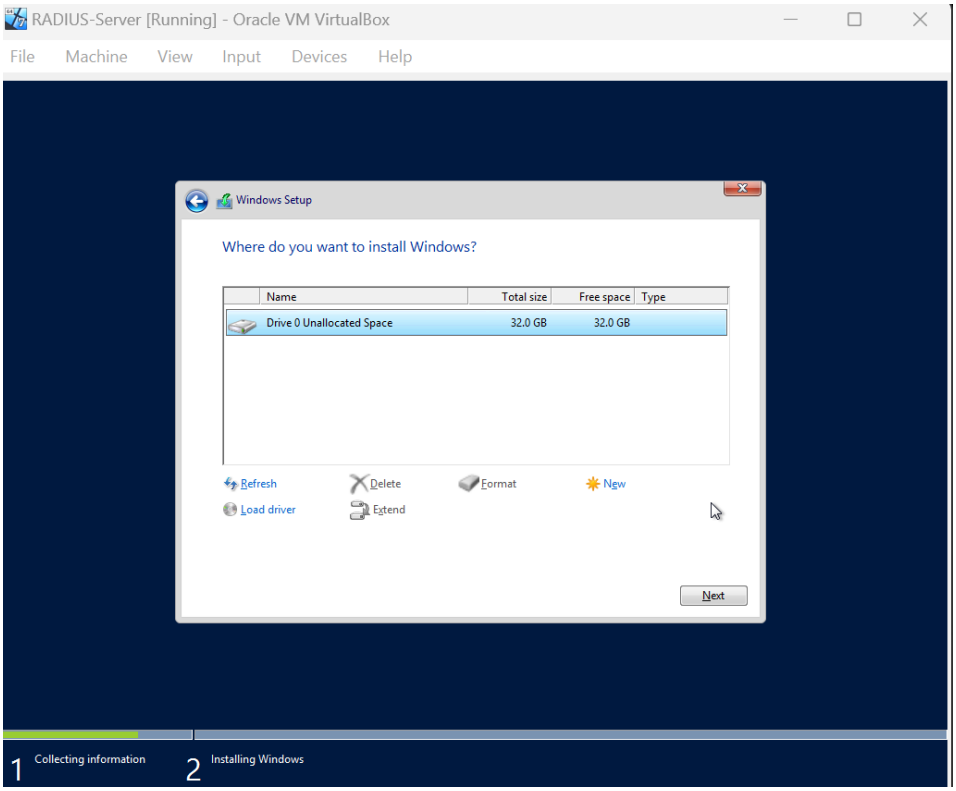
Choose the second option which is the Windows Server 20212 “with a GUI” and click “Next”.



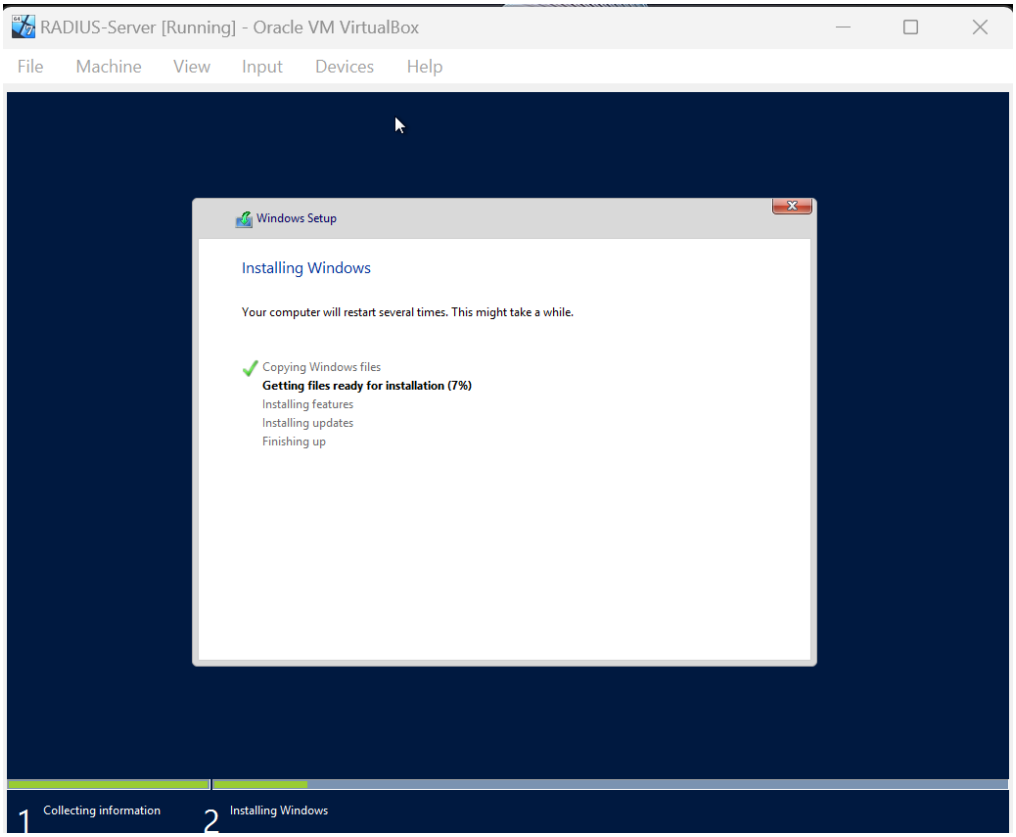
Check in “I accept the license terms” and click “Next”.

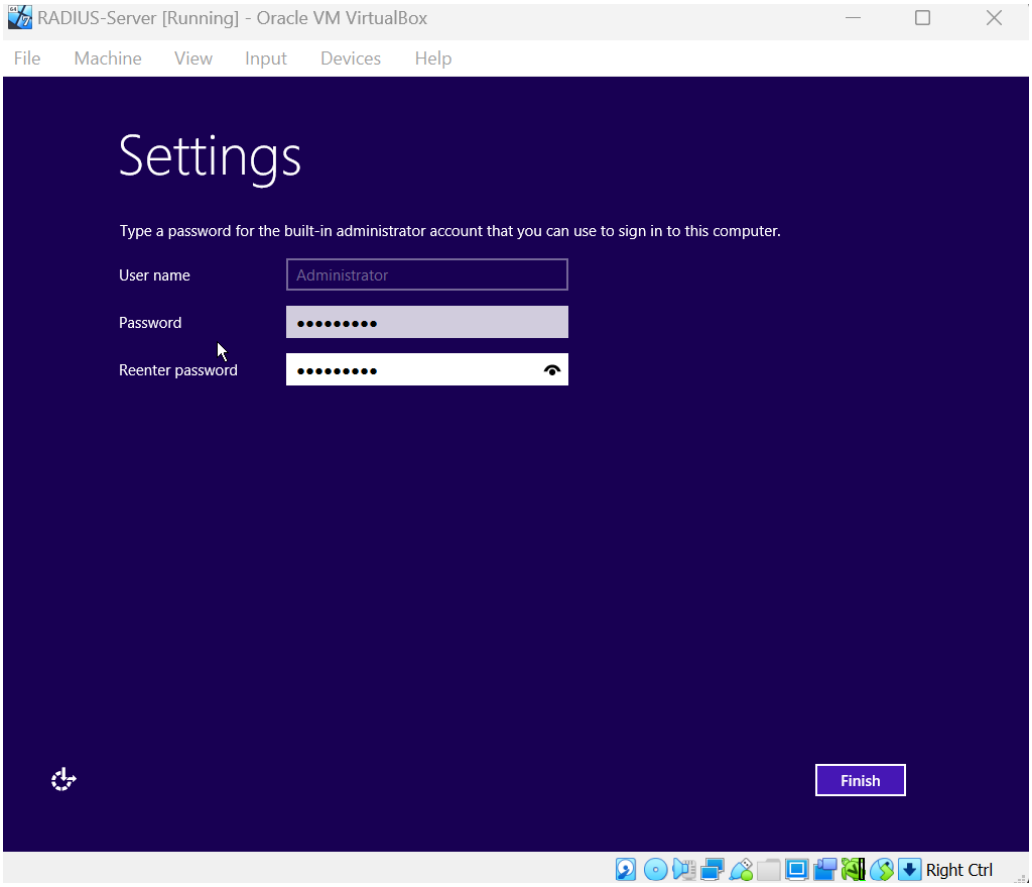


Choose/click “Upgrade Install Windows and keep files, settings, and applications”.



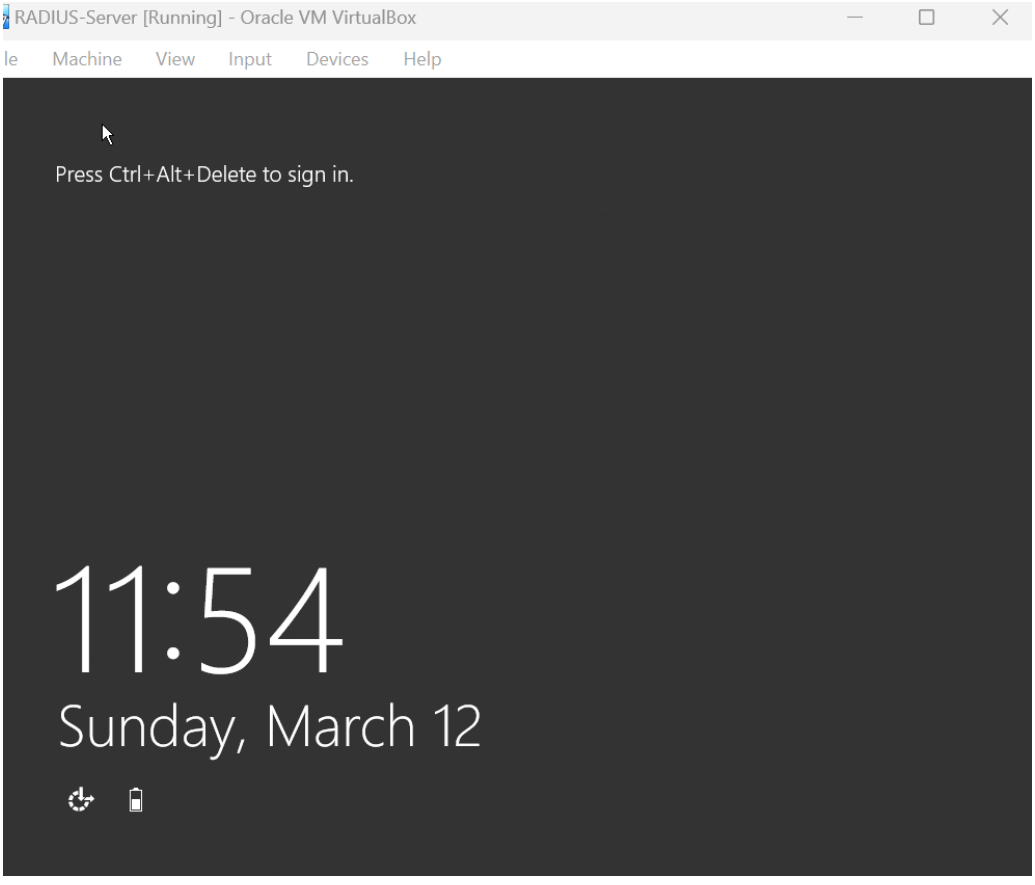
It will now automatically partition after clicking “Next”.



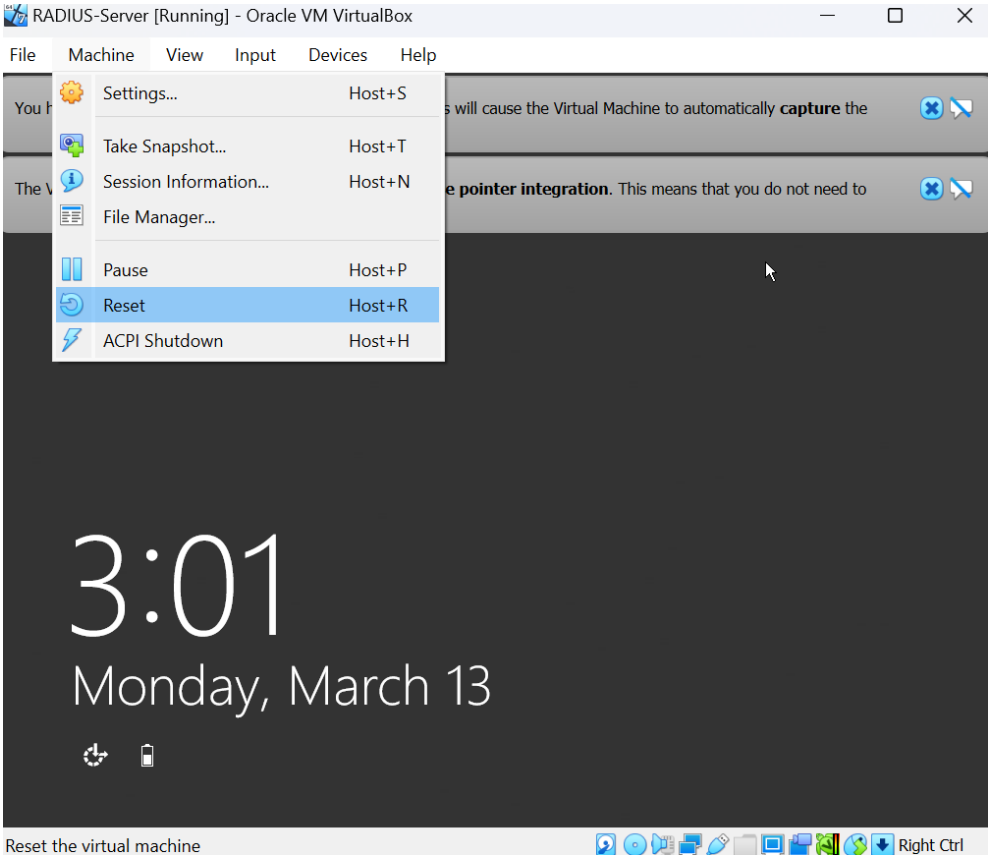


Create an admin password and click “Finish”.

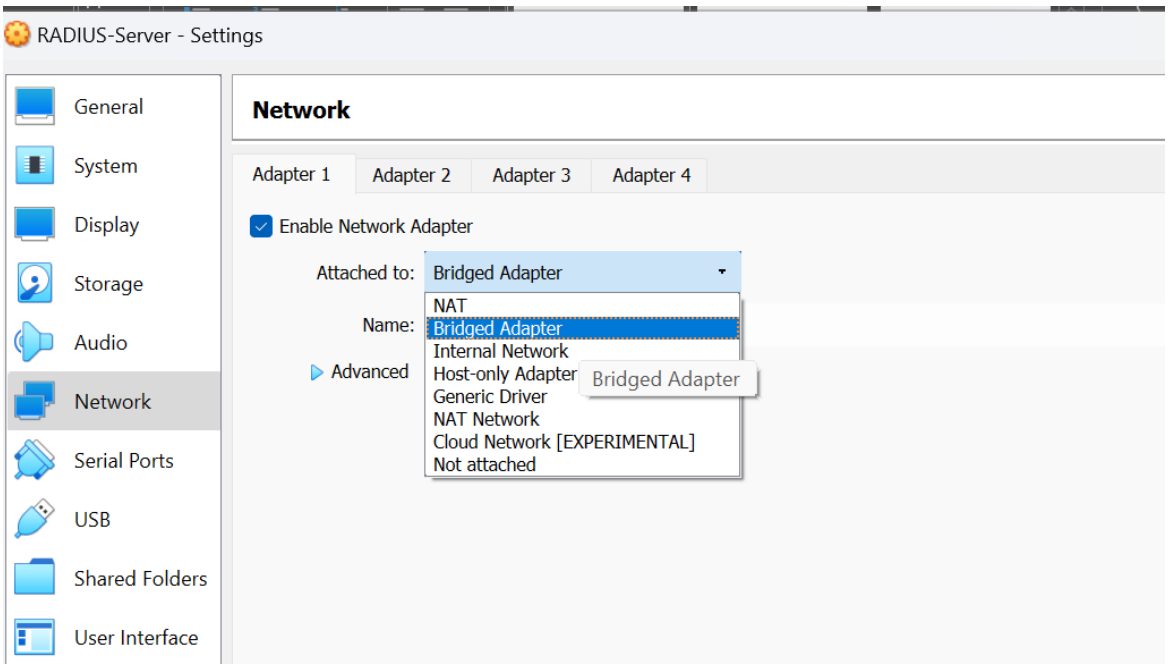
Restart VM.



Press ctrl + alt + delete buttons.

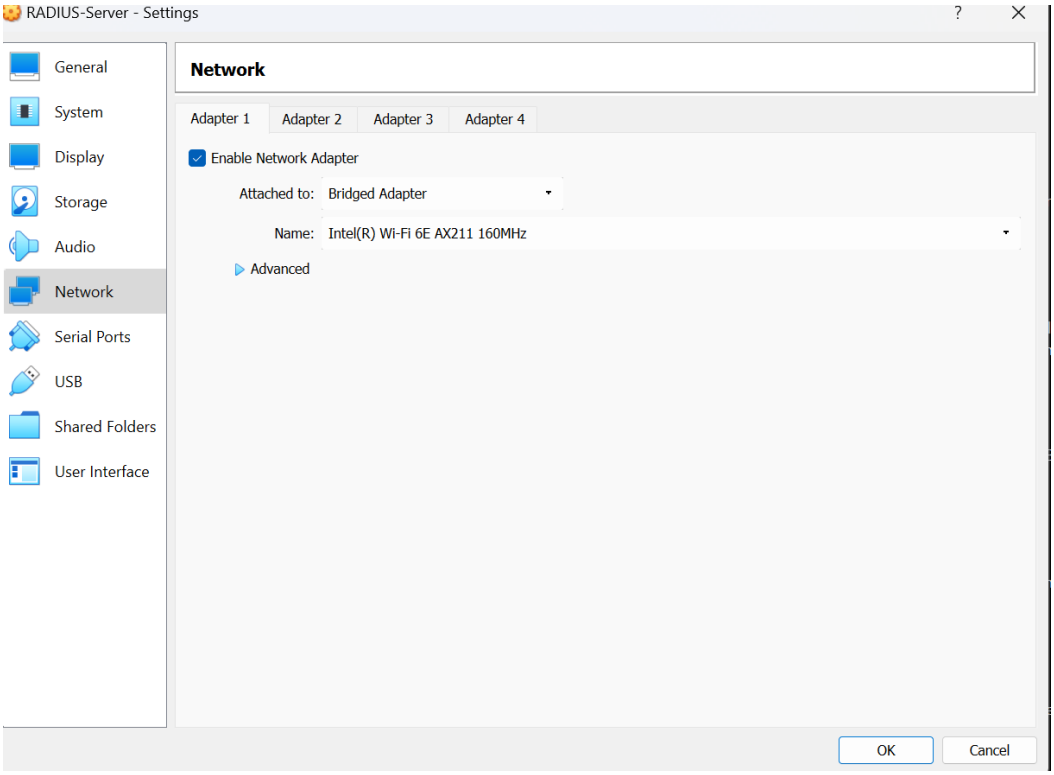


Go to “Machine” and click on “Reset”.

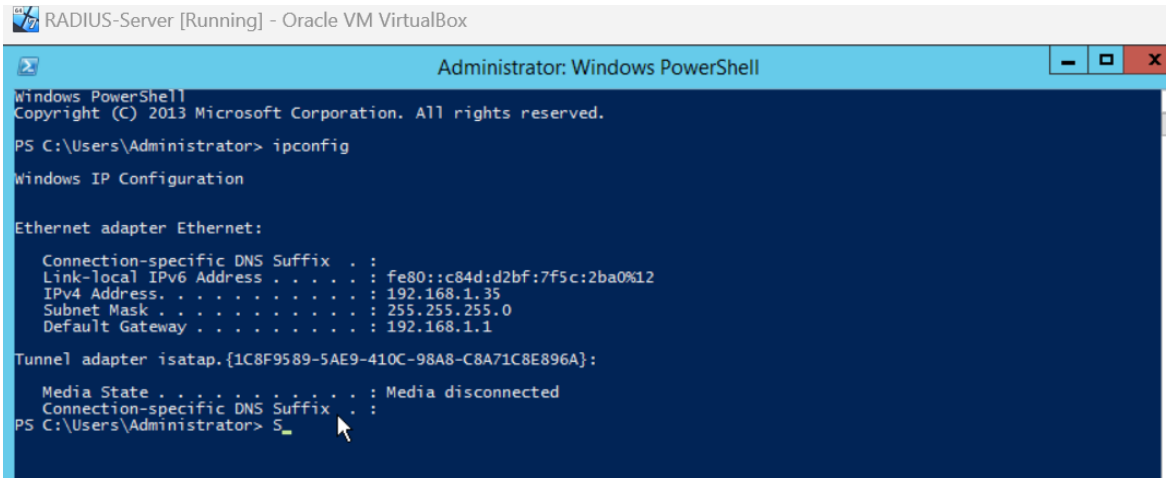


Click on “Settings” again and go to “Network” on left side of the column.

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



Click on “OK”.

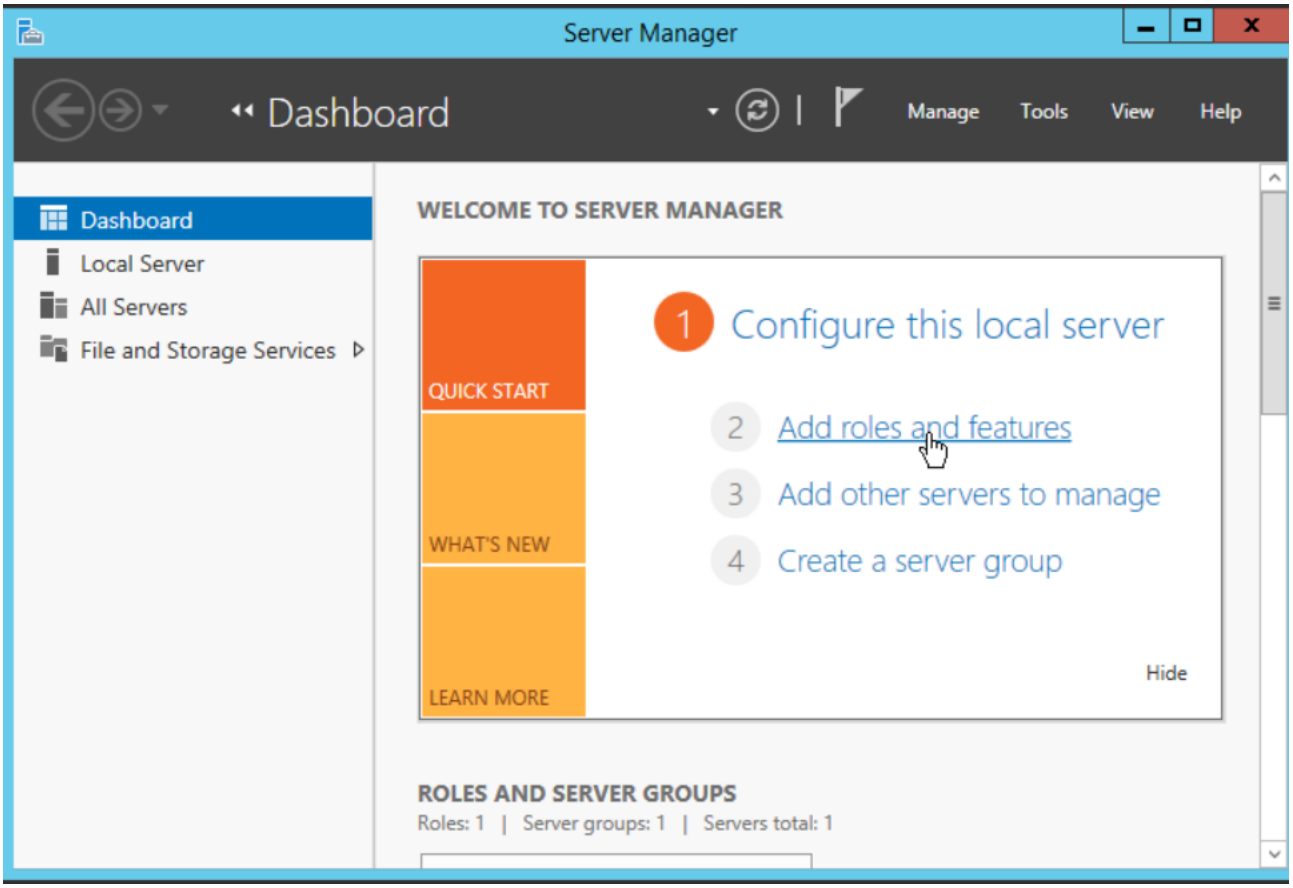


Go to Windows PowerShell.

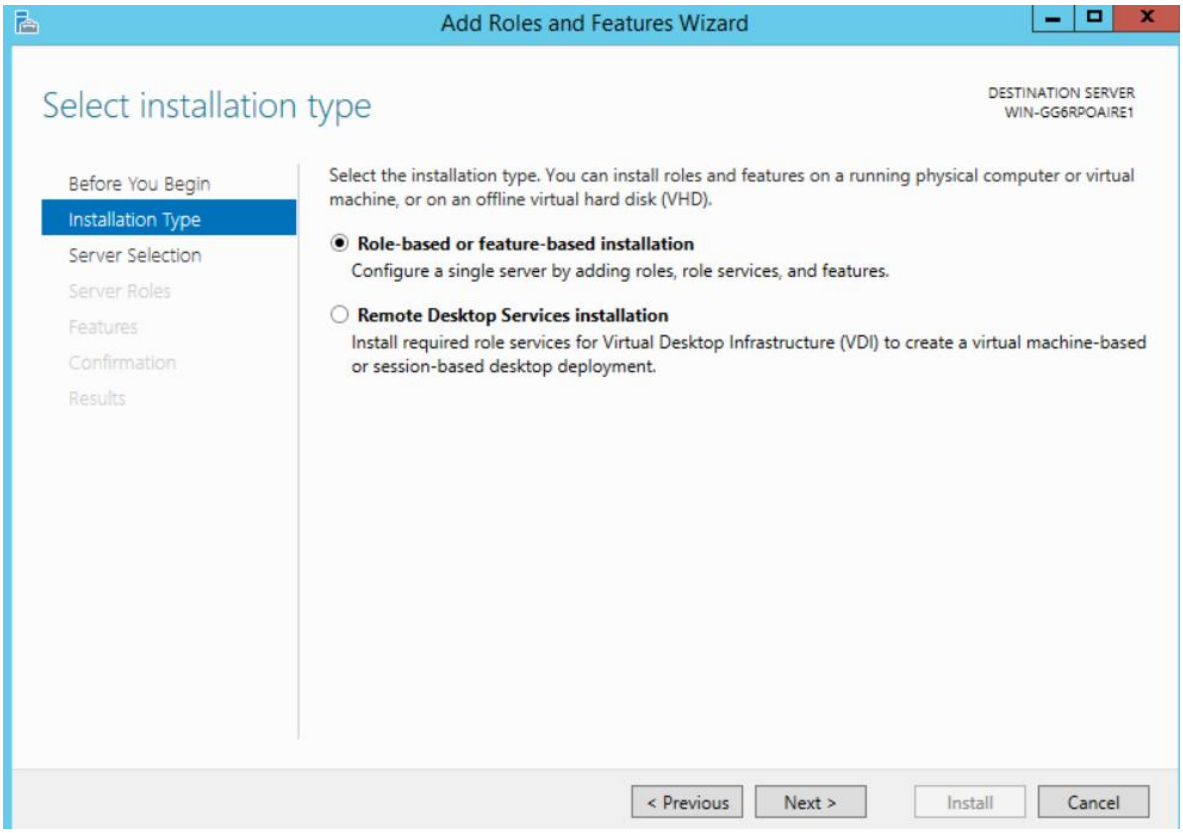
Type in “ipconfig” command.

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

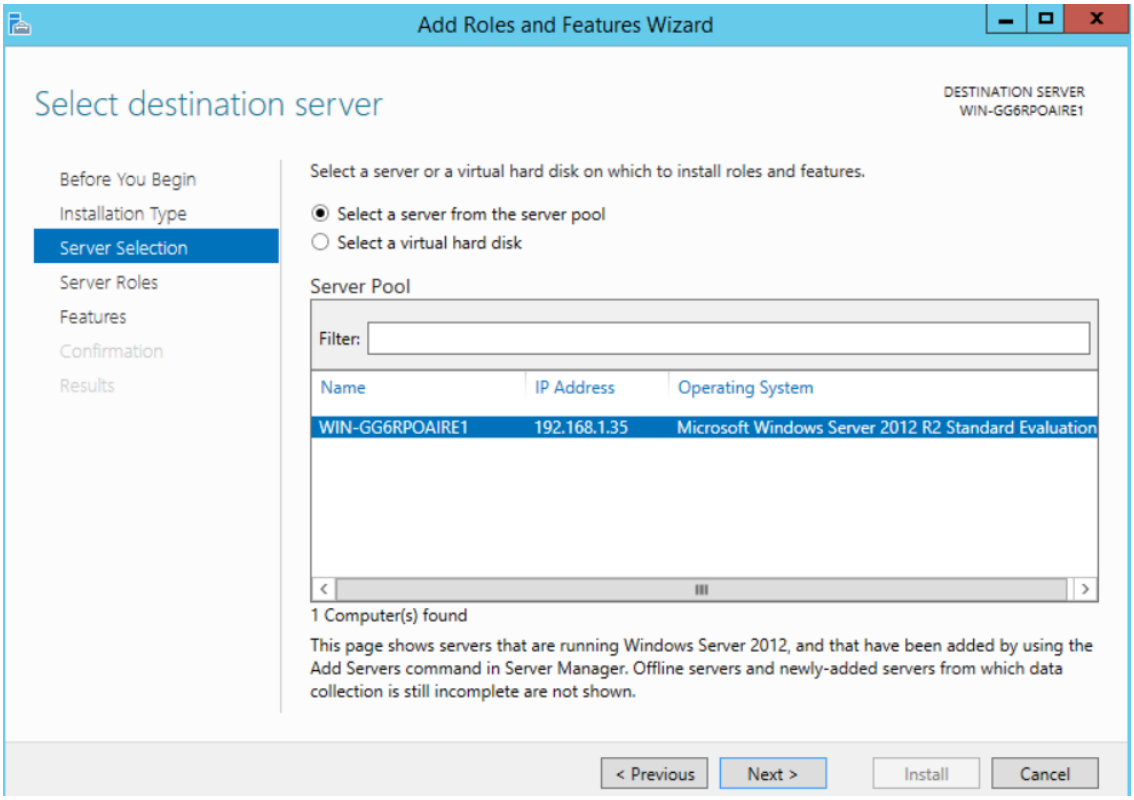
This is IP address for Windows Server through bridged adapter.



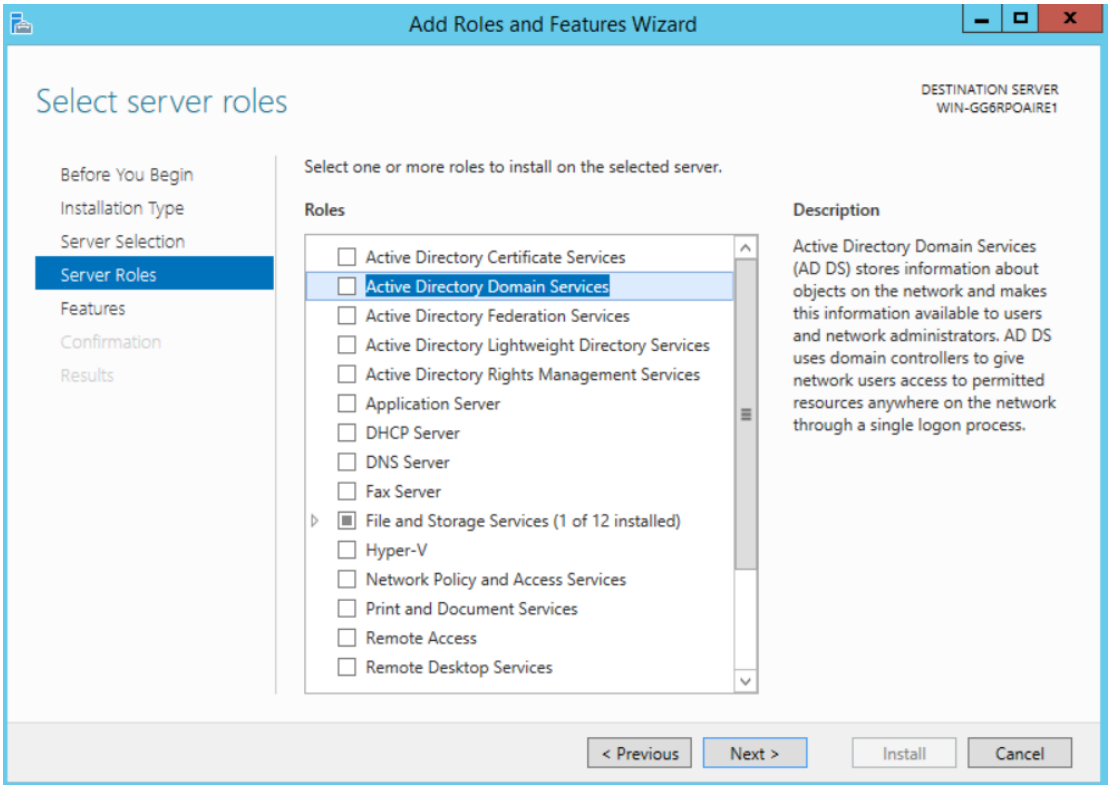
In Windows Server manager click “Add roles and features”.



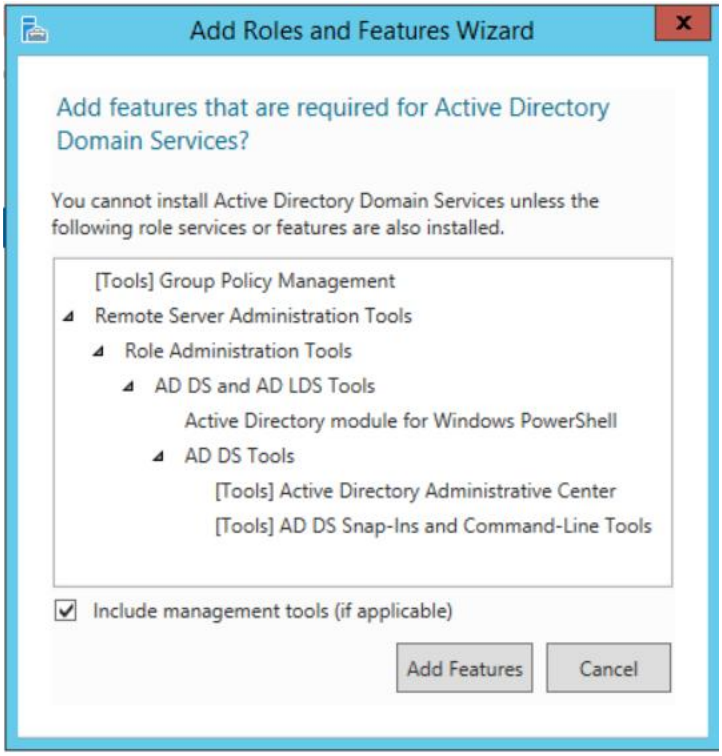
On left column select “Installation Type” and then make sure you select “Role-based or feature-based installation and click “Next”.



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

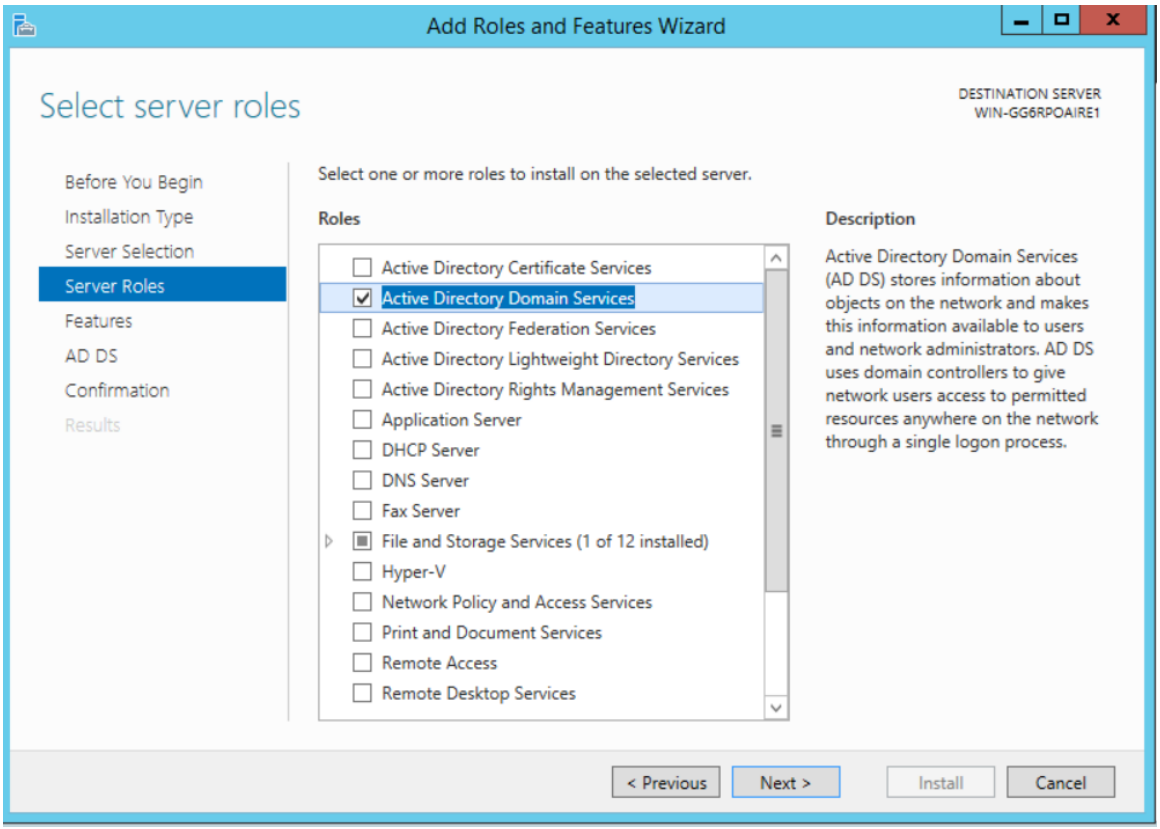


Now choose the roles “Active Directory Domain Services”.

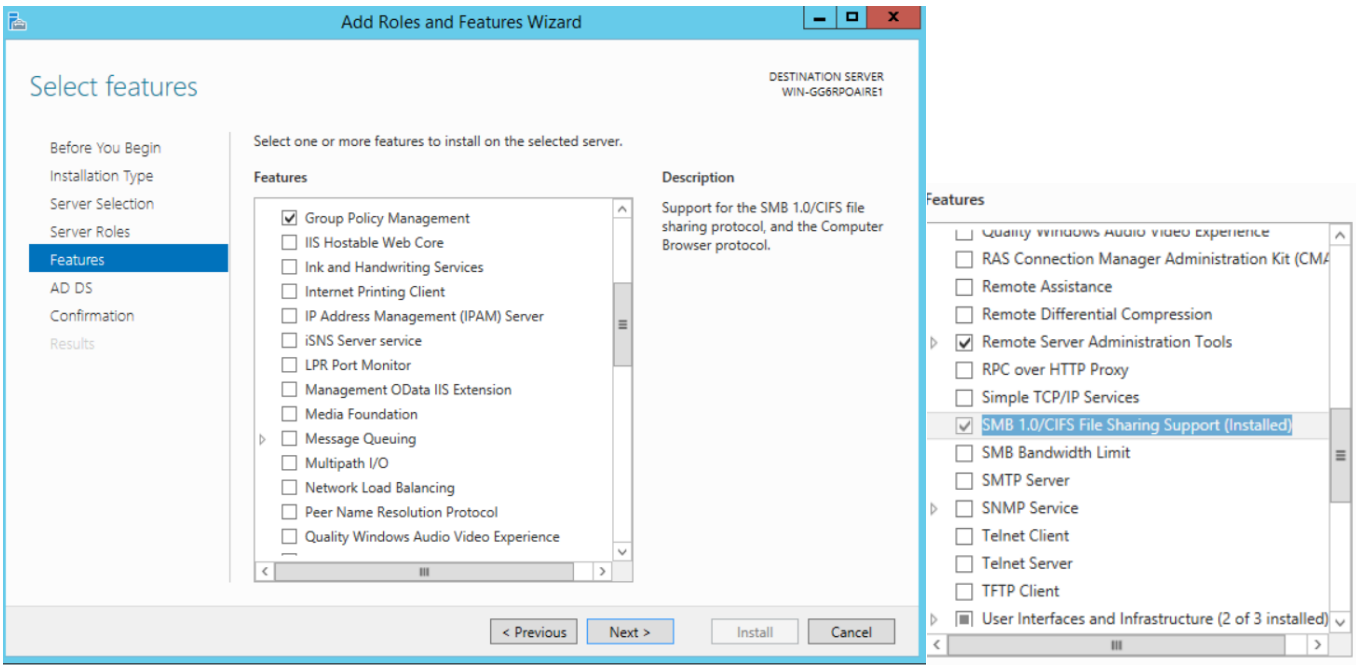


Then, a pop-up will appear so click on “Add Features” at the bottom.

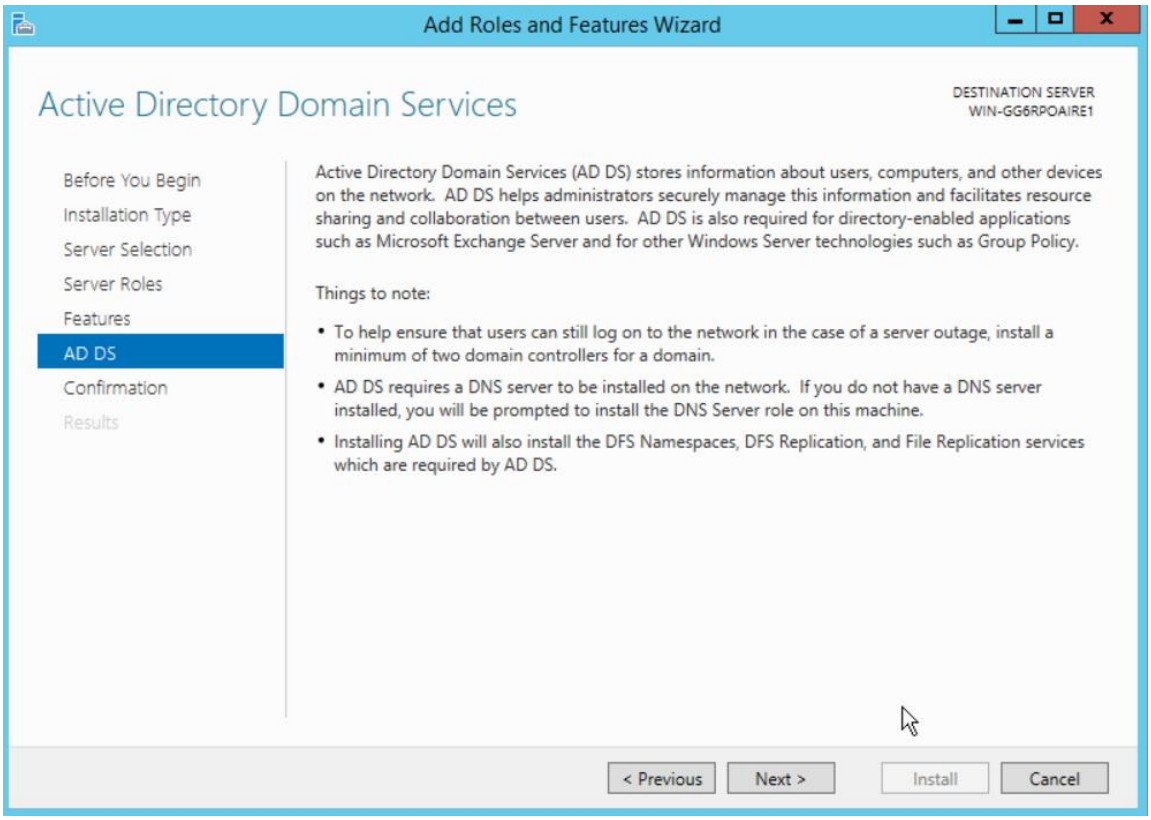
Keep “Include management tools (if applicable)” checked.



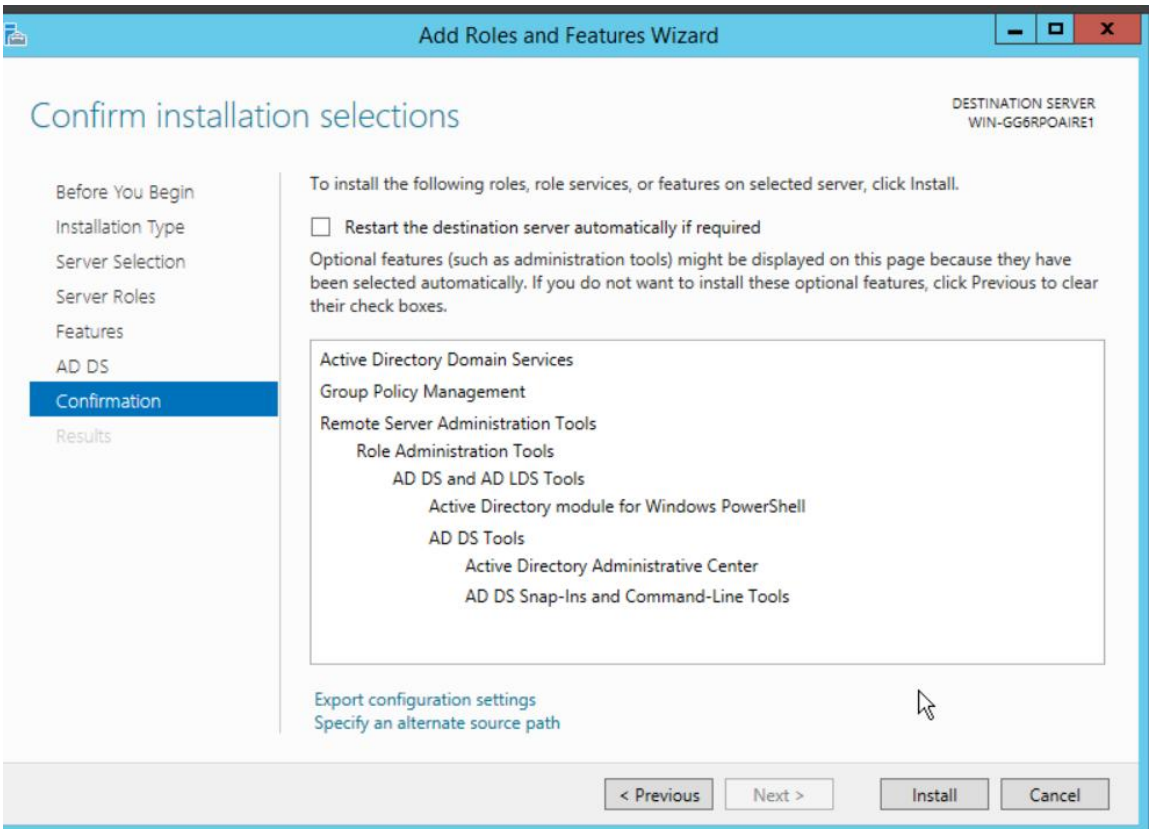
Now “Active Directory Domain Services” will be checked in, click “Next”.



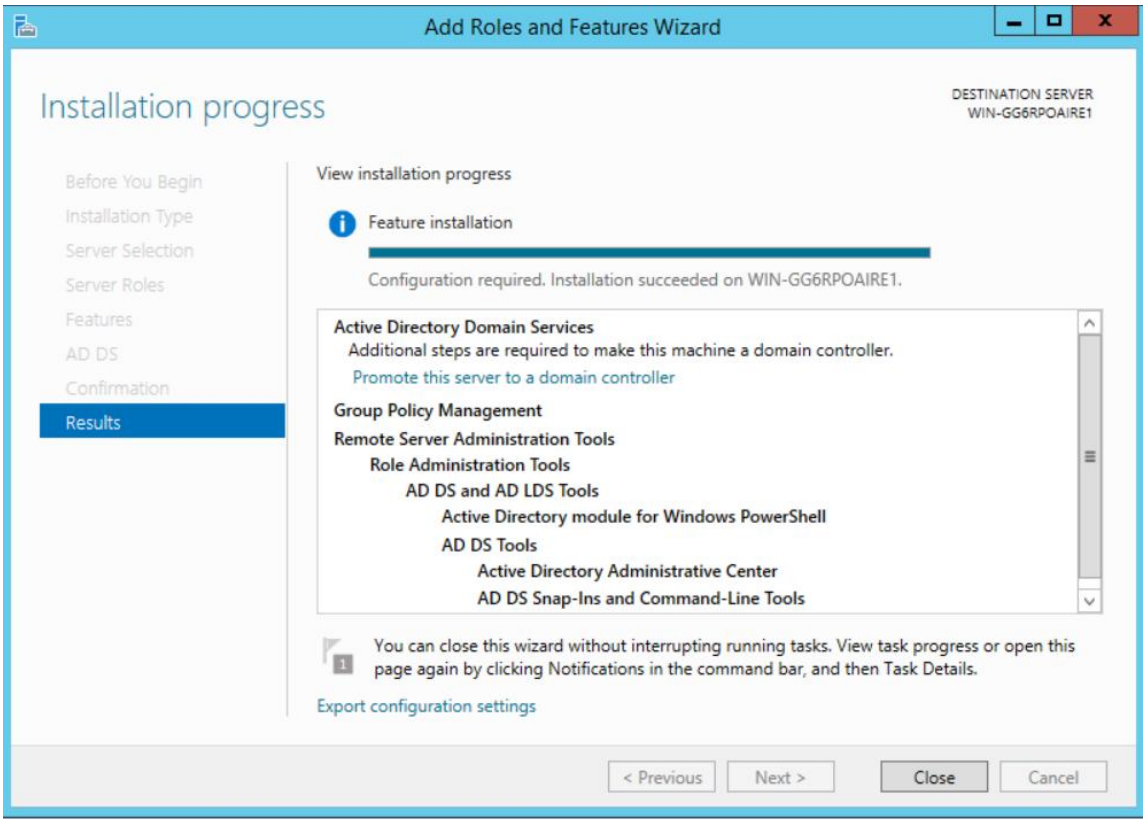
Keep “Group Policy Management” and “Remote Serve Administration Tools” checked, which should automatically be by default. Click “Next”.



