Secure Access:
Demo Server Configuration

HOW TO GUIDE

December 2012

Revision 0.01

Table of Contents

1. Overview

1.1 Components

1.2 Wizard

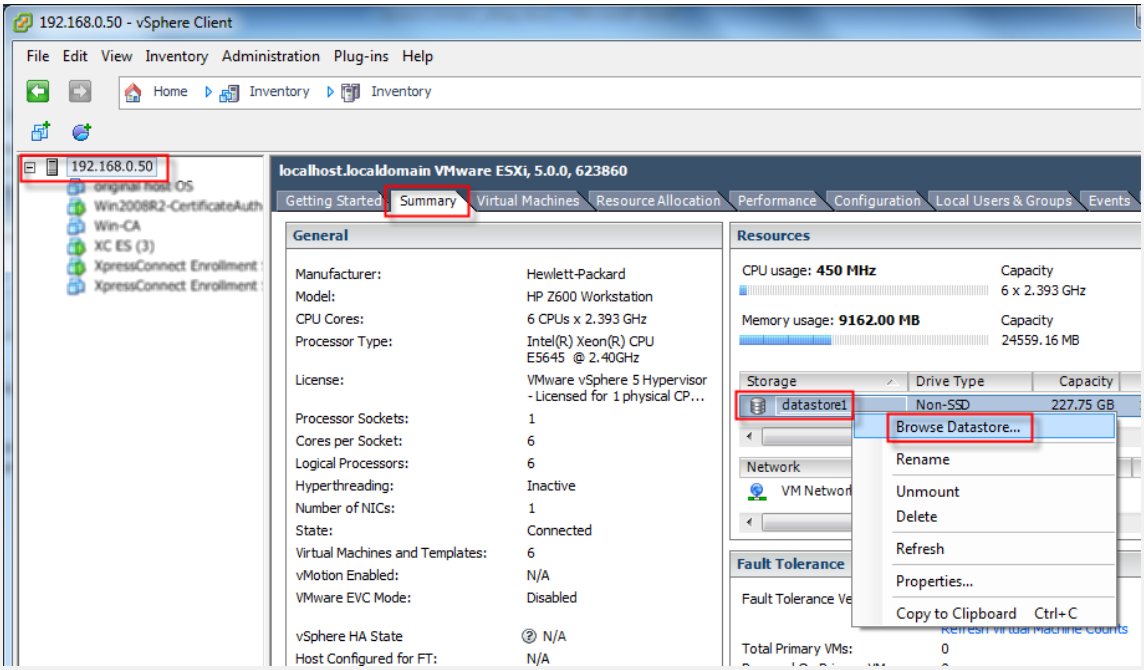
1.3 Enrollment Server

2. Demo Configuration

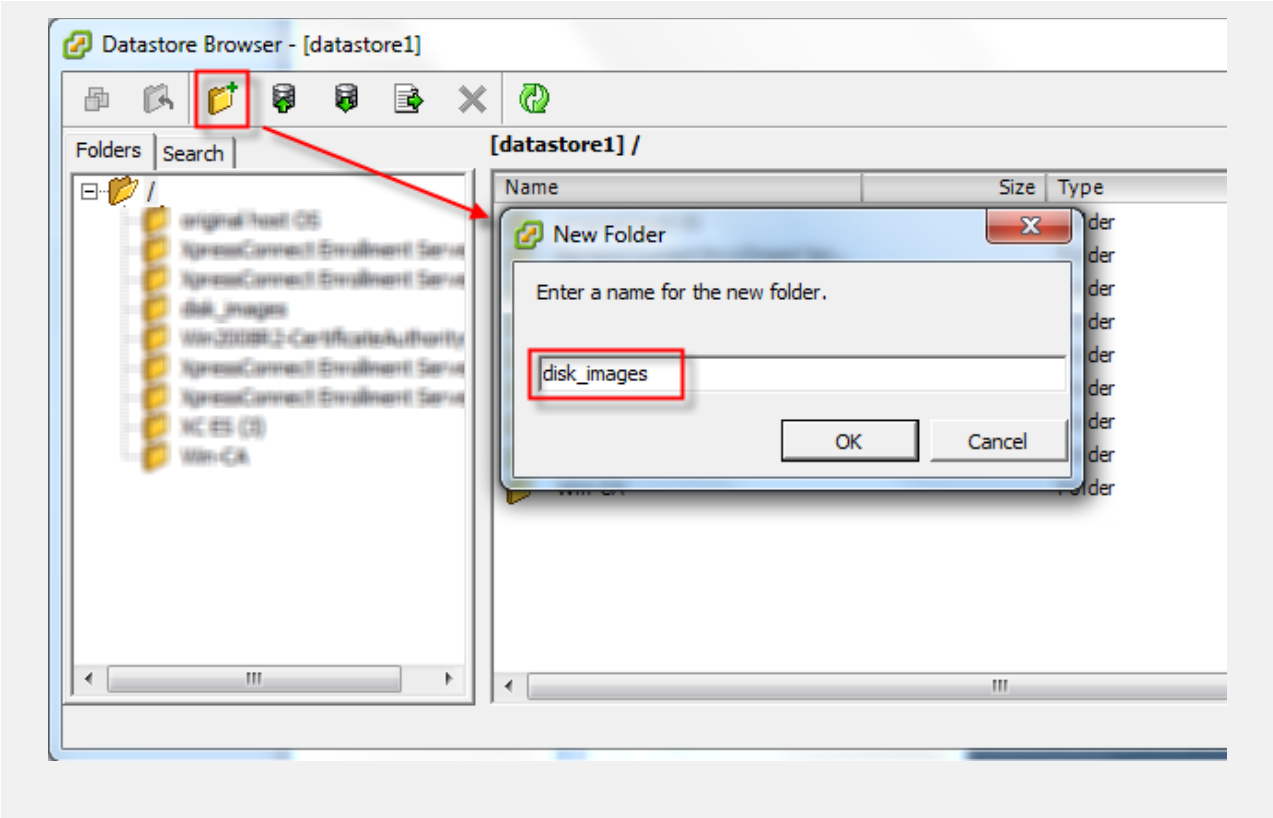
2.1 Initial ESXi Setup

One convenient tool for setting up an ESXi server is to upload any operating system CD/DVD images for VMs to the datastore so they can be mounted as virtual drives. This makes it easy to setup new VMs, reload VMs, or add services from the setup disks. These steps will show how to create a repository for operating system disk images.

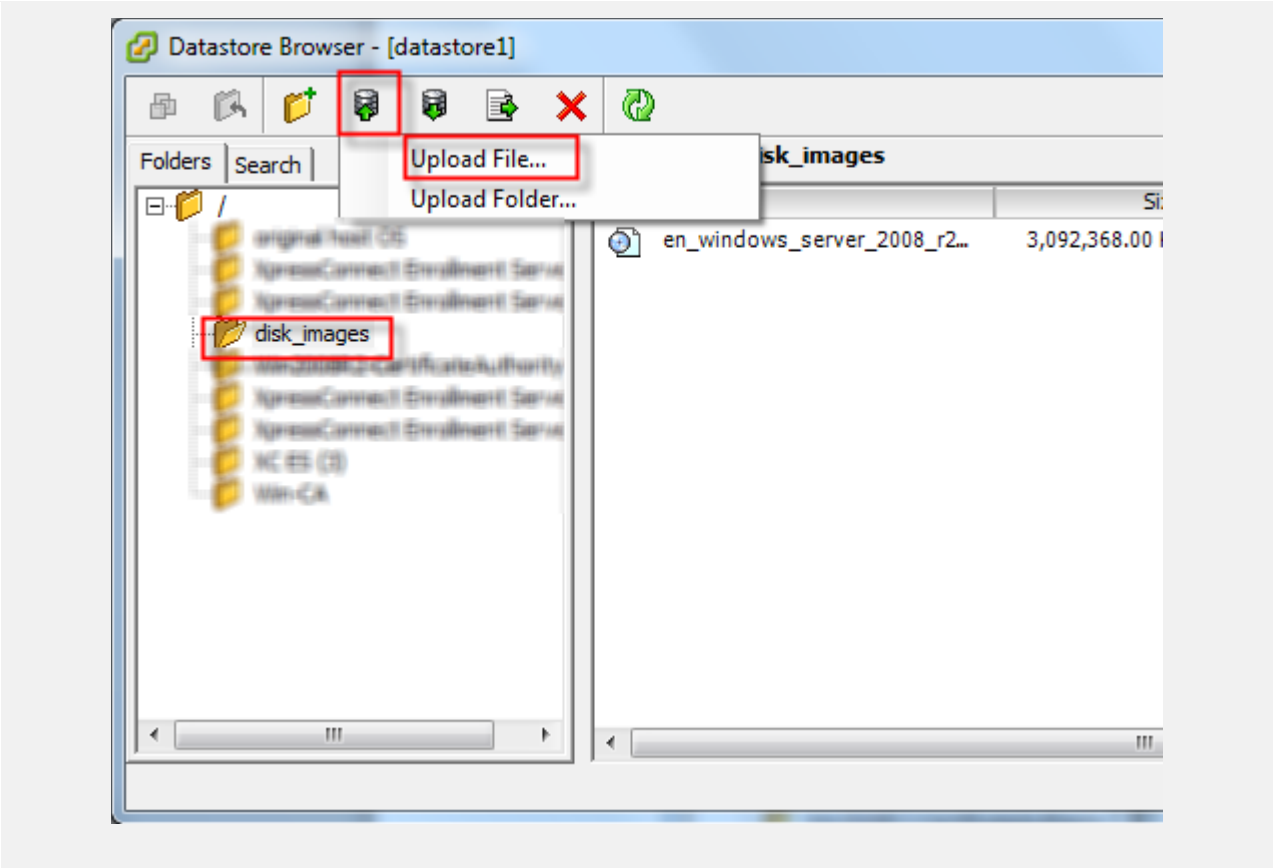
1	**Using vSphere Client, select the VM server node. Click on the Summary tab. Right click on the datastore1 item in the right hand pane, and select Browse Datastore.**



2	**Click on the new folder icon. Give the folder a name such as “disk_images”. This is where you will store ISO images of your OS installation CD/DVDs. Click OK.**



3	**Click on the new folder you just created. Click on the upload icon, and choose Upload File. Browse to the ISO file on your hard drive for the Windows Server setup disk ISO file. Highlight the file. Click Open. Choose Yes at the prompt to overwrite files. Close the Datastore Browser window.**