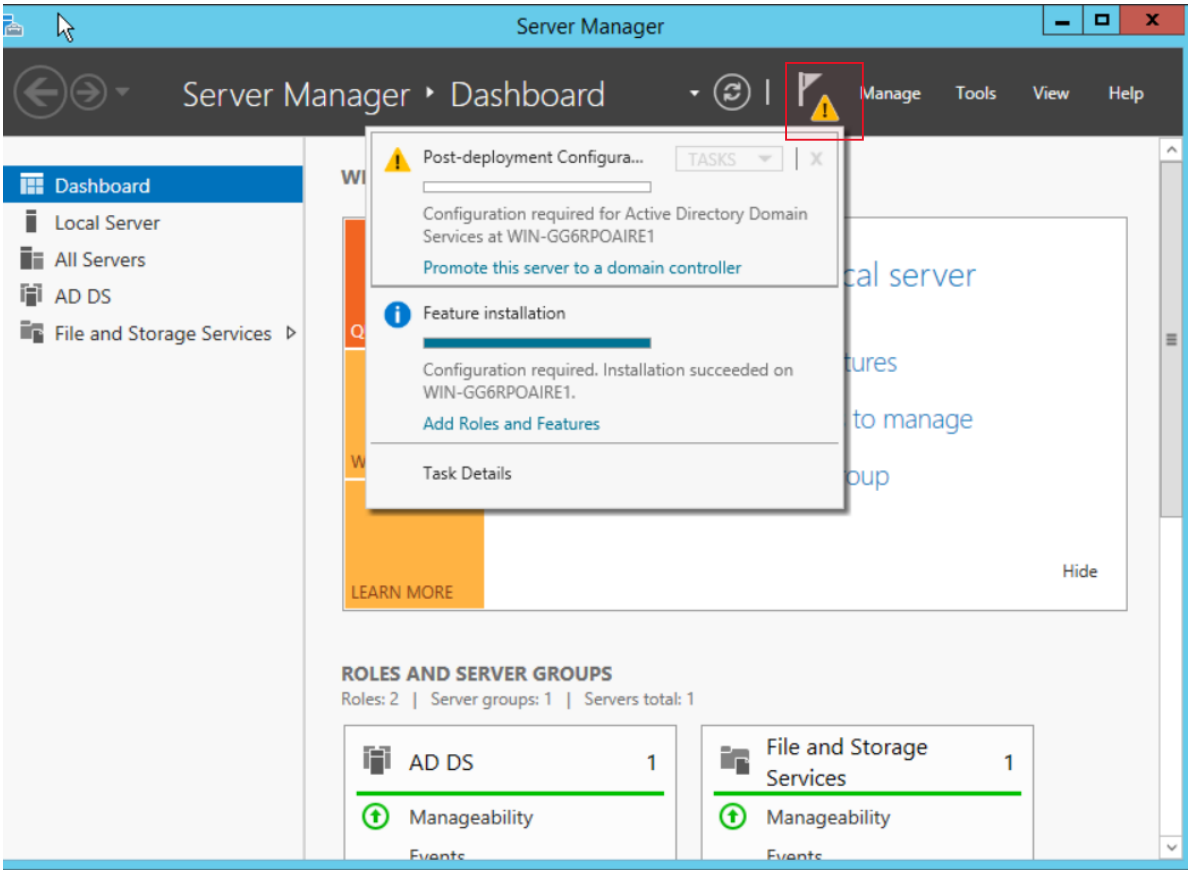
Click “Next” again.



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

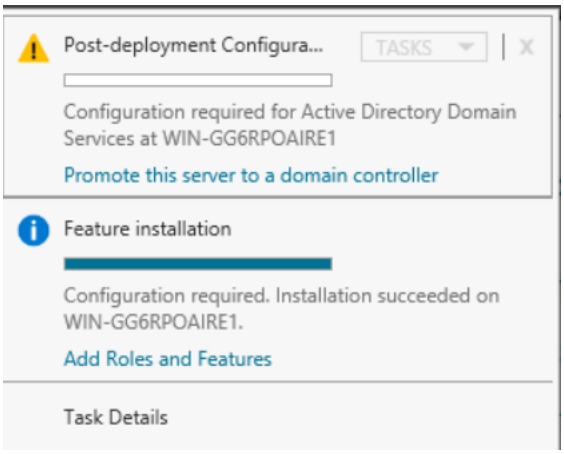


After all features were installed successfully and click “Close” so you can apply configuration as reminded above.

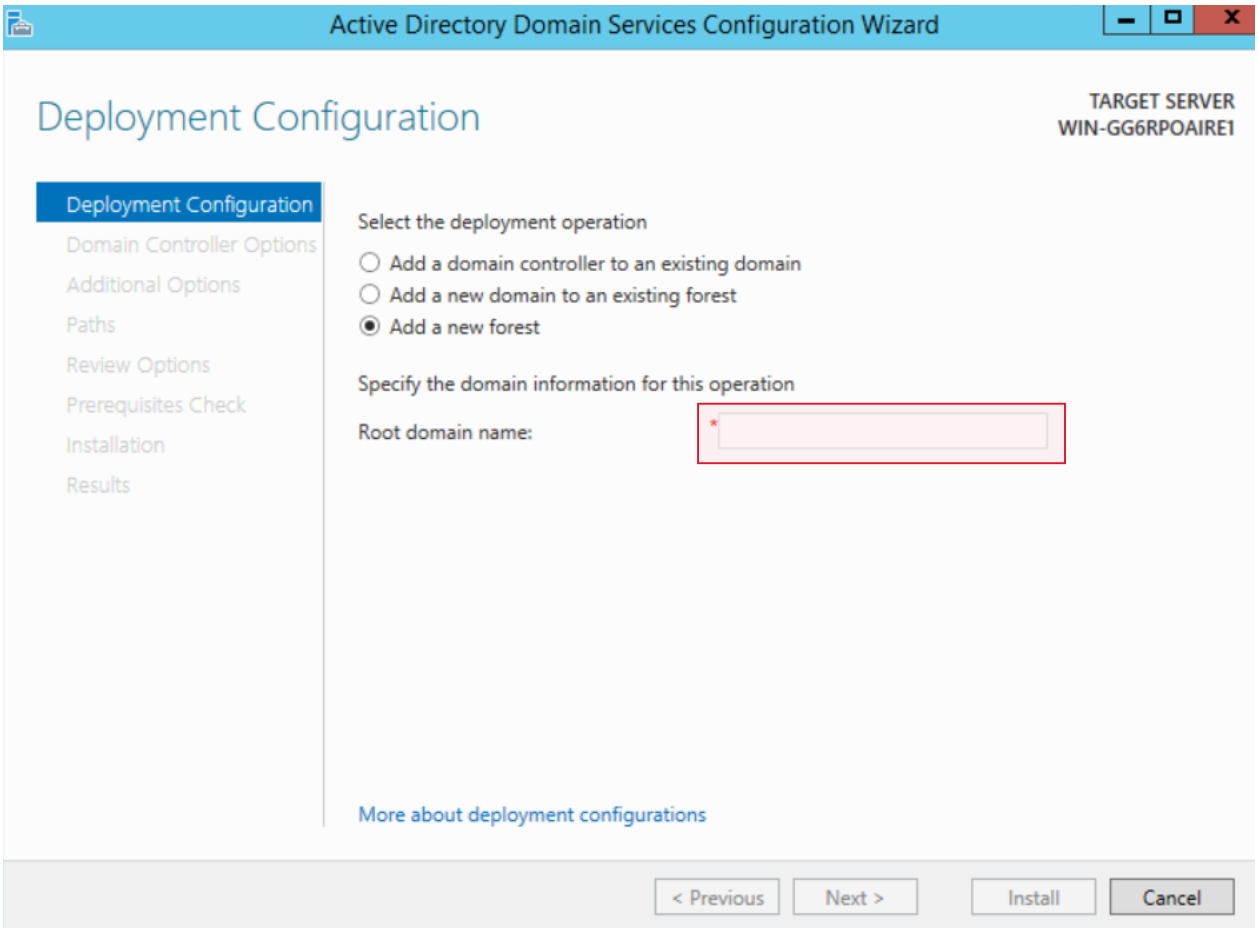


In the red box above there is a yellow triangle with an explanation point next to a flag. Click on that.

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

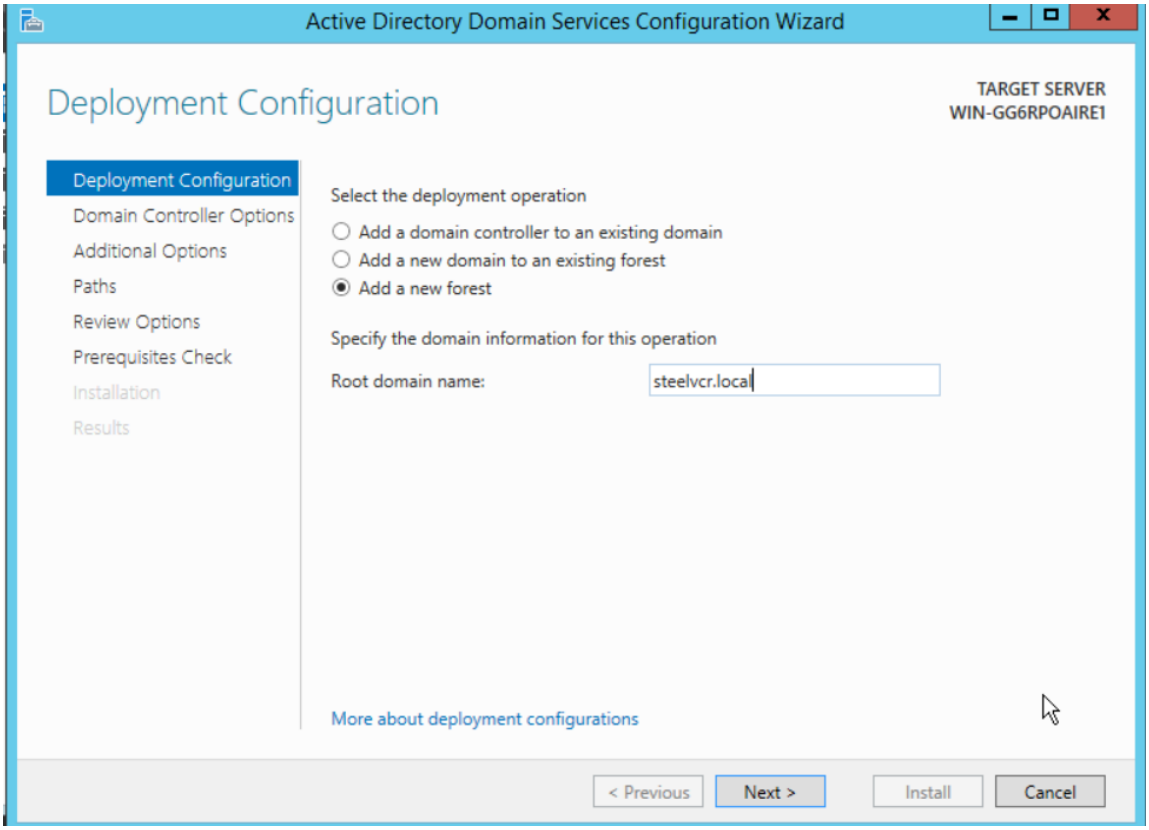


Click “Promote this server to domain controller”.

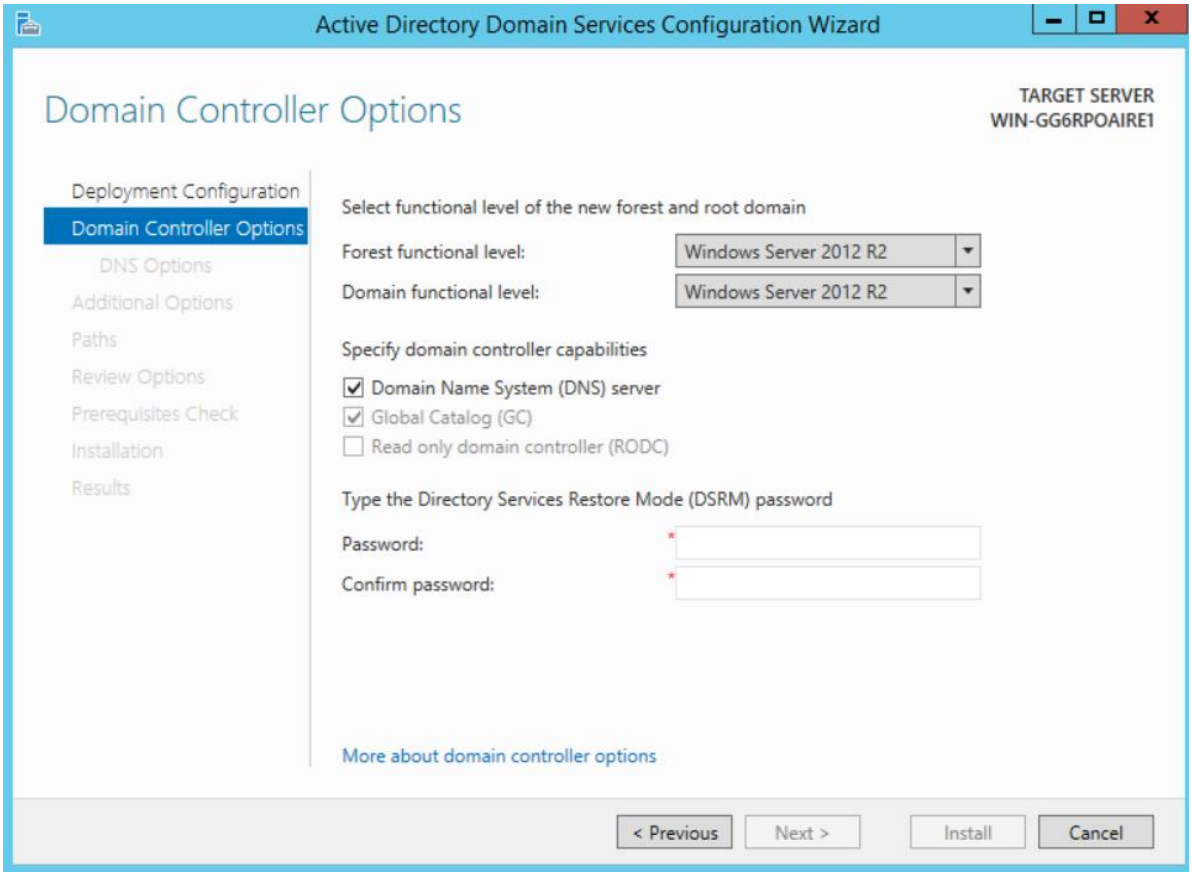


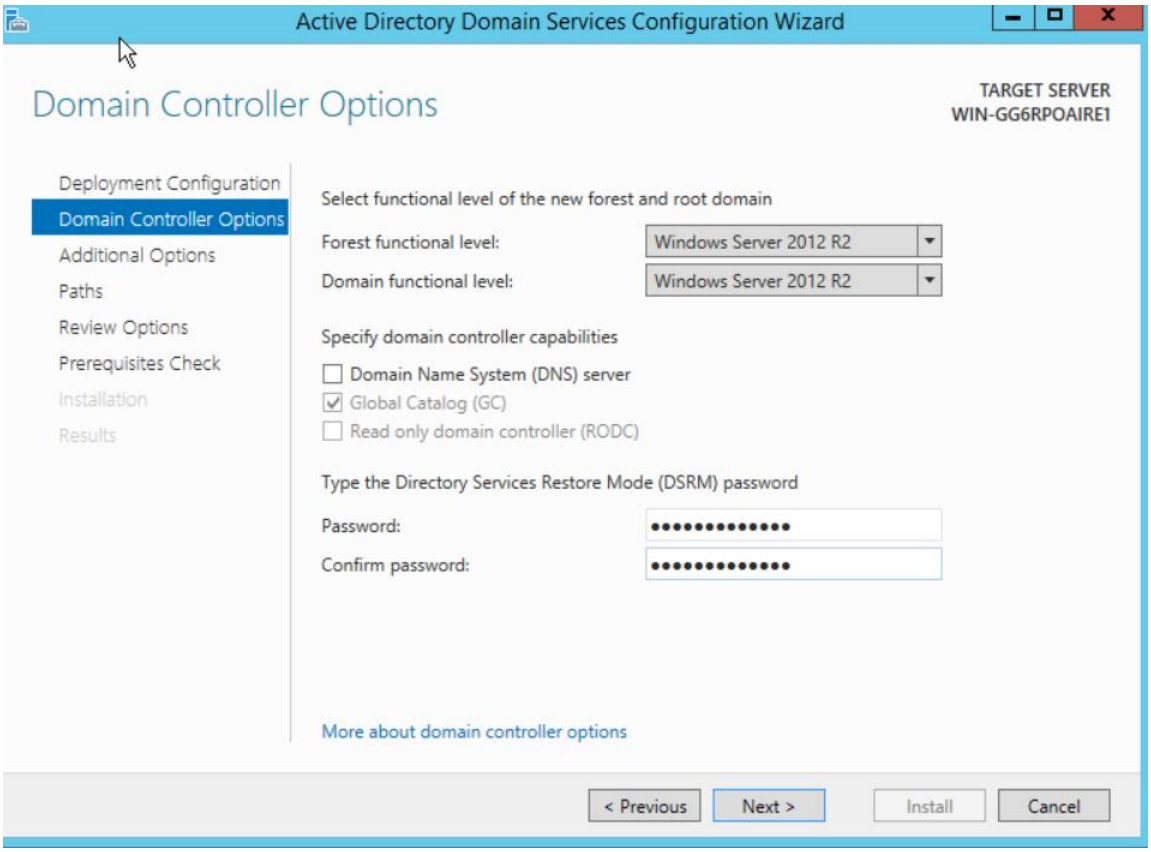
Choose the 3rd option or “Add a new forest”.

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



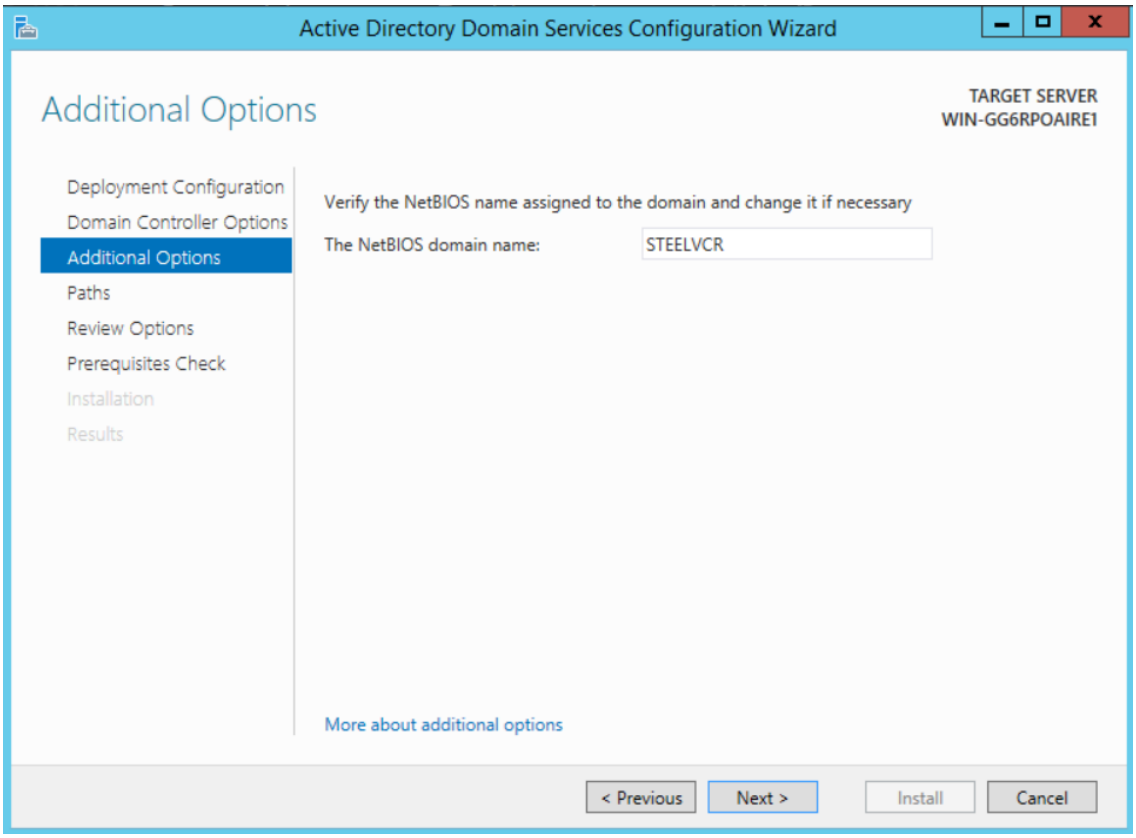
After typing root domain name click “Next”.



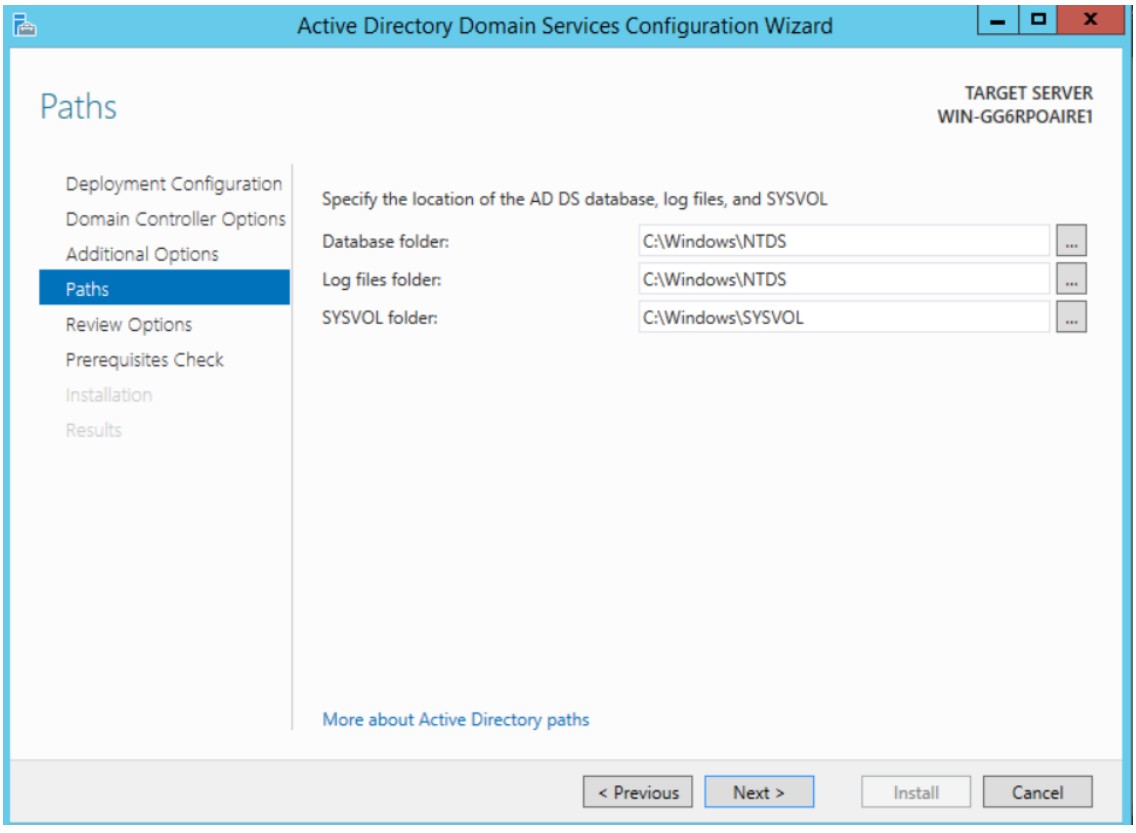


Take off the checkmark on first checkbox that read “Domain Name System (DNS) server”.

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

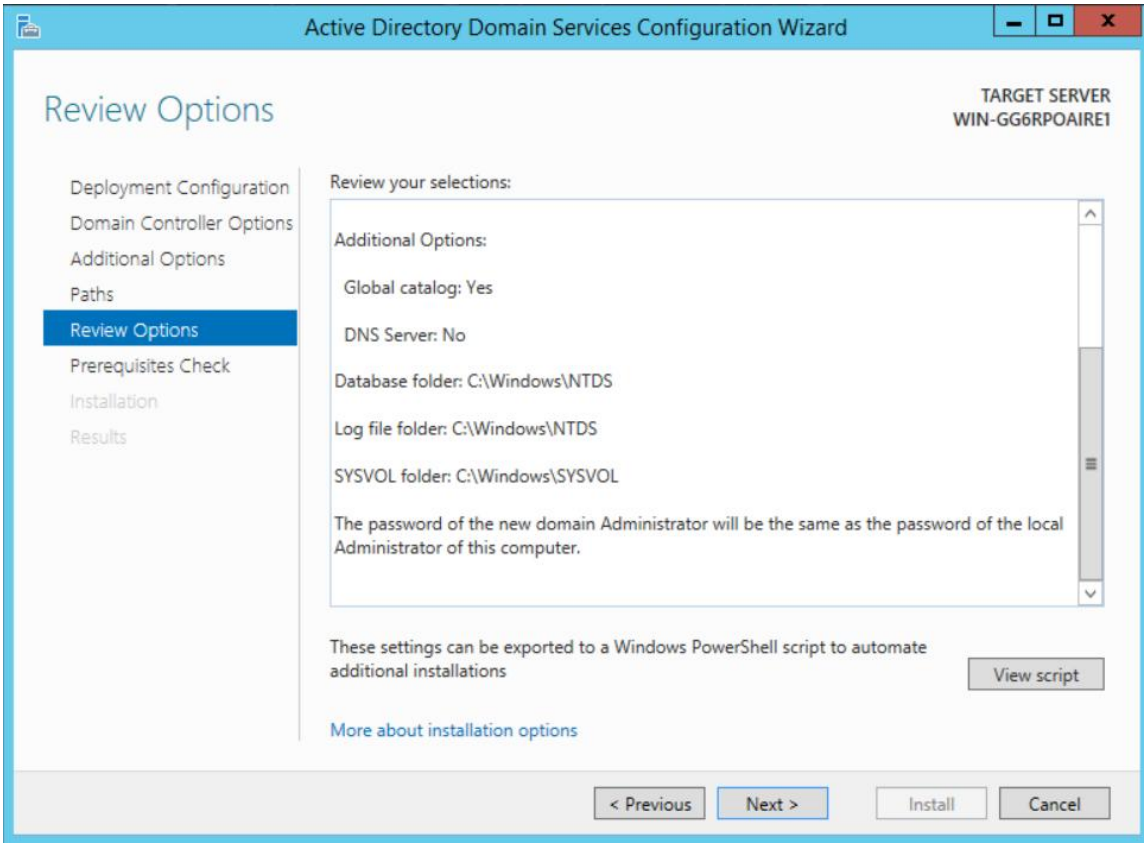


Keep or change NetBIOS domain name (addition option for Domain Controller), and click “Next”.

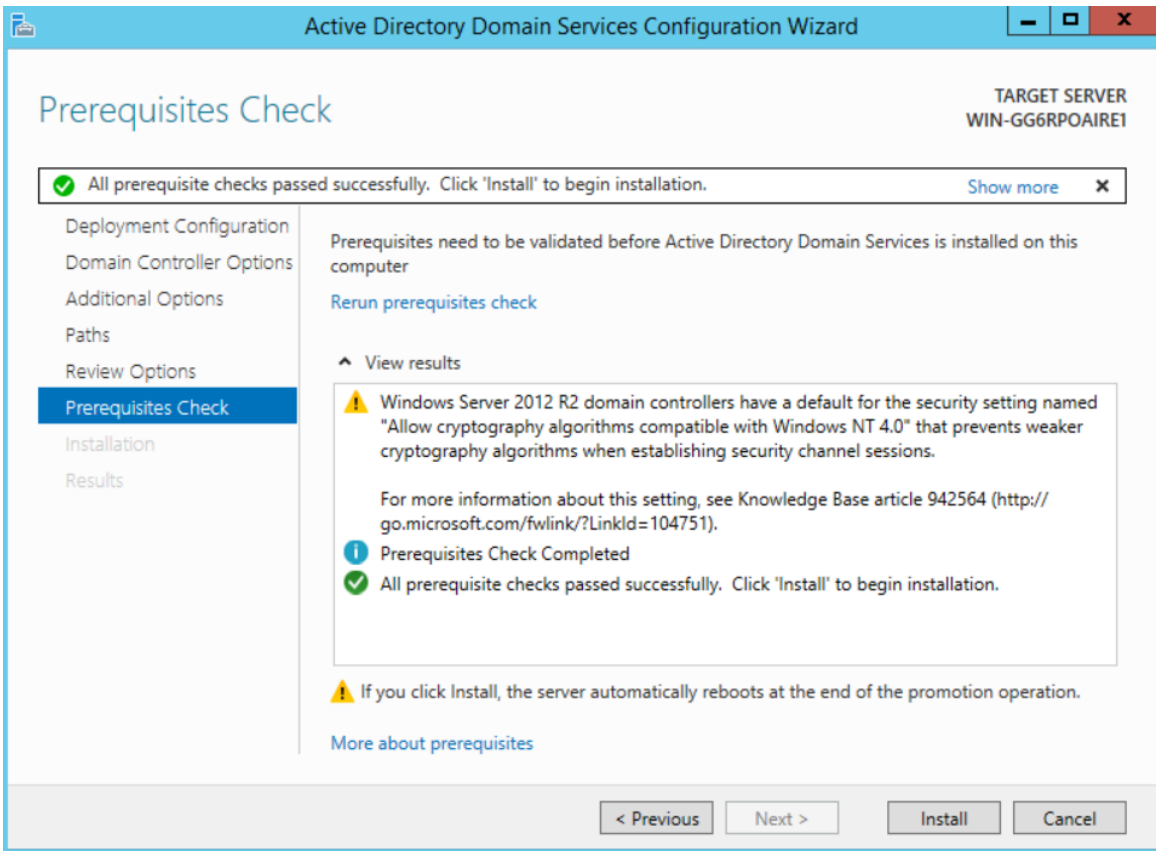


The paths are shown automatically and can be edited.

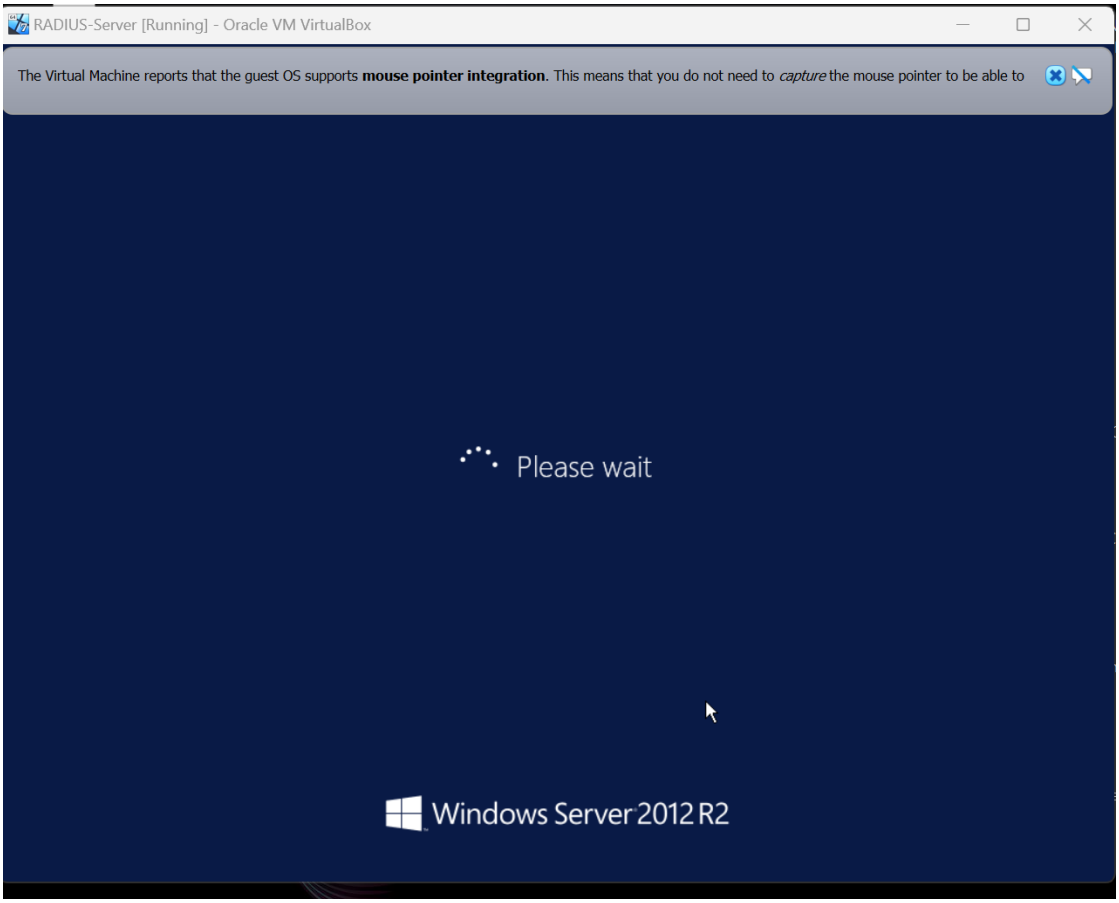
These paths are for Active Directory “database, log files, and SYSVOL” directories/folders. Click “Next”.



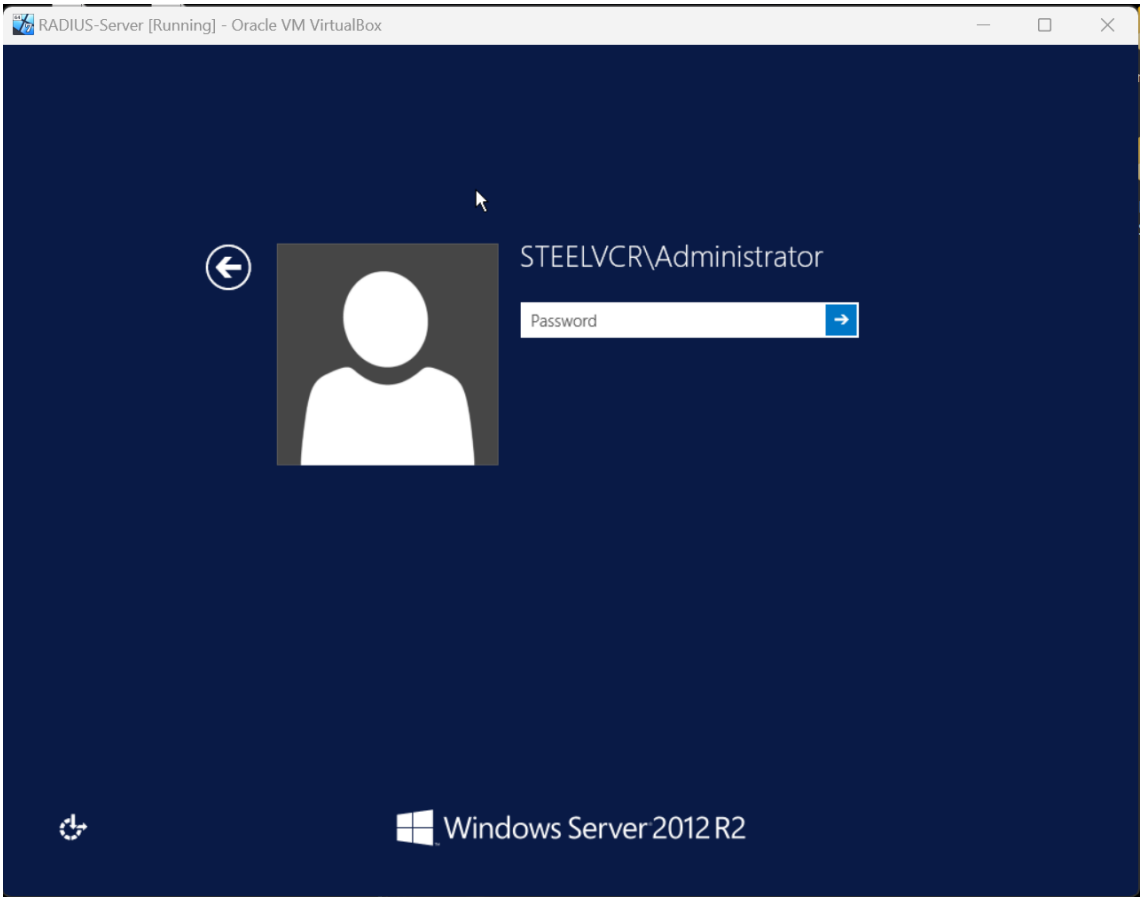
Check to make sure everything is right and click “Next”.



After prerequisite check is successful, click “Install”.

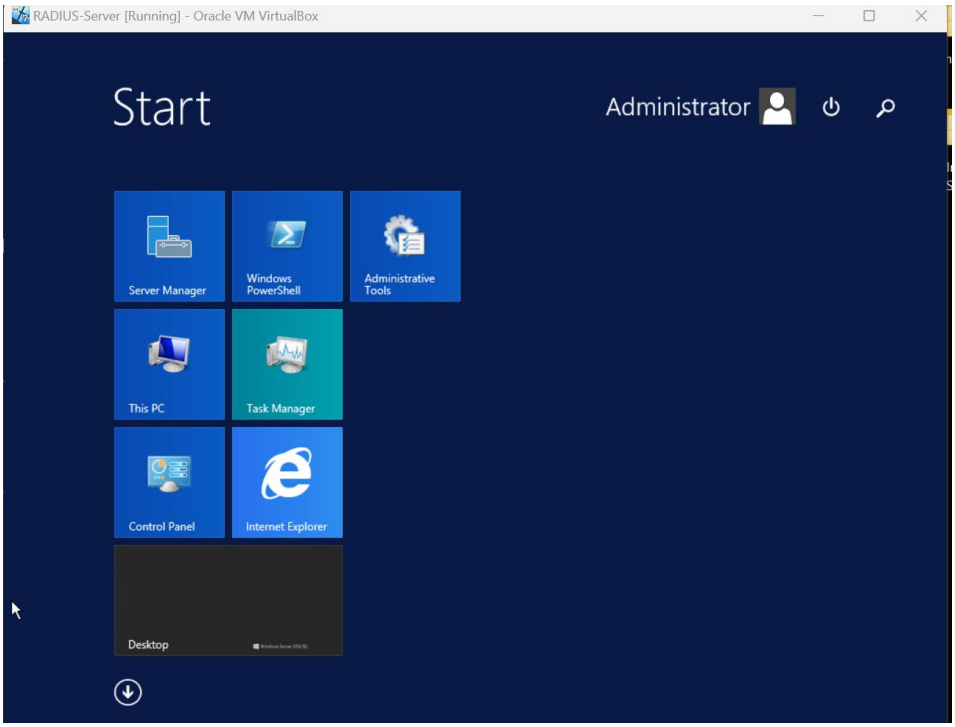


Wait 10 minutes or maybe longer depending on your connection.

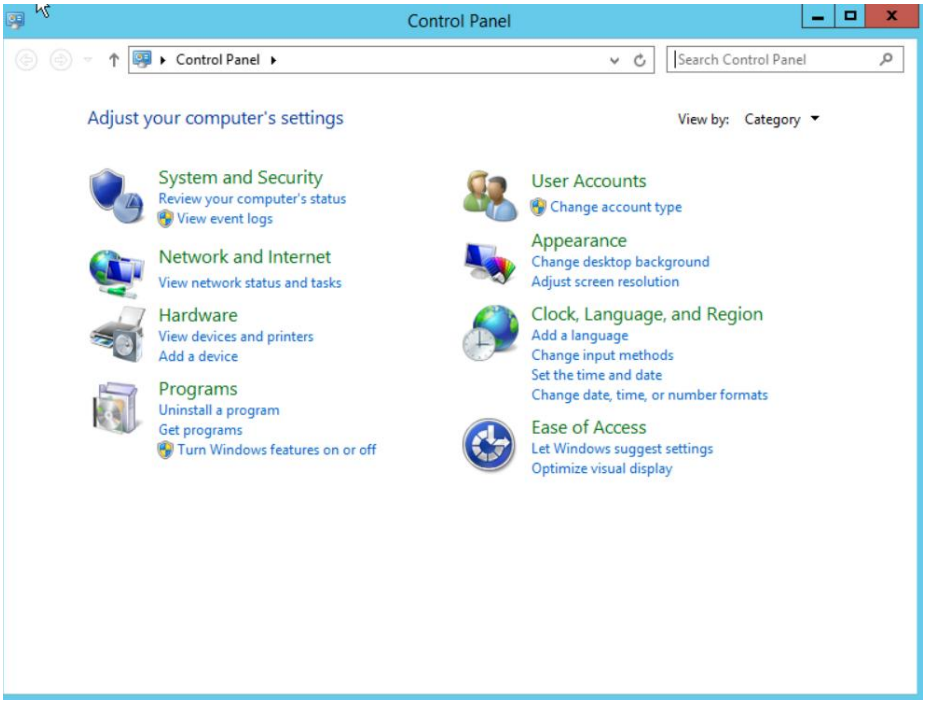


Login again.

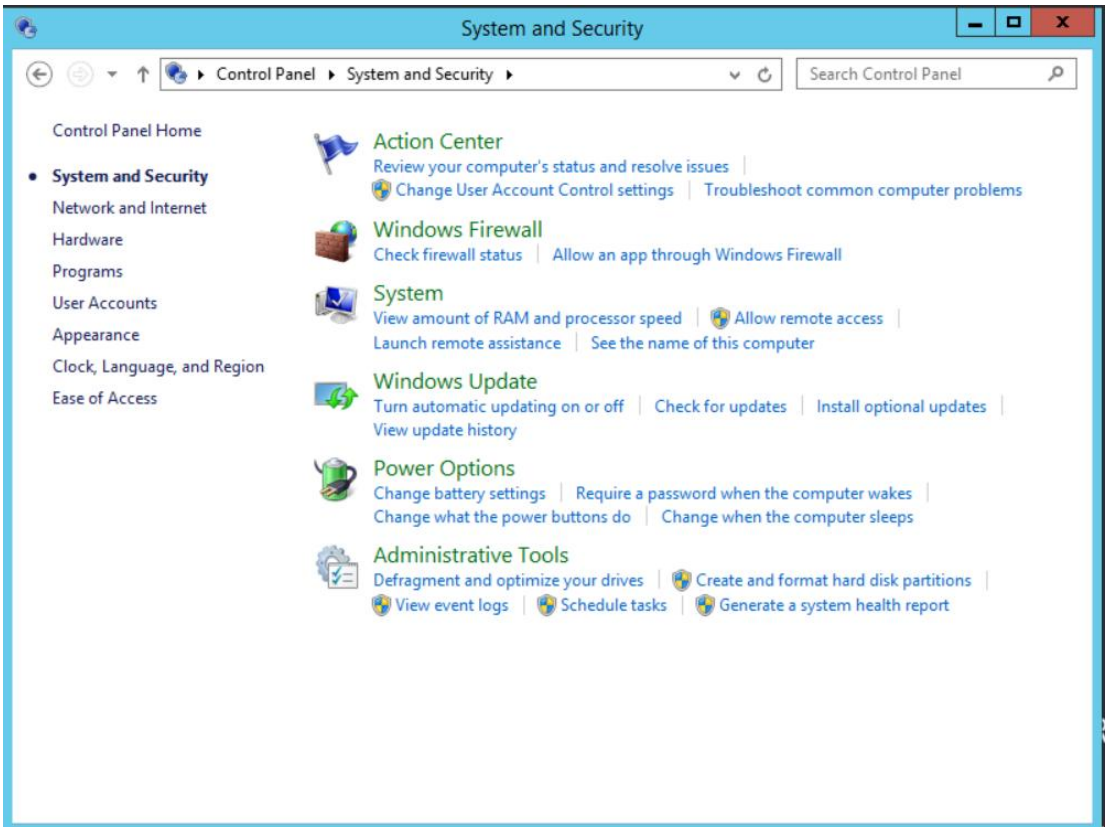
(Might get a pop up about password expiring in 5 days, ignore that for now)



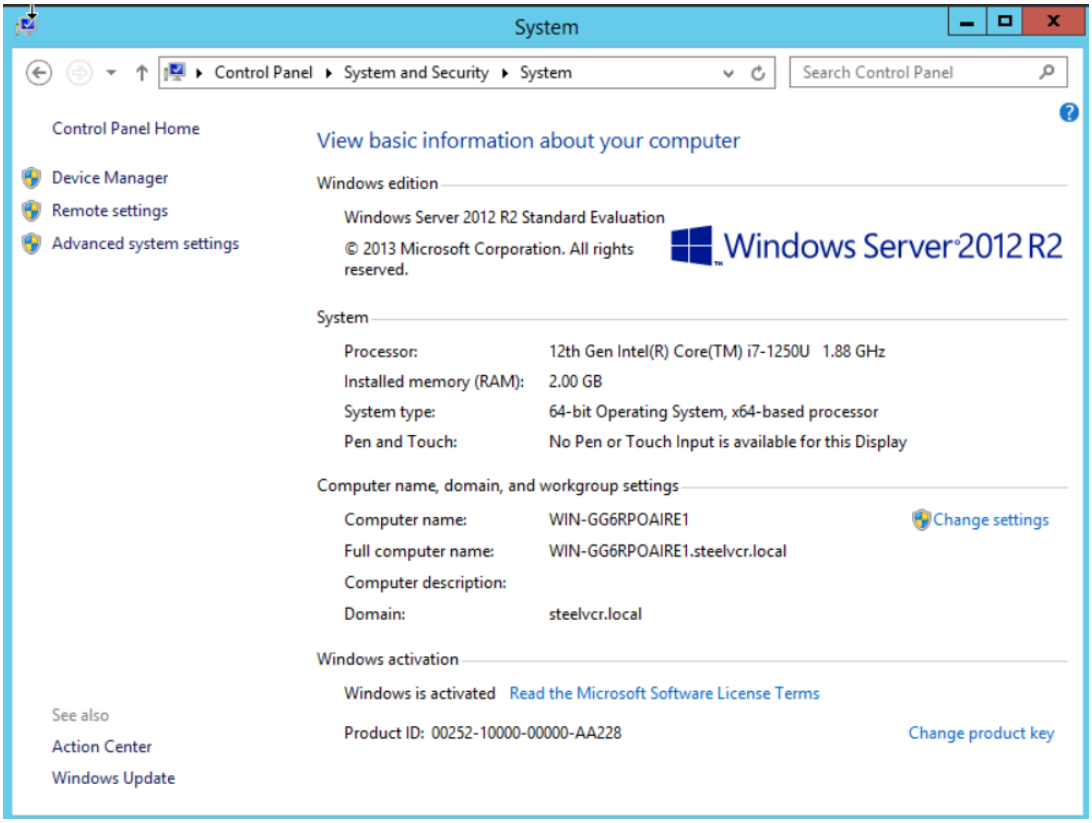
Go to Control Panel on the Start Menu.