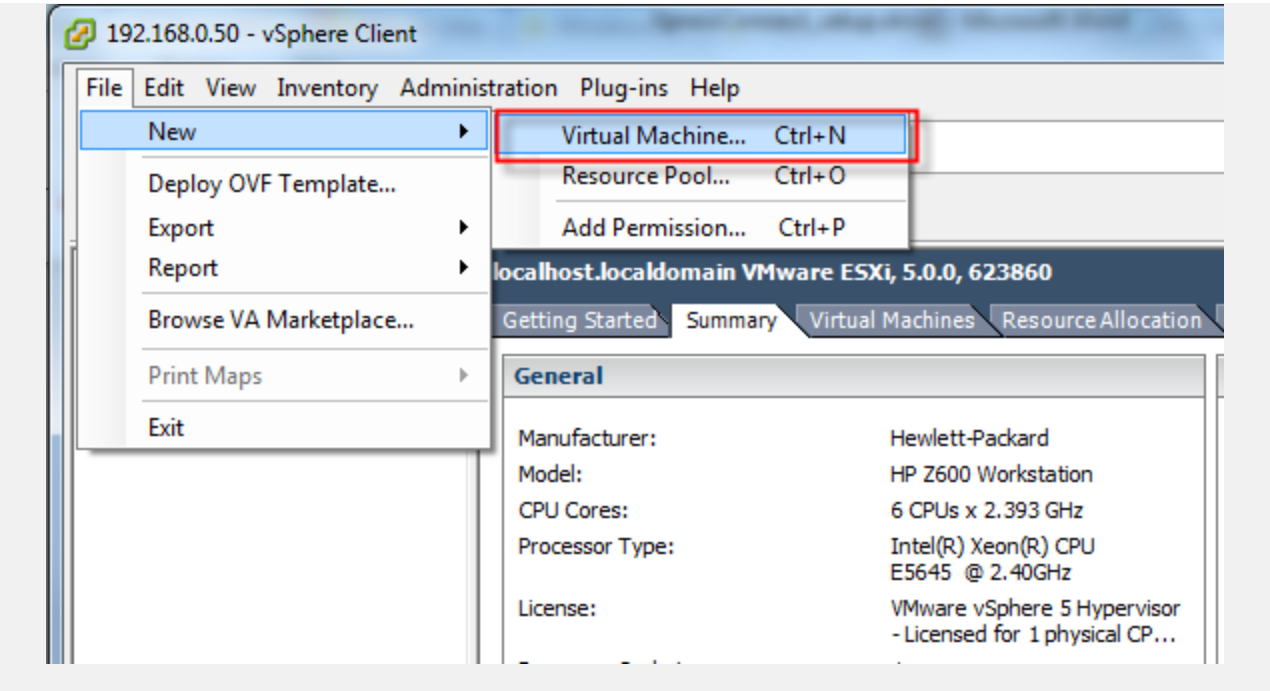


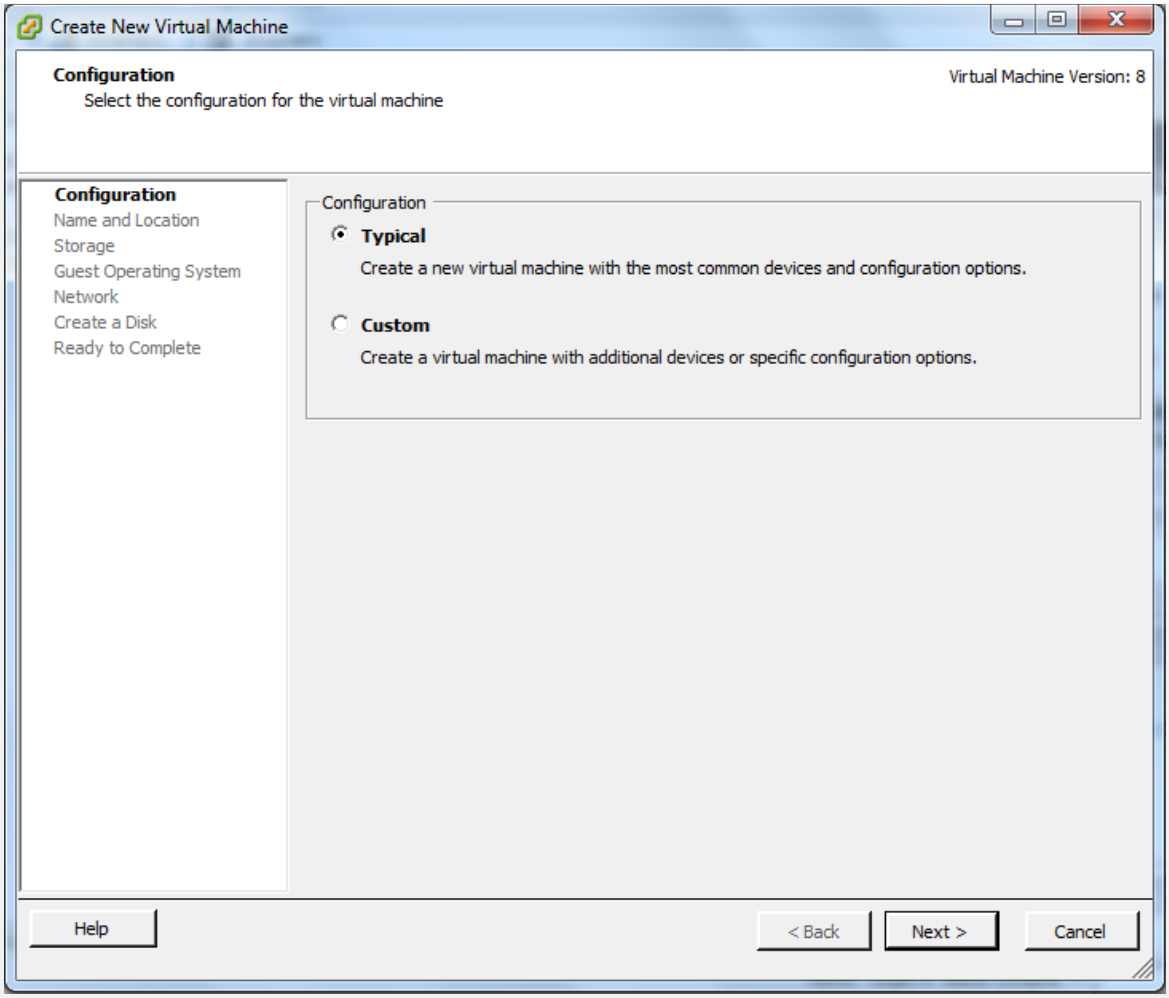
2.2 Windows Server Configuration

You will need to configure a number of services as supporting infrastructure, such as Active Directory, DNS, Certificate Authority, Network Policy Server, etc. Some of these are optional, or may differ in a more complicated lab configuration.

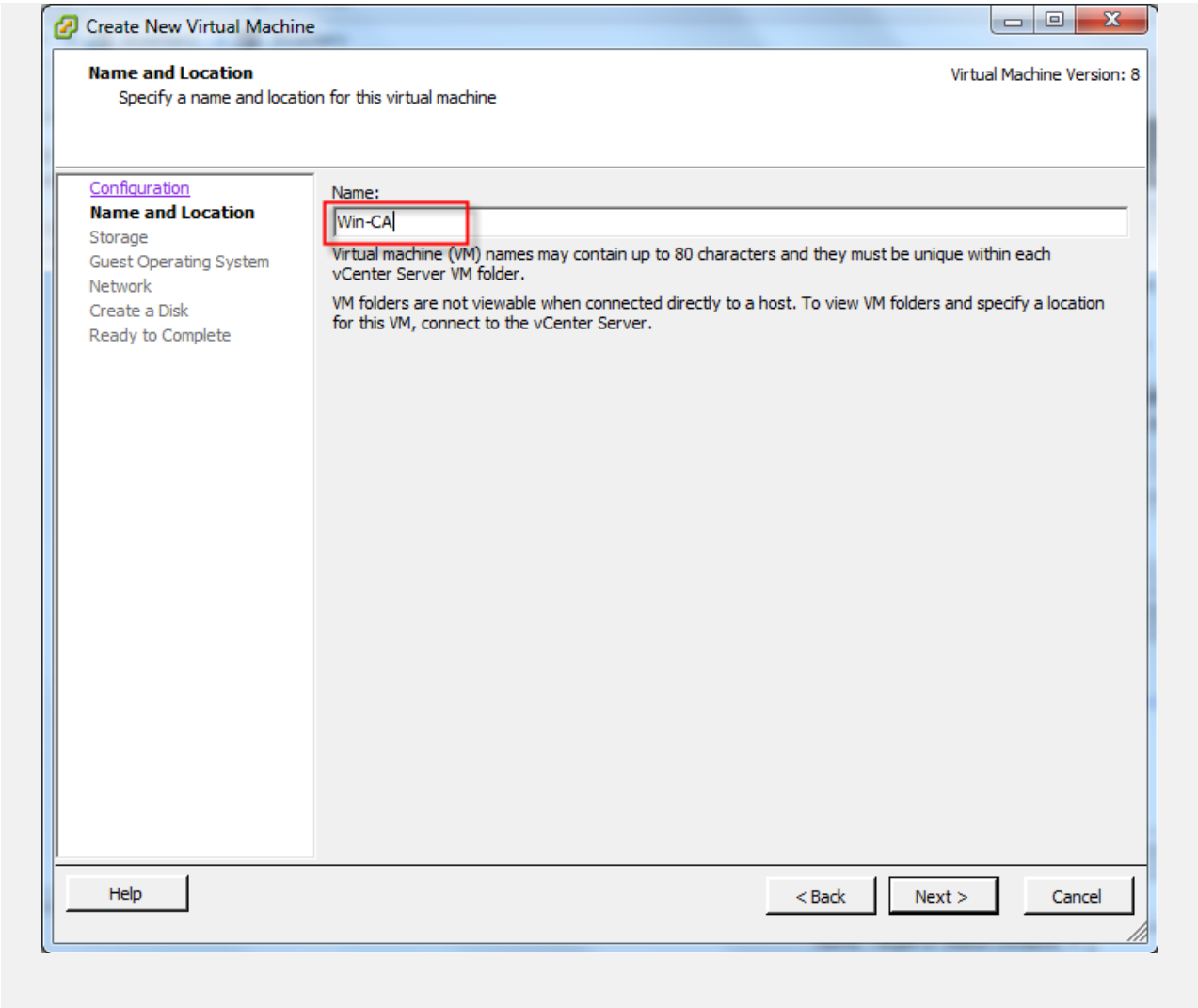
2.2.1 Initial Setup of Windows Server VM