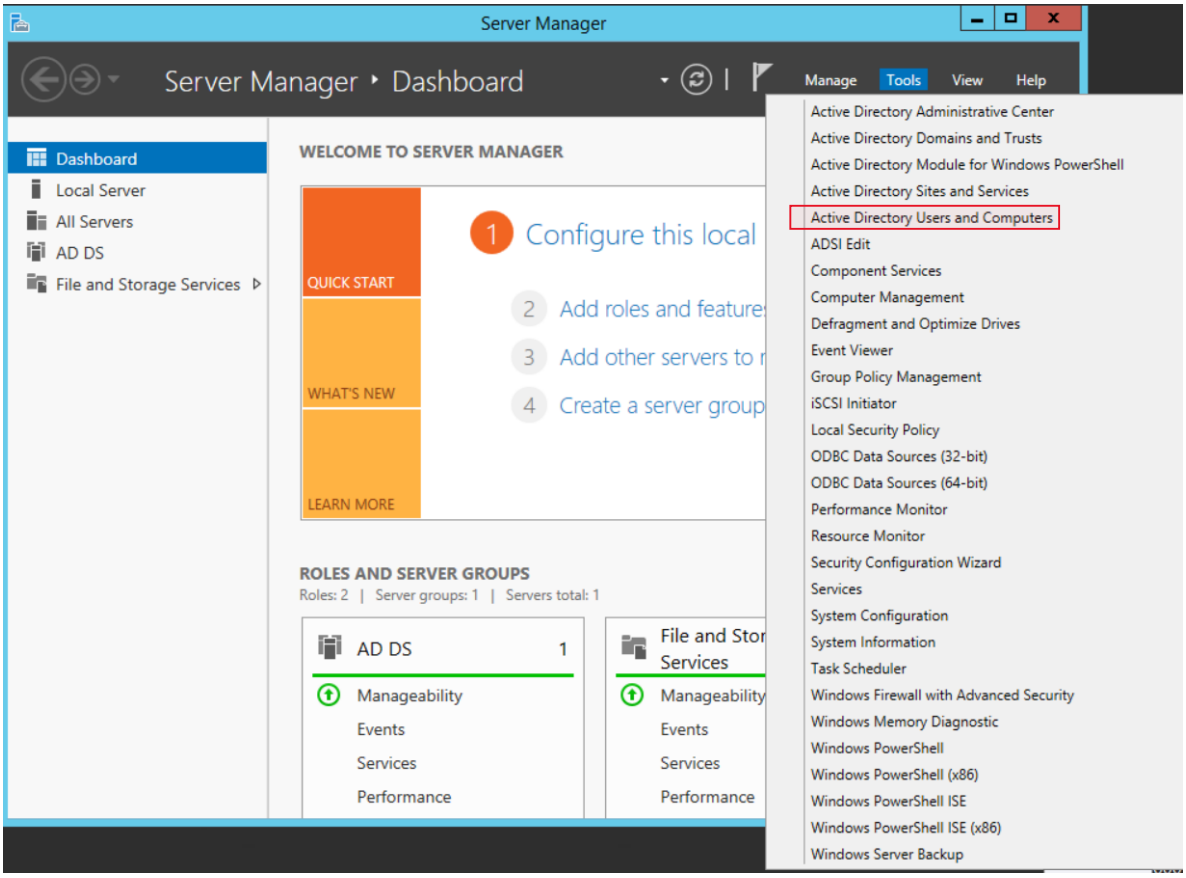
In the Control Panel go to “System and Security”.


System and Security
Control Panel ▸ System and Security ▸
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware
Programs
User Accounts
Appearance
Clock, Language, and Region
Ease of Access
Action Center
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Windows Firewall
Check firewall status
Allow an app through Windows Firewall
System
View amount of RAM and processor speed
Allow remote access
Launch remote assistance
See the name of this computer
Windows Update
Turn automatic updating on or off
Check for updates
Install optional updates
View update history
Power Options
Change battery settings
Require a password when the computer wakes
Change what the power buttons do
Change when the computer sleeps
Administrative Tools
Defragment and optimize your drives
Create and format hard disk partitions
View event logs
Schedule tasks
Generate a system health report

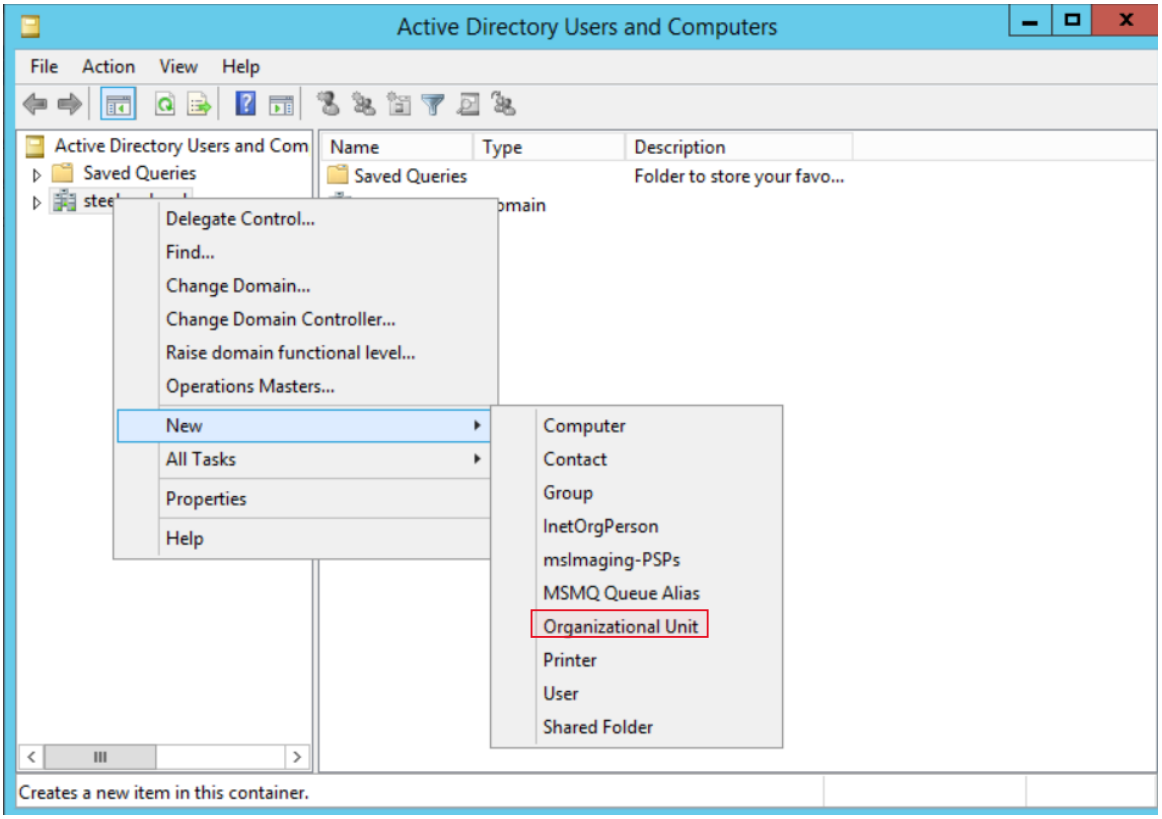
Go to “System”.


System
Control Panel ▸ System and Security ▸ System
Search Control Panel
Control Panel Home
Device Manager
Remote settings
Advanced system settings
View basic information about your computer
Windows edition
Windows Server 2012 R2 Standard Evaluation
© 2013 Microsoft Corporation. All rights reserved.
Windows Server 2012 R2
System
Processor: 12th Gen Intel(R) Core(TM) i7-1250U 1.88 GHz
Installed memory (RAM): 2.00 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display
Computer name, domain, and workgroup settings
Computer name: WIN-GG6RPOAIRE1
Change settings
Full computer name: WIN-GG6RPOAIRE1.steelvcr.local
Computer description:
Domain: steelvcr.local
Windows activation
Windows is activated Read the Microsoft Software License Terms
Product ID: 00252-10000-00000-AA228
Change product key
See also
Action Center
Windows Update

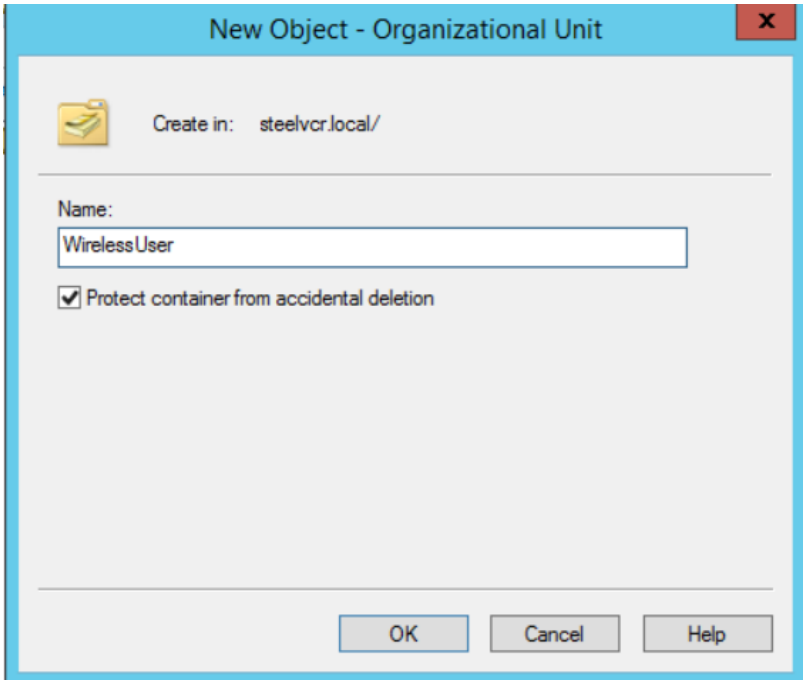
In the System there is information regarding O.S. and more.



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

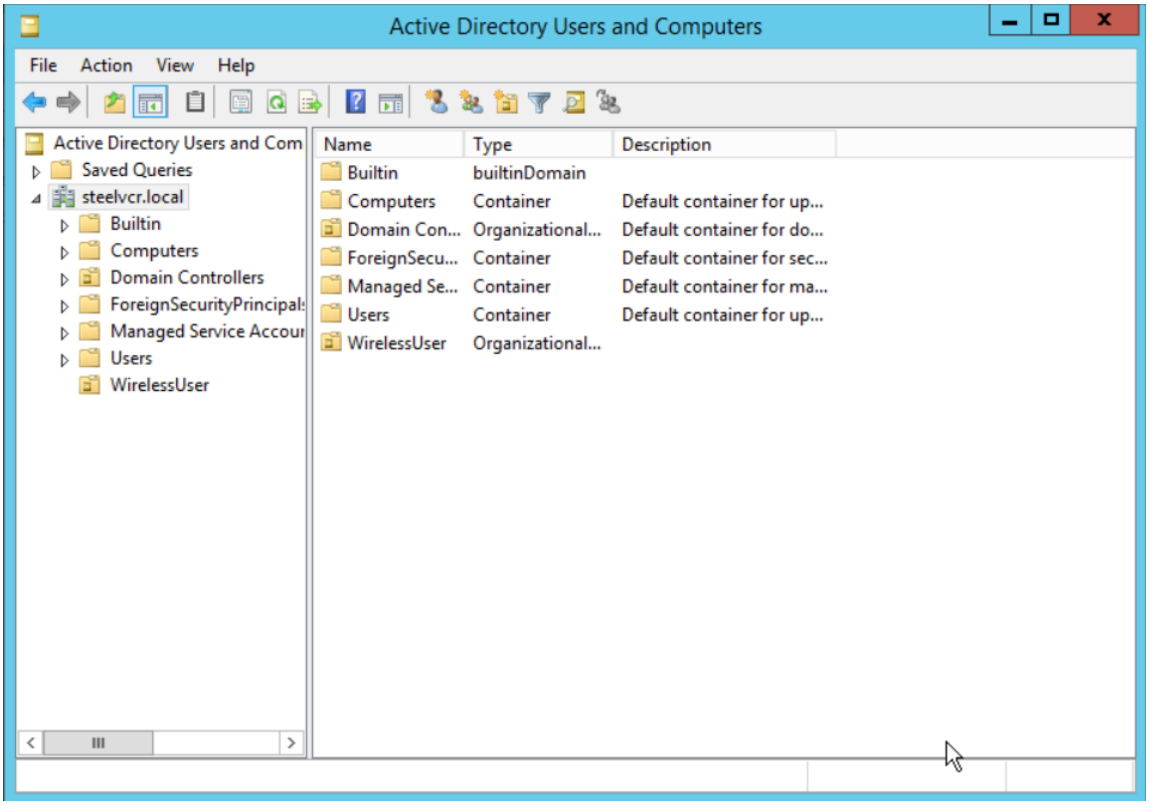


Right-click on your root domain name and select "New”, and then click on “Organizational Unit”.

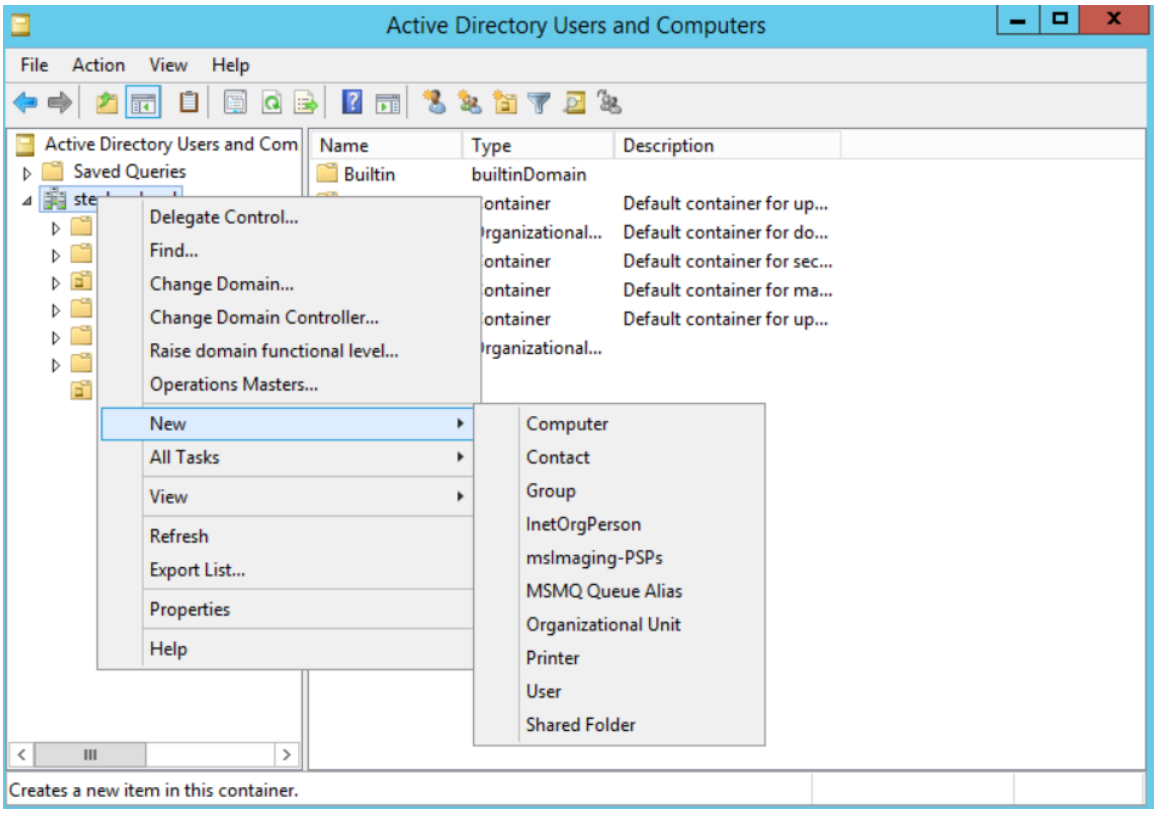


Now create a new object for OU or **organizational unit** keep “Protect container from accidental deletion” checked. Click “Ok” when done.

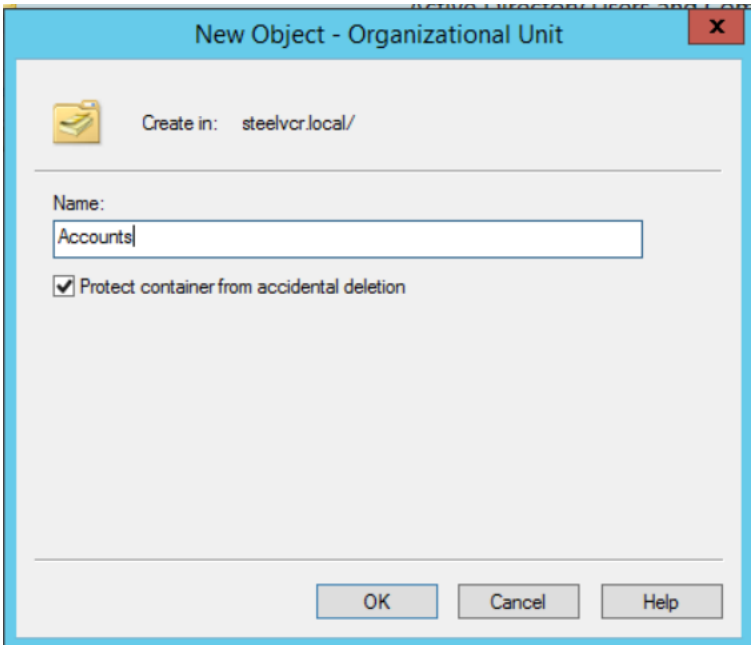
This **object** will be located within the directory of root domain user.



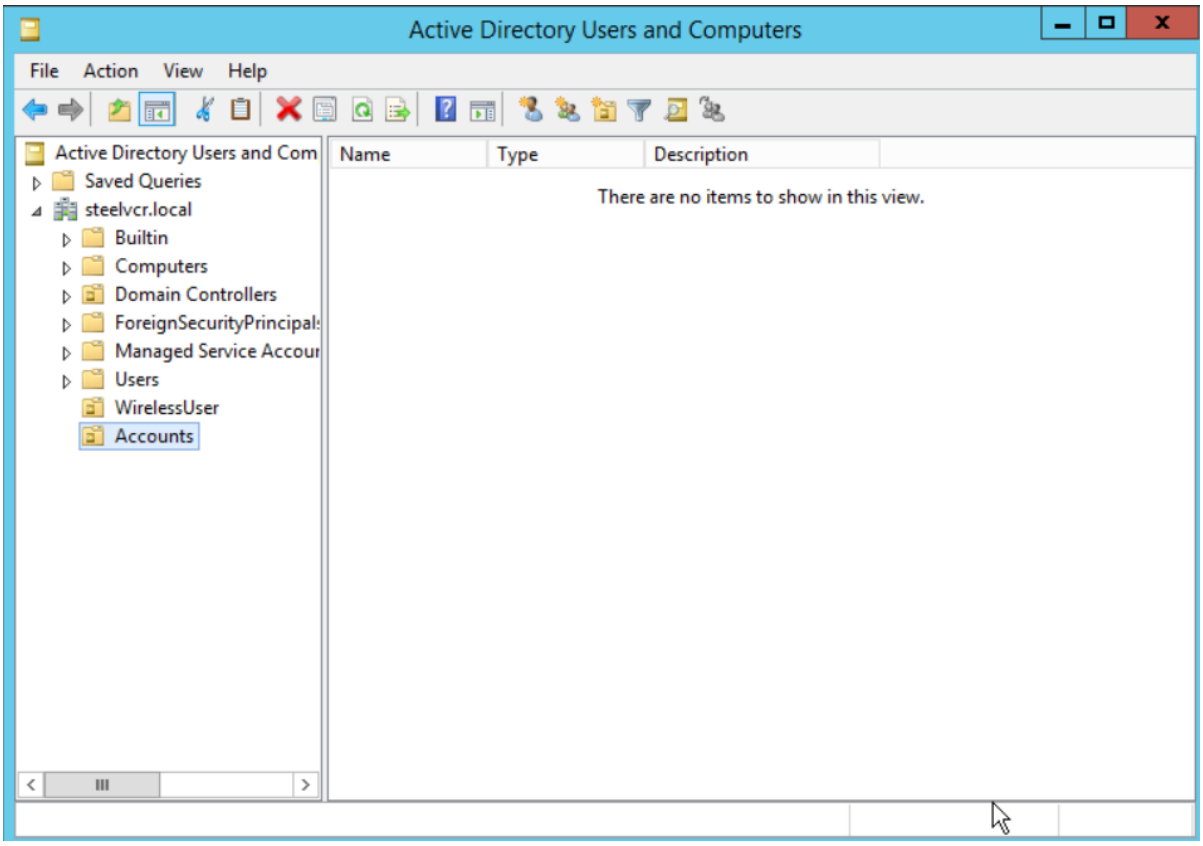
The new organizational unit as been created.



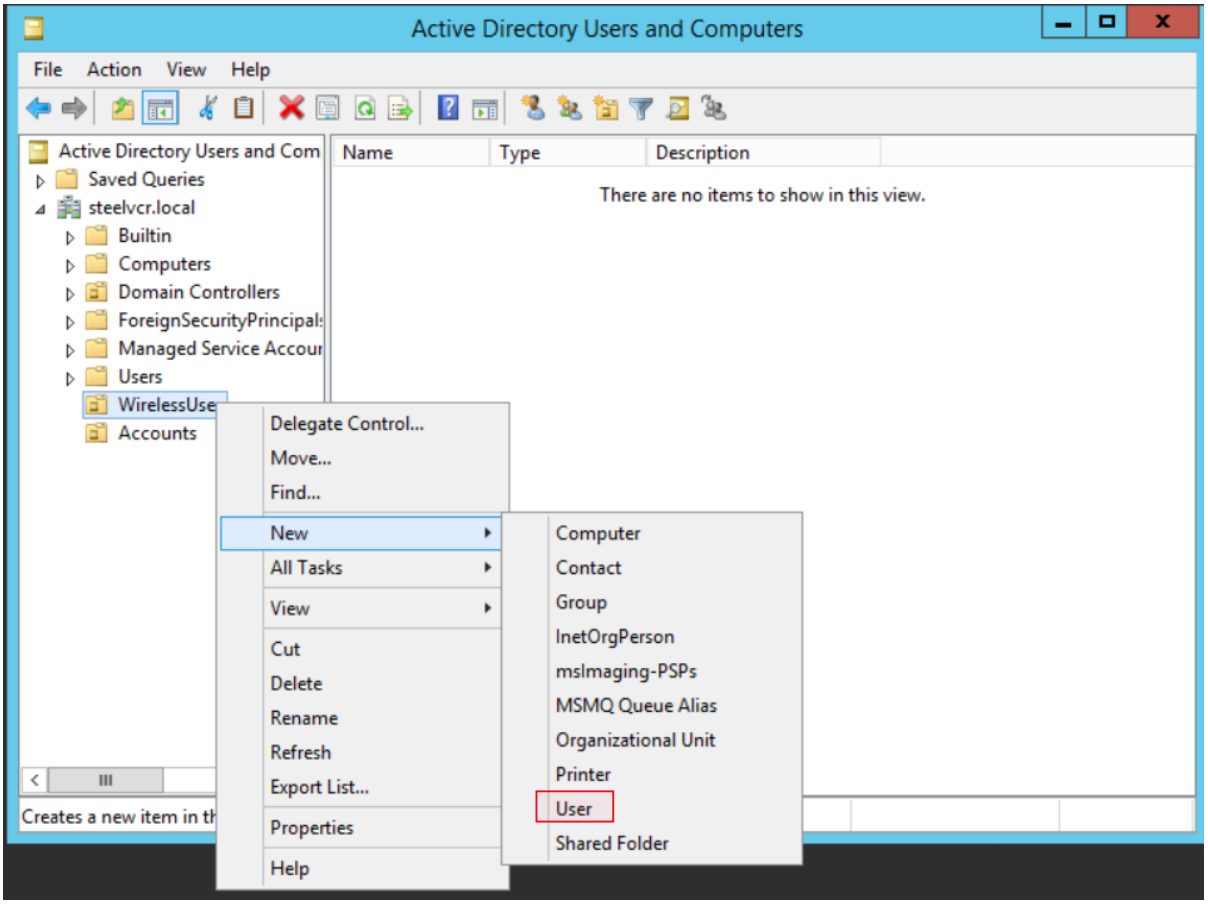
Do the same thing again to create another Organizational Unit.



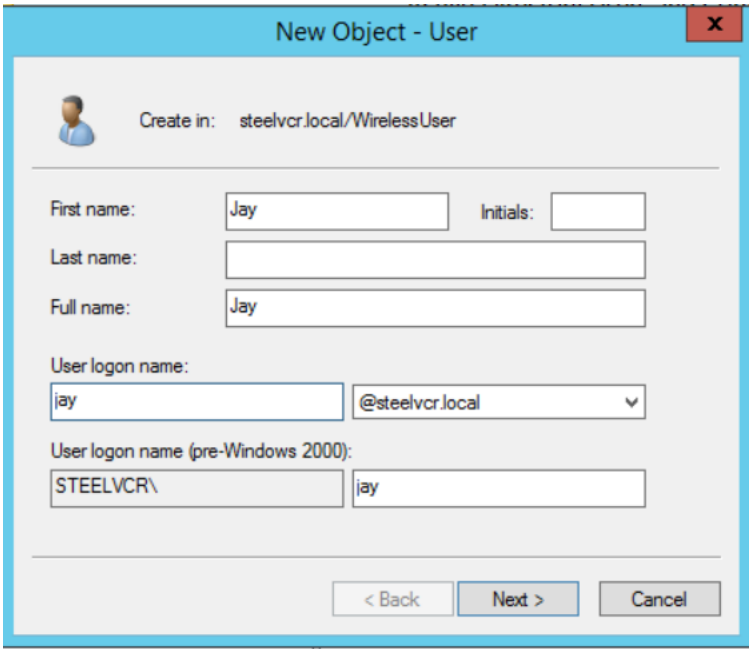
Add the new object which is another organizational unit and click “Ok”.



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

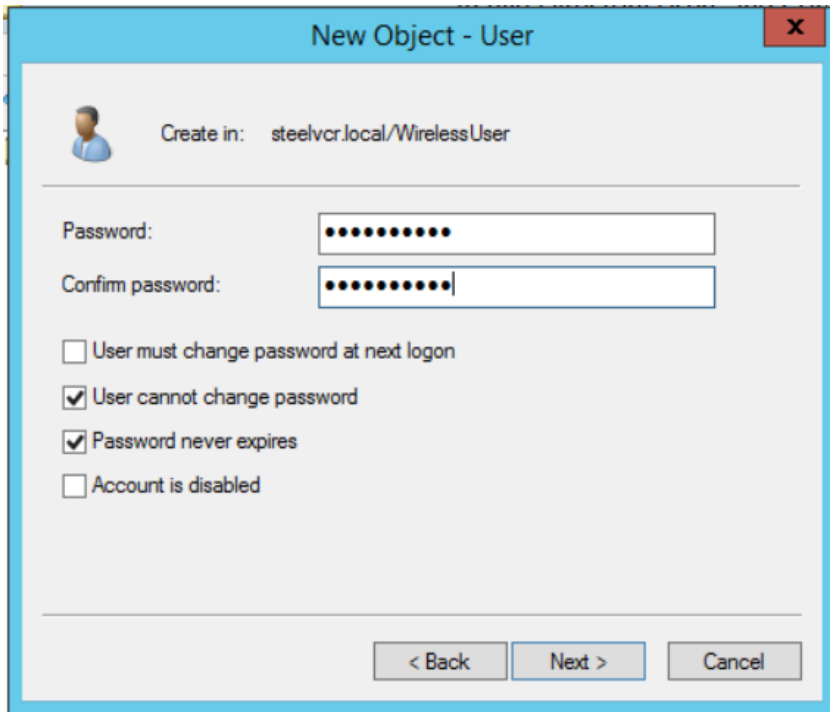


Right-click on first newly created object/folder and go to “New” and then click on “User”.



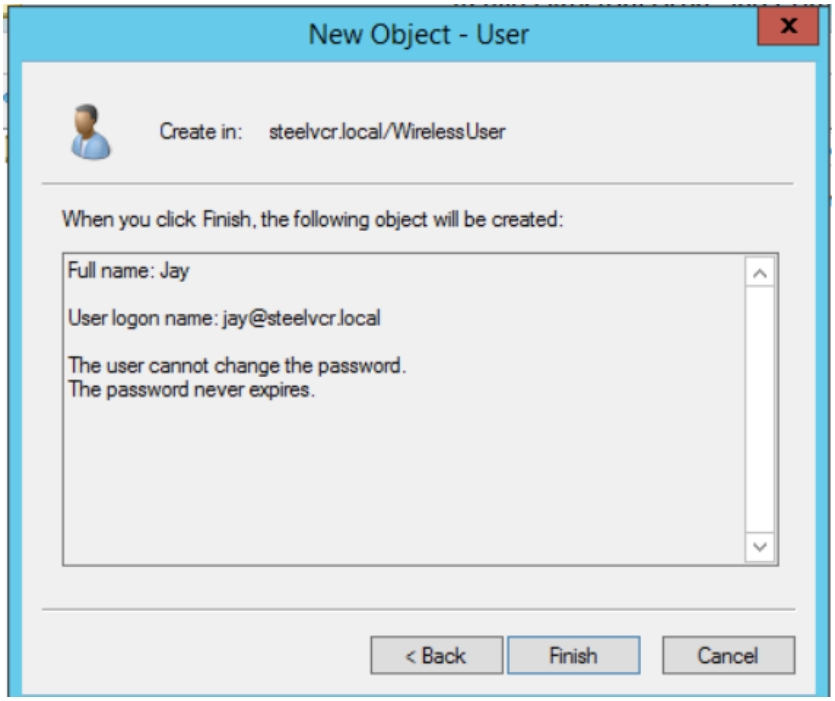
Enter a first name (optional last name) and the “User logon name” can be same as your name @ the root domain name.

Click “Next”.

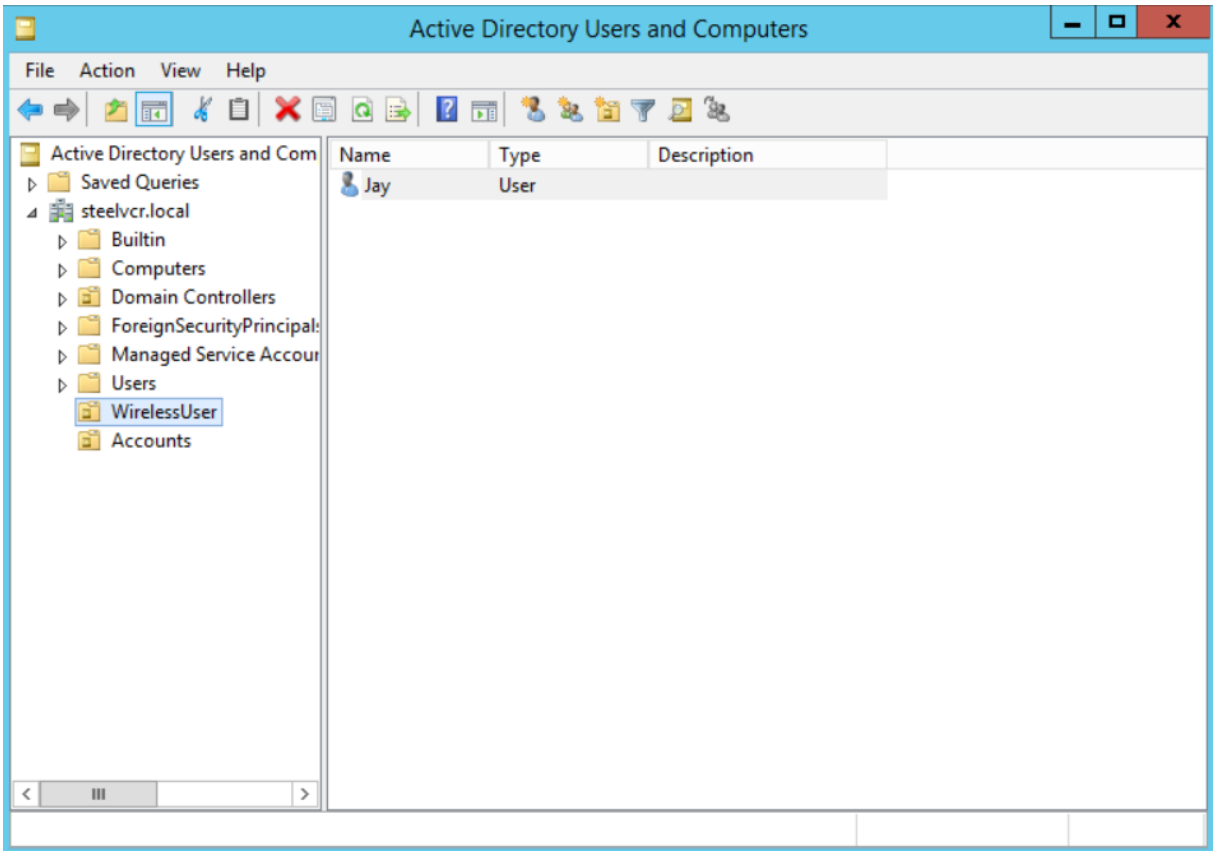


Uncheck the “User must change password at next logon” and keep “Account is disable” unchecked.

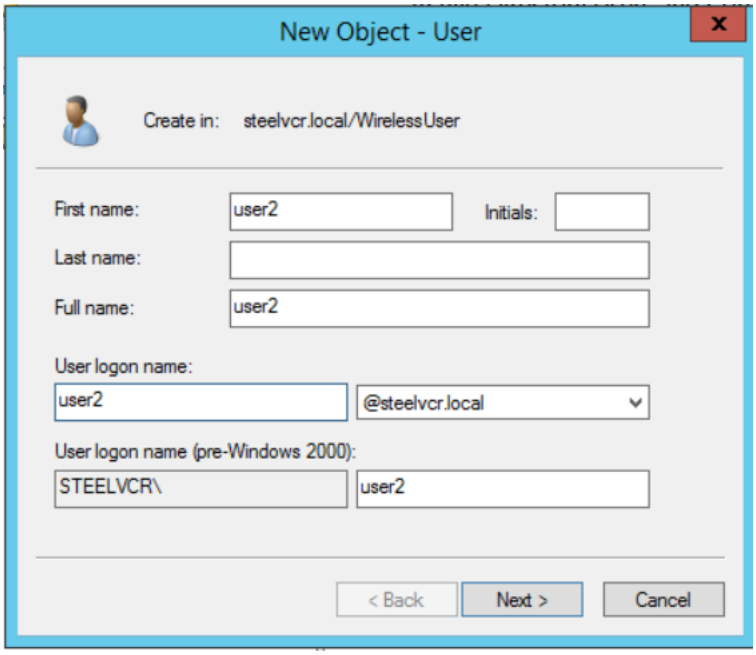
Check in the “User cannot change password” and the “Password never expires” checkboxes.



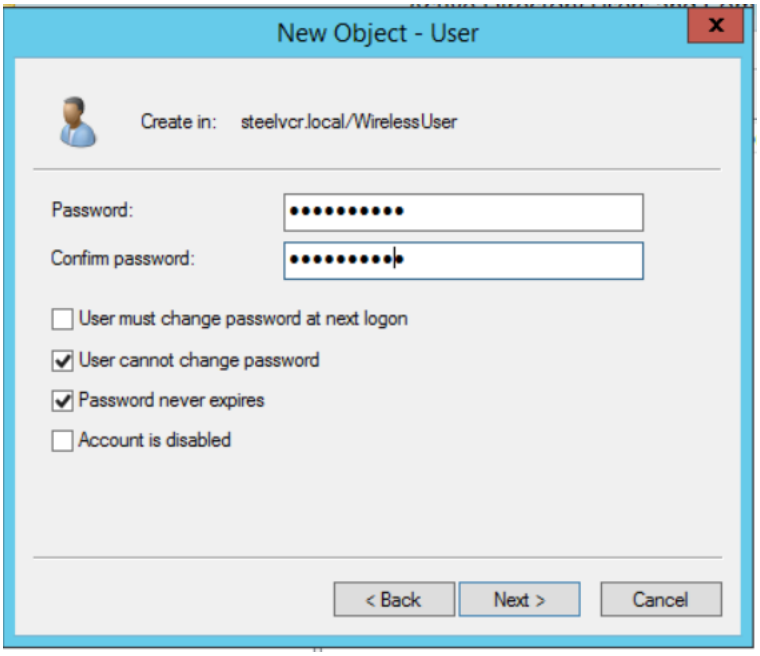
Click “Finish” after user is created.



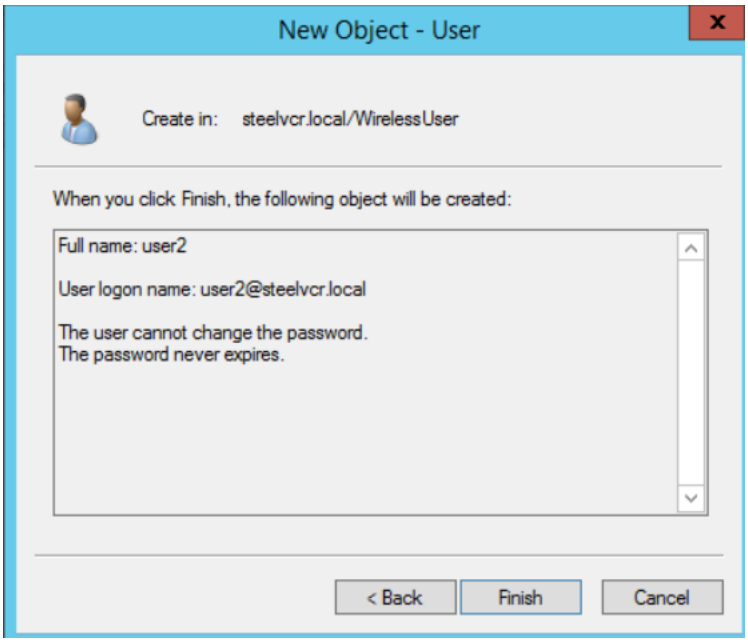
The new user “Jay” is now displayed under that folder.



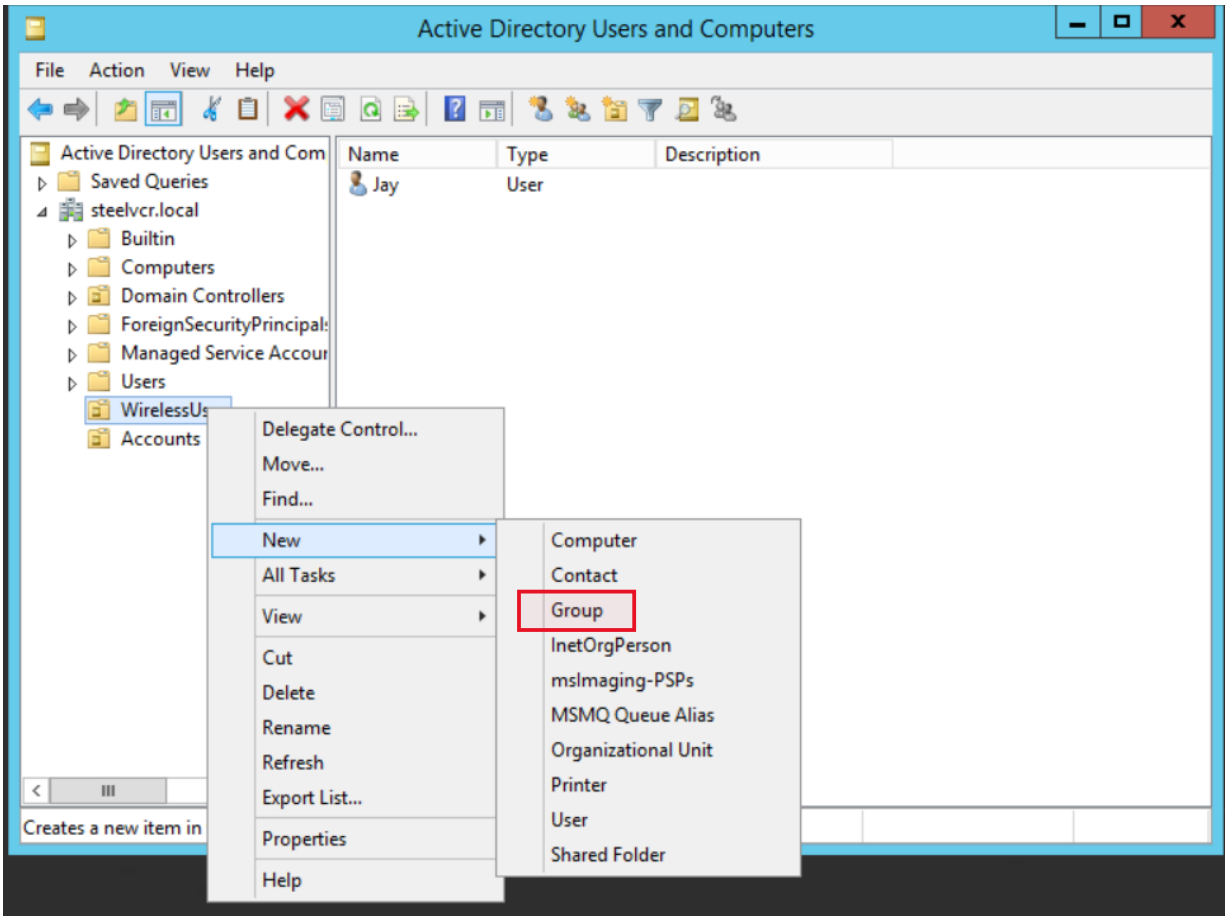
Can create a second user or however many users you want in that same organizational unit.



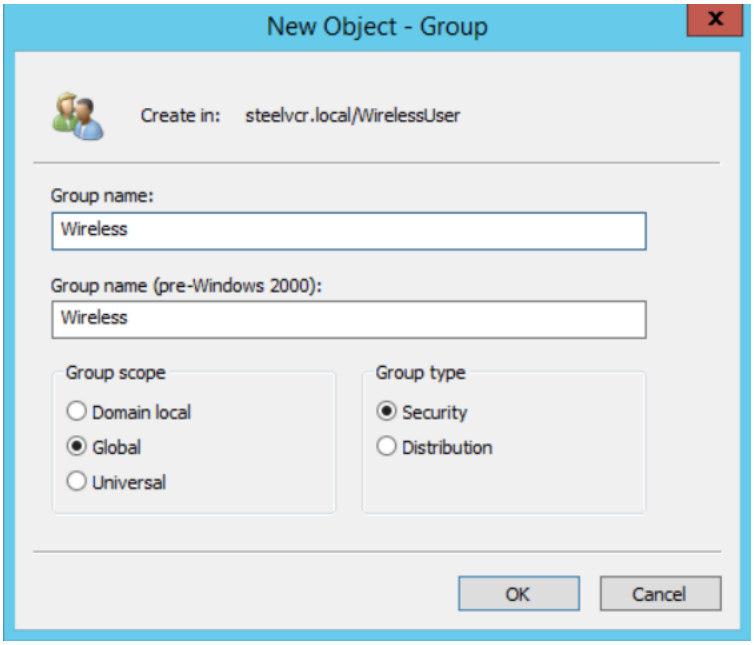
Do same checkboxes as before.



Click “Finish” for second user.

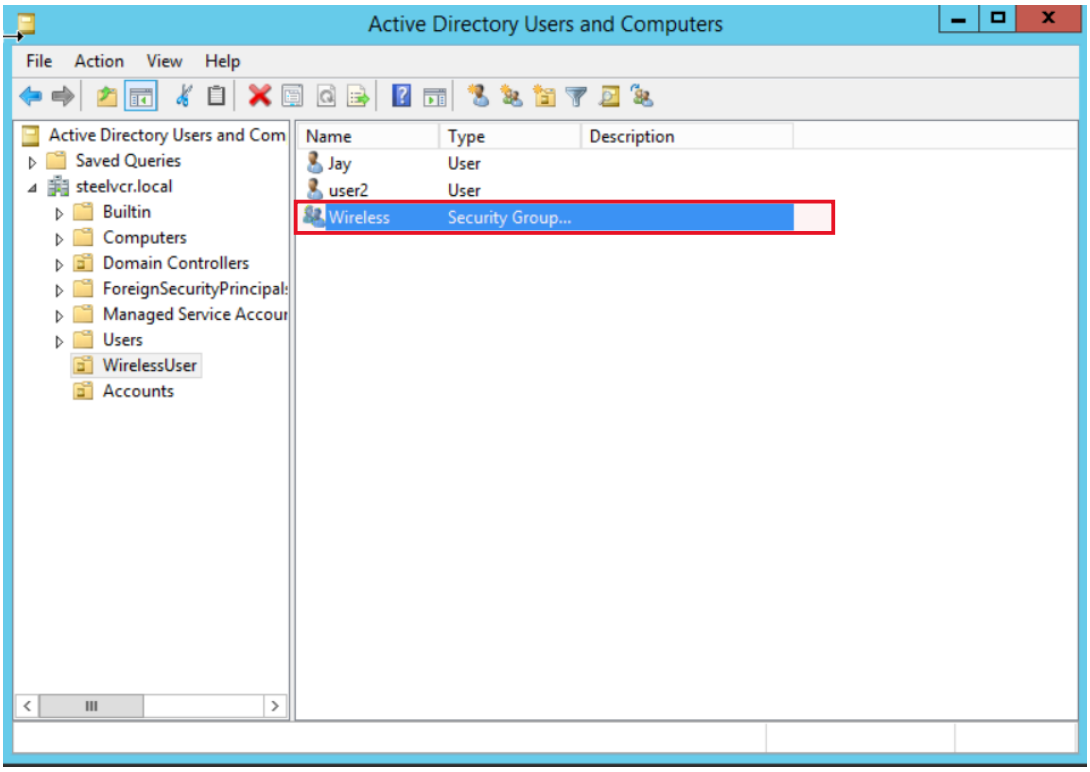


Right-click on that first organizational unit again, but this time select “New” and then “Group” to create a new group.

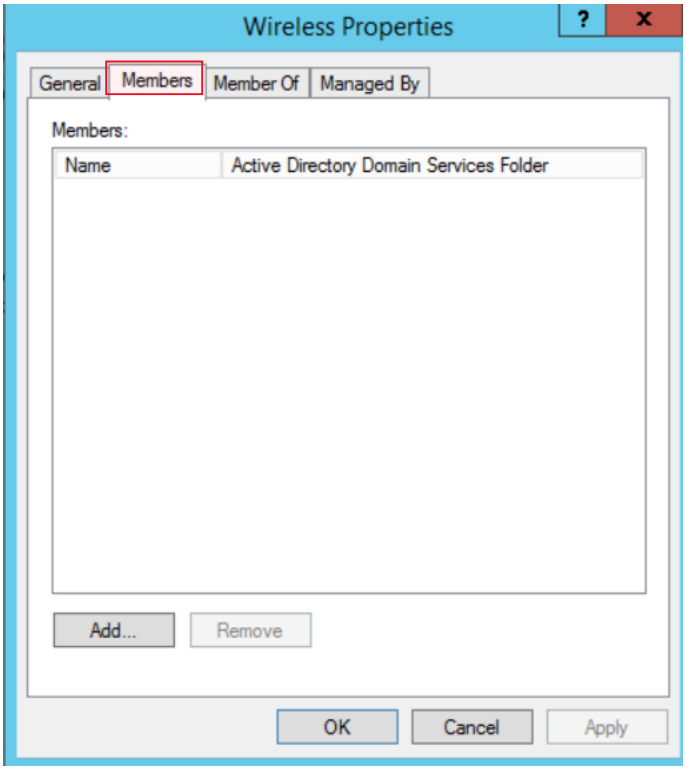


Type in a group name.

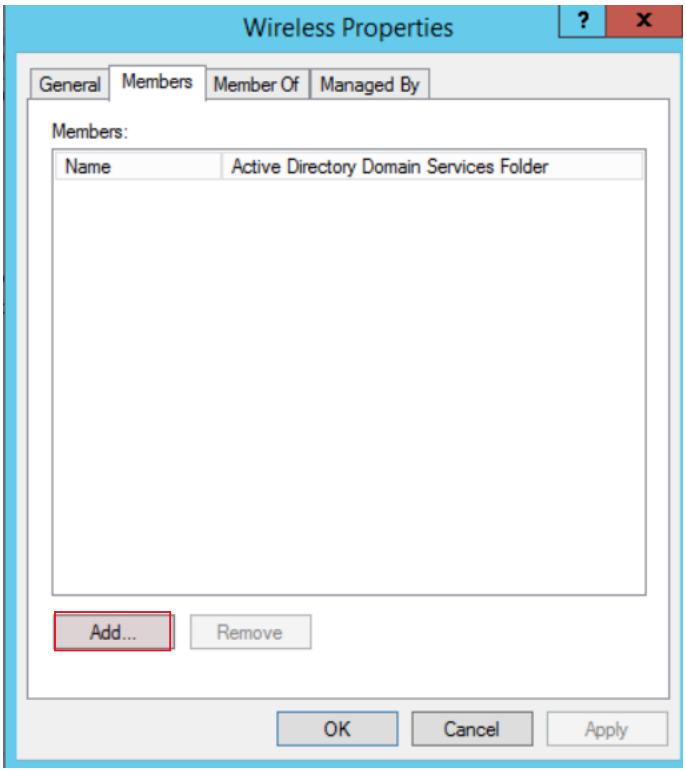
Keep “Group scope” as “Global”, and keep “Group type” as “Security”.



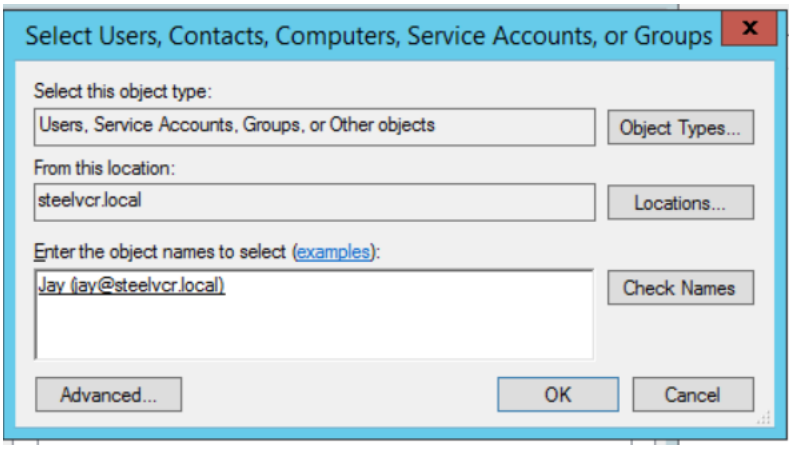
After the group has been added to the organizational unit, double-click on that newly created group within your first OU/organizational unit.