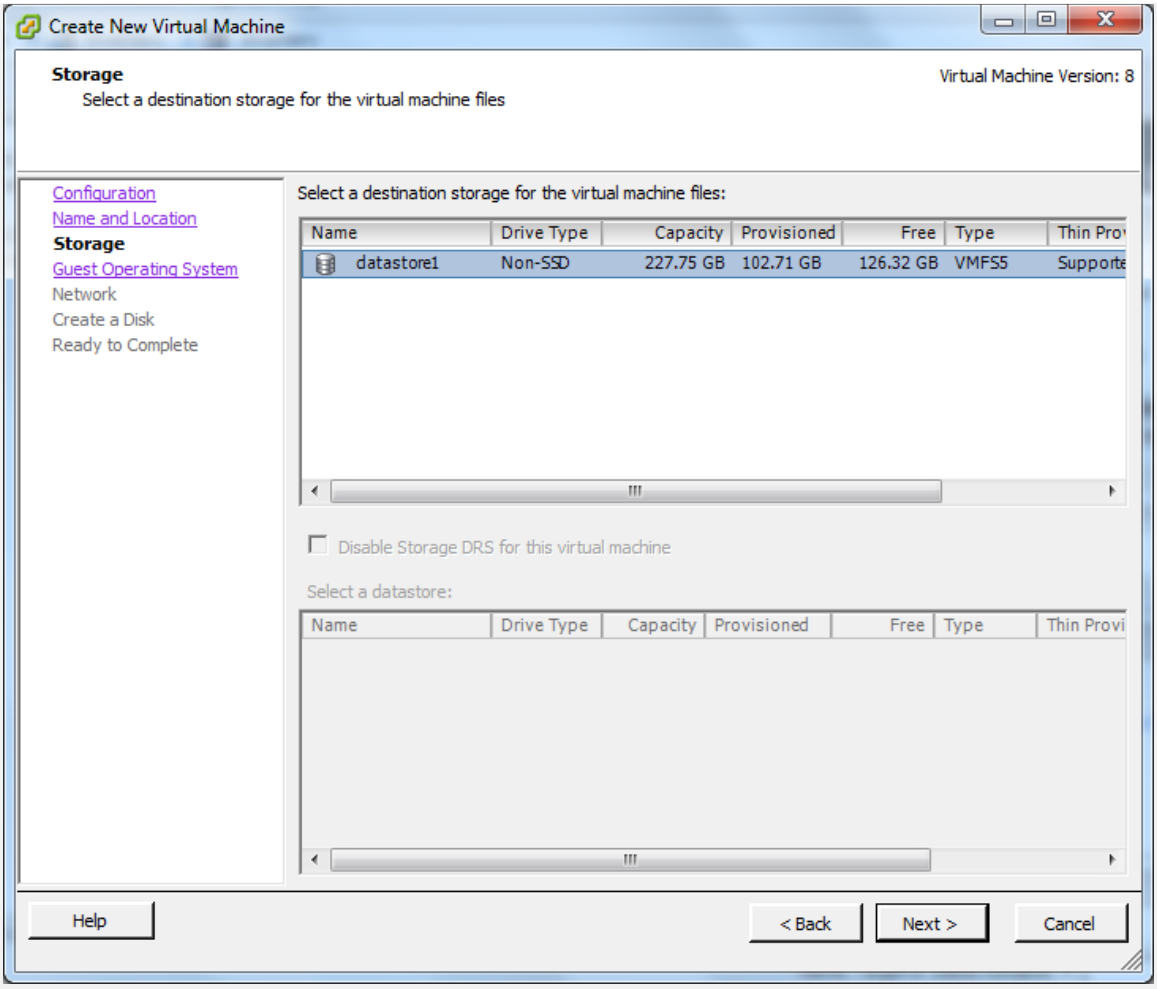
1	**From vSphere Client, click File, New, Virtual Machine. Click Next**


192.168.0.50 - vSphere Client
File
Edit
View
Inventory
Administration
Plug-ins
Help
New
Deploy OVF Template...
Export
Report
Browse VA Marketplace...
Print Maps
Exit
Virtual Machine... Ctrl+N
Resource Pool... Ctrl+O
Add Permission... Ctrl+P
localhost.localdomain VMware ESXi, 5.0.0, 623860
Getting Started
Summary
Virtual Machines
Resource Allocation
General
Manufacturer:
Hewlett-Packard
Model:
HP Z600 Workstation
CPU Cores:
6 CPUs x 2.393 GHz
Processor Type:
Intel(R) Xeon(R) CPU E5645 @ 2.40GHz
License:
VMware vSphere 5 Hypervisor - Licensed for 1 physical CP...

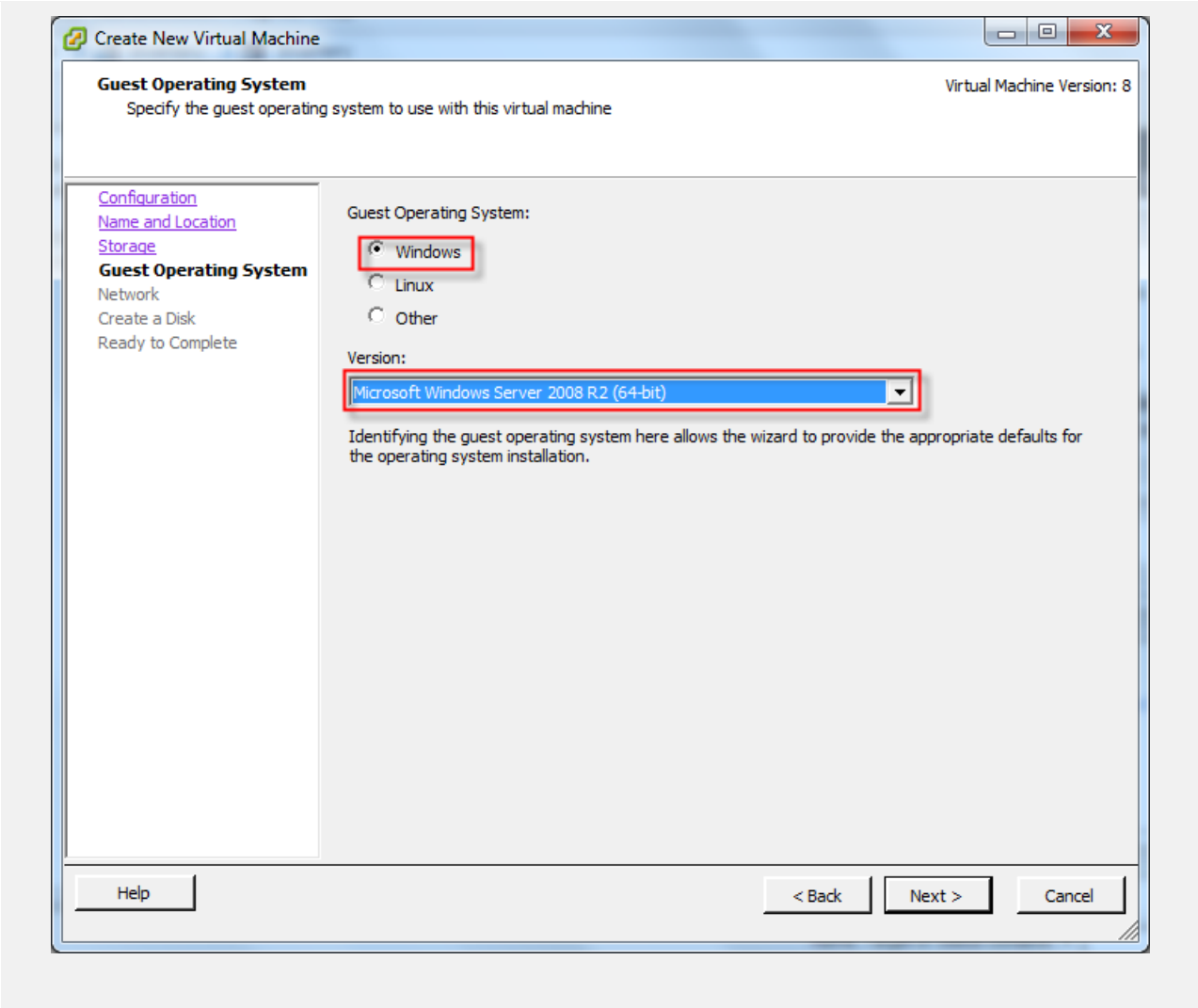


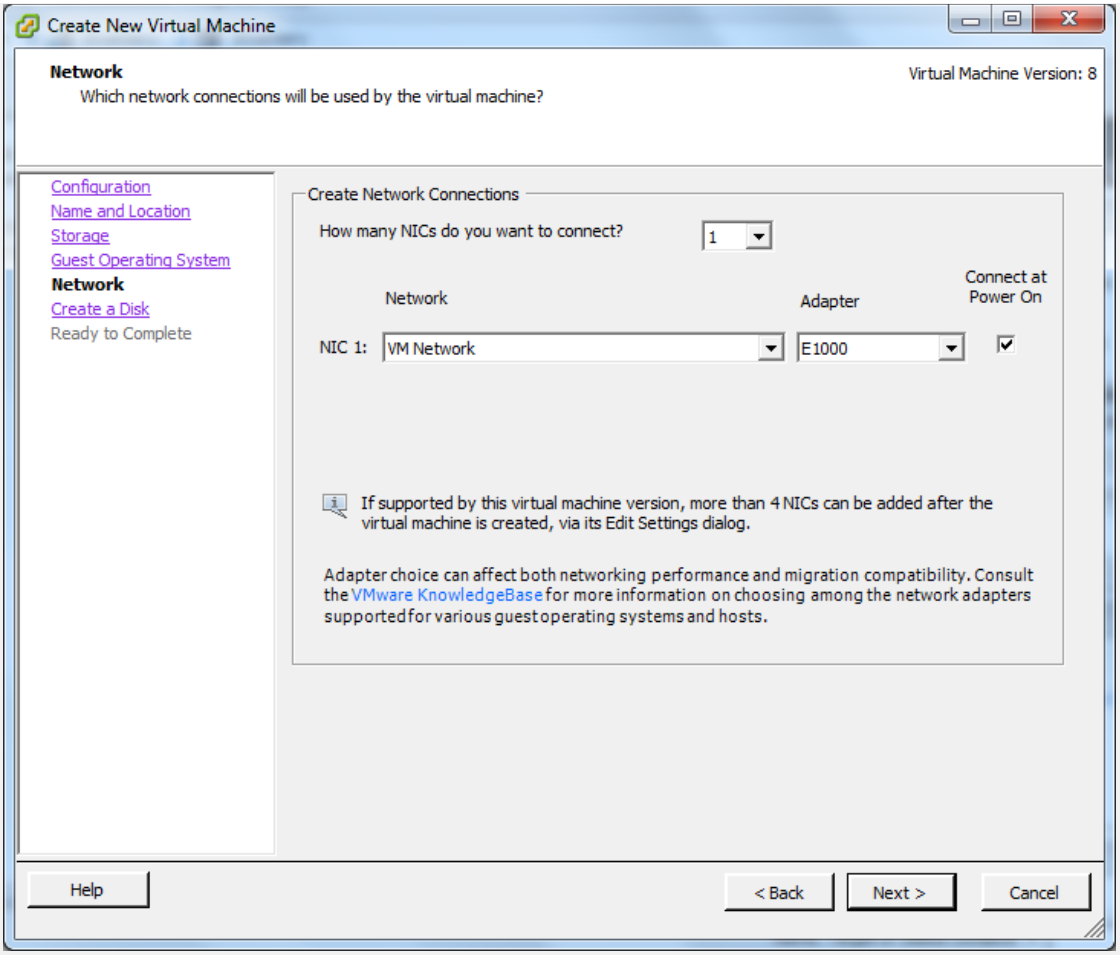
2	**Give the VM a name, such as “Win-CA”. Click Next, and then click Next again.**