Click on “Members”.

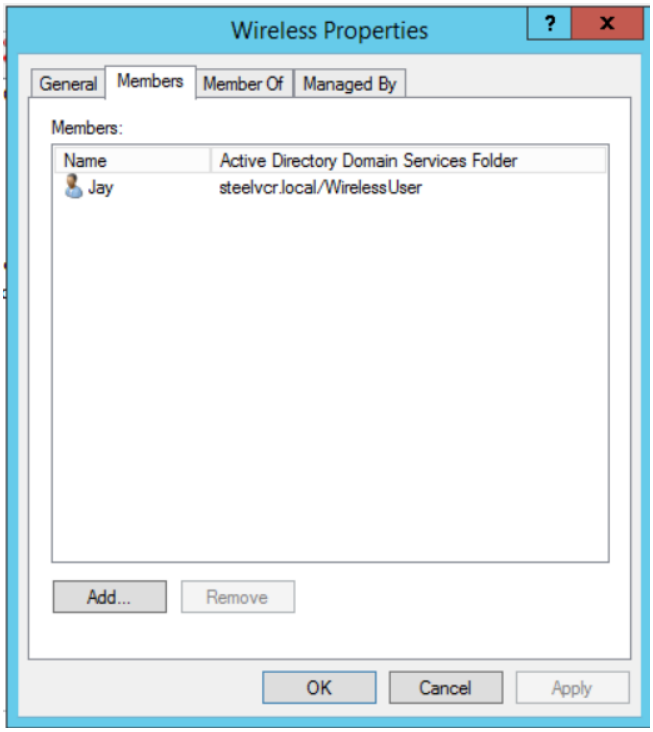


Click on “Add”.

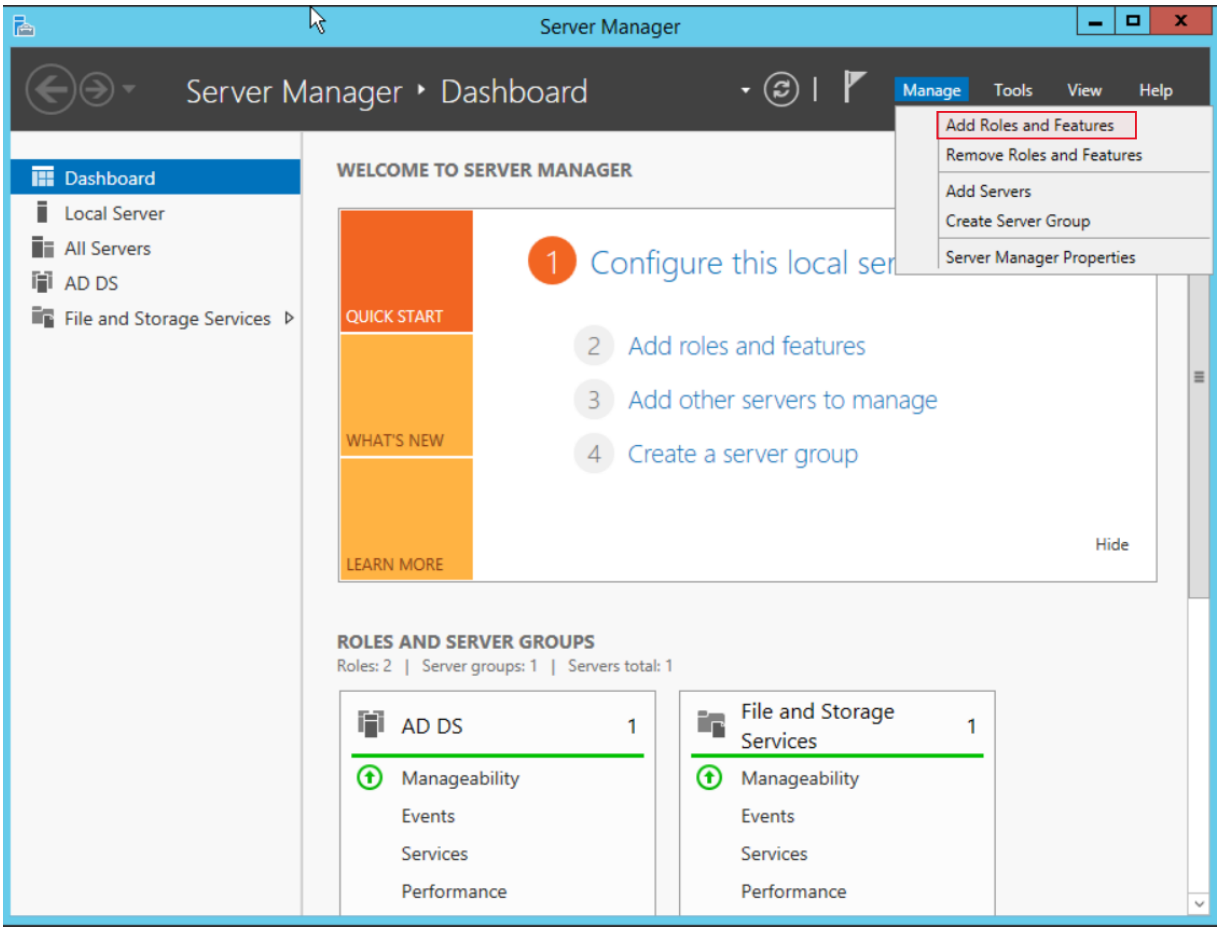


At the bottom under “Enter the object names to select”, enter your object name or enter beginning of it and then click “Check Names” on the right-hand side.

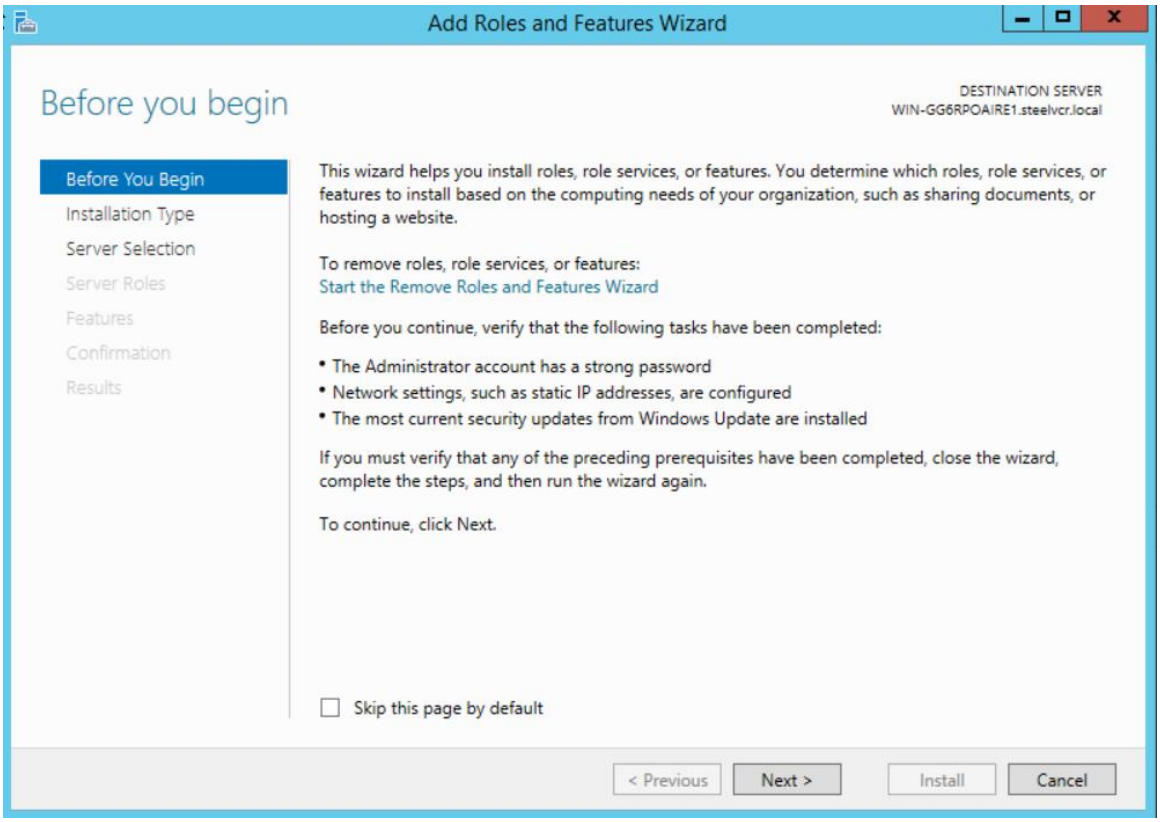
Click “OK” when finished.



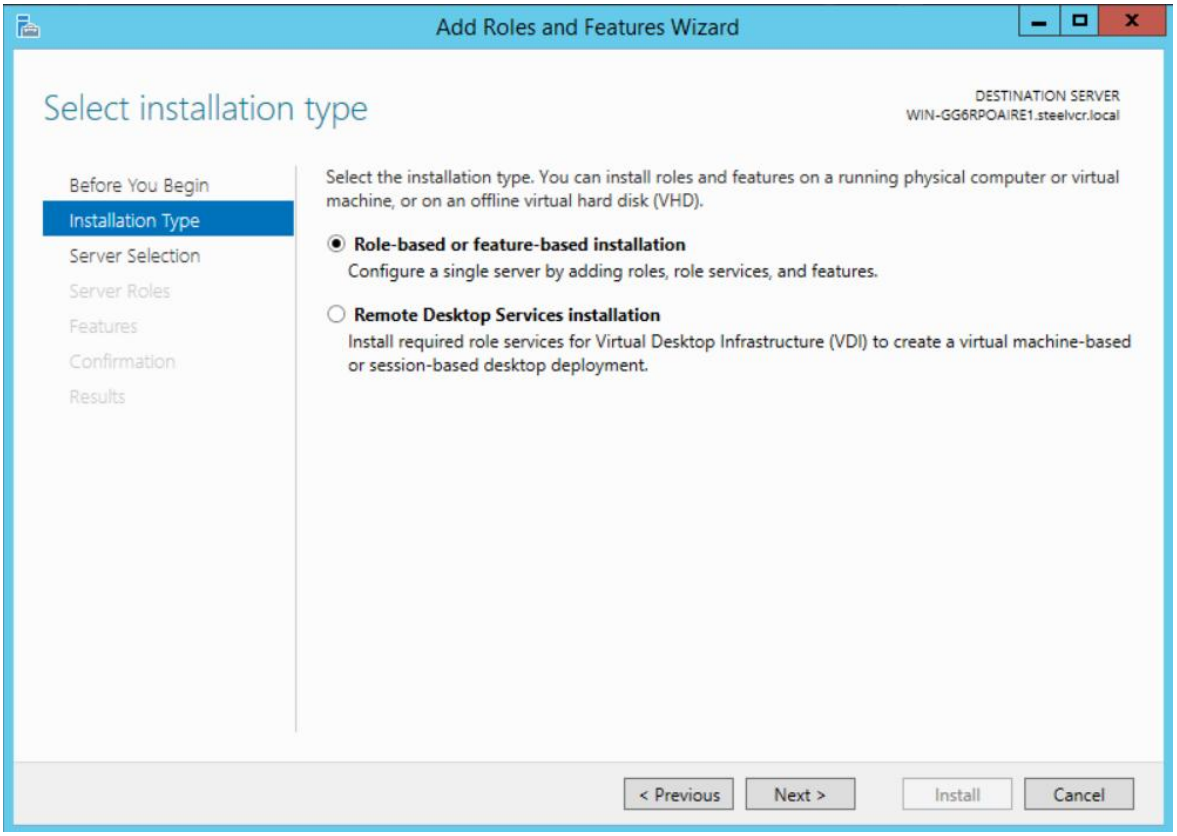
Click on “Apply” and then click on “OK”.



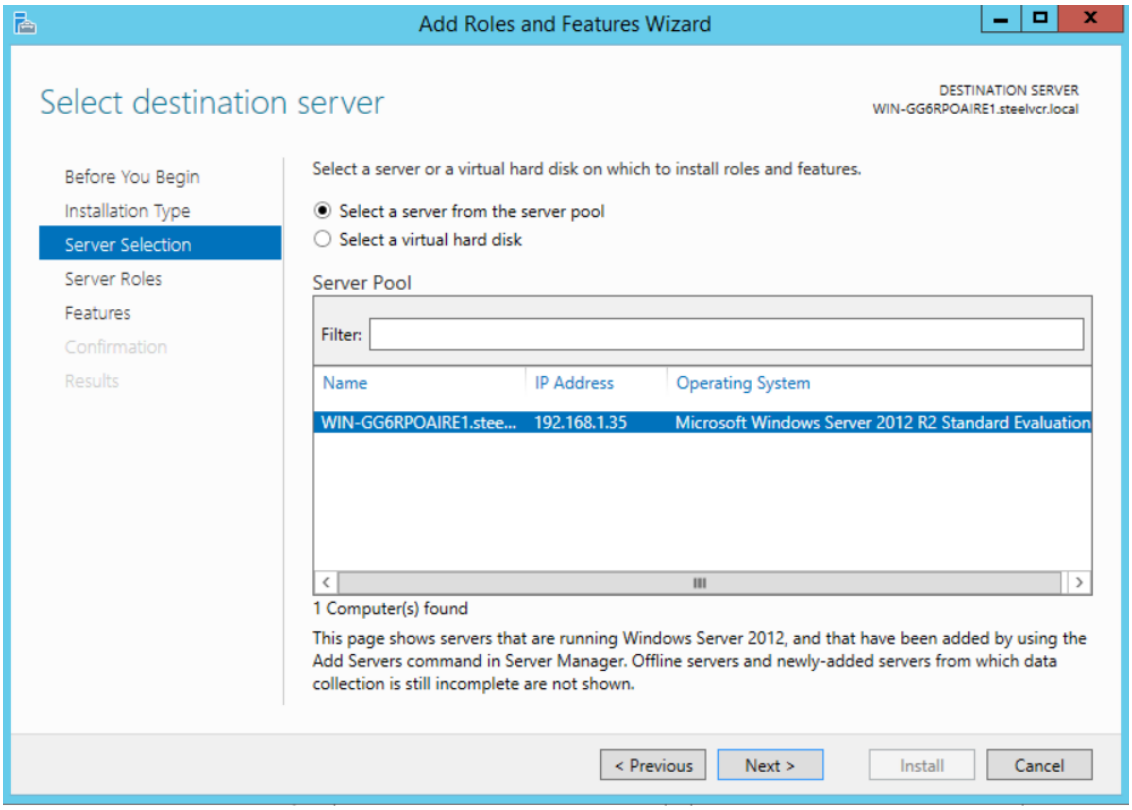
In upper right-hand corner click on “Manage” and then click on “Add Roles and Features”.



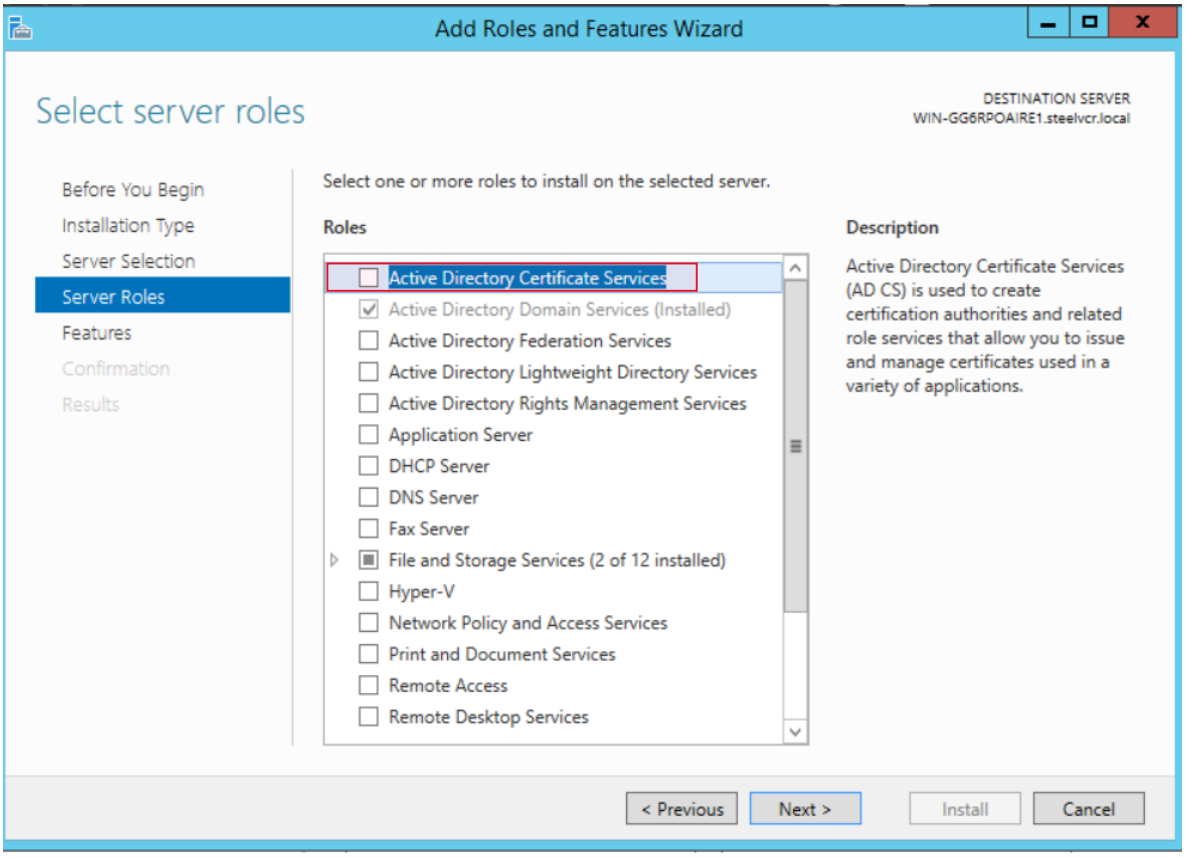
Click on “Next” after reading.



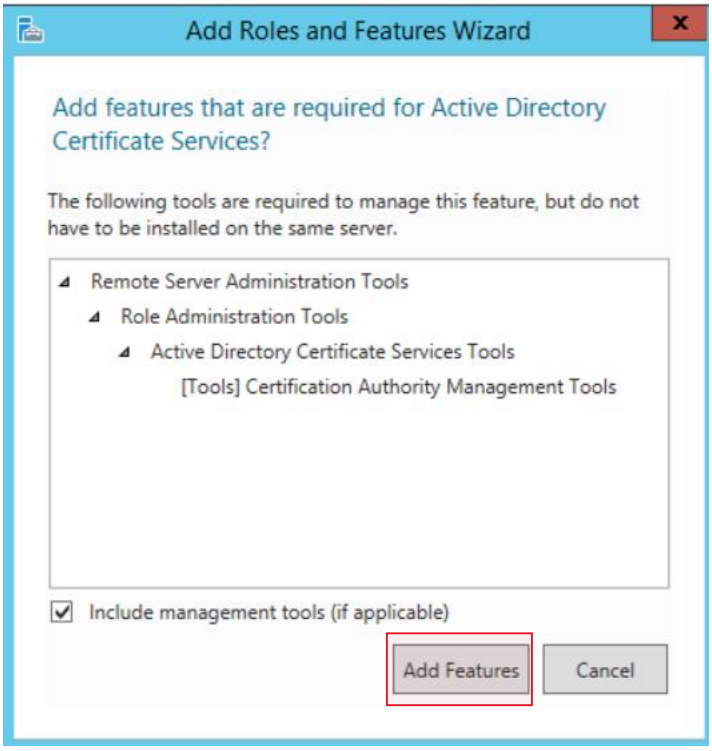
Select “Role-based or feature based installation” and click “Next”.



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

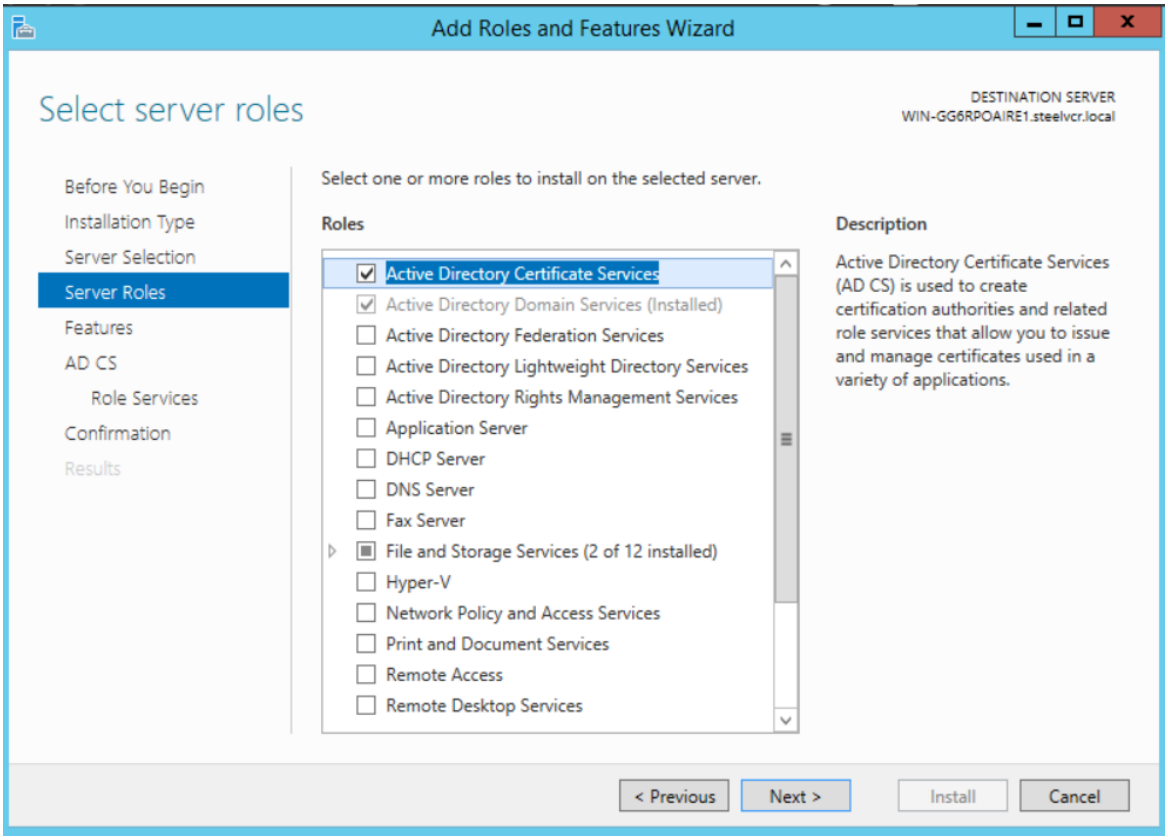


Click on “Active Directory Certificate Services” checkbox.

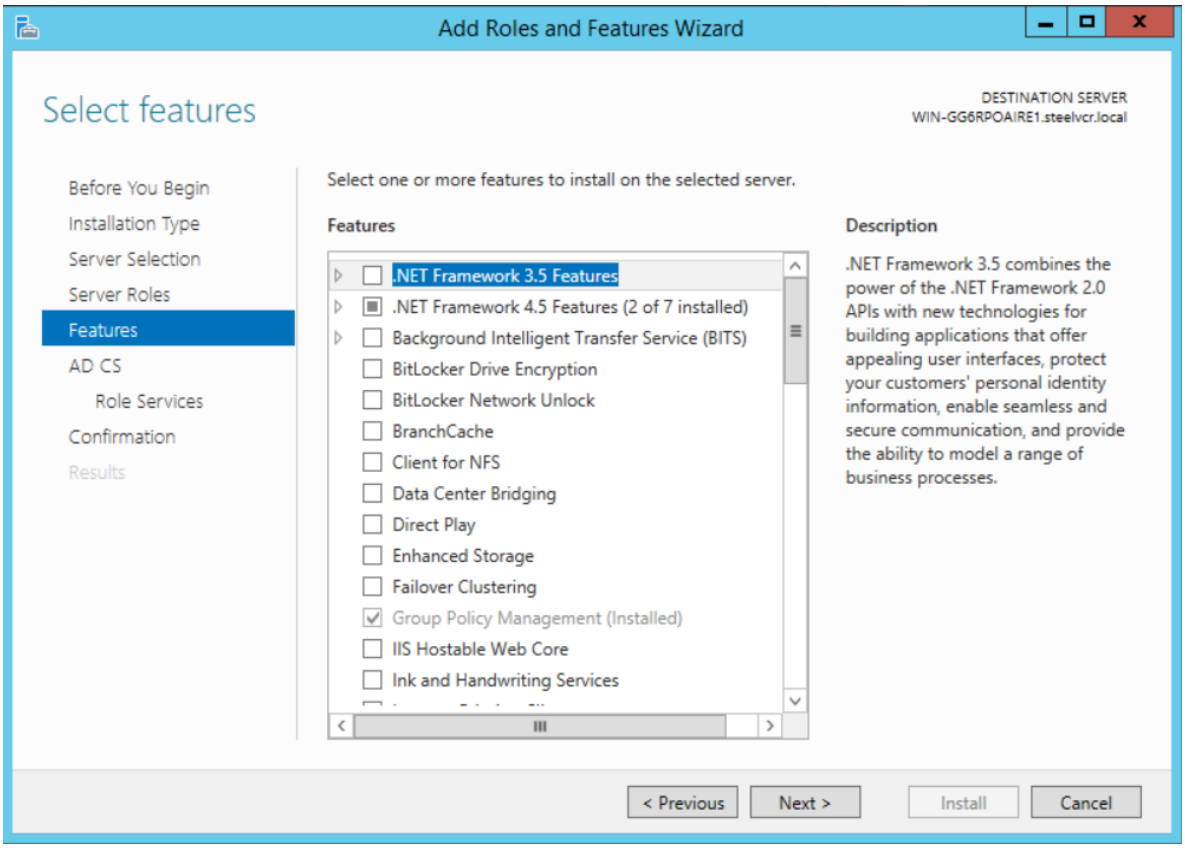


Click on “Add Features”.

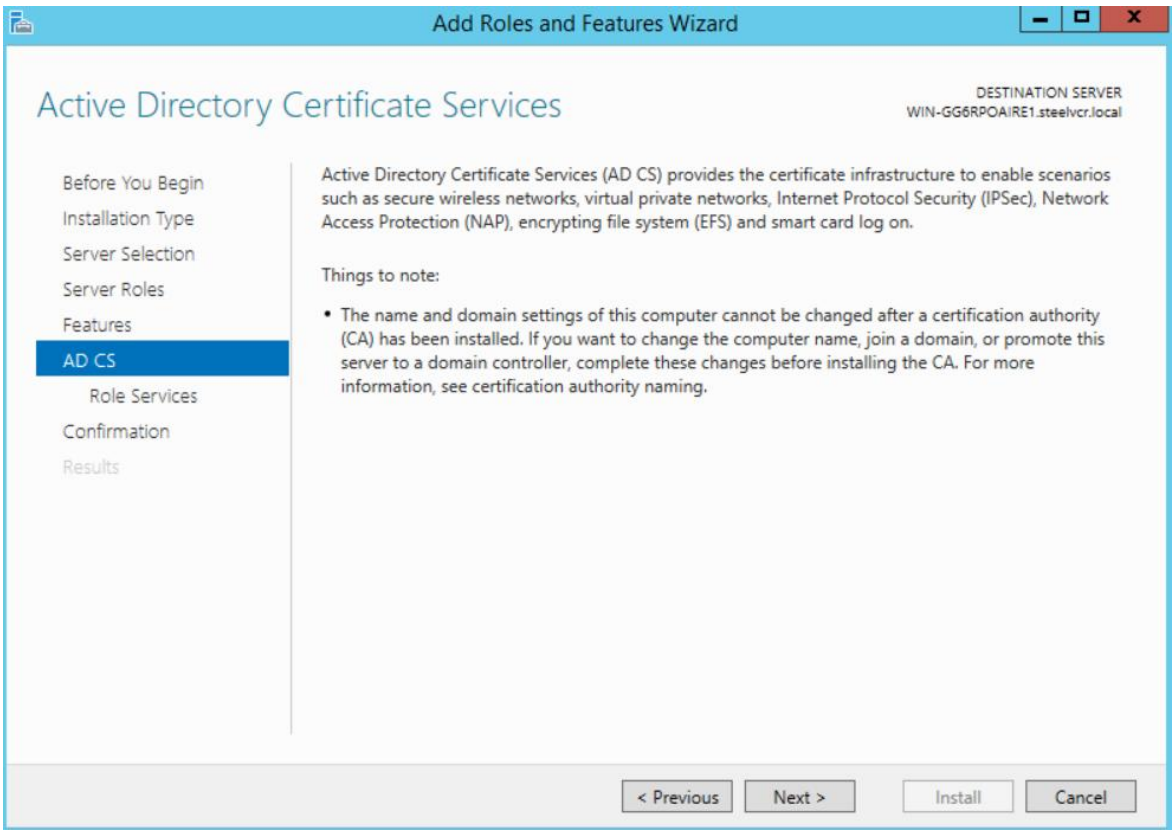
Keep “Include management tool (if applicable)” box checked.



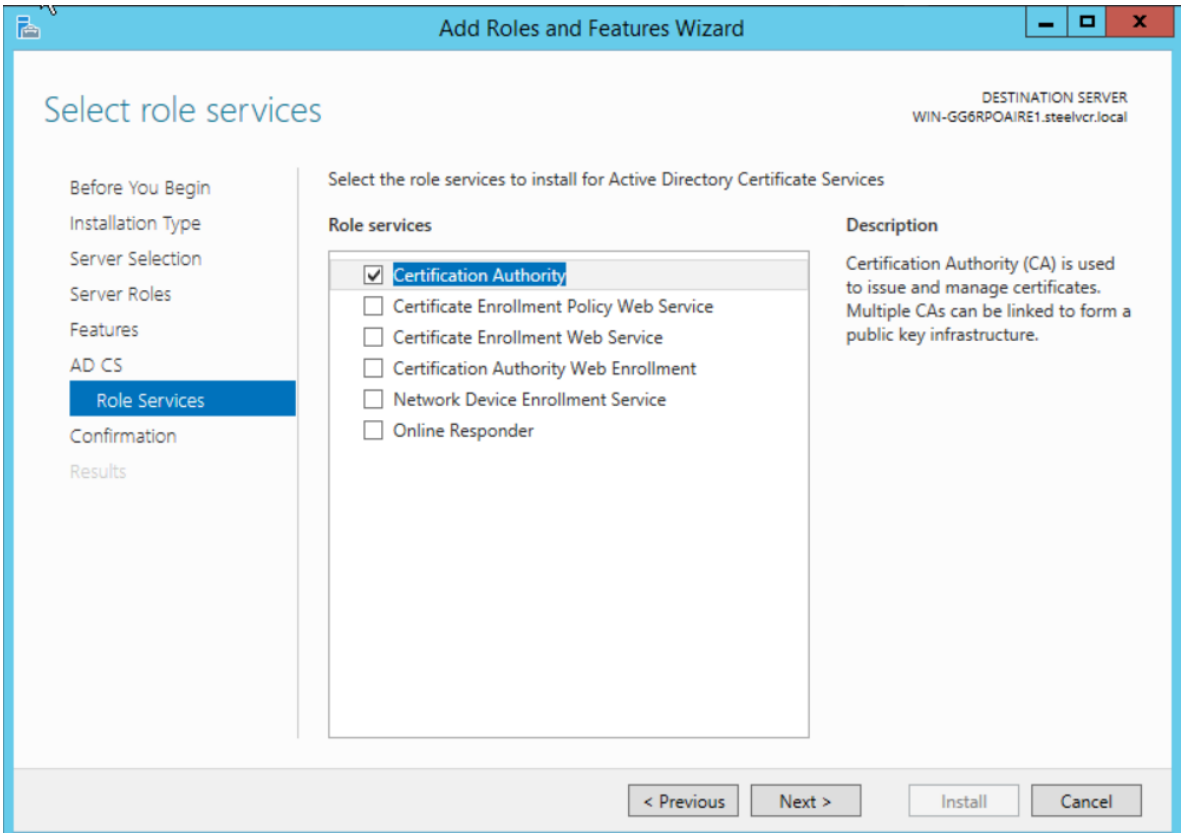
Click “Next”.



Click “Next” without changing anything.

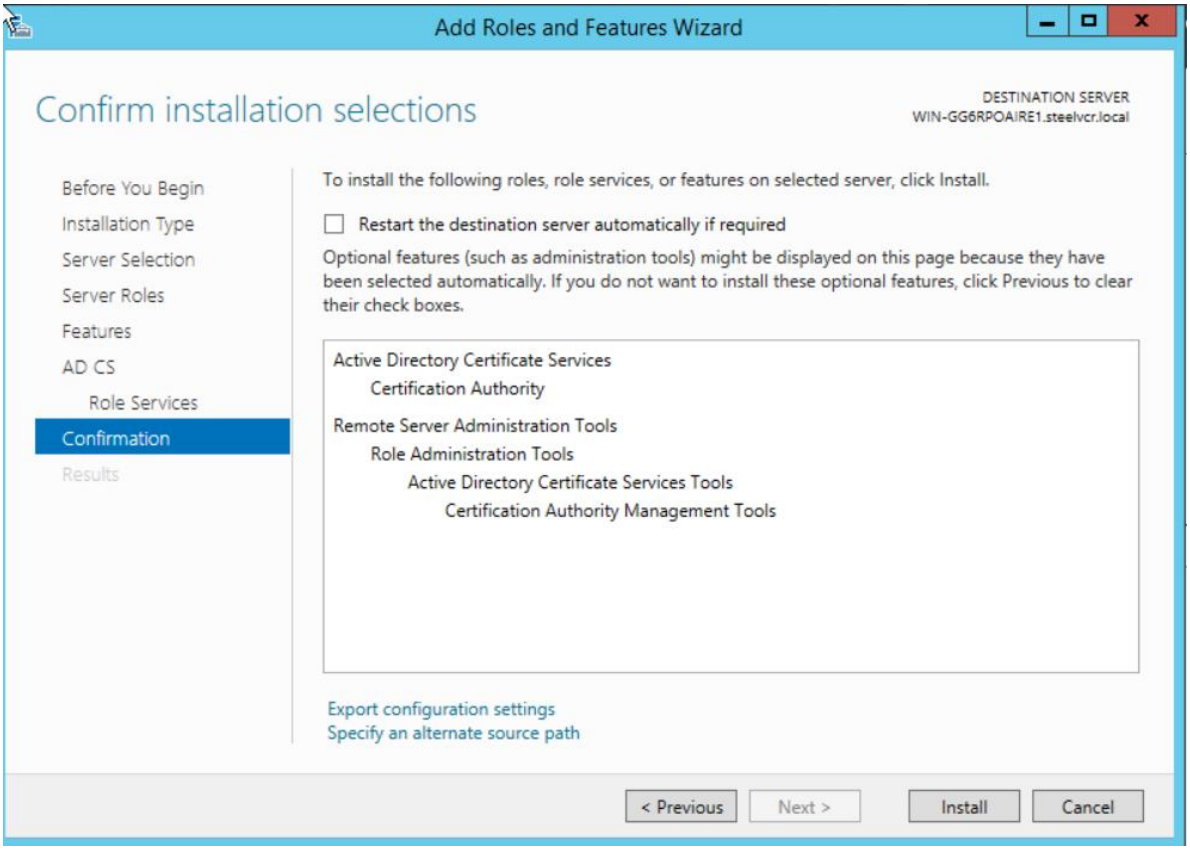


click "Next” again.

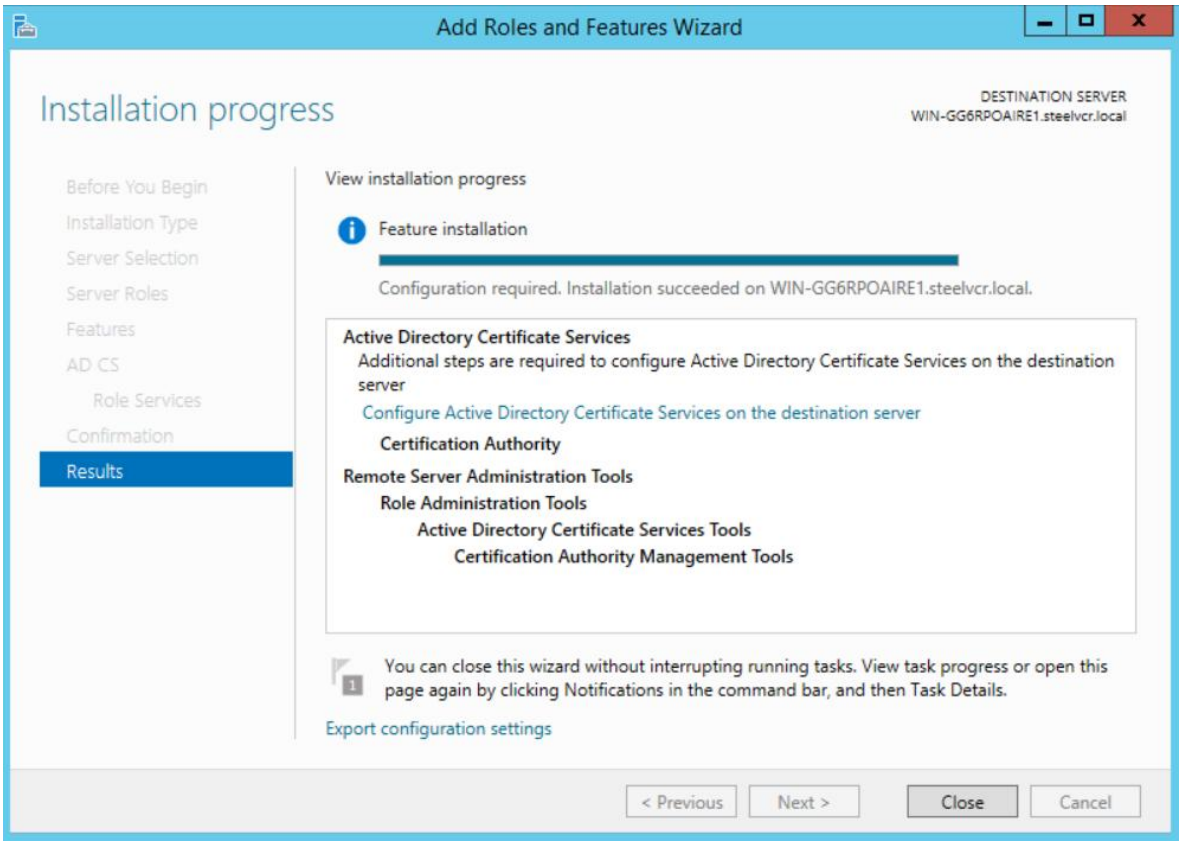


Keep “Certificate Authority” checked for issuing/managing certificates.

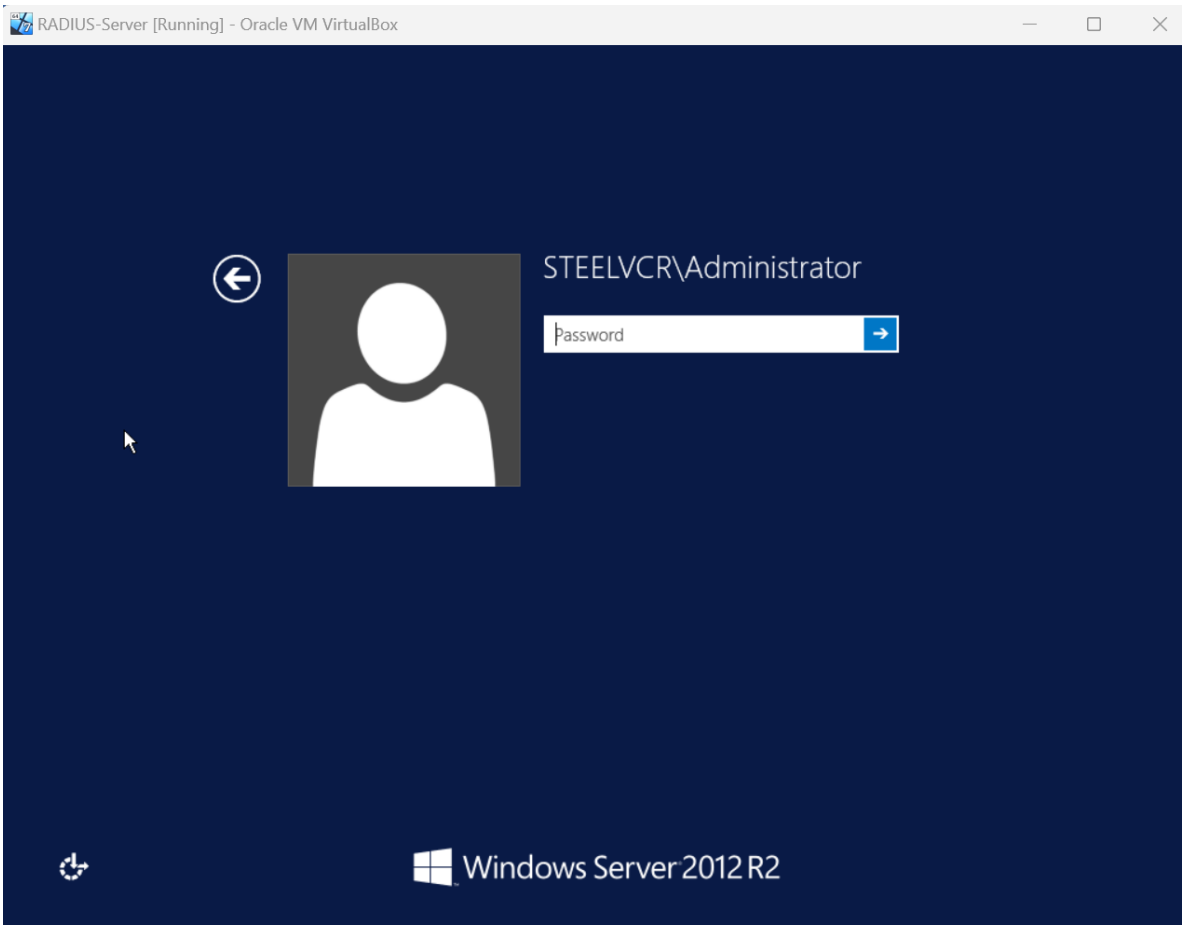
Leave everything else unchecked.



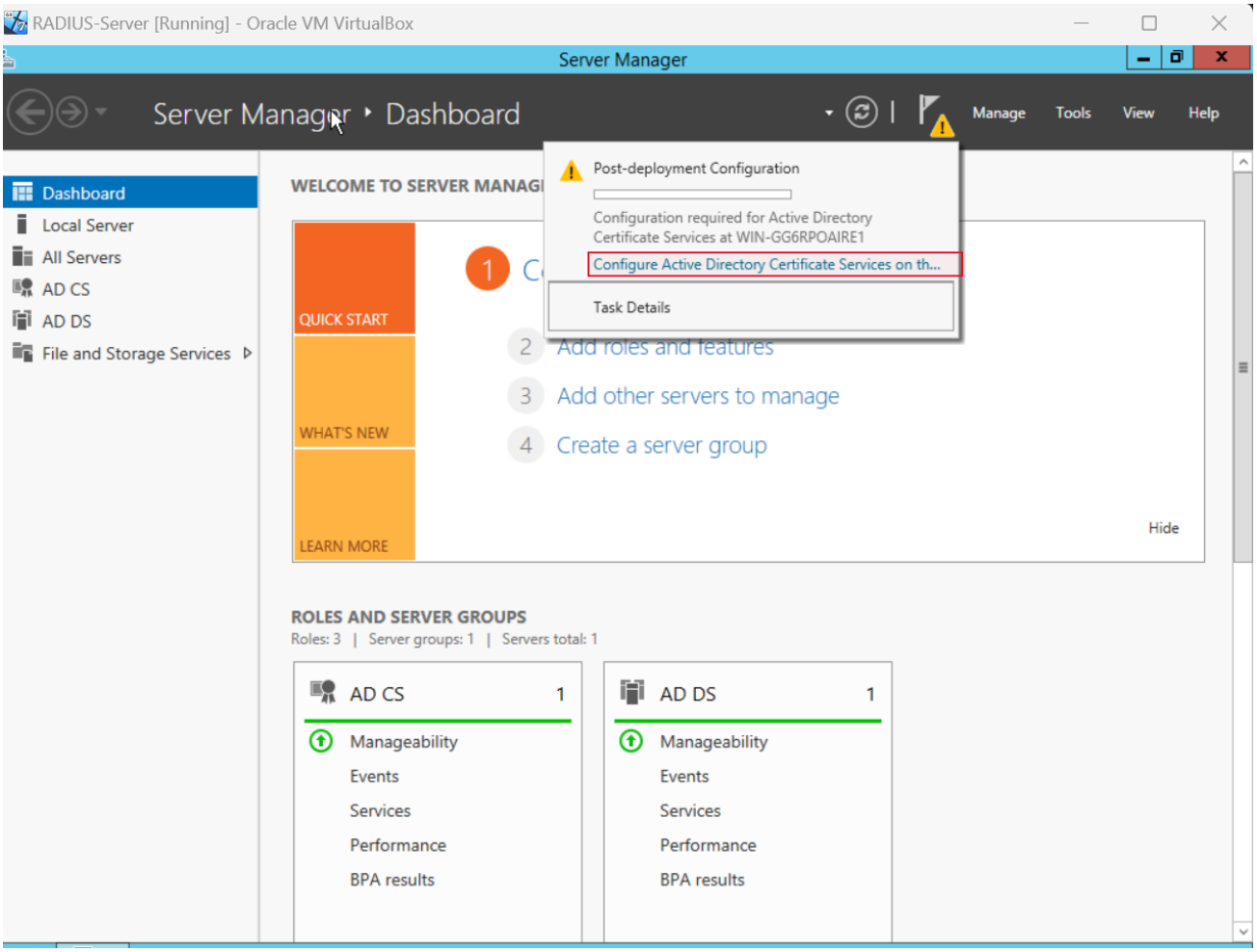
Click “Install” and leave the Restart box unchecked.



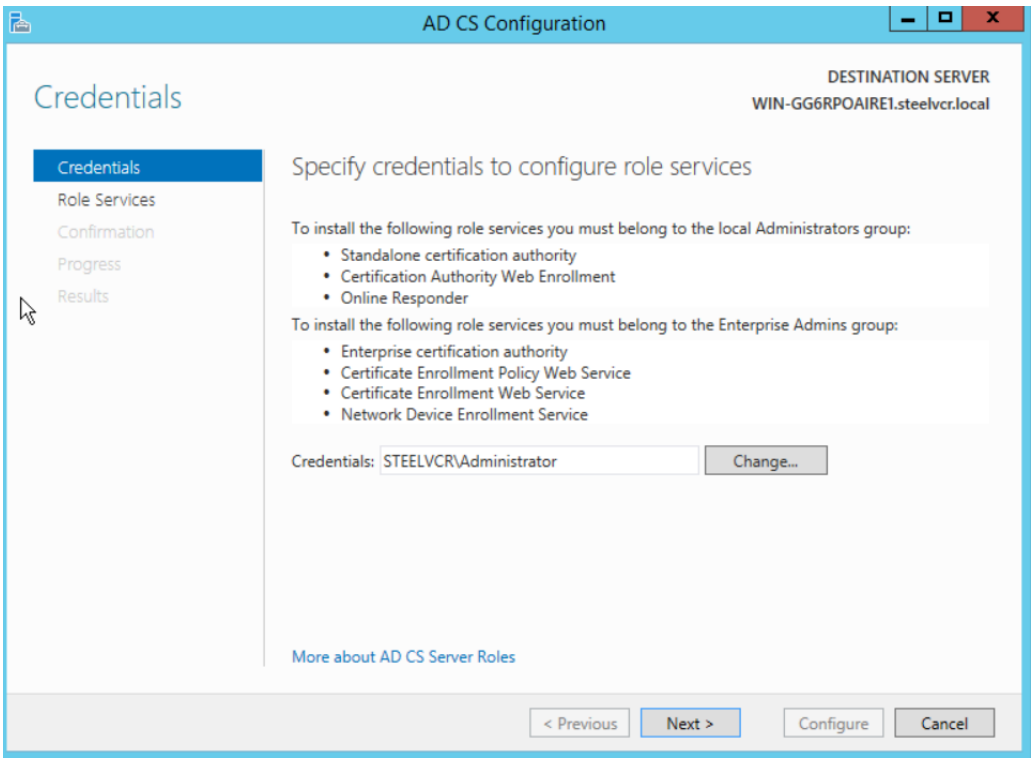
After install if successful click the “Close” button.
Do a manual reboot if one is not done automatically after this step.