Create New Virtual Machine
Name and Location
Specify a name and location for this virtual machine
Virtual Machine Version: 8
Configuration
Name and Location
Storage
Guest Operating System
Network
Create a Disk
Ready to Complete
Name:
Win-CA
Virtual machine (VM) names may contain up to 80 characters and they must be unique within each vCenter Server VM folder.
VM folders are not viewable when connected directly to a host. To view VM folders and specify a location for this VM, connect to the vCenter Server.
Help
< Back
Next >
Cancel

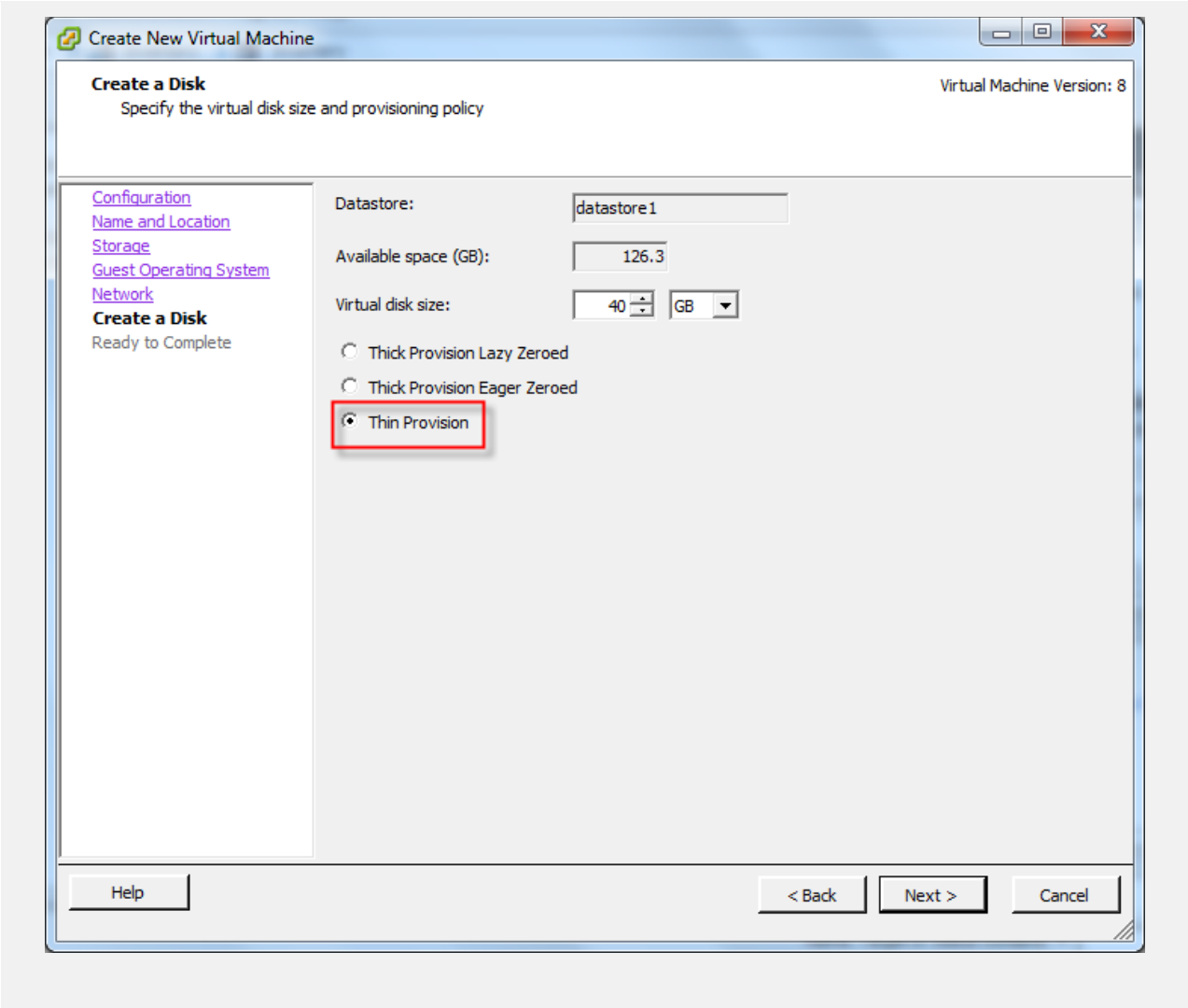


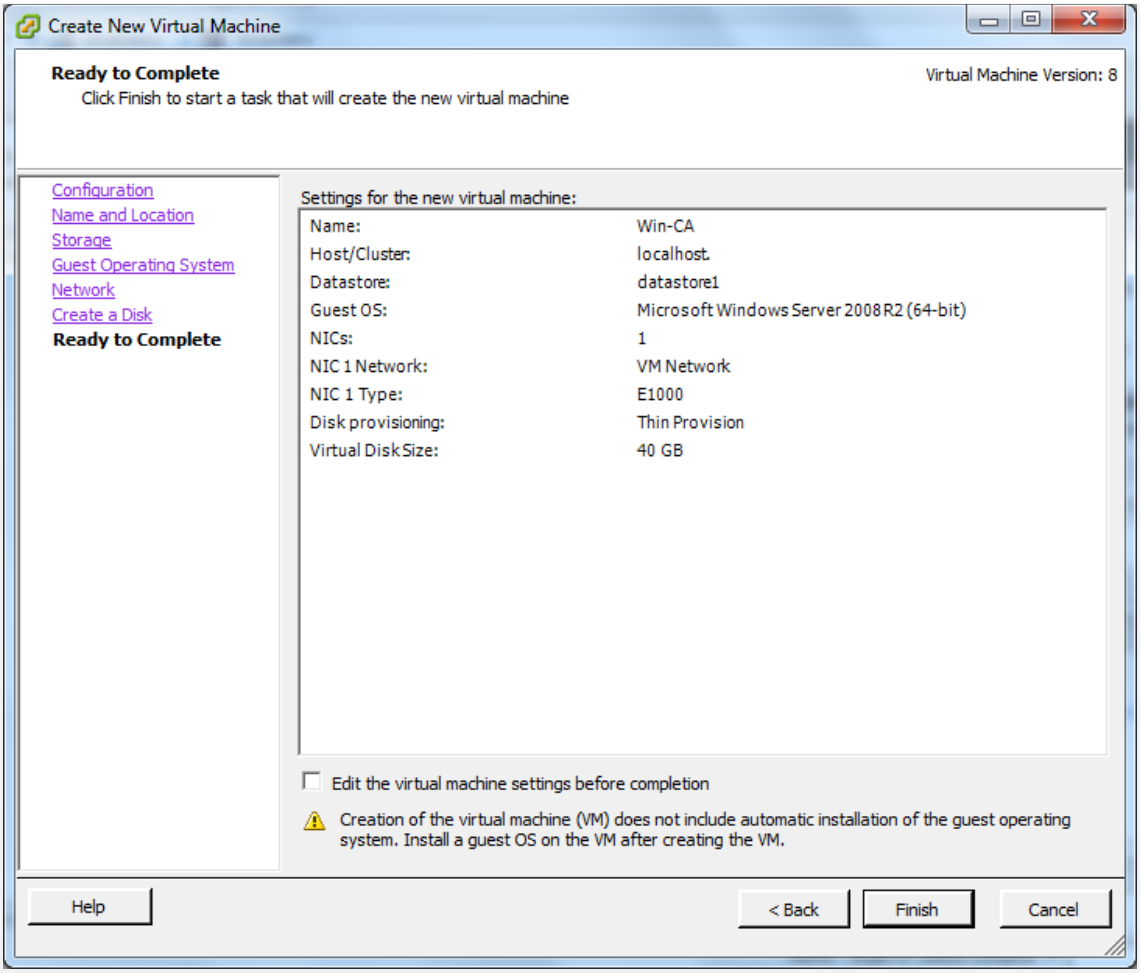