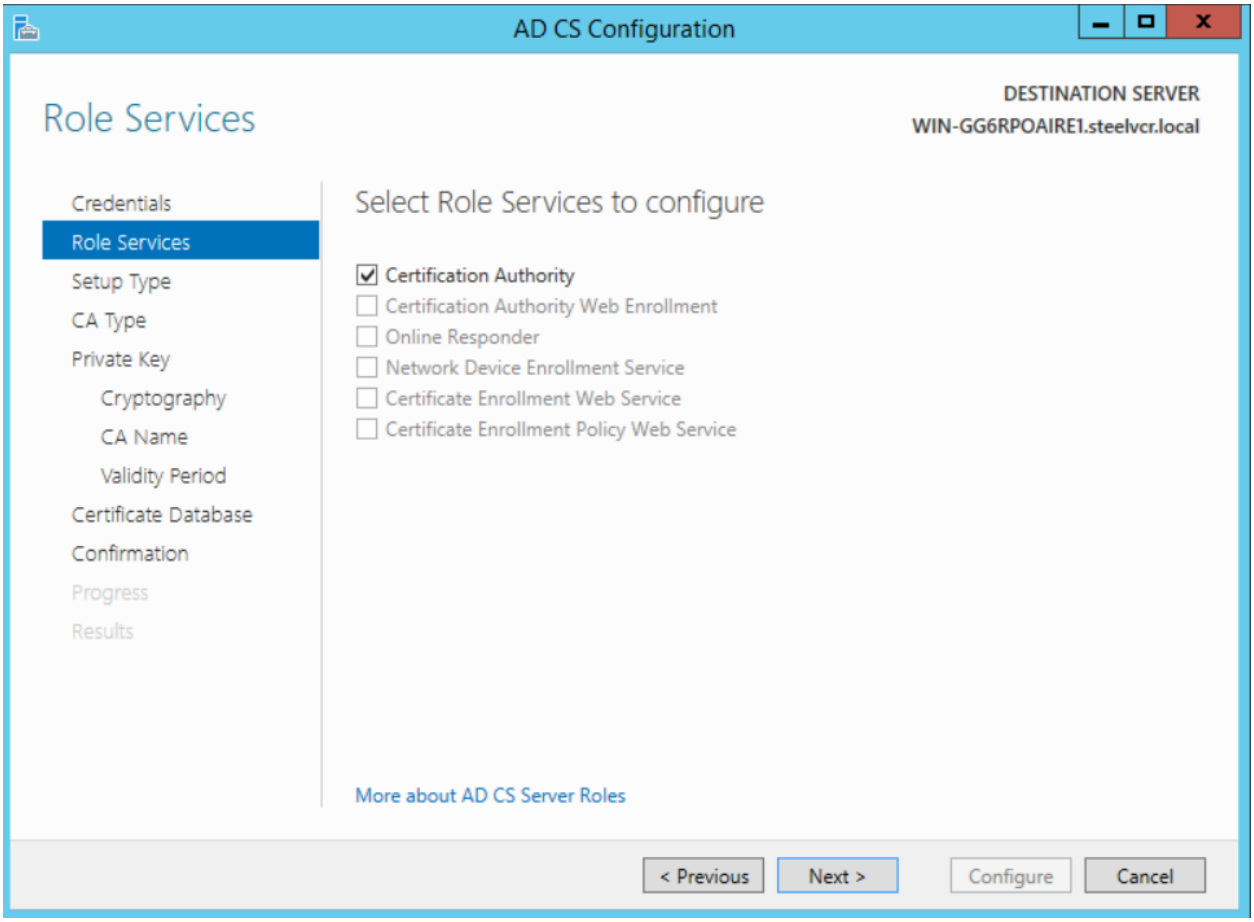
Log back in.



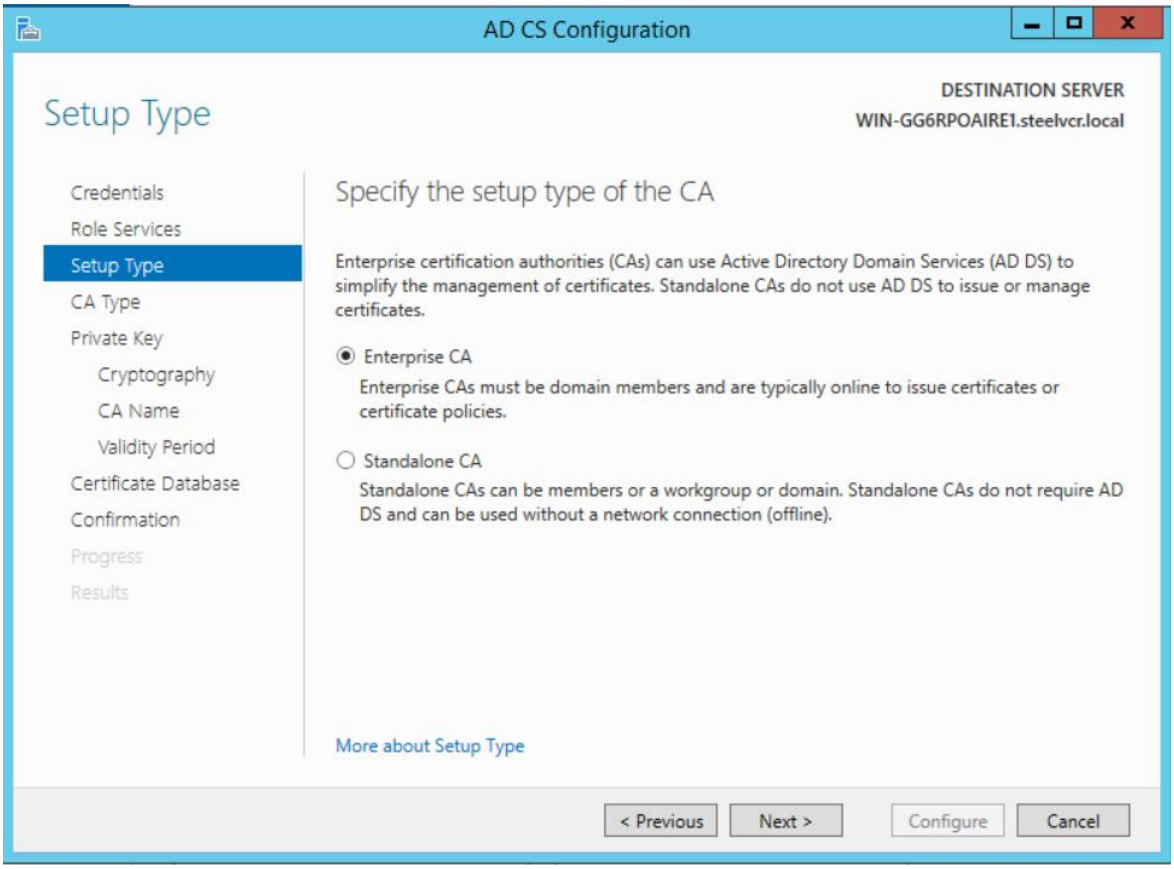
Click on notifications or the flag with yellow triangle and under “Post-deployment Configuration” click on “Configure Active Directory Certificate services on the destination server”.



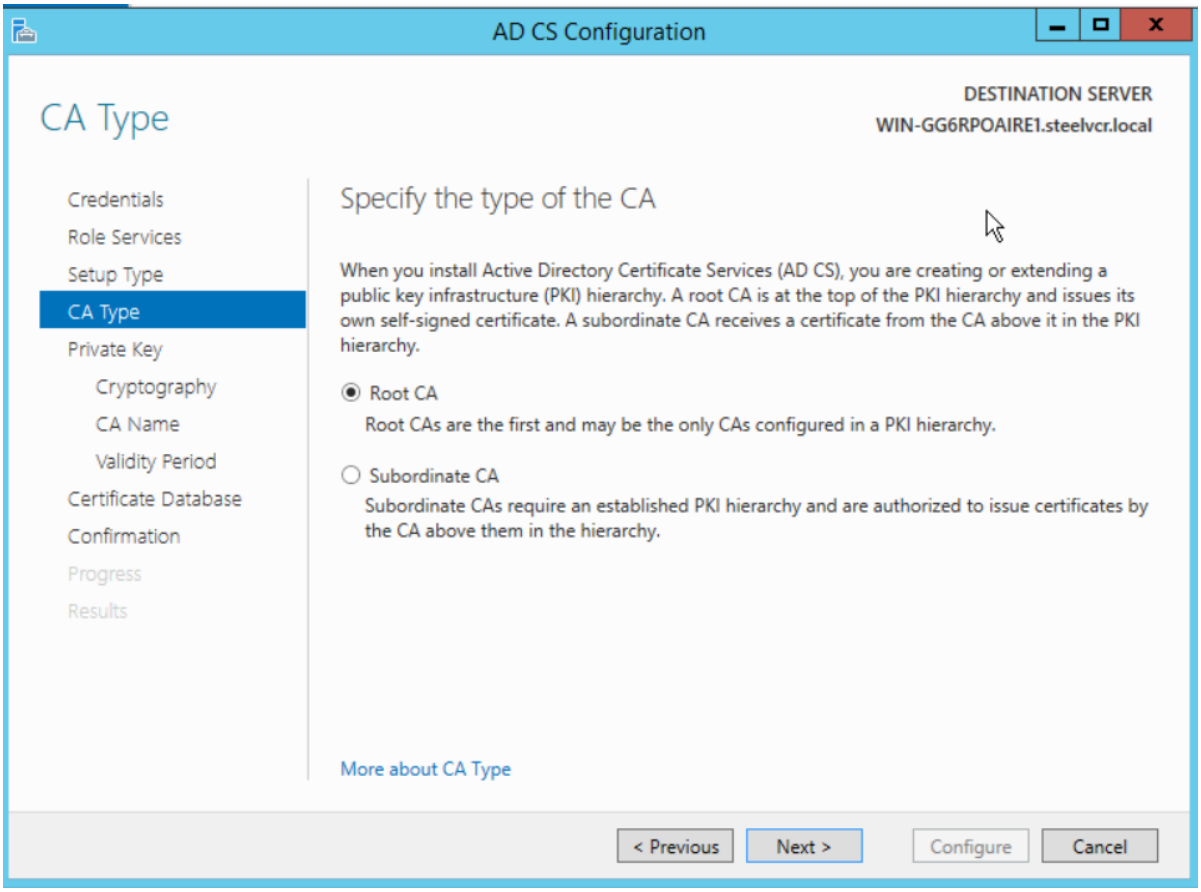
Click “Next” after credentials are confirmed.



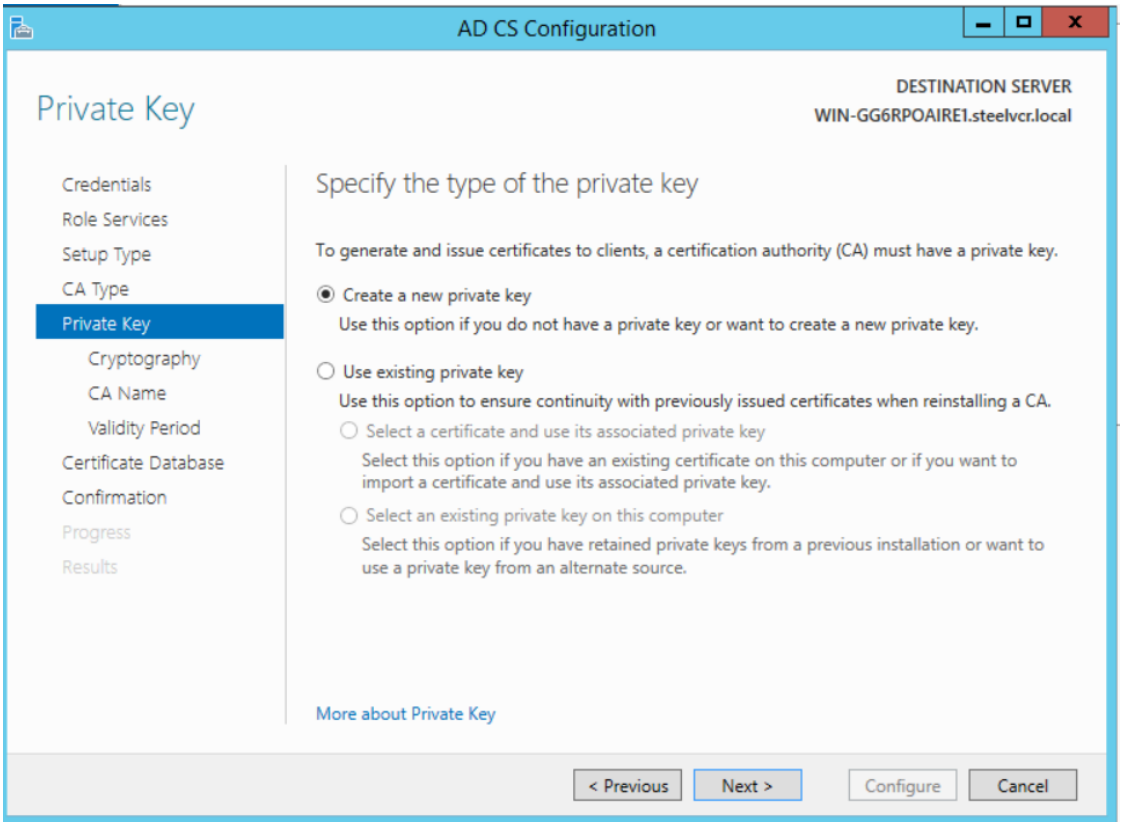
Click in the checkbox “Certificate Authority” as a role service to be configured, and click “Next”.



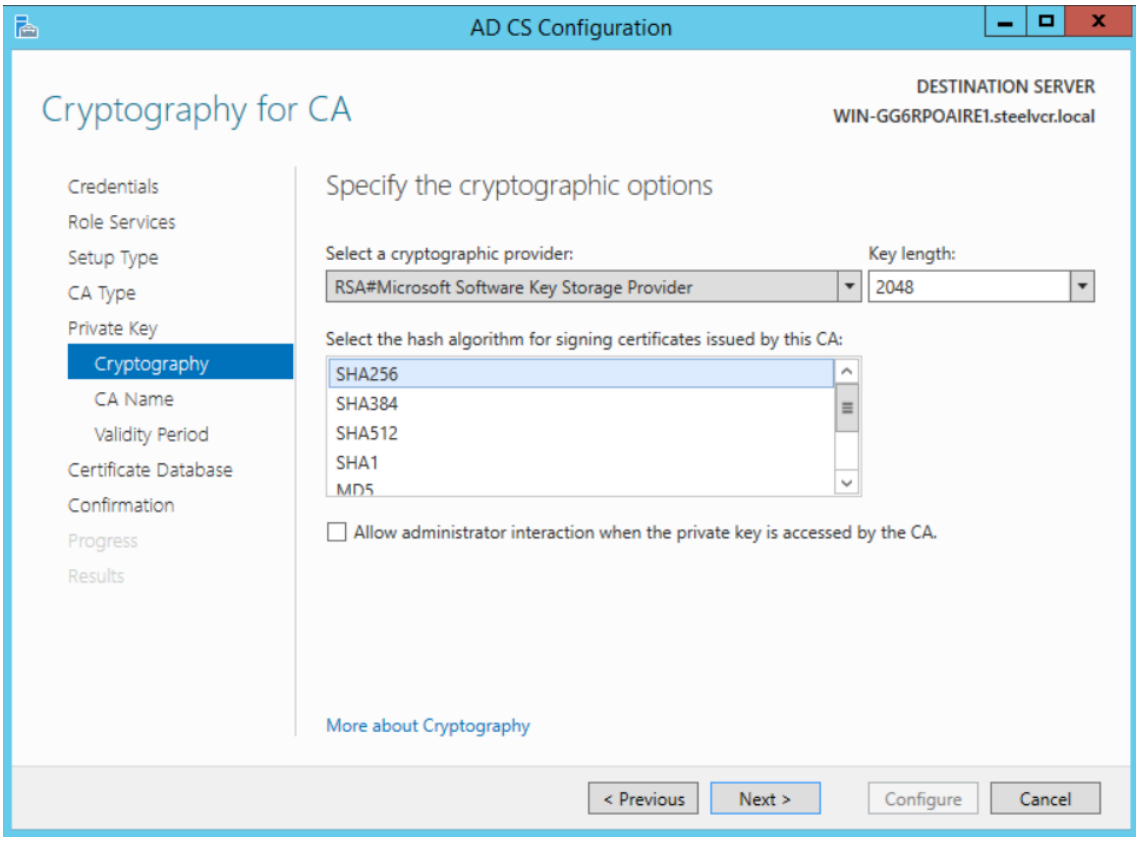
Keep “Enterprise CA” selected and click “Next”. Enterprise CA will issue certificates and their polices.



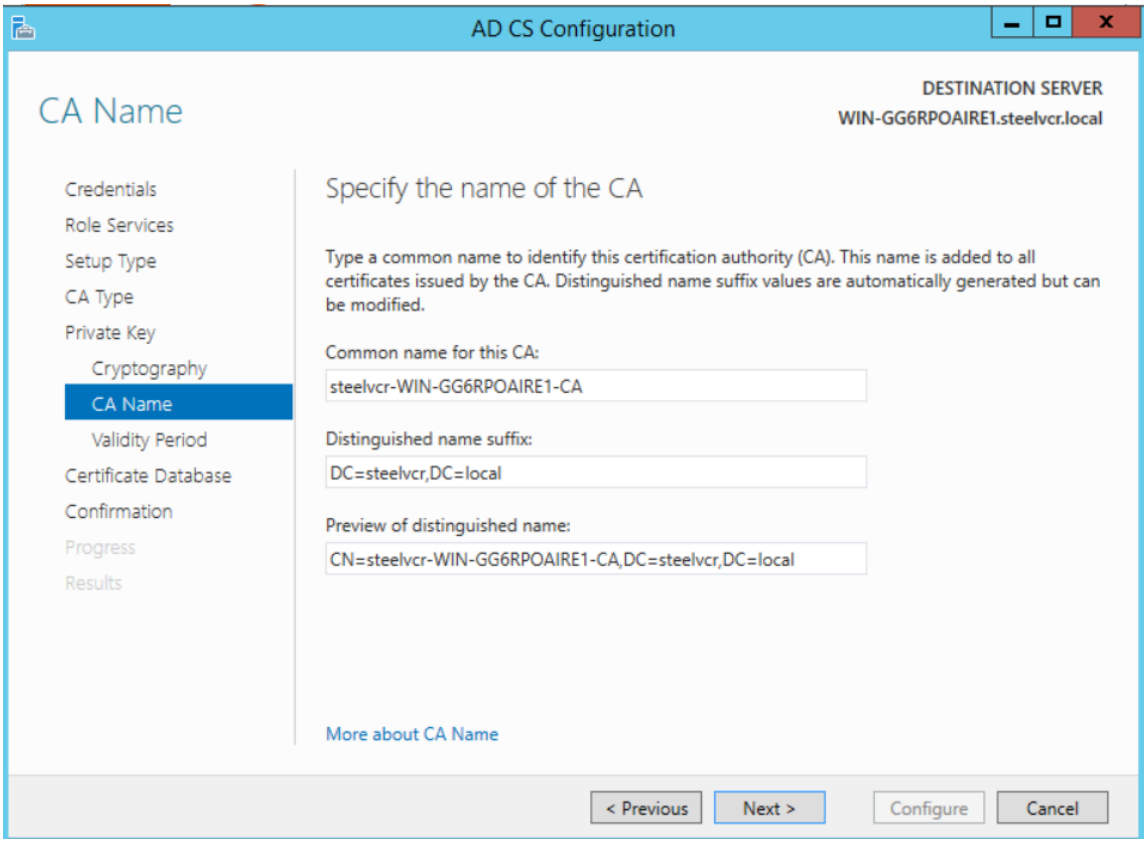
Keep “Root CA” selected so they are at top of PKI hierarchy.



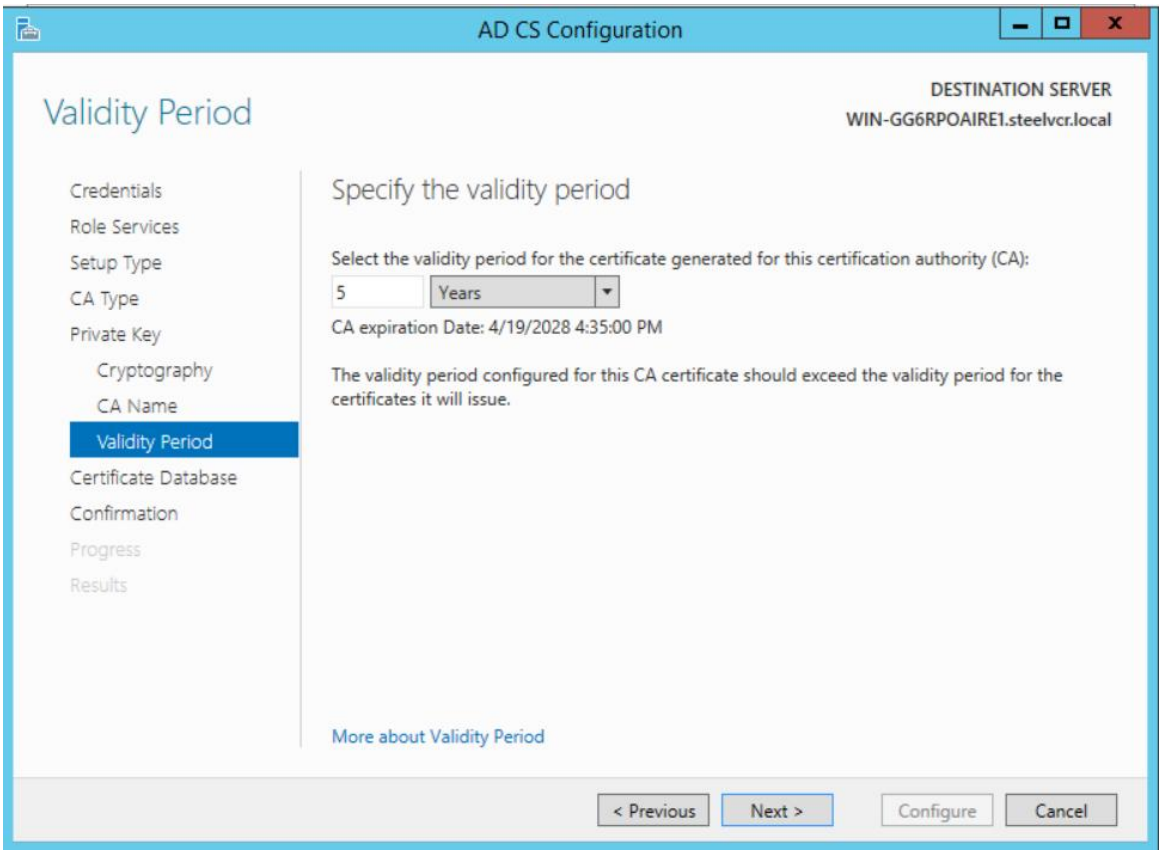
Select “Create a new private key” so a private key is created and click “Next”.



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

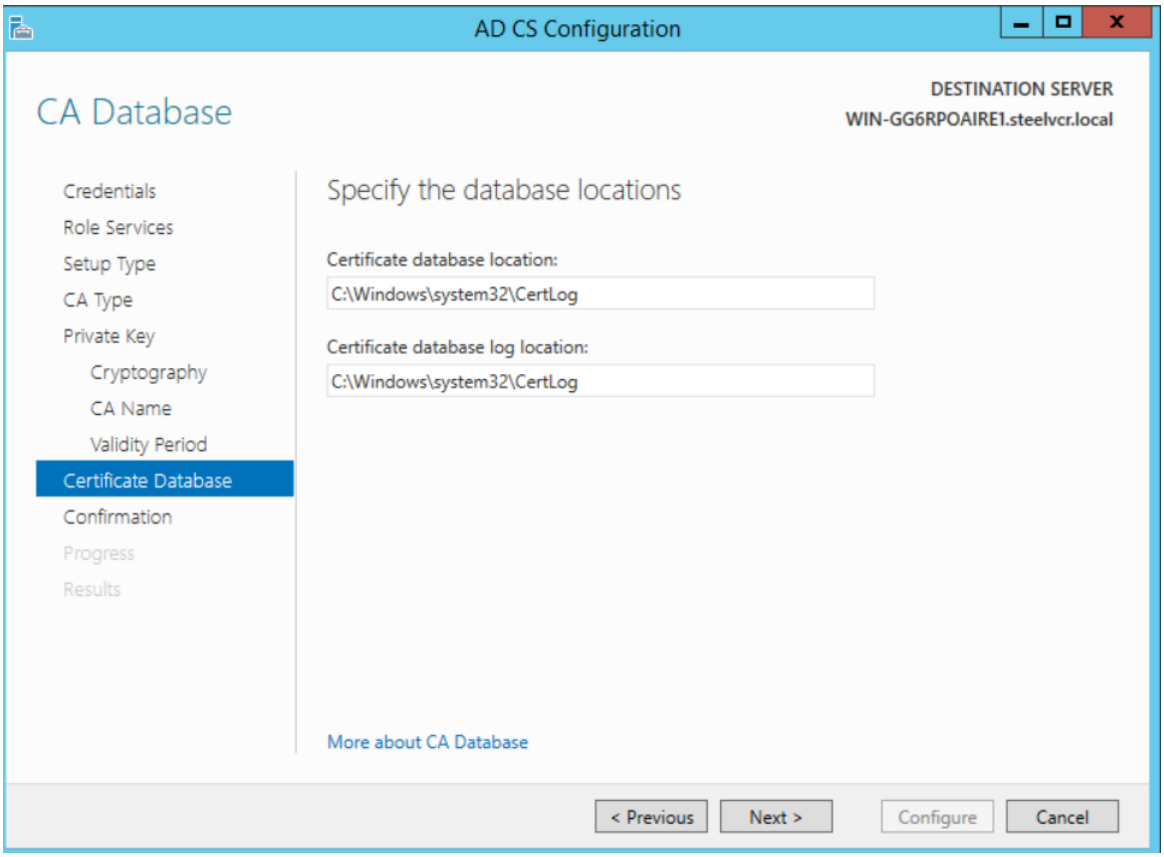


The “Common name for this CA”, “Distinguished name suffix”, and “Preview of distinguished name” should be filled in automatically. Click “Next”.

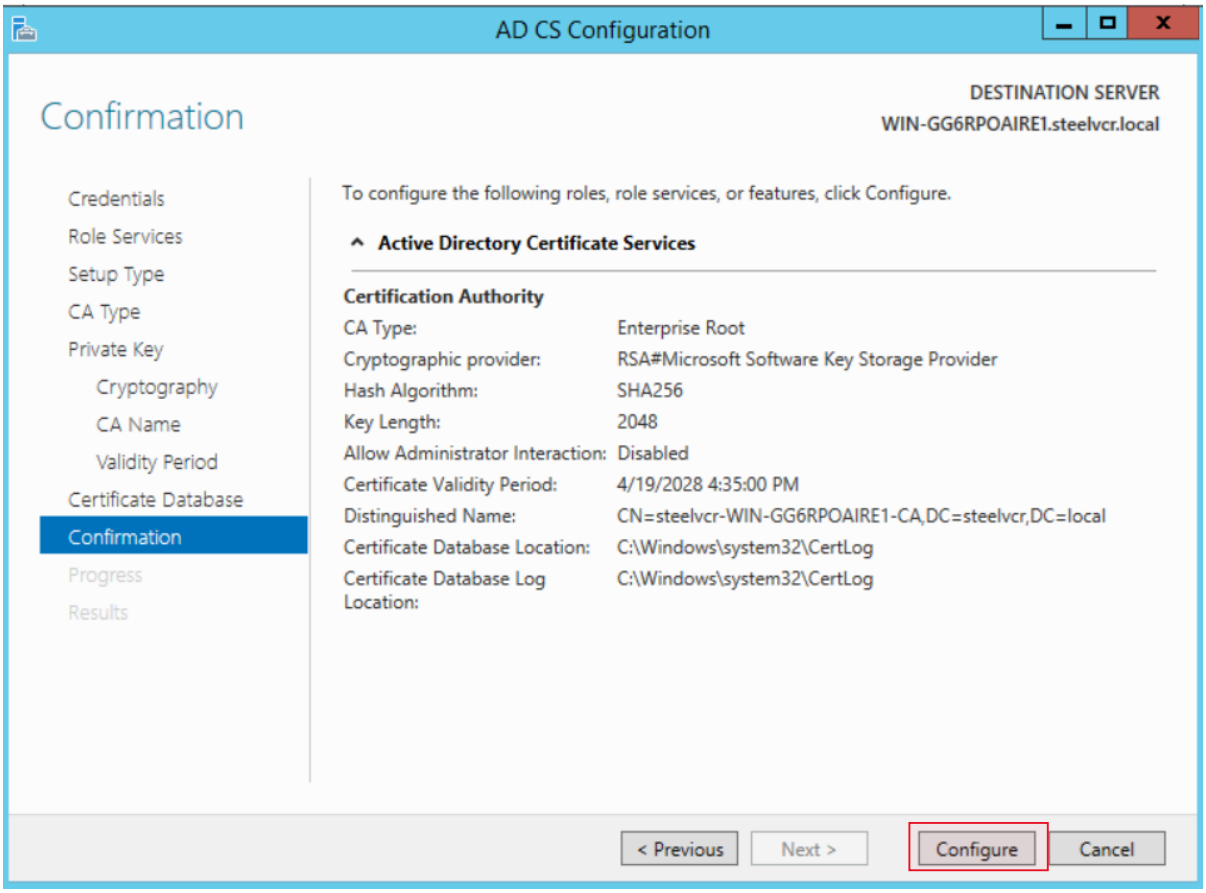


Keep or change validity period and click “Next”.

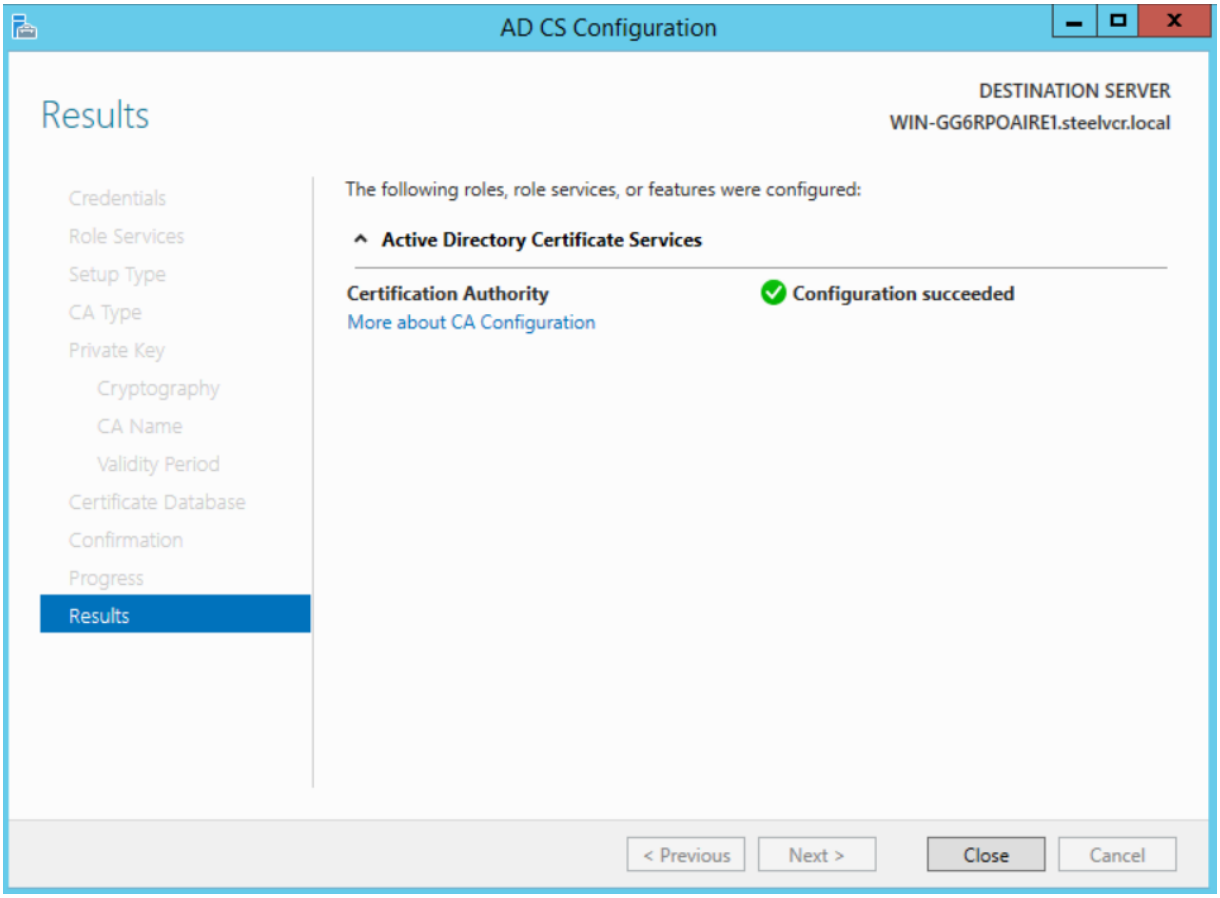
Can change “years” to “days”, “weeks”, or “months”.



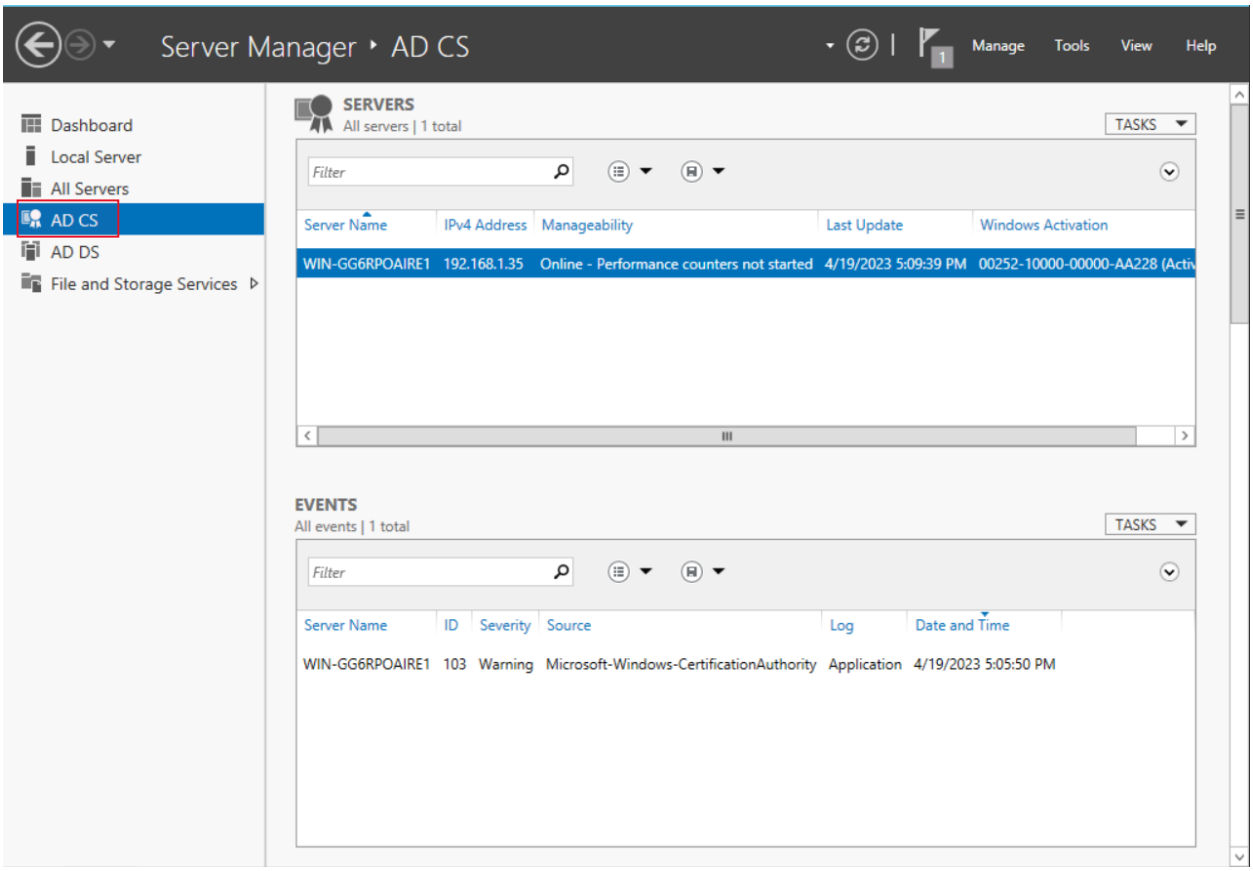
Keep the locations for certificate database and log database. Click “Next”.



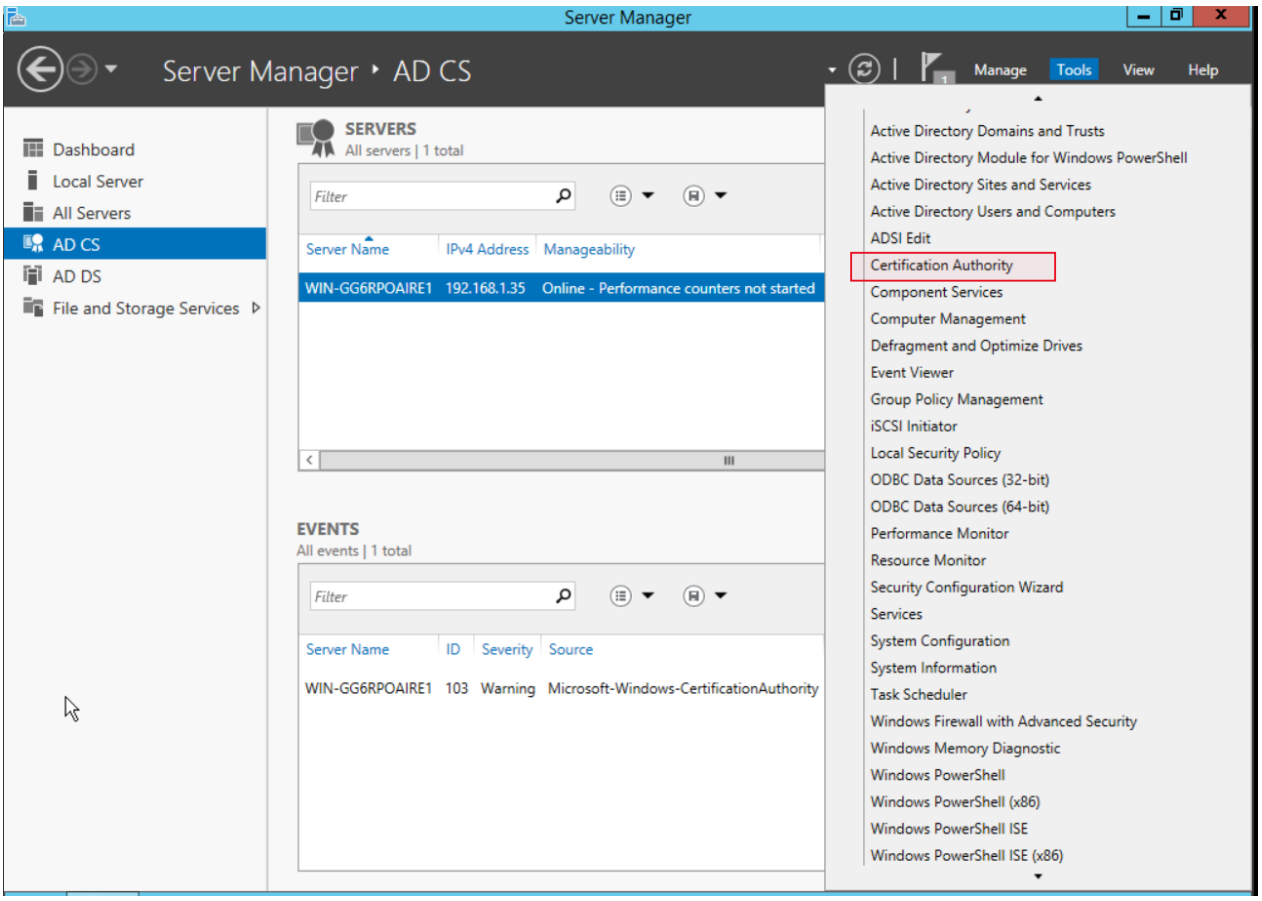
Review everything and click “Configure”.



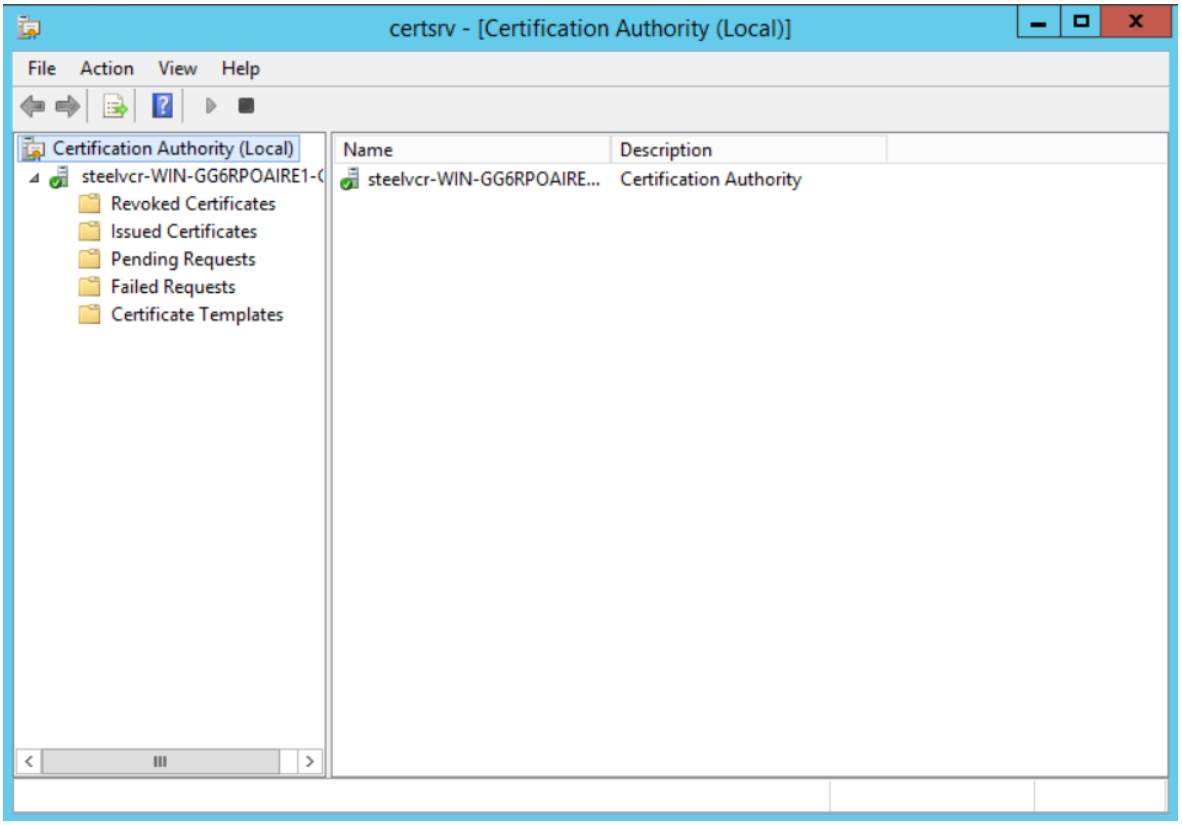
After a successful configuration click on “Close”.



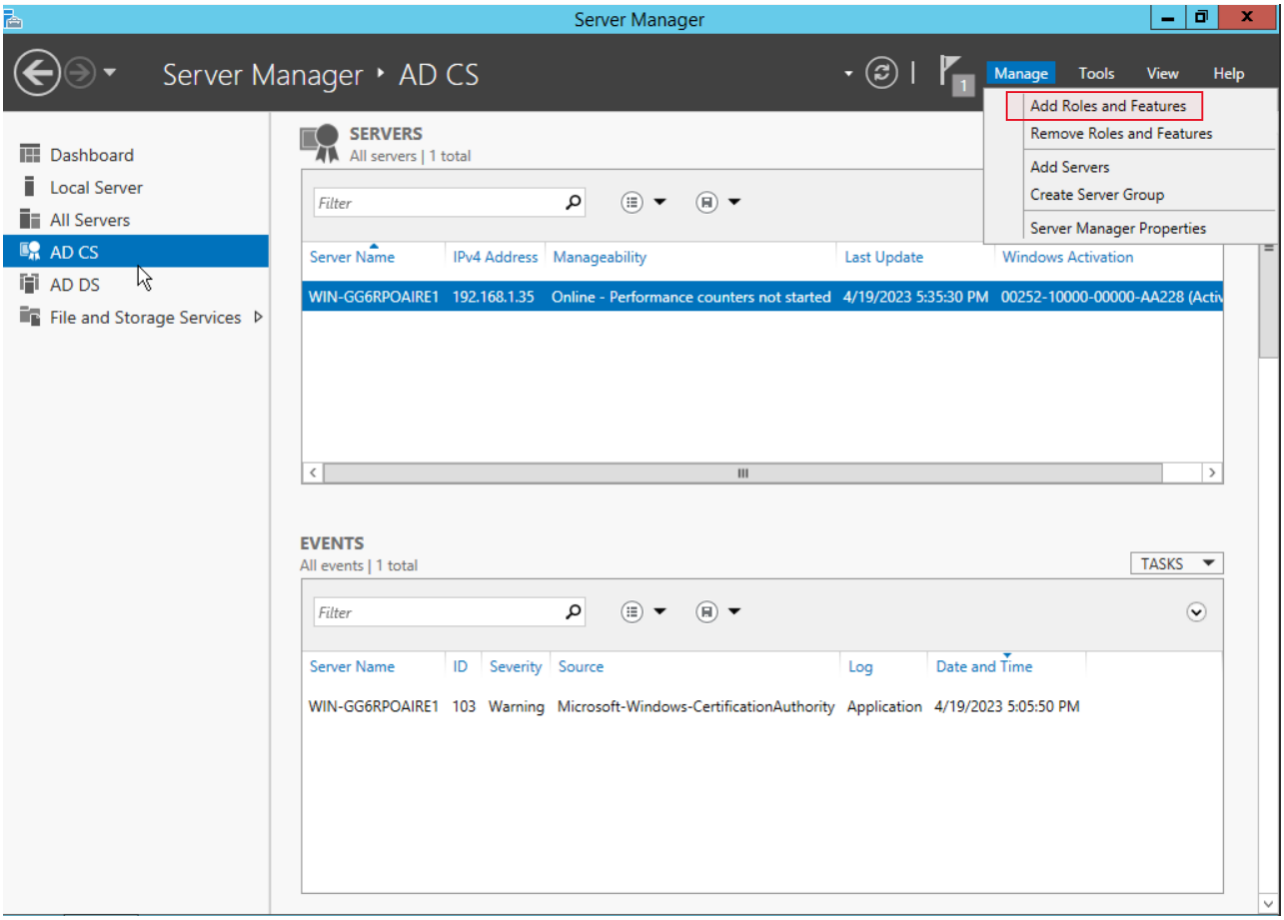
In Server Manager click on “AD DS” on left-hand side.



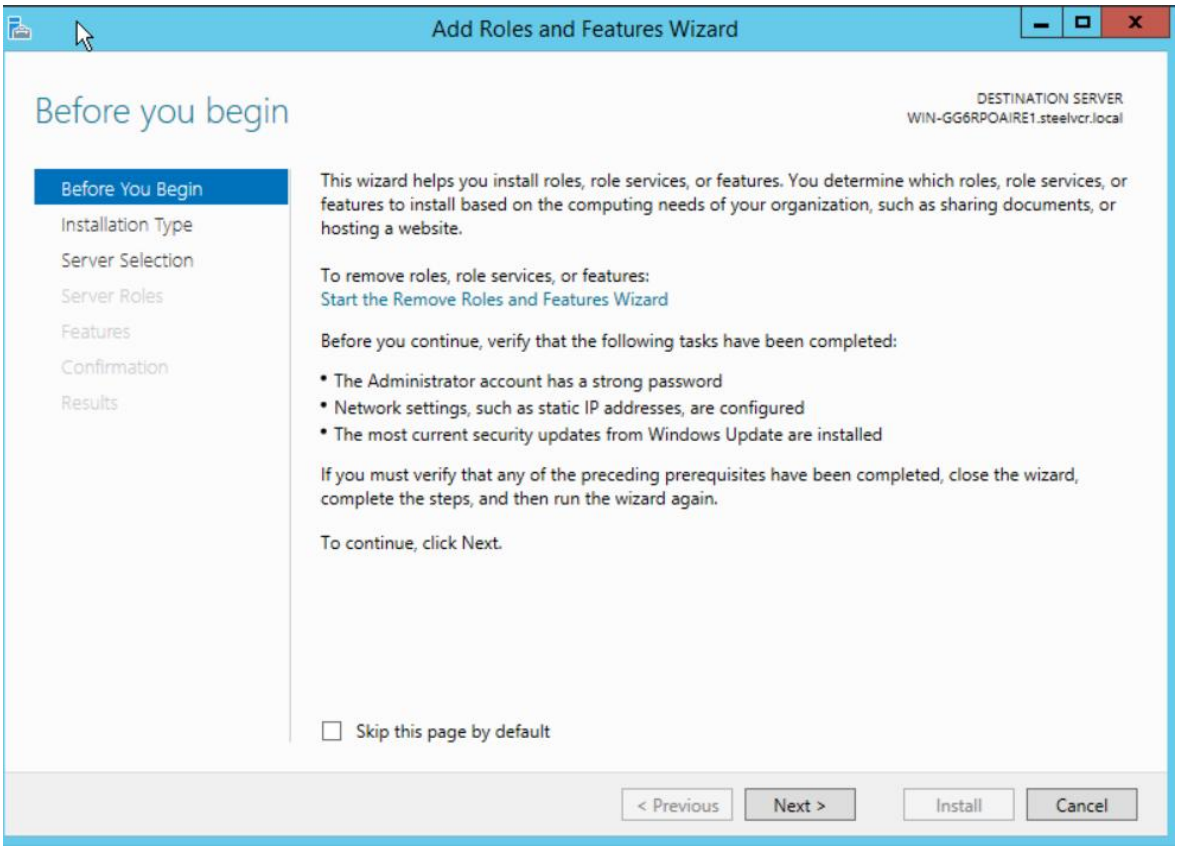
While in “AD CS” (left side column), Click on “Tools” in upper right-hand corner and then click on “Certificate Authority”.



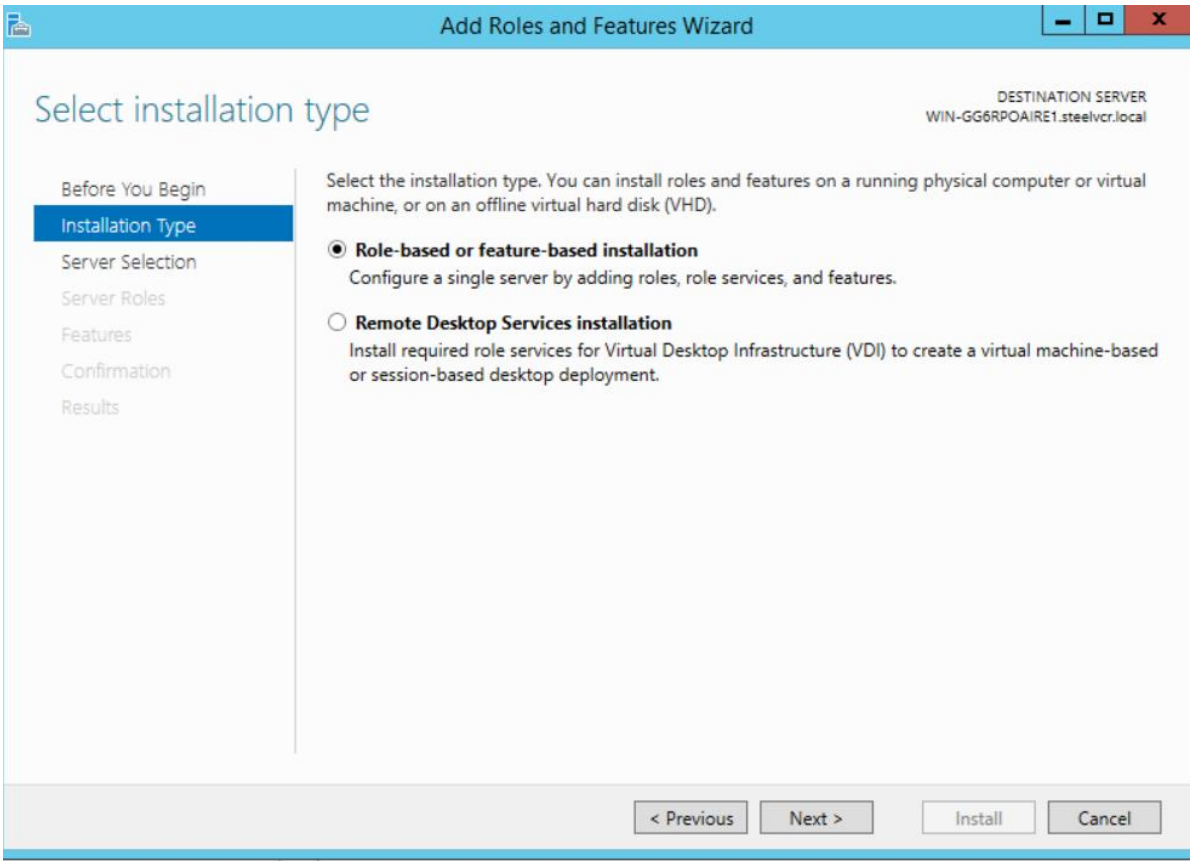
This is the CA/certificate authority that we just installed. Exit out of this.



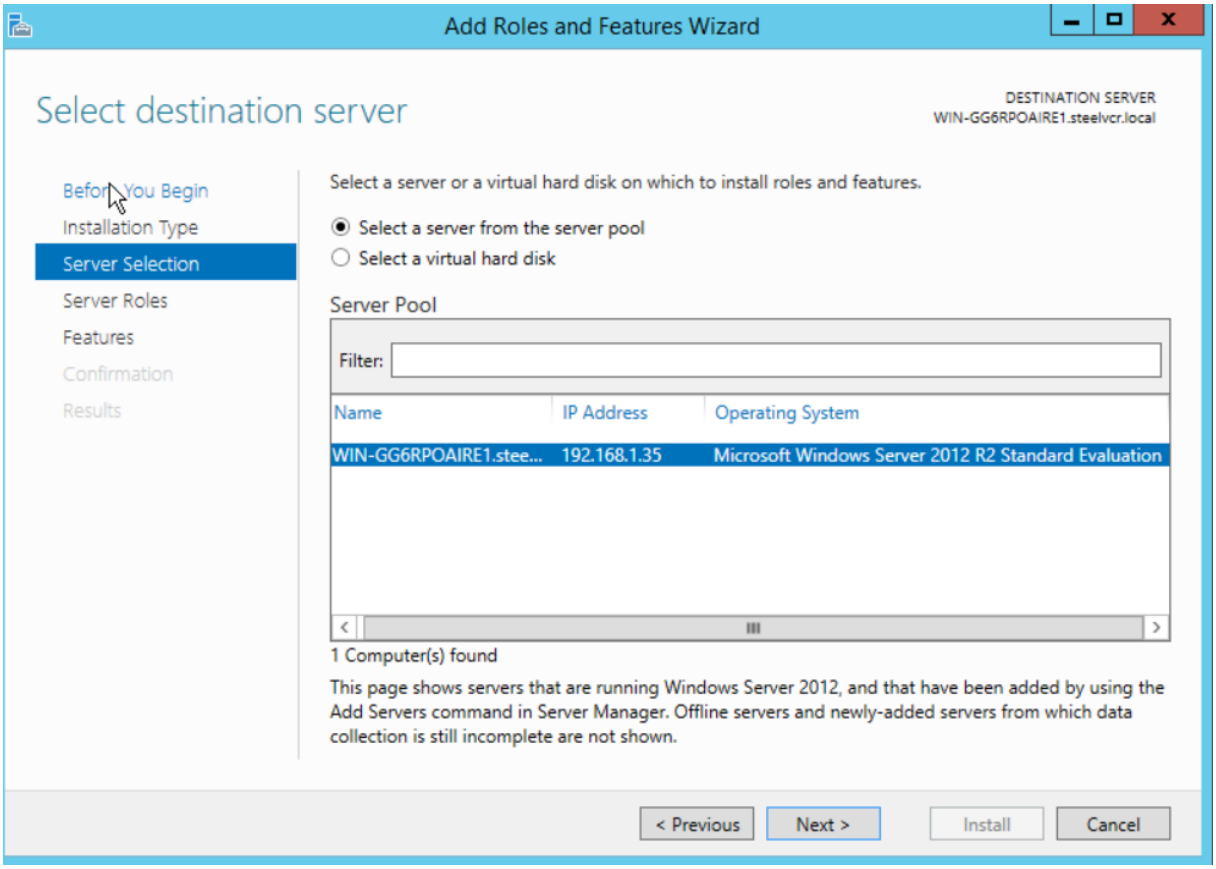
In “AD CS” go to “Manage” in top right corner and click on “Add Roles and Features”.



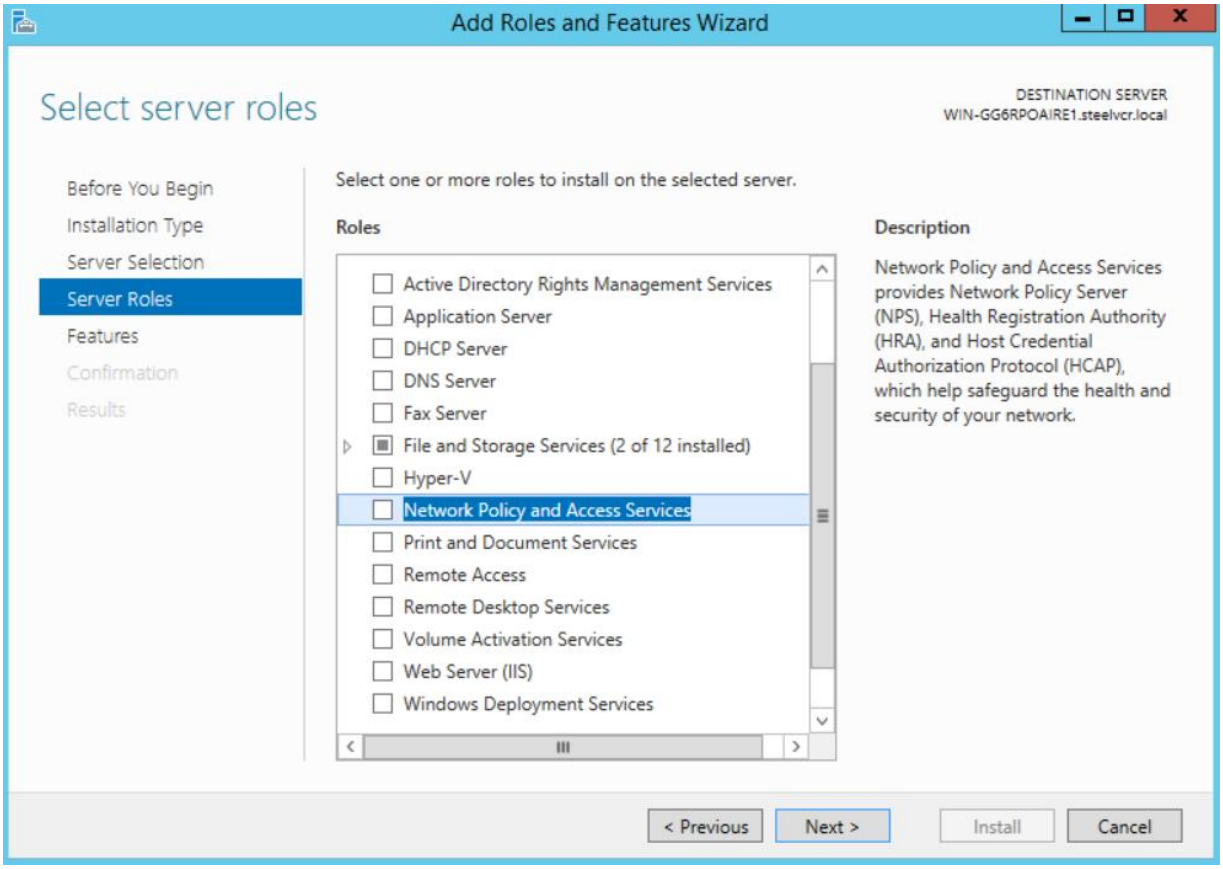
Read and click “Next”.



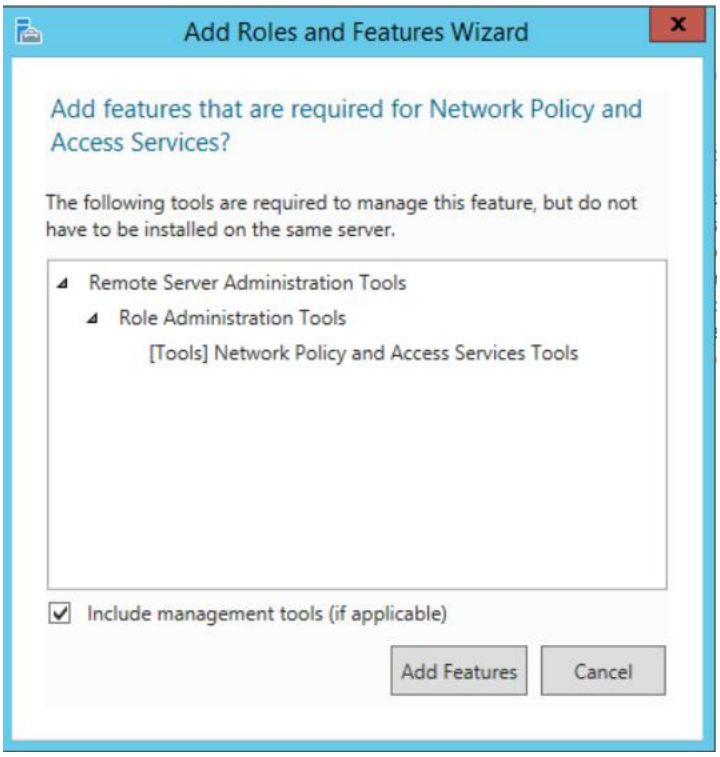
Keep “Role-based or feature-based installations” selected.



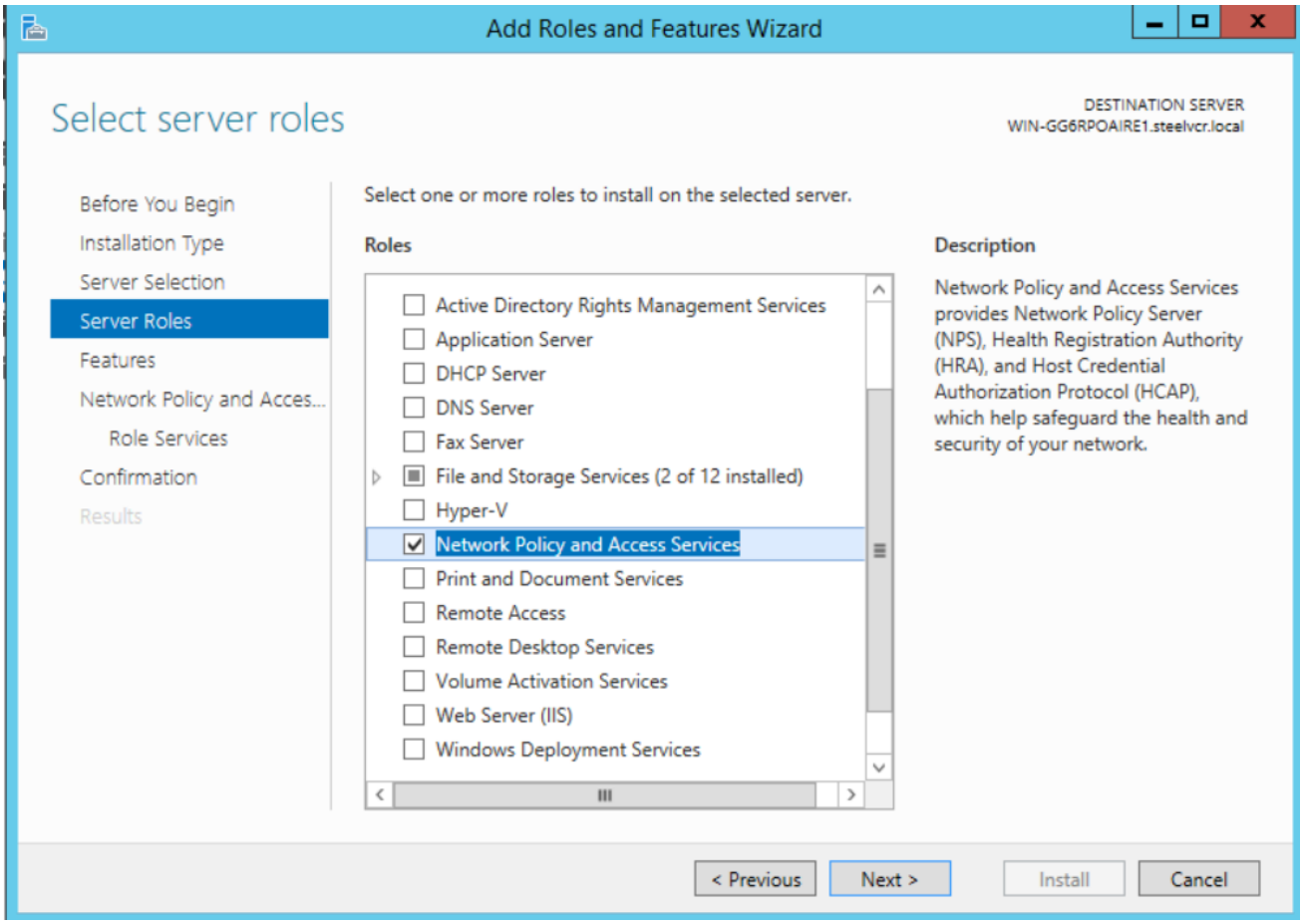
Keep server selected and click “Next”.



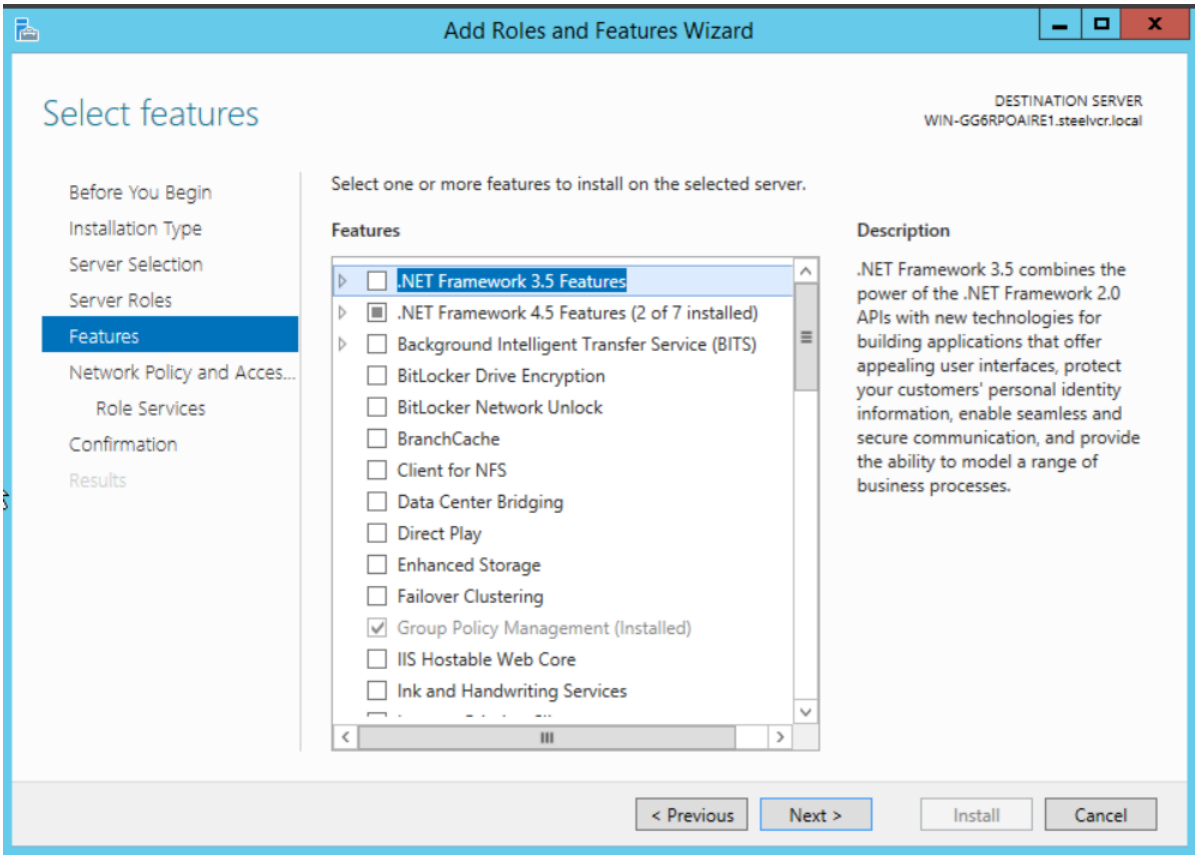
Click on checkbox for “Network Policy and Access Services”.



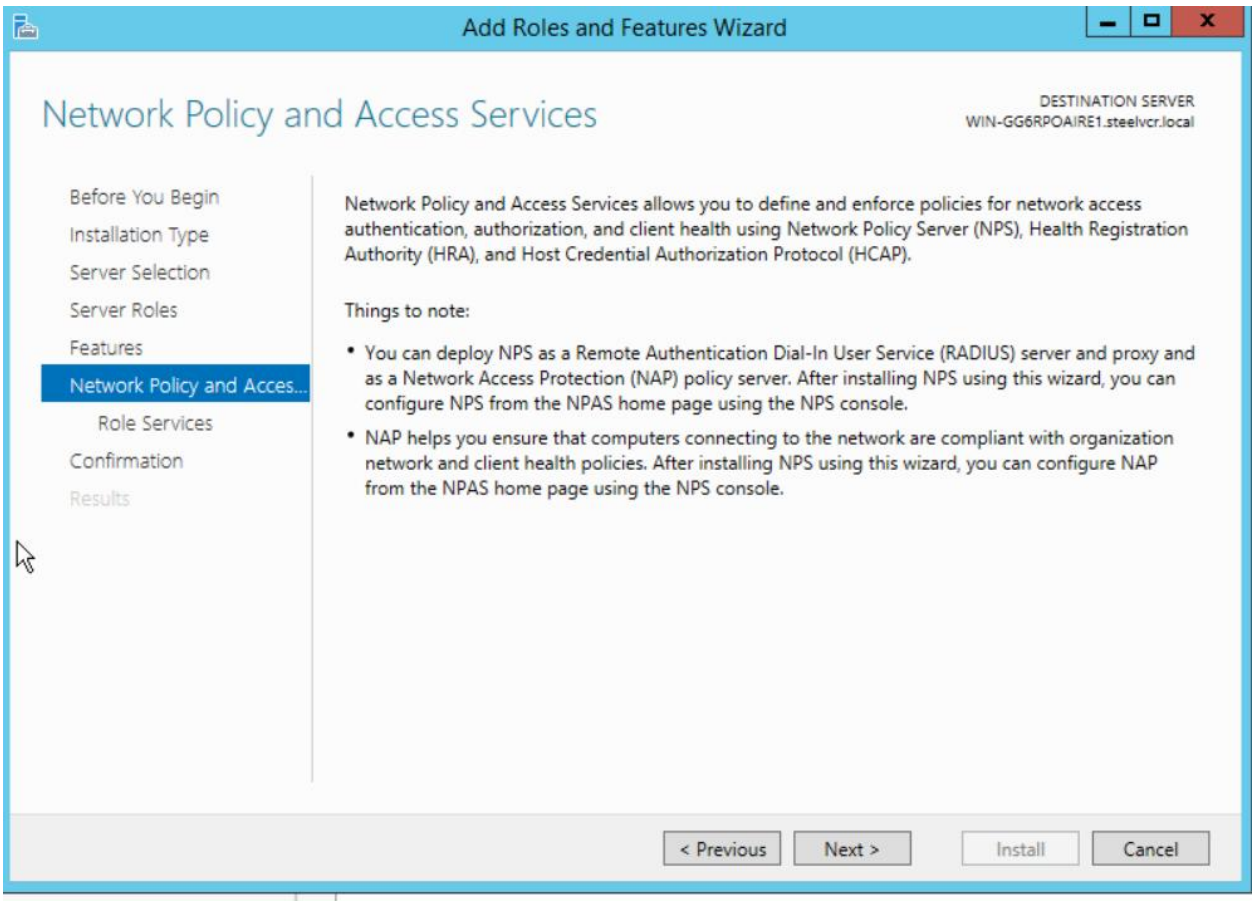
Click on “Add Features”. (This feature is for network security/protection)



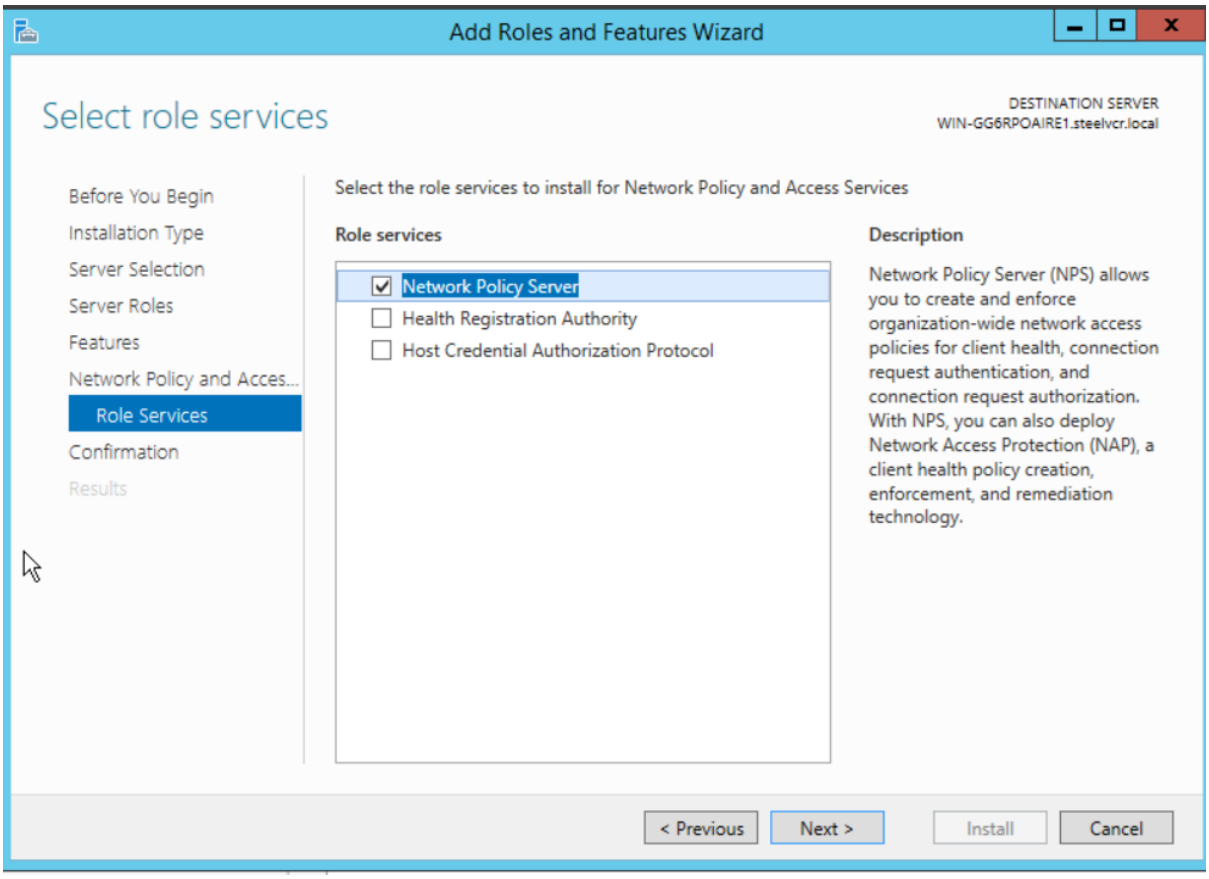
Click “Next”.



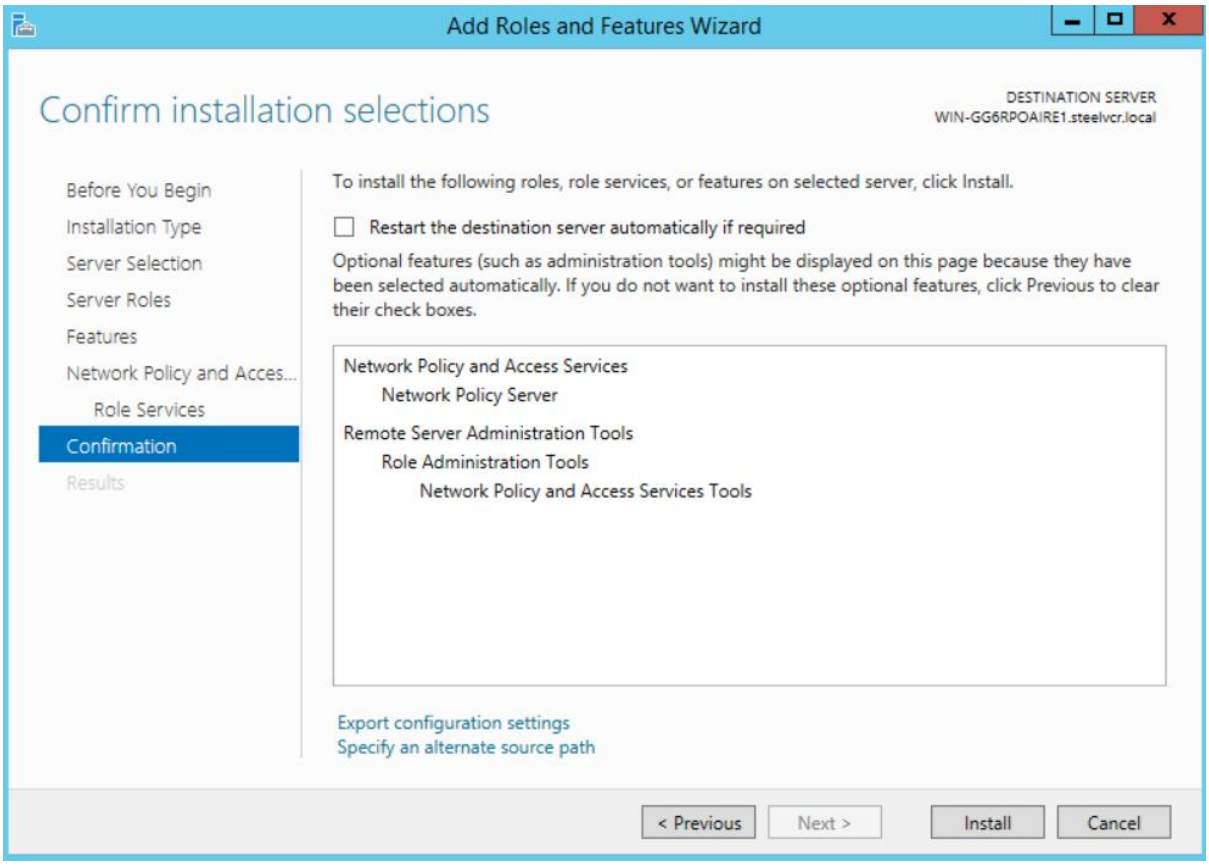
Don’t check anything here and click “Next”.



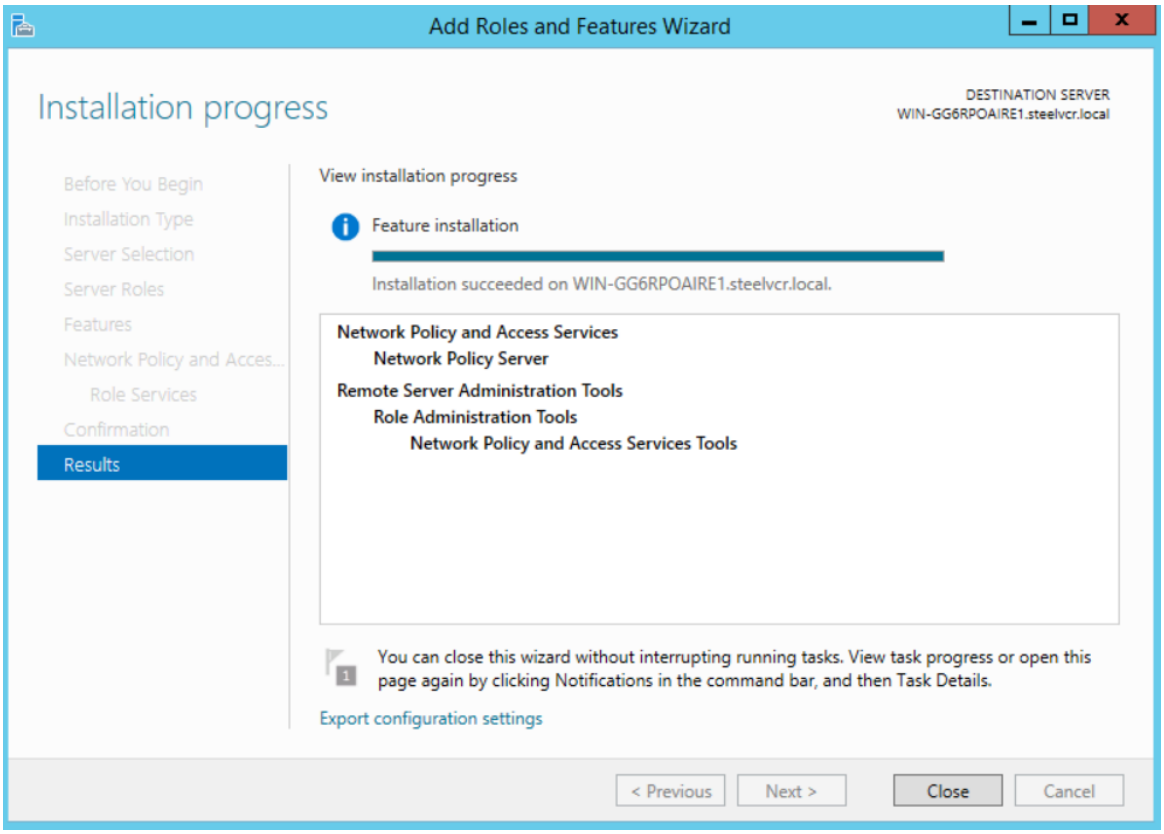
Read and click “Next”.



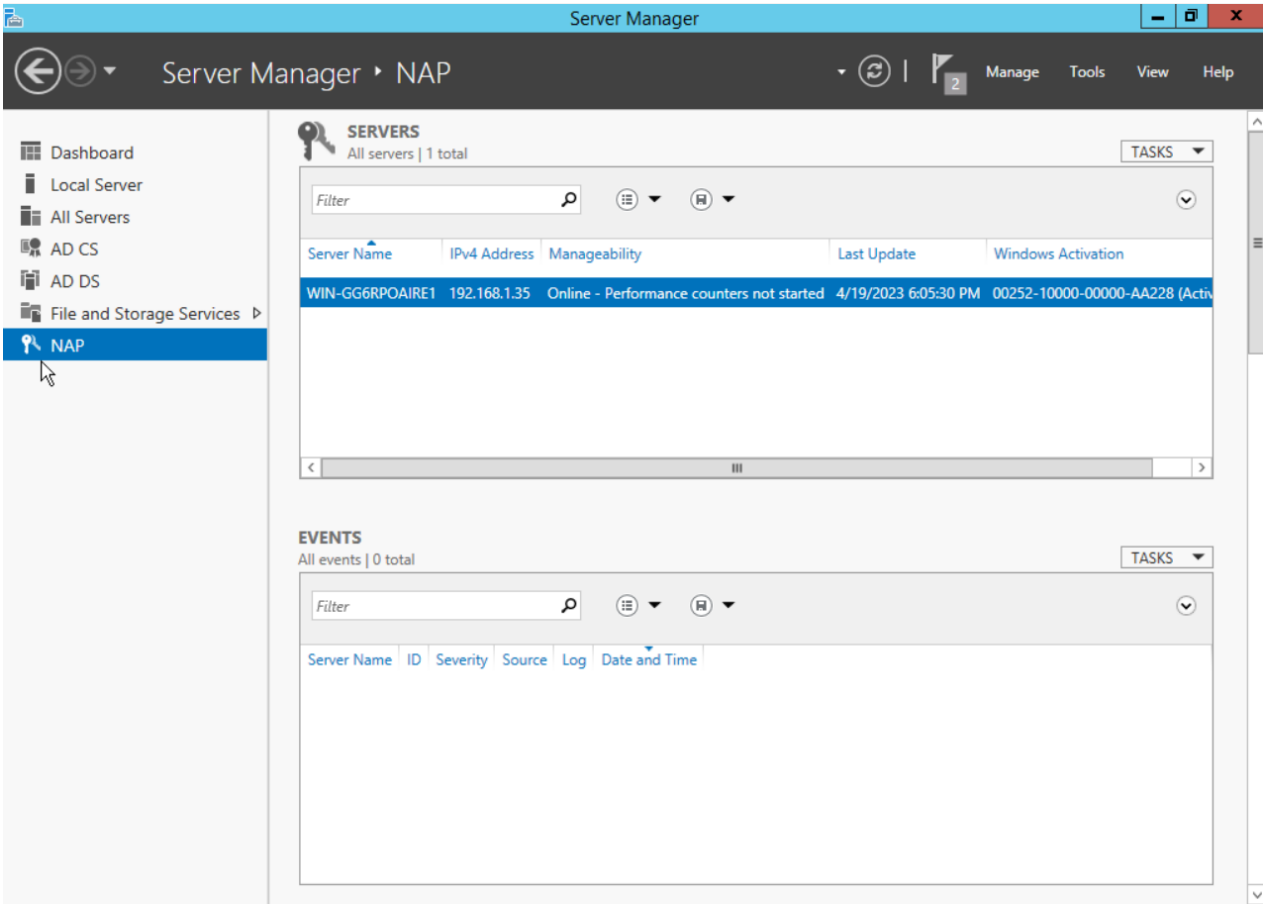
Keep “Network Policy Server” and click “Next”.



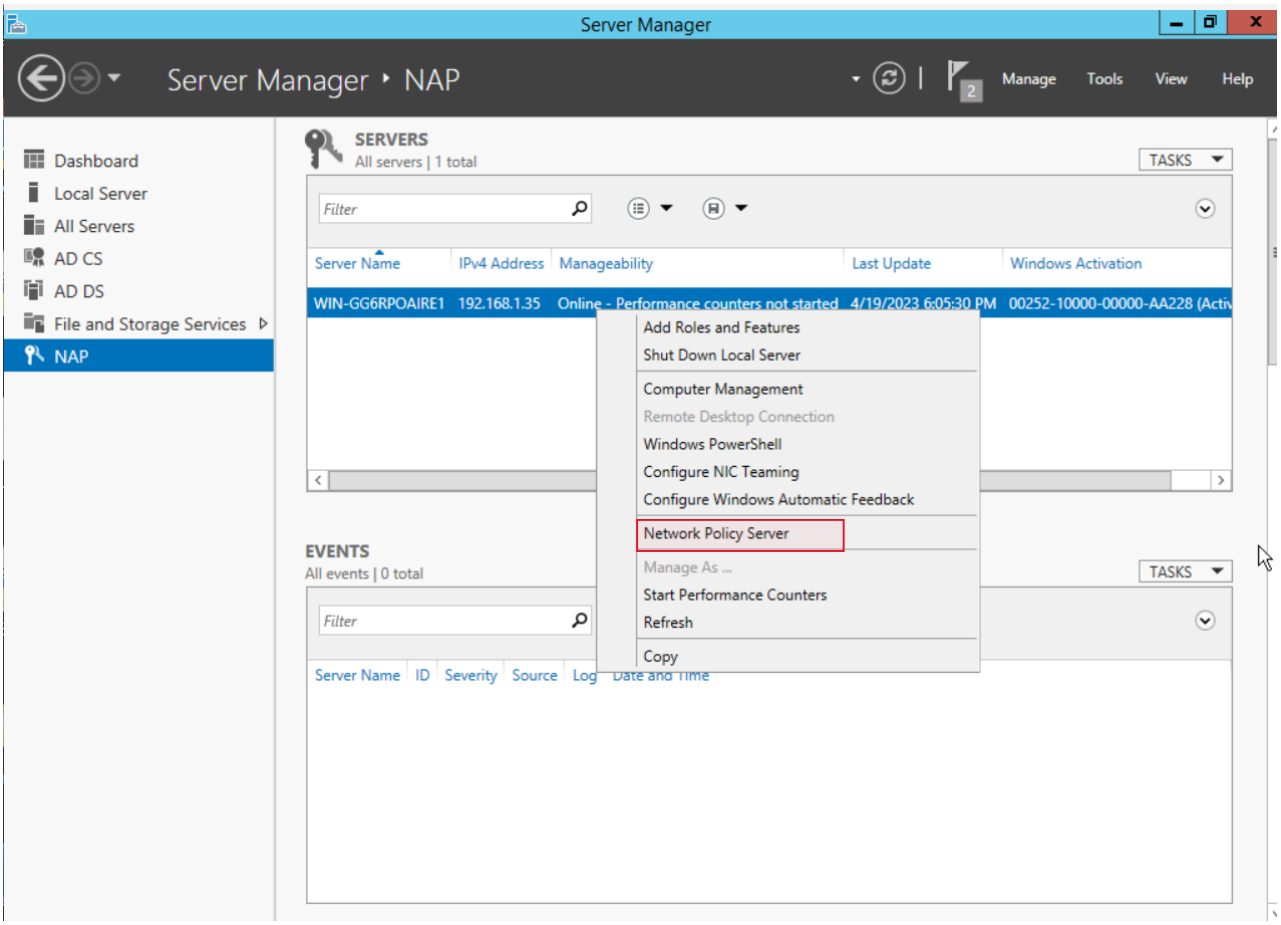
Click “Install”.



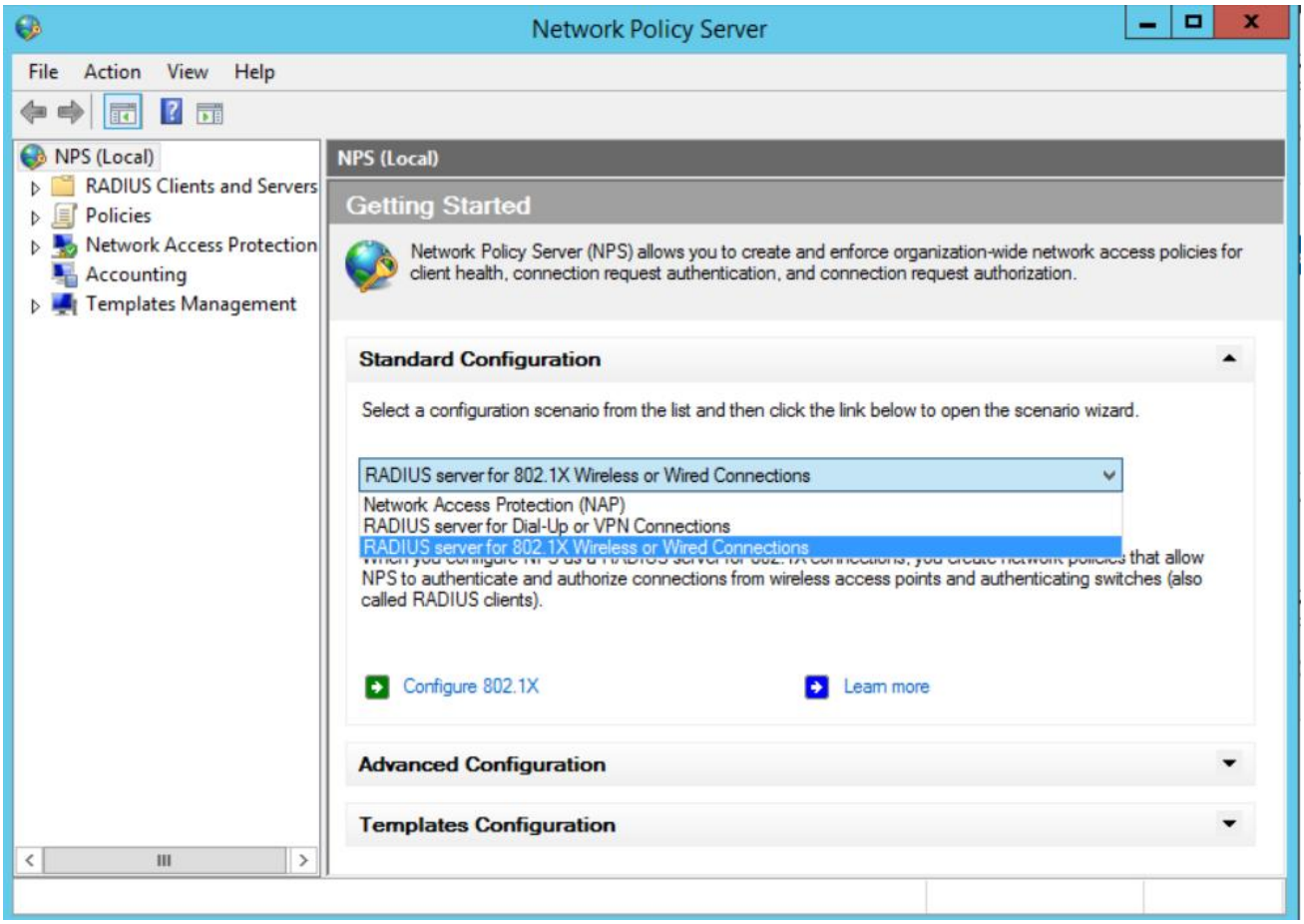
After successful installation click “Close”.



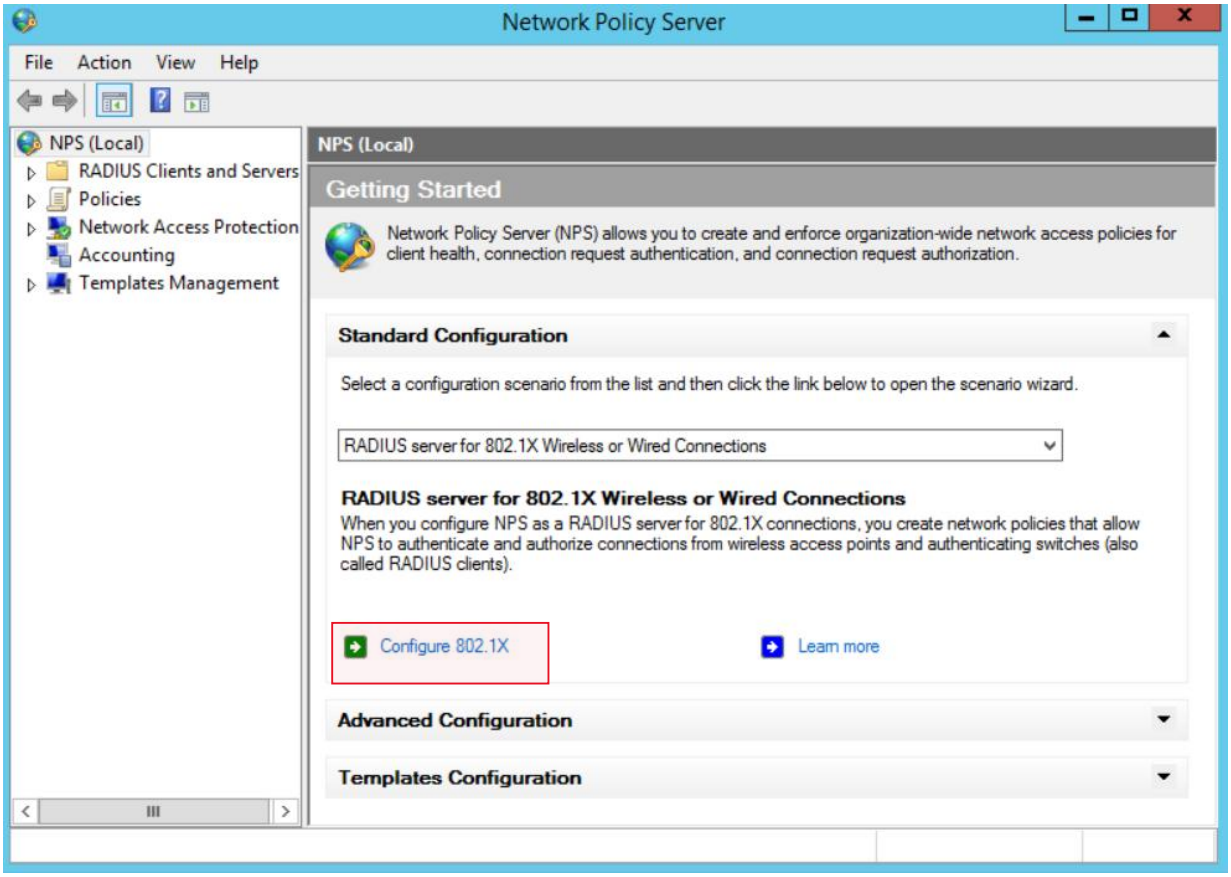
On left side column click on “NAP” (Windows Server 2012). This could be “NPAS” on Windows Server 2016.



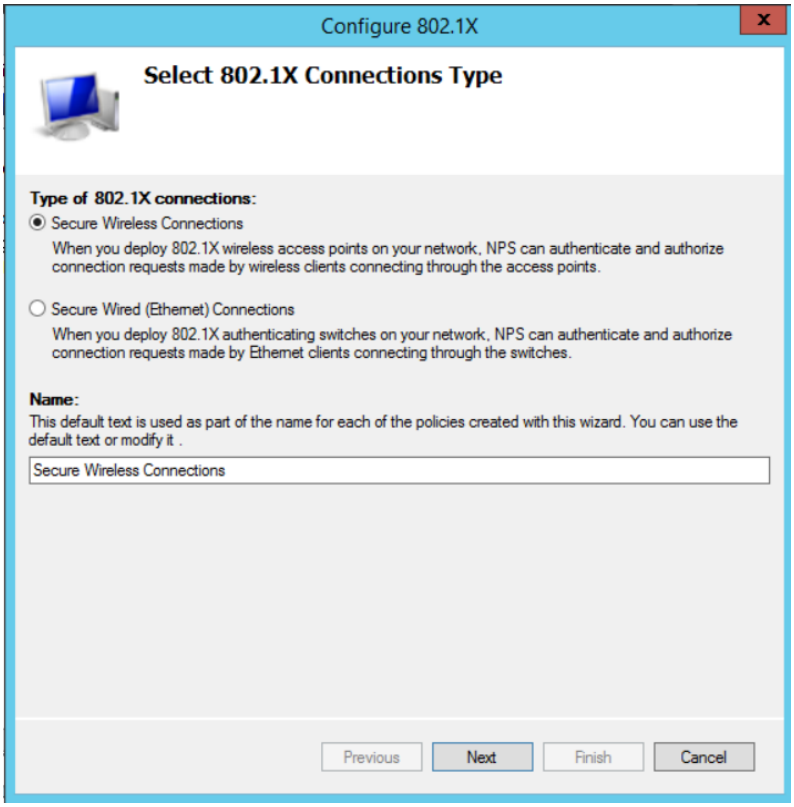
Right-click on Server in “NAP” and click on “Network Policy Server”.



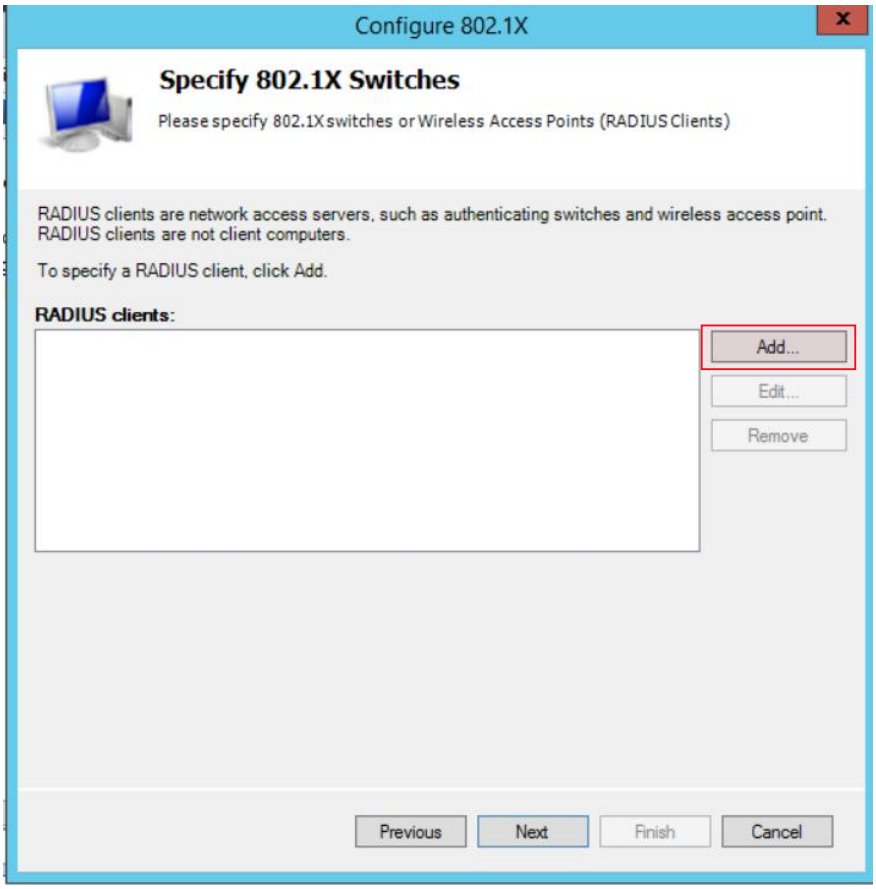
Click under “Standard Configuration” on “NPS (Local)” and select “RADIUS server for 802.1X Wireless or Wired Connections”.



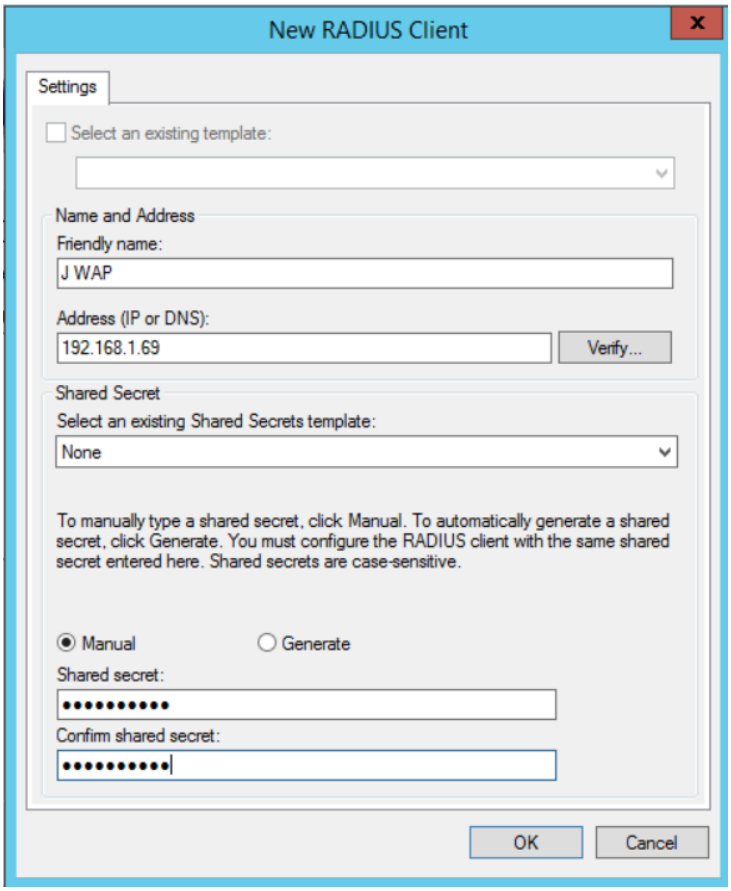
Then click on “Configure 802.1X”.



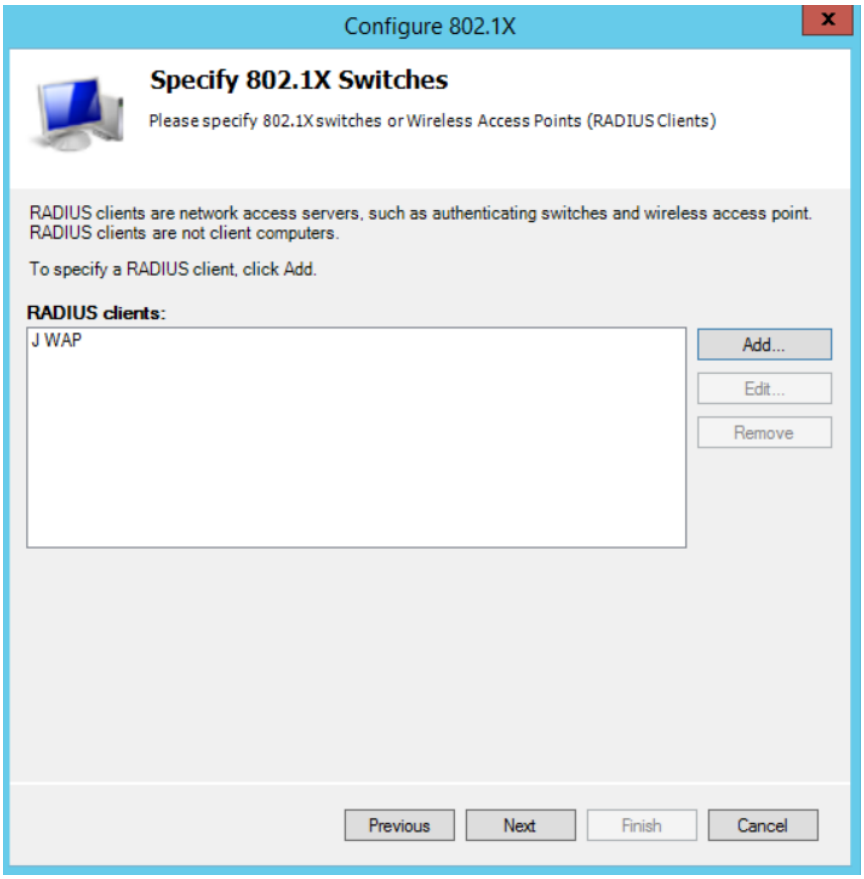
Choose/click on “Secure Wireless Connections” and click “Next”. (Name should fill in automatically)



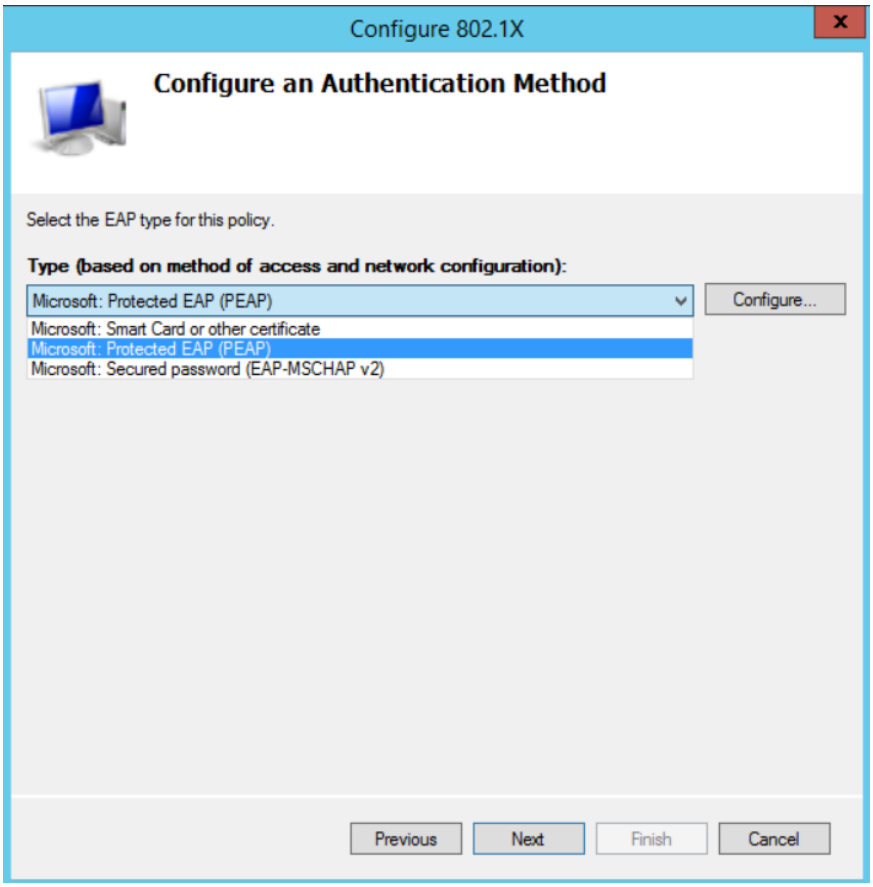
Click on “Add” to add RADIUS clients.



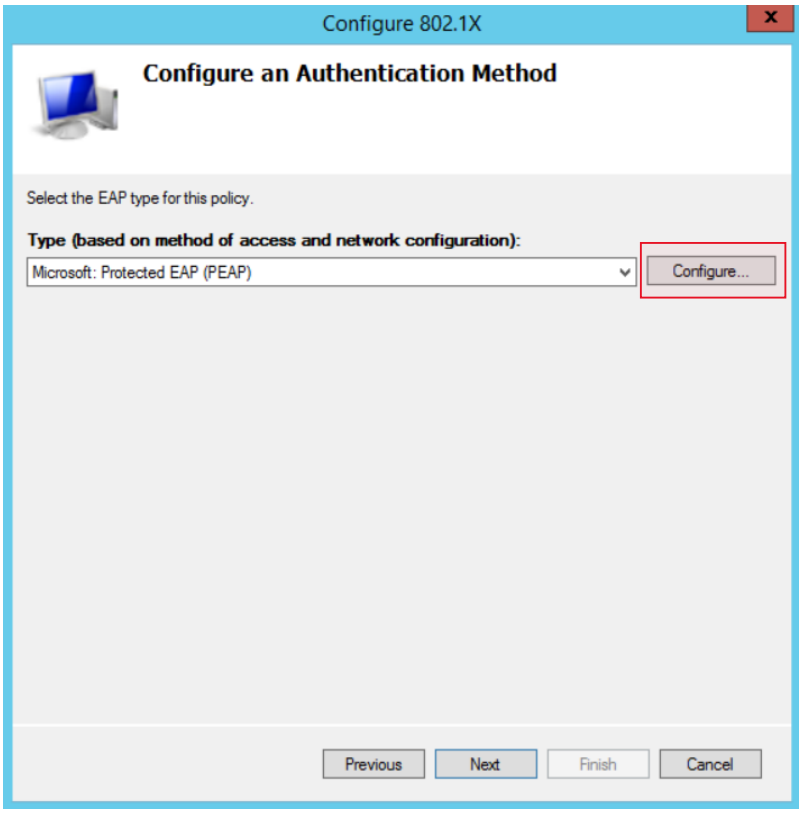
Enter a name and IP address for RADIUS client, create a secret password, and click “OK”.



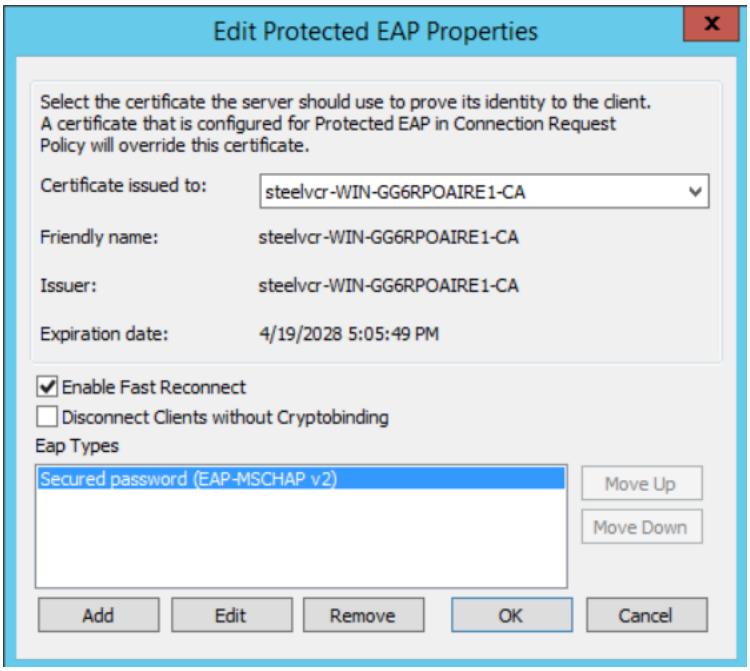
Then click “Next”.



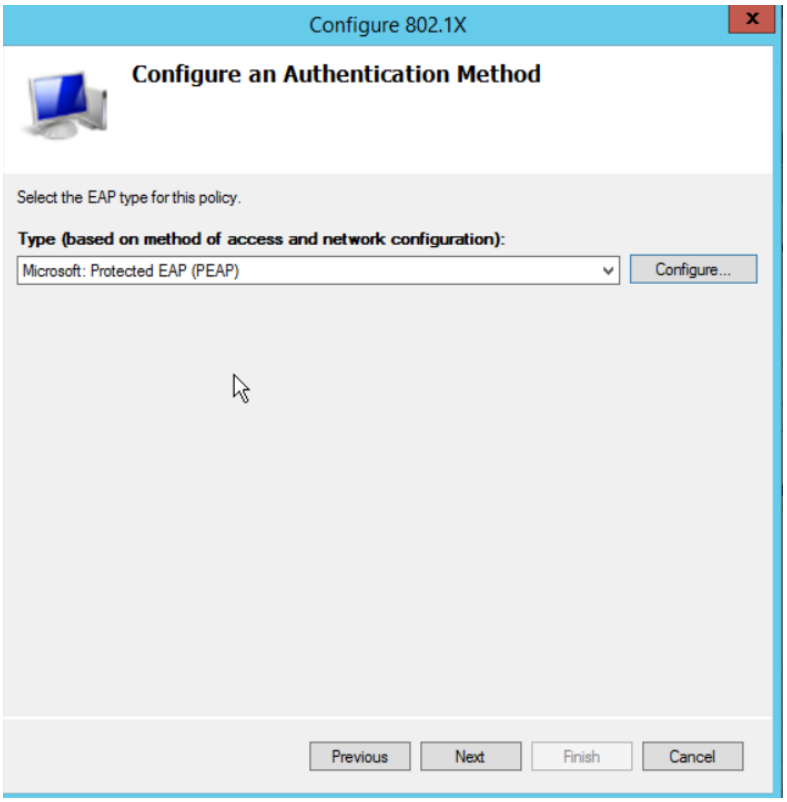
For Type select the option “Microsoft: Protected EAP (**PEAP**)”.



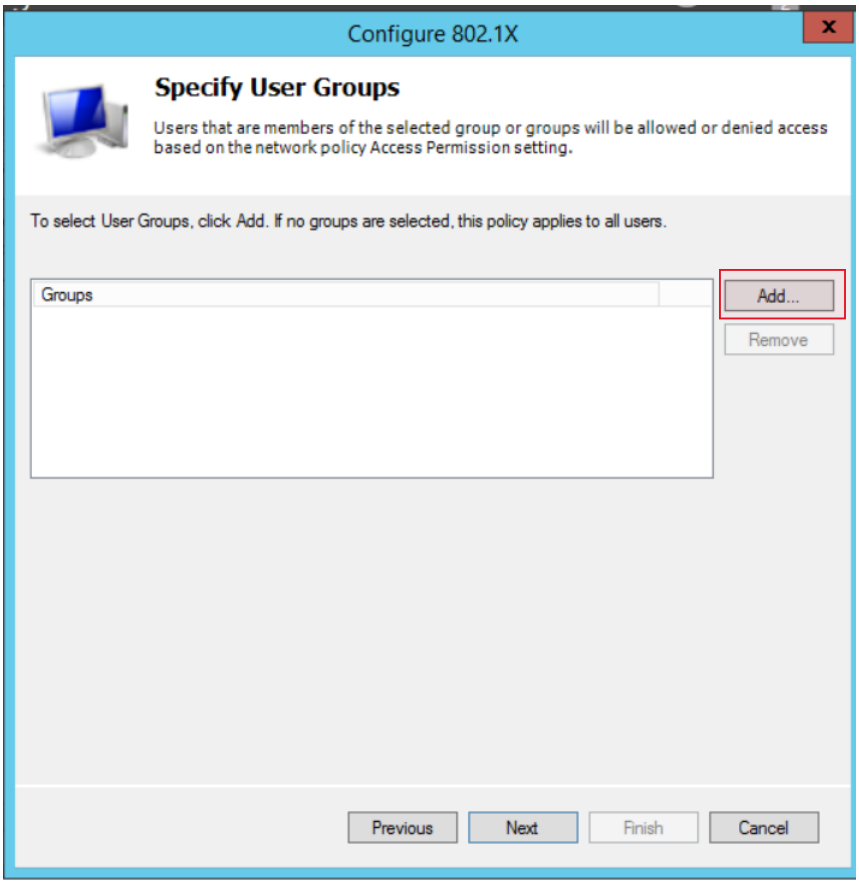
Click on “Configure…”



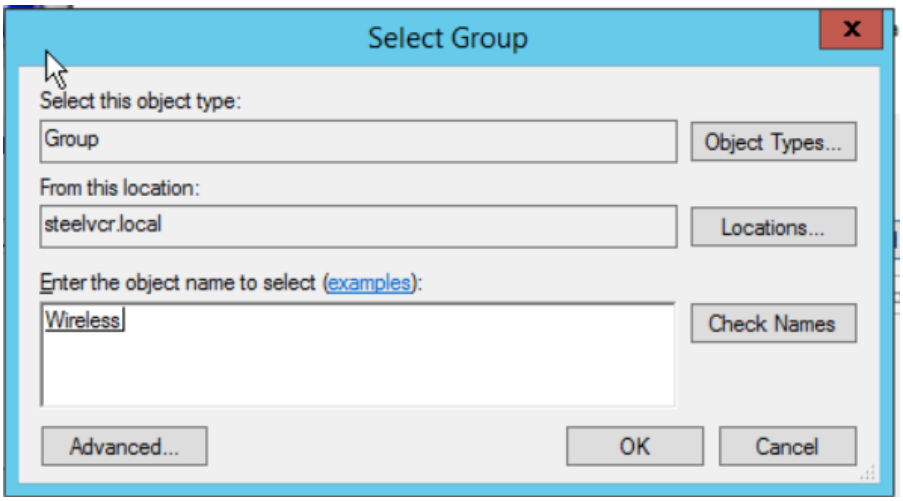
Click “OK” and everything here should appear automatically.



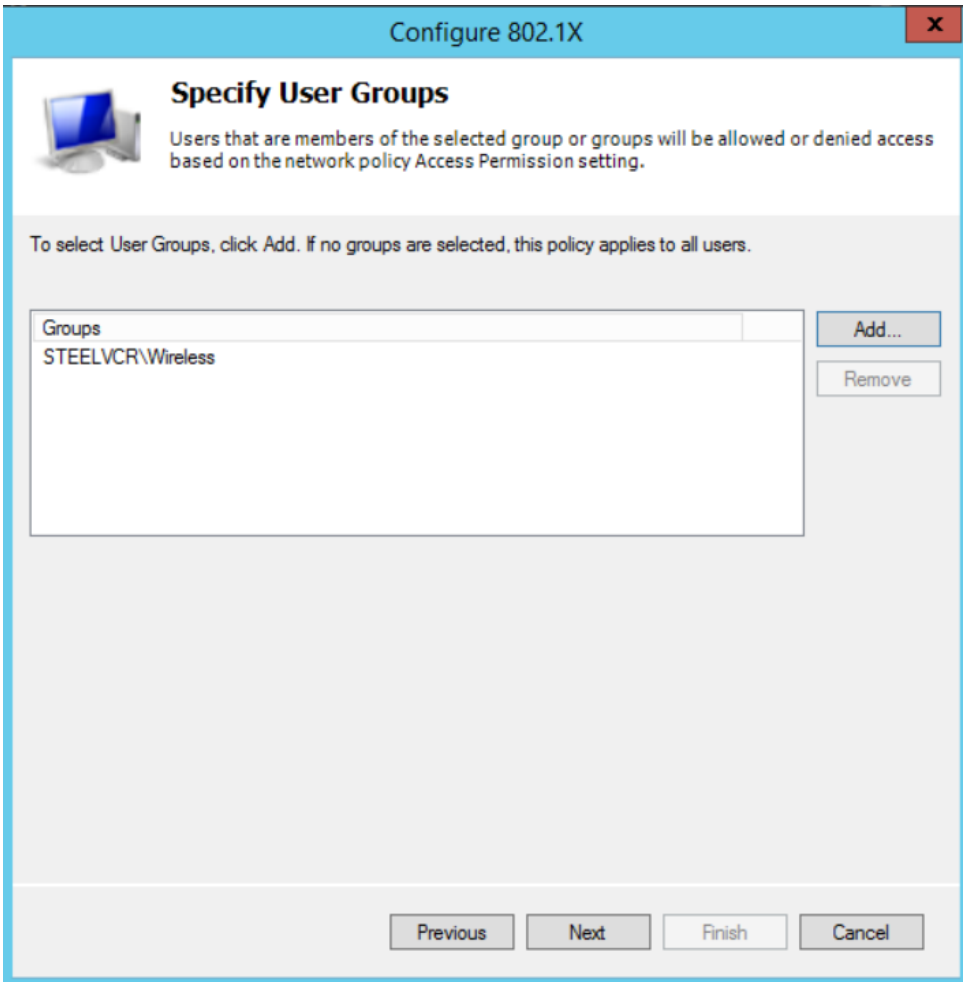
Click “Next”.



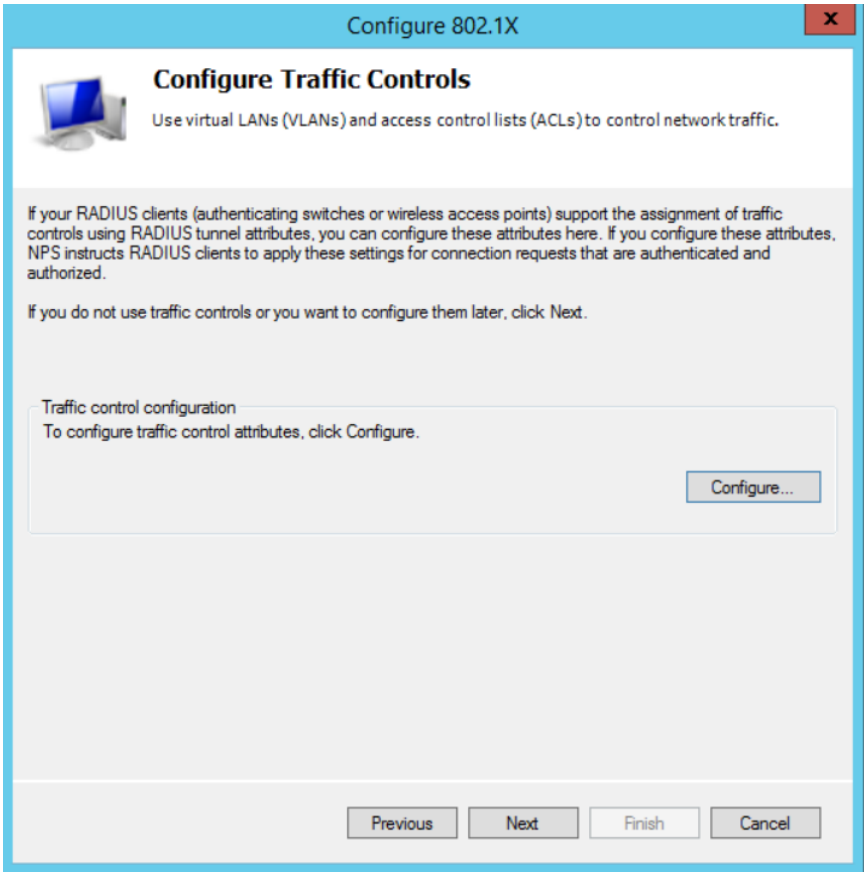
Click on “Add” to add groups.



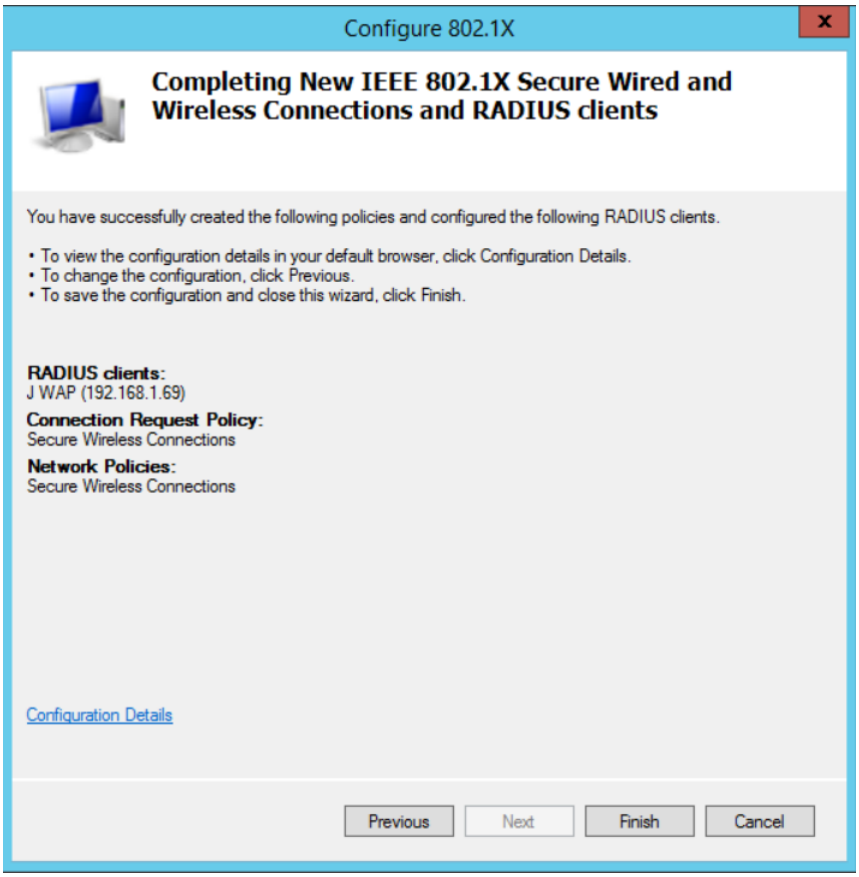
Type in beginning of group/object and click “Check Names” and then click “OK”.



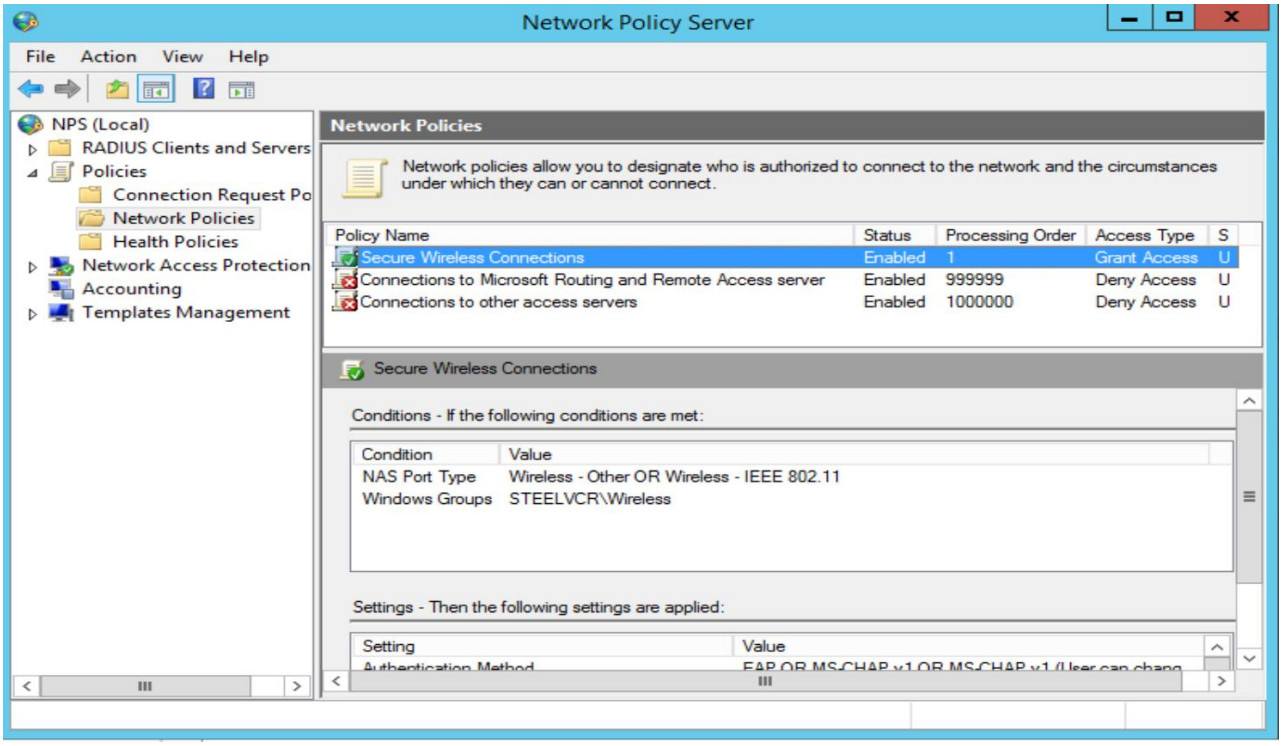
Click “Next”.



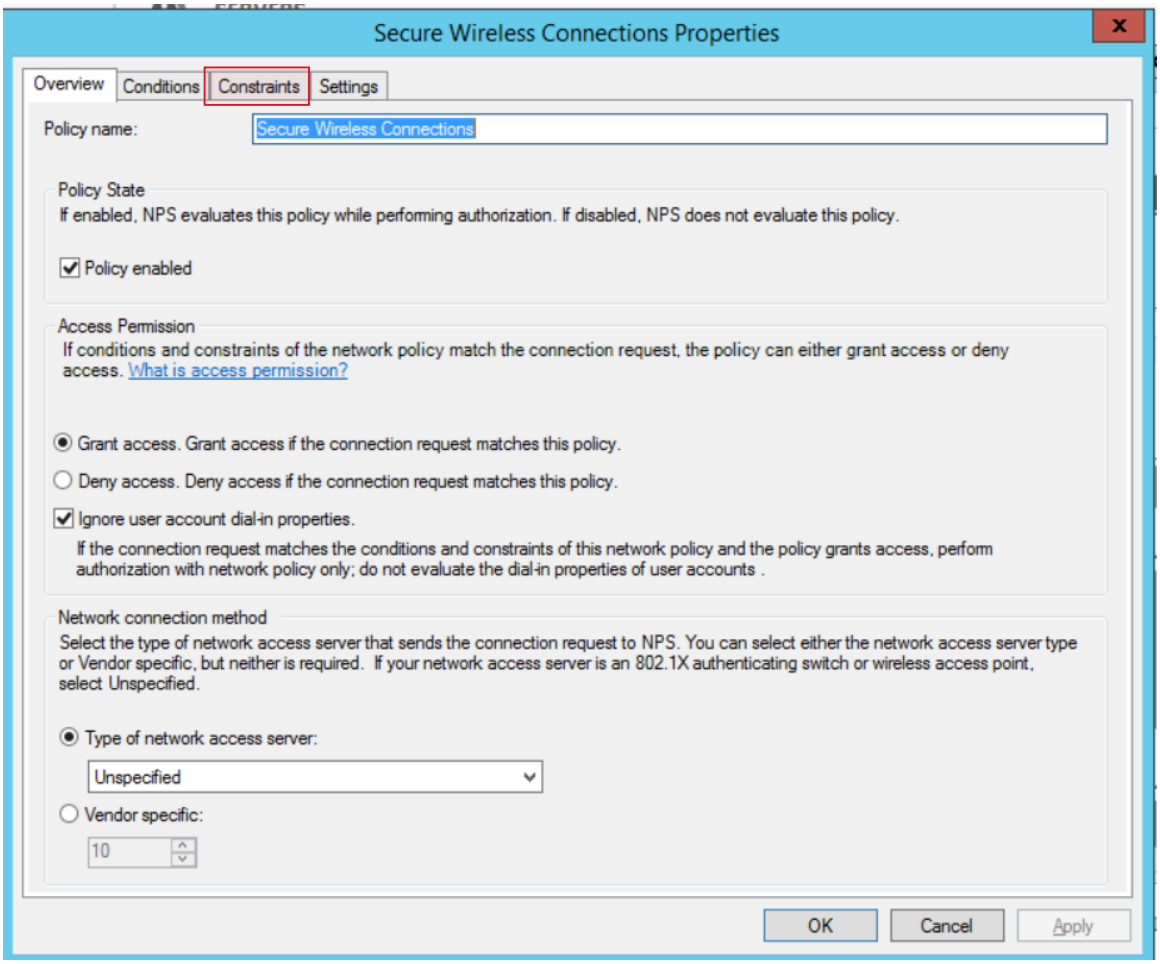
Don't have to configure traffic control attributes so click "Next".



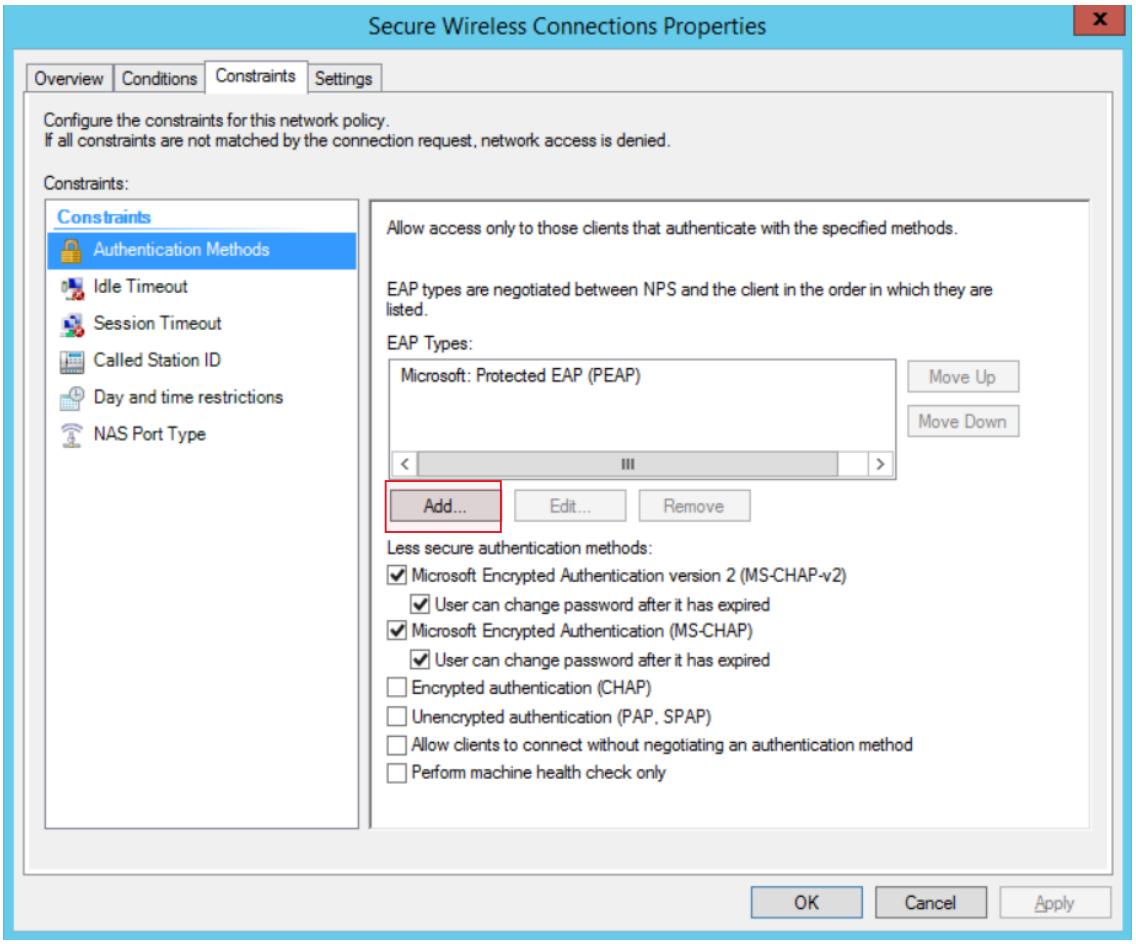
Click "Finish".



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

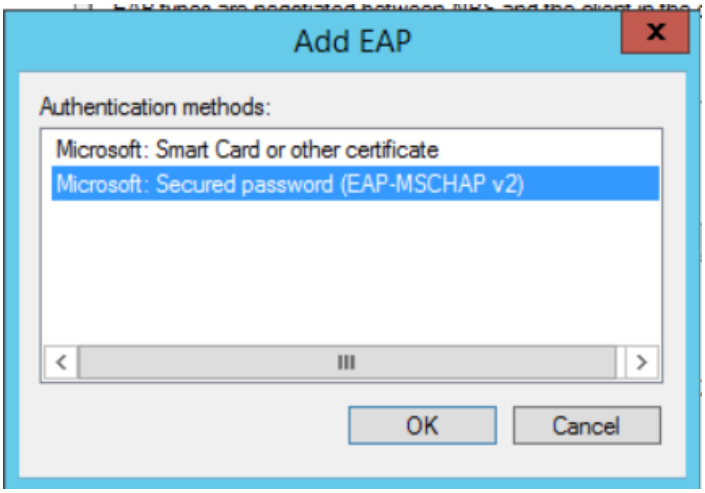


Click on “Constraints”.

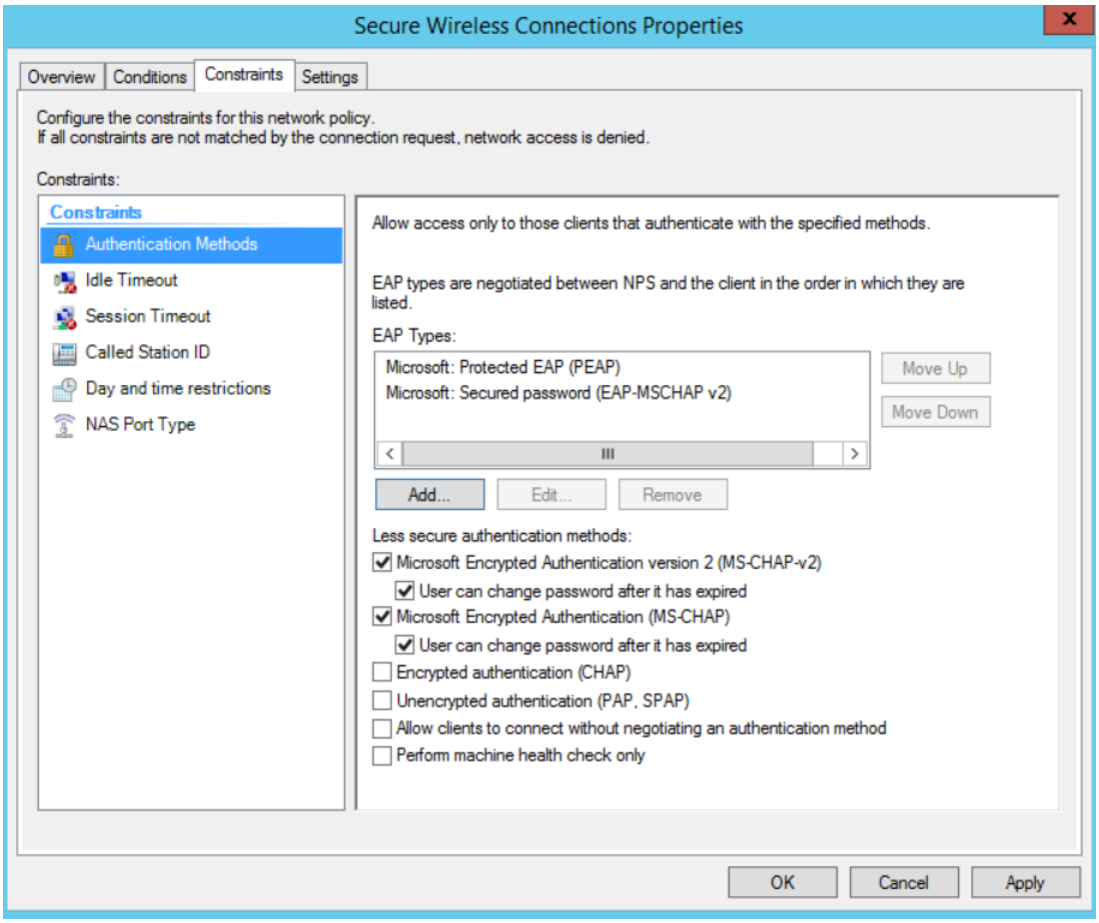


Keep every checked that is checked in automatically as shown above.

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

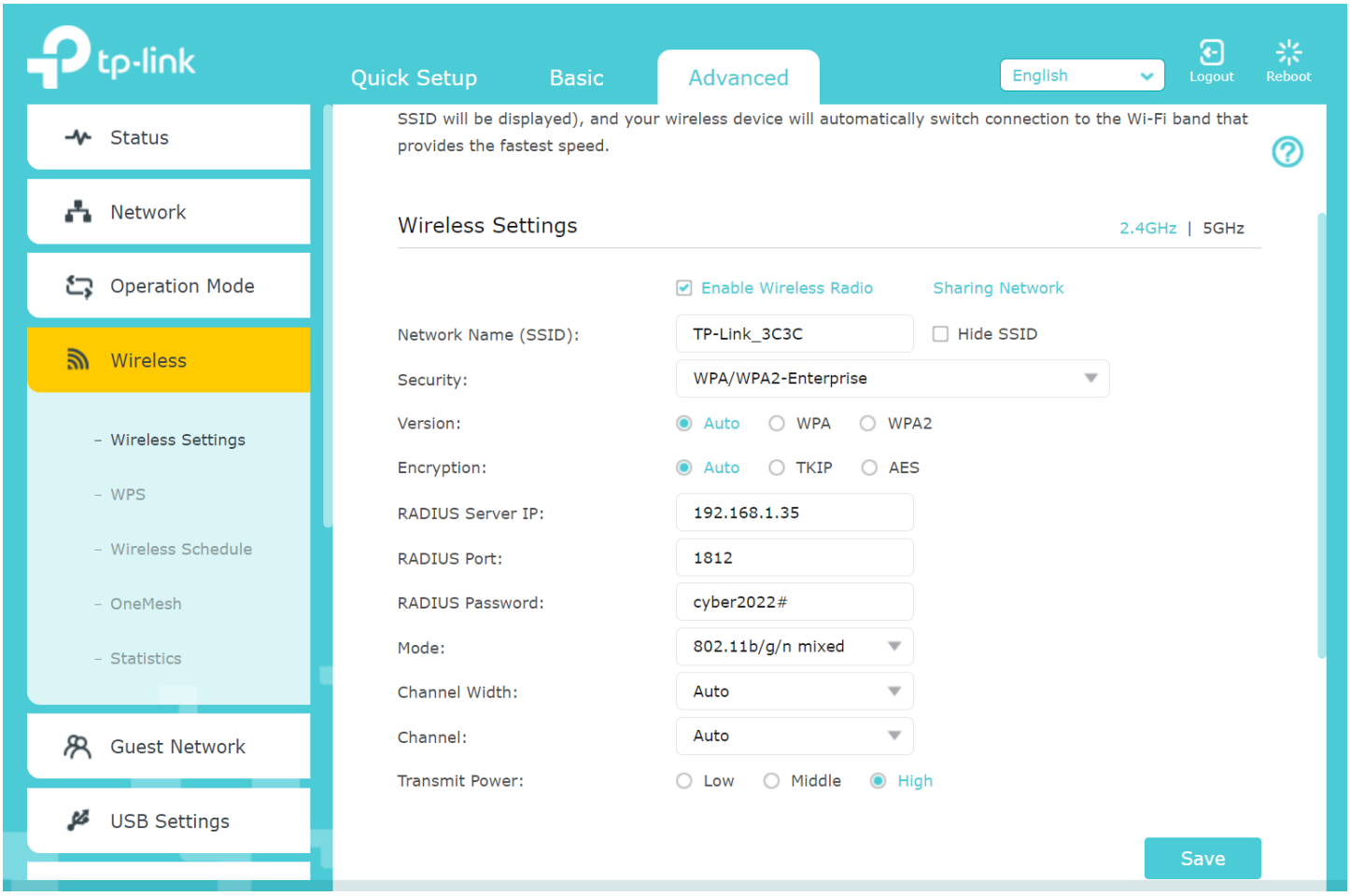


Click “Microsoft: Secured password (**EAP-MSCHAP v2**)” and then click “OK”.



The new EAP type has been added.

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



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.

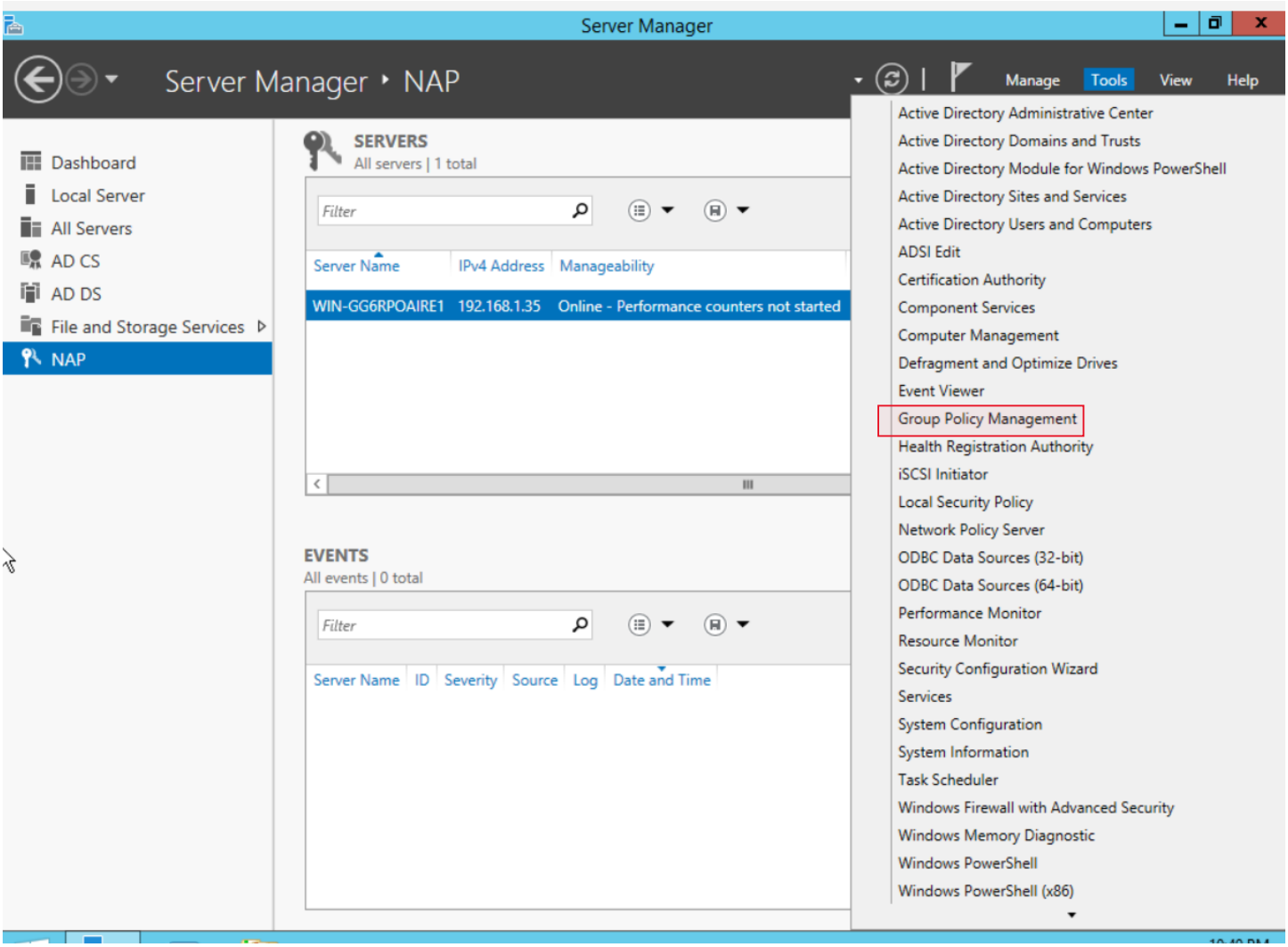
Then, enter in the IP address of RADIUS server located on Windows Server.

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

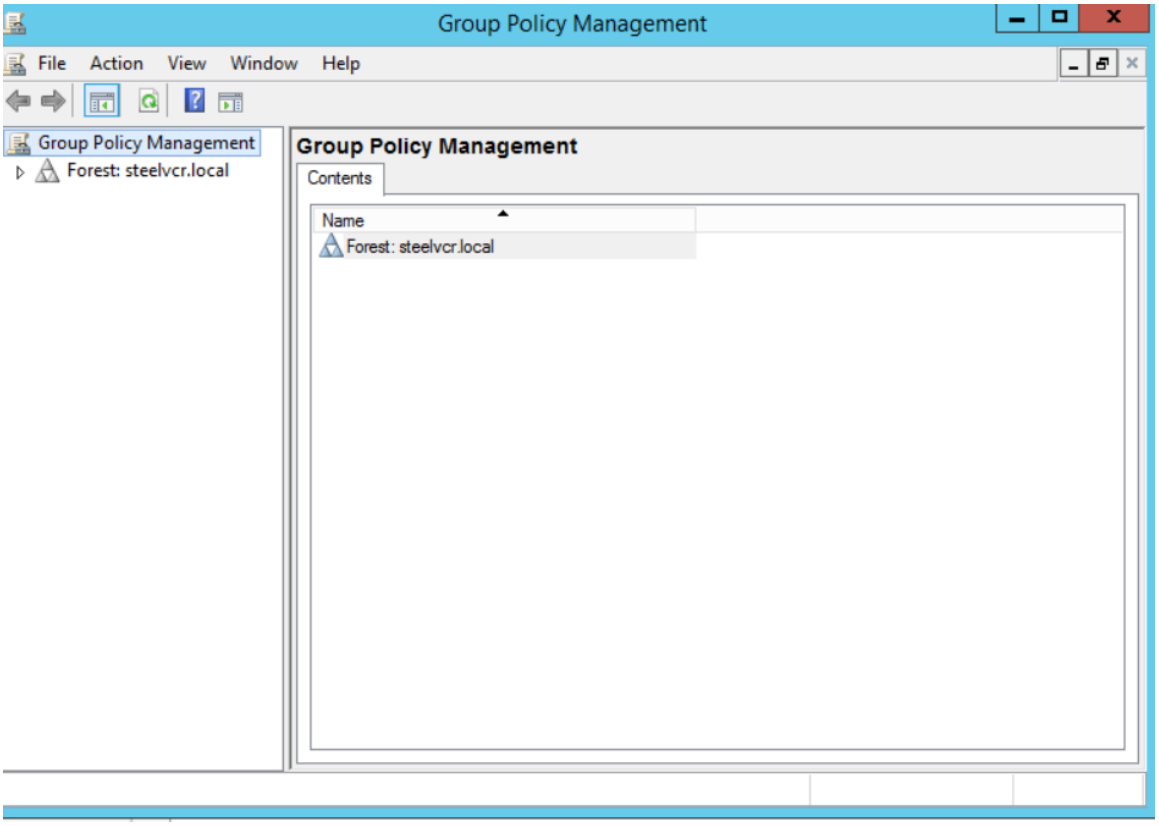
Click save, reboot, and logout.

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

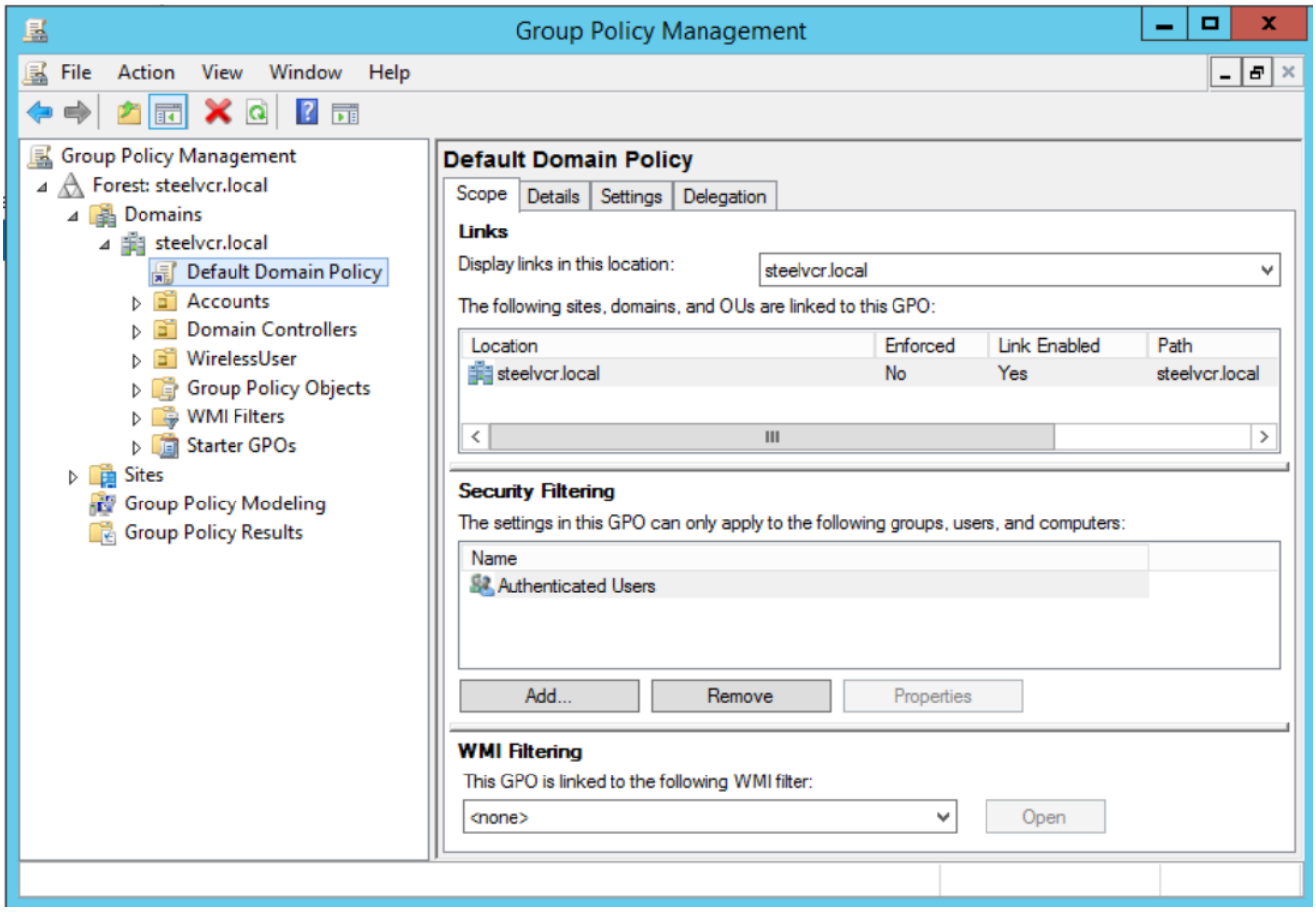
NOTE: make sure you are on same network (RADIUS client and server)



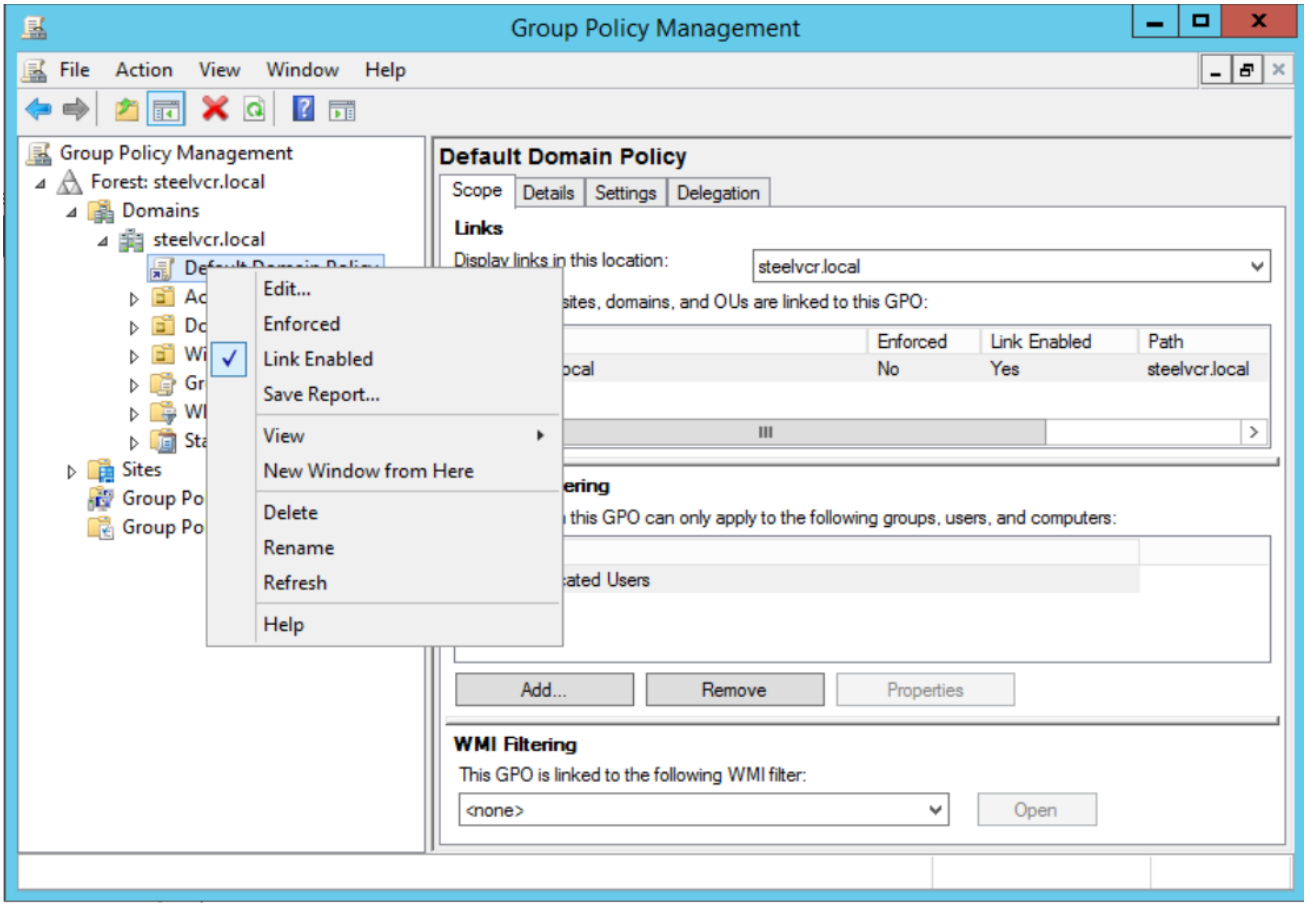
Within Server Manager click on “NAP”, then click “Tool” at the top right menu and select “Group Policy Management”.



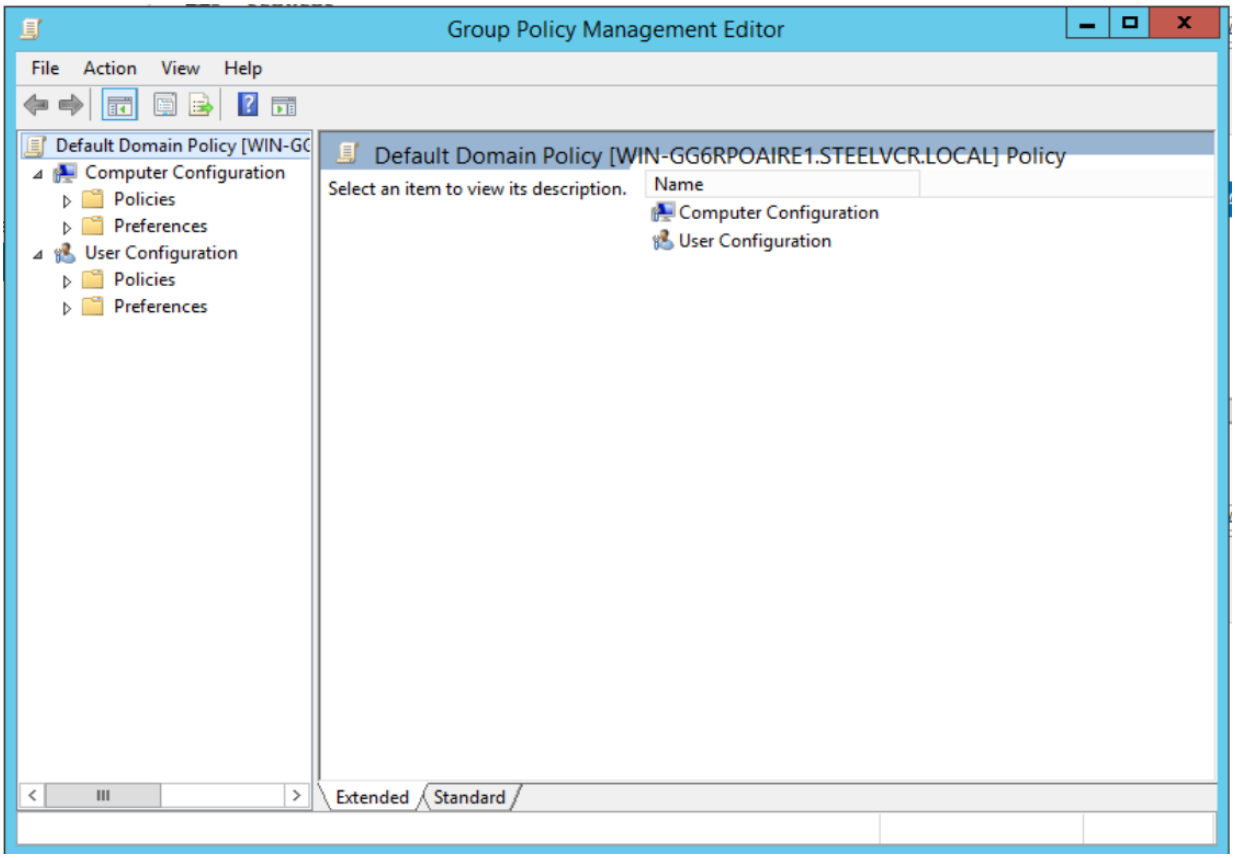
Click on first drop down “Forest:”



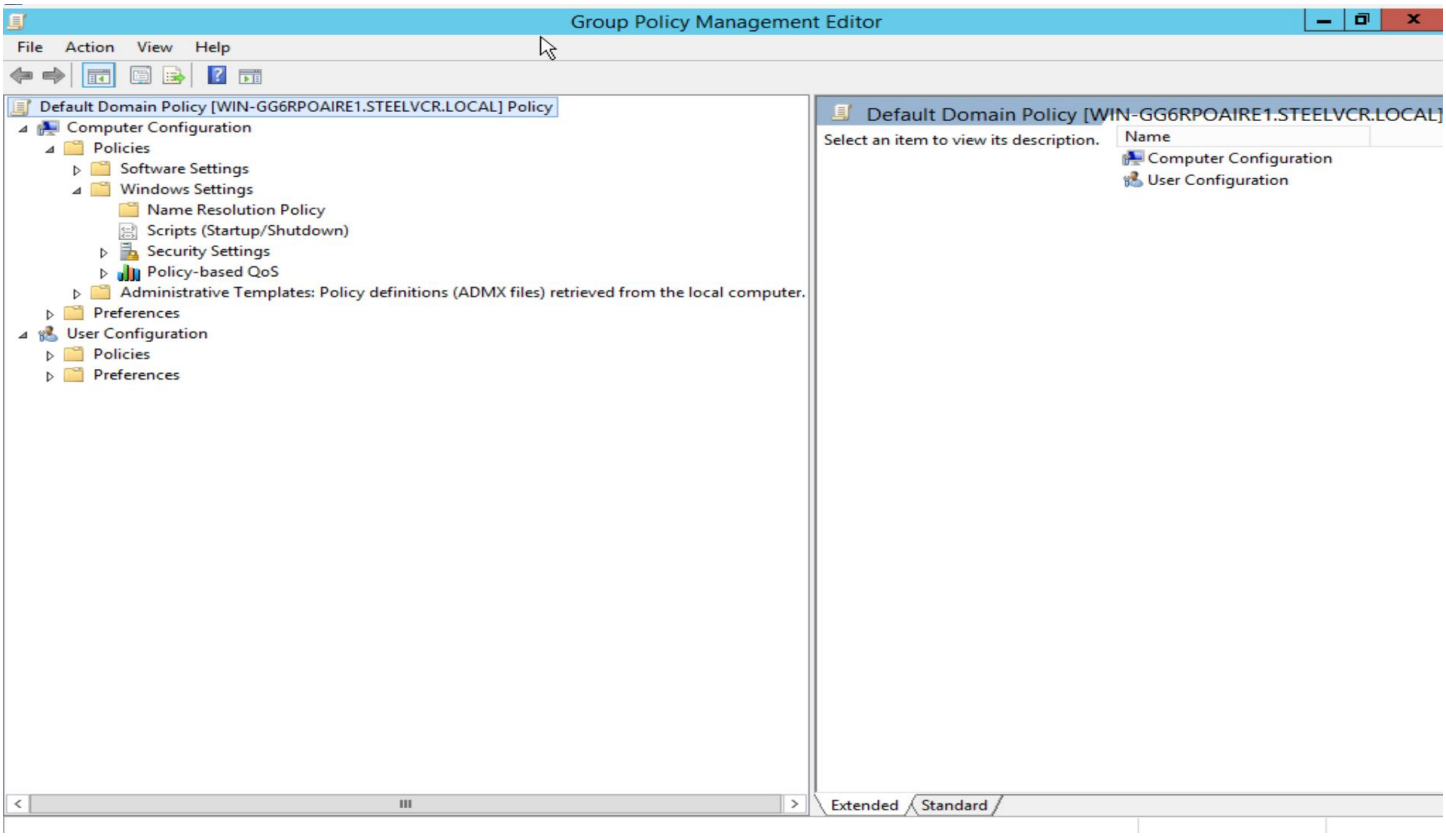
Click on “Domains” dropdown menu, then click your root domain name “steelvcr.local”, and then click on “Default Domain Policy”.



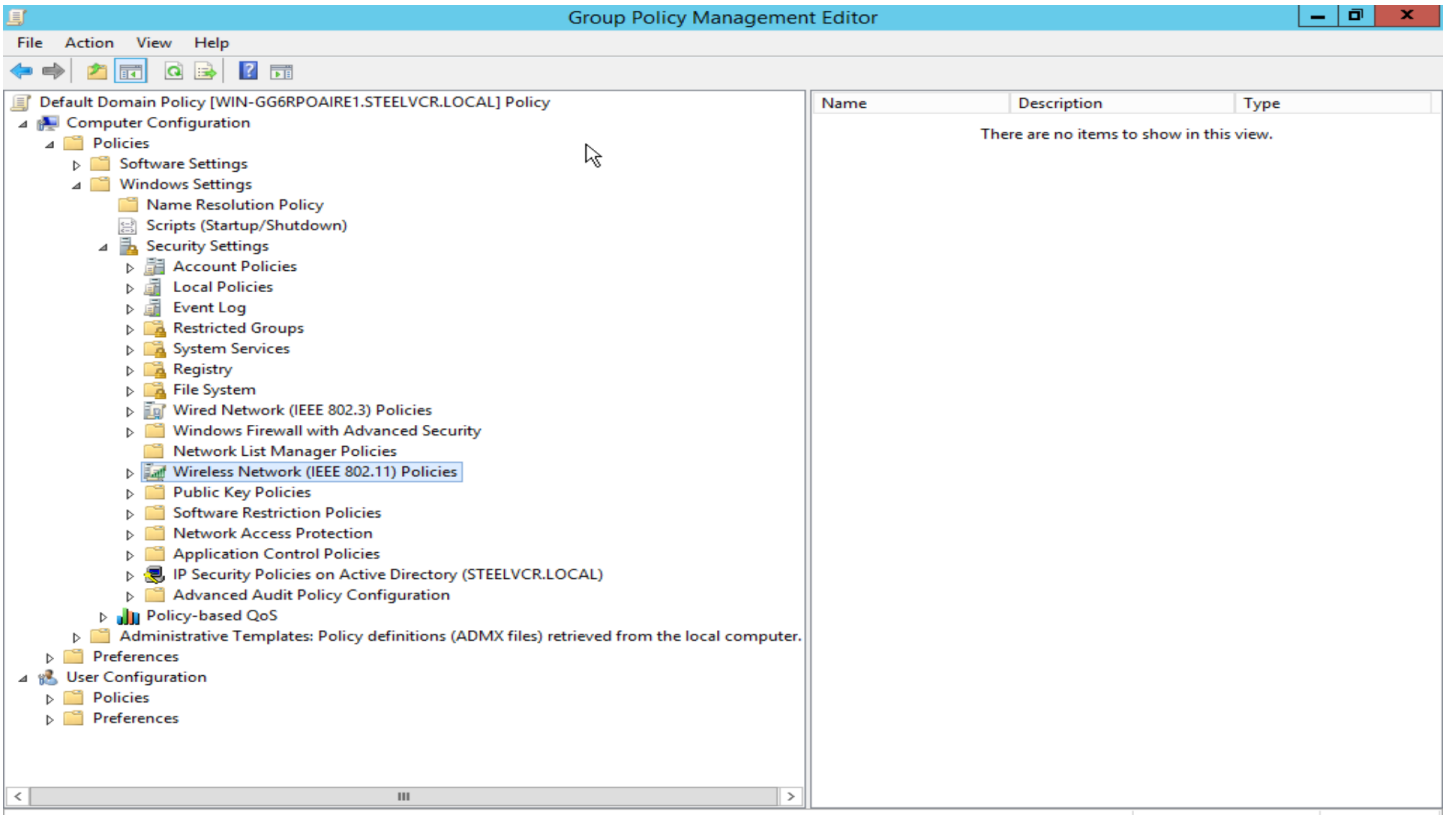
Right-click on “Default Domain Policy” and select “Edit”.



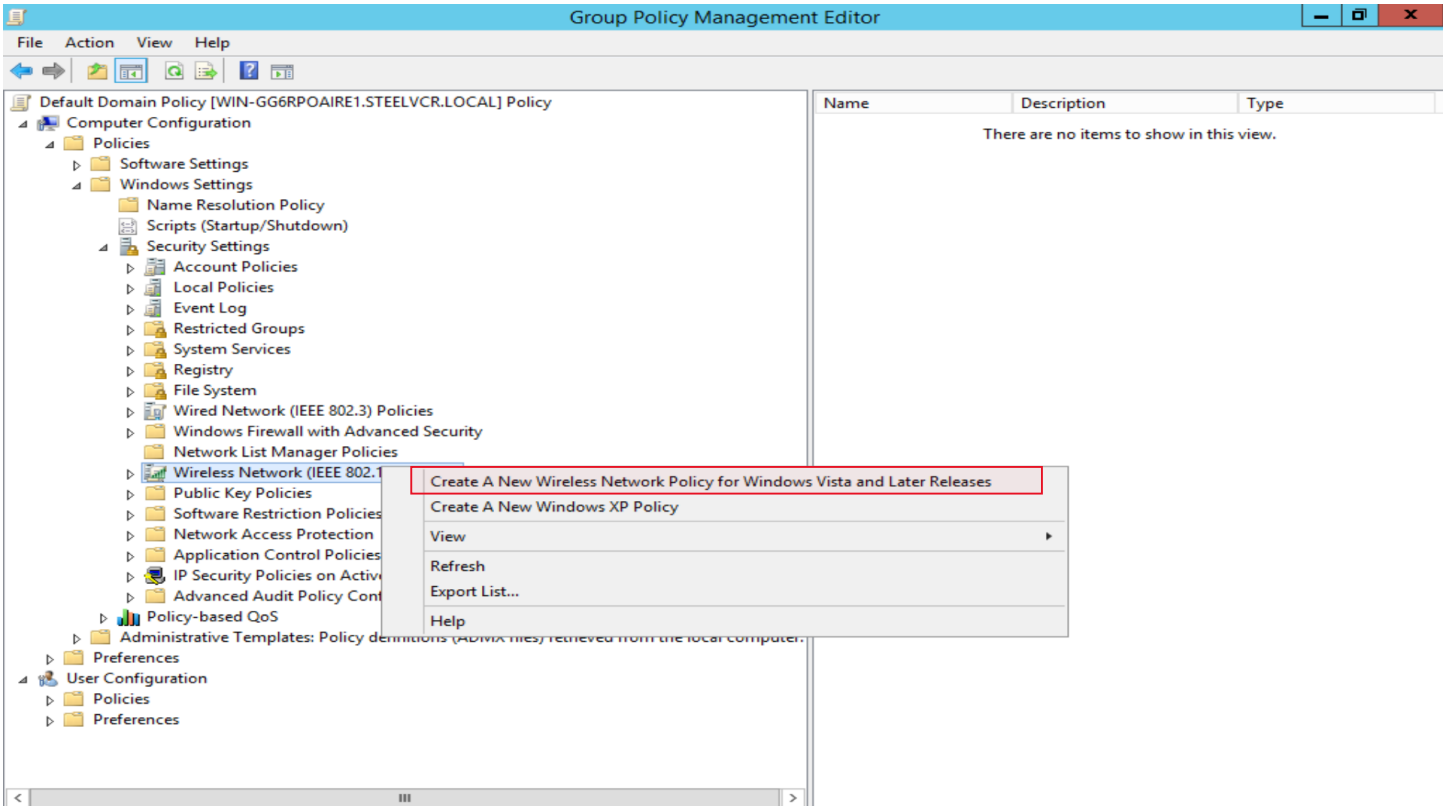
Click on “Policies”.



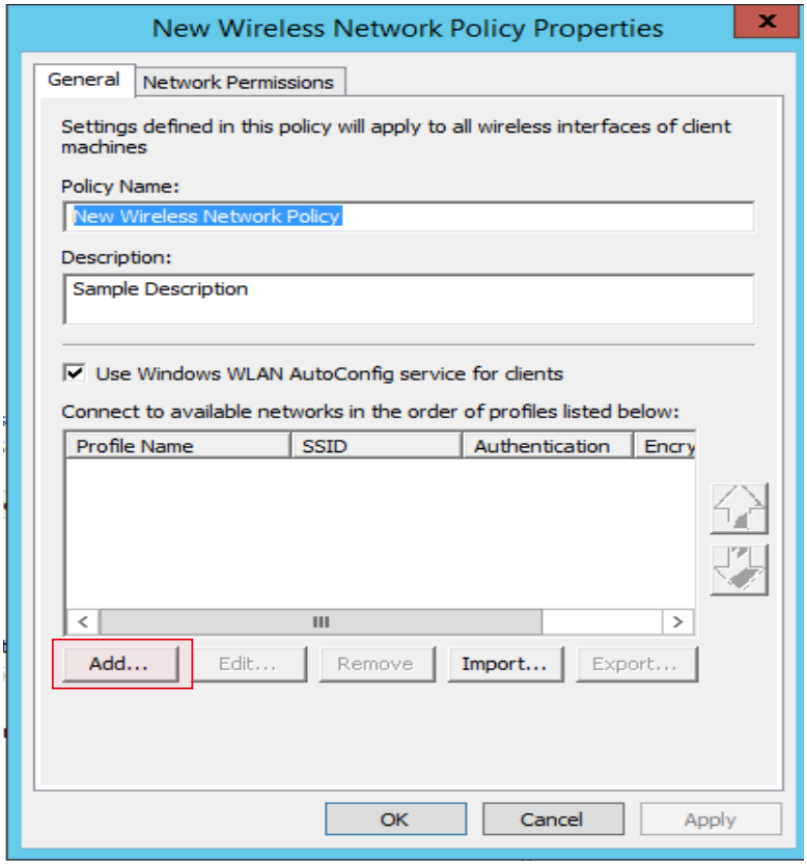
Click on “Windows Settings” and then click “Security Settings”.



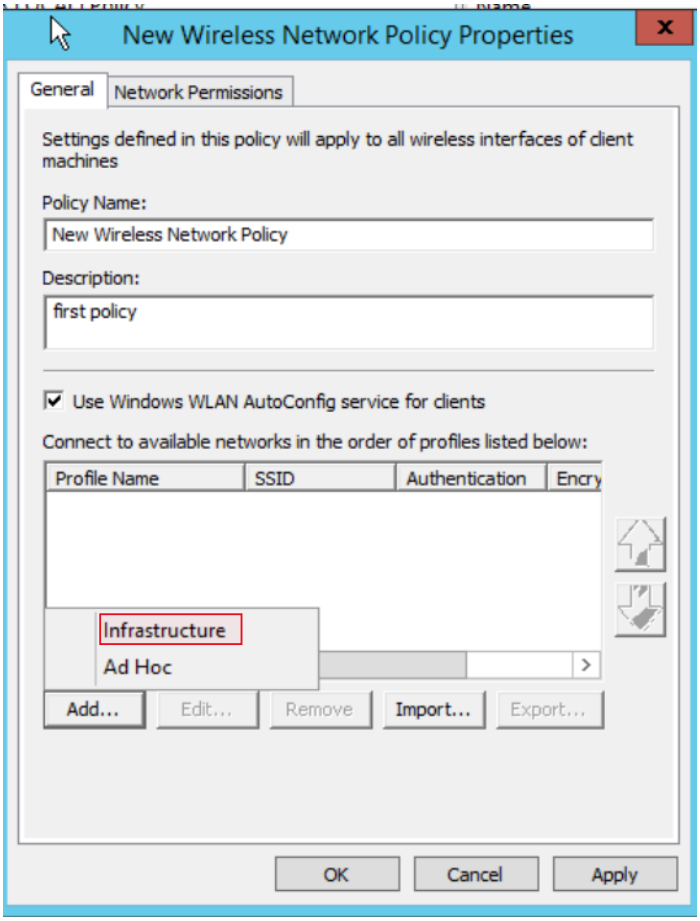
Click on “Wireless Network (IEEE 802.11) Policies”.



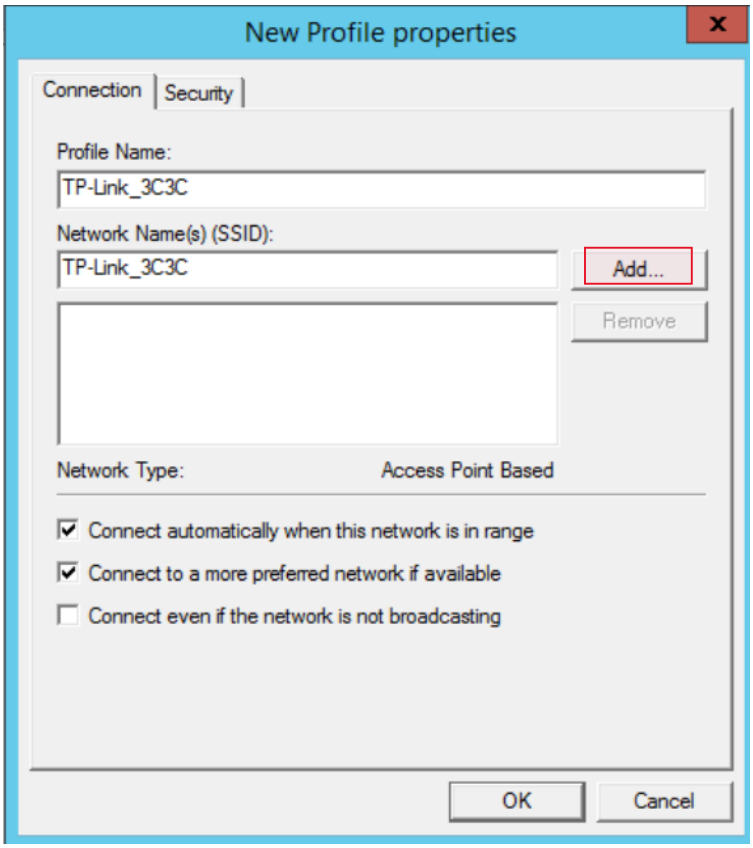
Right-click on that and select “Create a New Wireless Network Policy for Windows Vista and Later Releases”.



Click on “Add”.



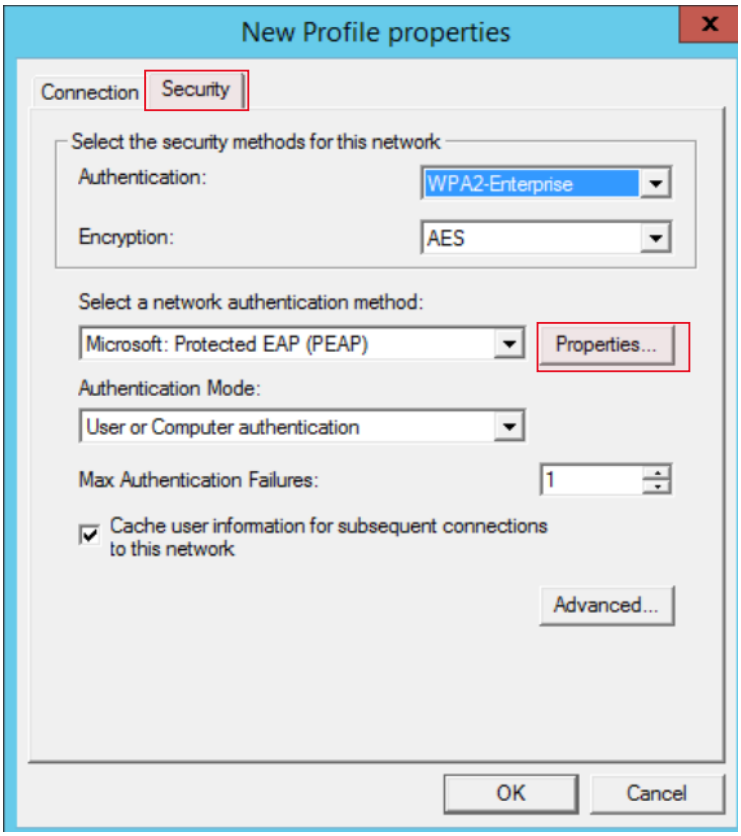
Click on “Infrastructure”.



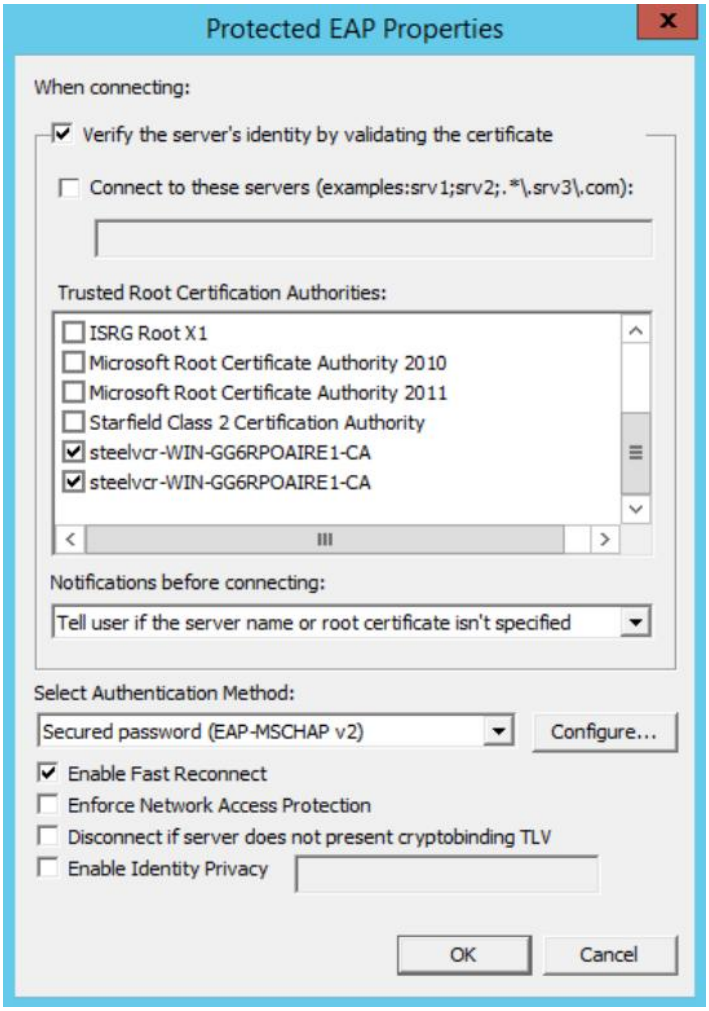
Type in profile name, and SSID for access point/RADIUS client then click “Add…”

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

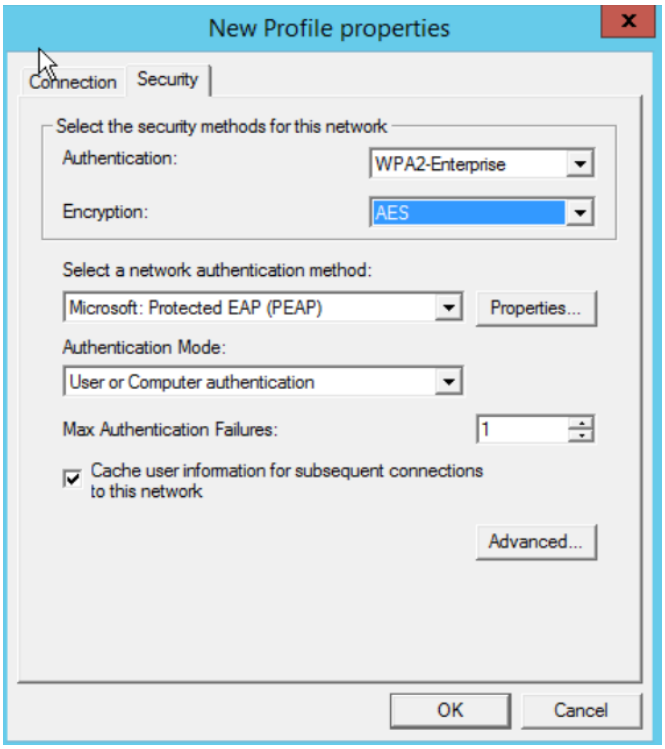
Click on “Security” at the top right.



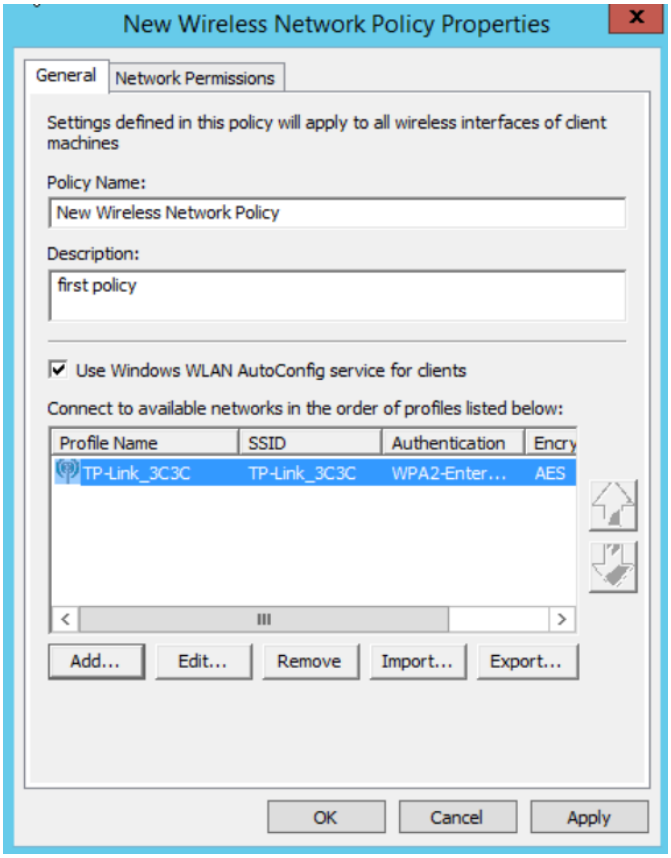
Click on “Properties”.



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

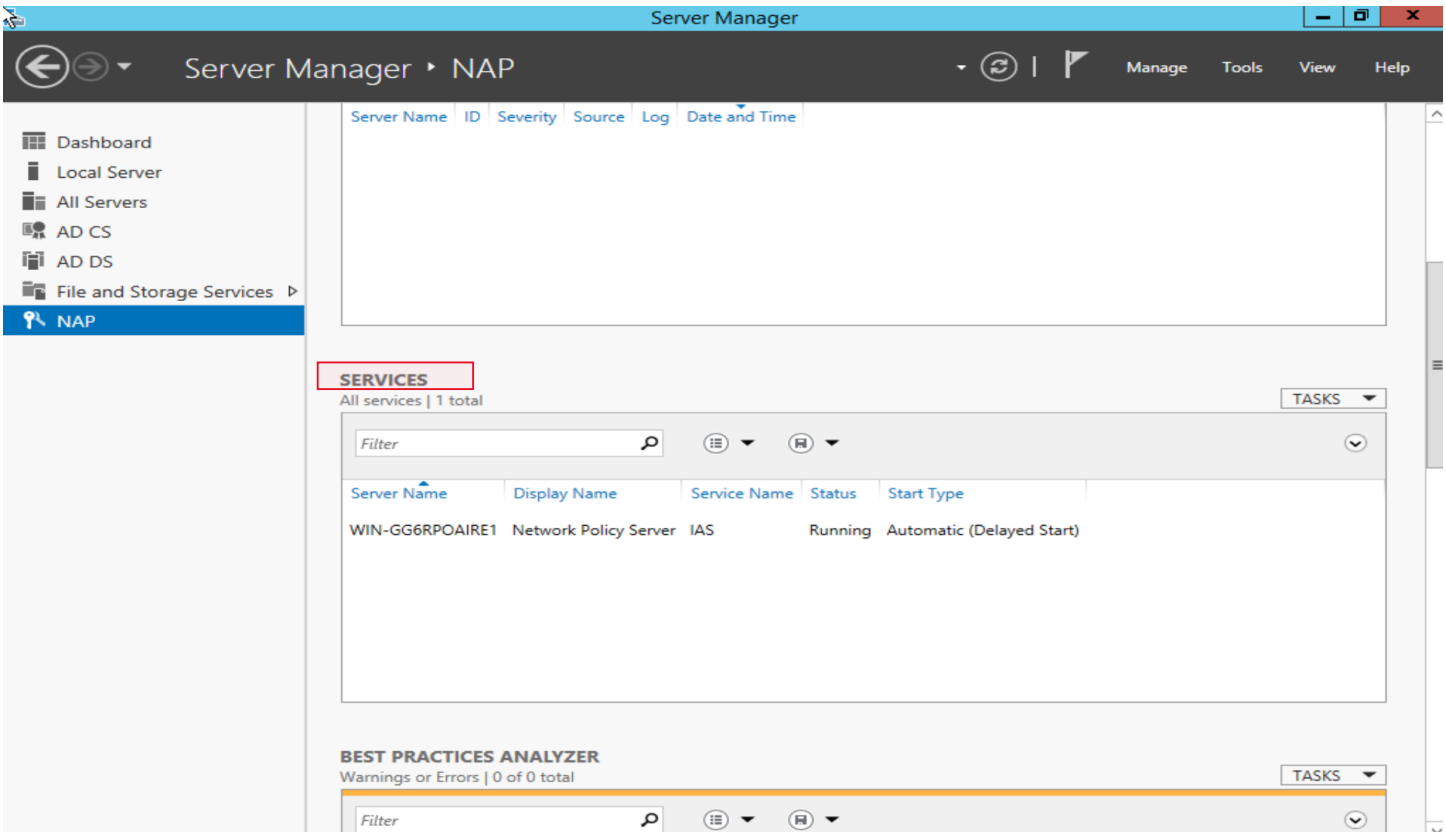


Click “OK”.

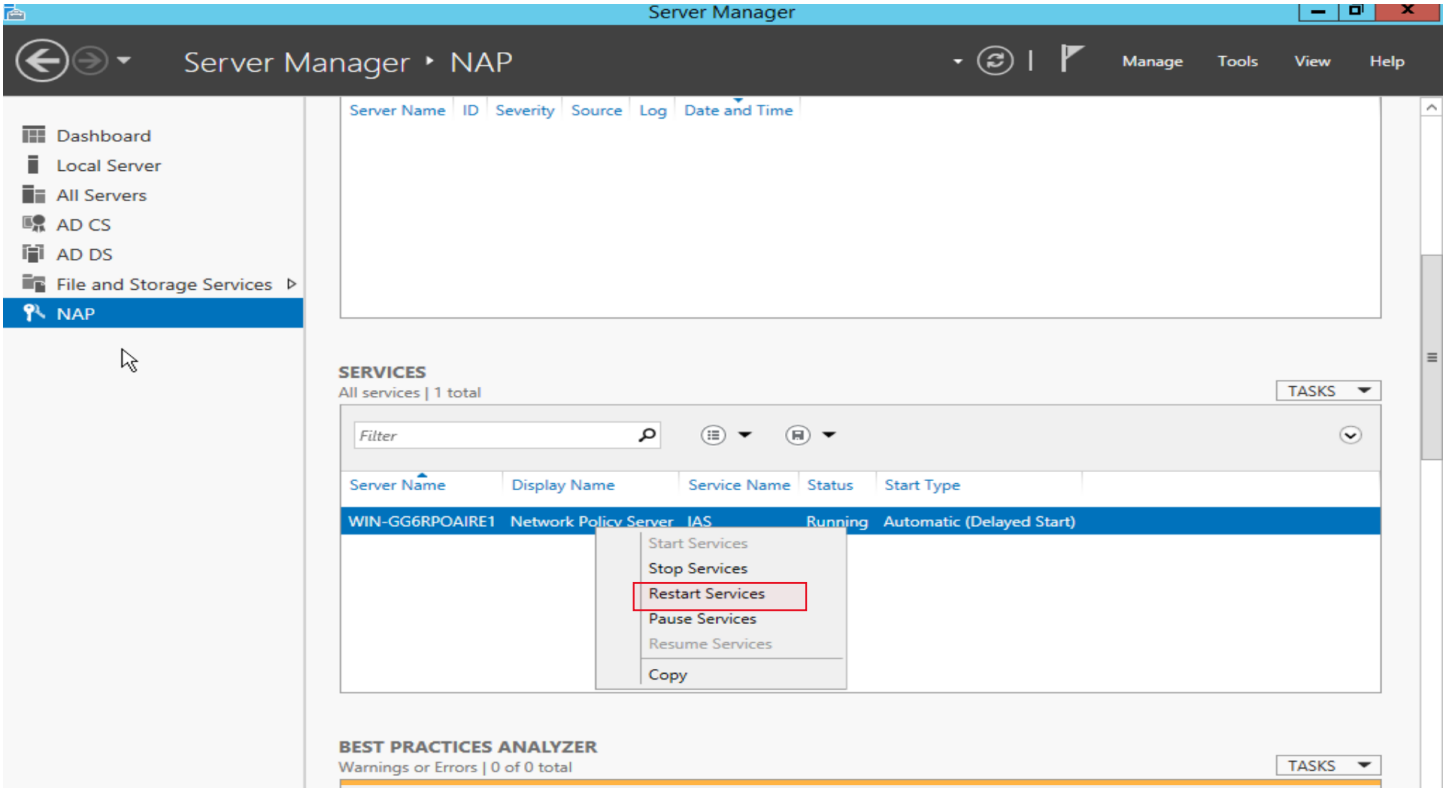


Click “Apply” and then “OK”.

Exit out of any opens tabs besides Server Manager.



Scroll down until you see “SERVICES”.



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.