3	**Select Windows as the Operating System and Microsoft Windows Server 2008 R2 (64-bit) as the Version (or select appropriate alternatives depending on which version of Windows server you have available). Click Next. Click Next again.**


Create New Virtual Machine
Guest Operating System
Specify the guest operating system to use with this virtual machine
Virtual Machine Version: 8
Configuration
Name and Location
Storage
Guest Operating System
Network
Create a Disk
Ready to Complete
Guest Operating System:
Windows
Linux
Other
Version:
Microsoft Windows Server 2008 R2 (64-bit)
Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.
Help
< Back
Next >
Cancel

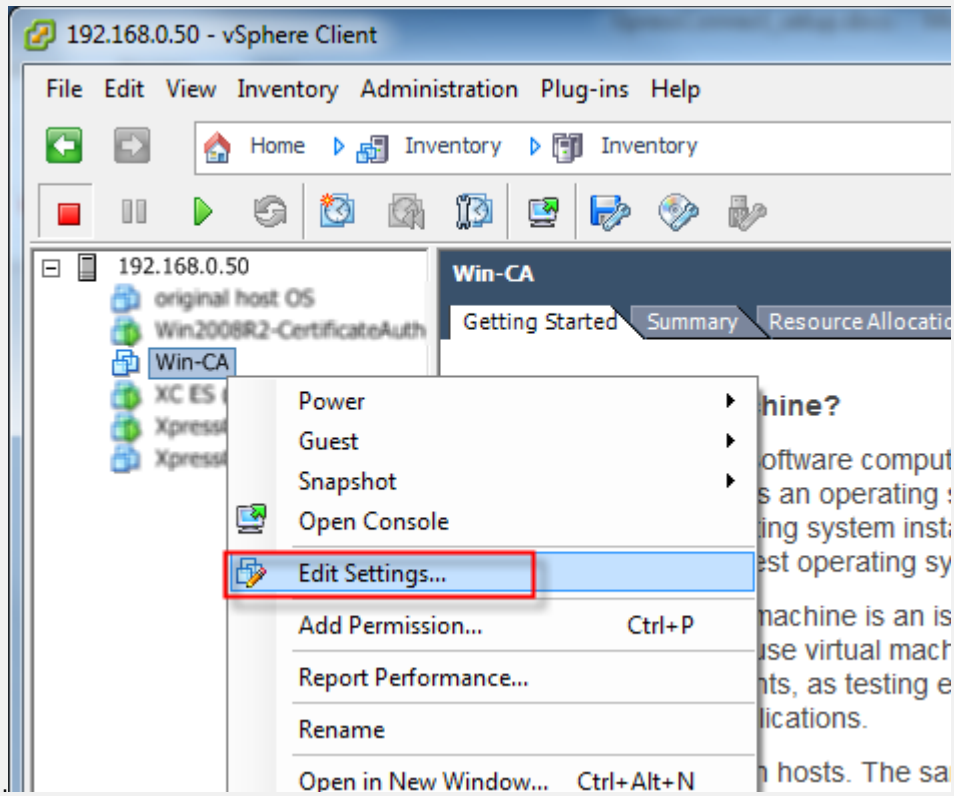


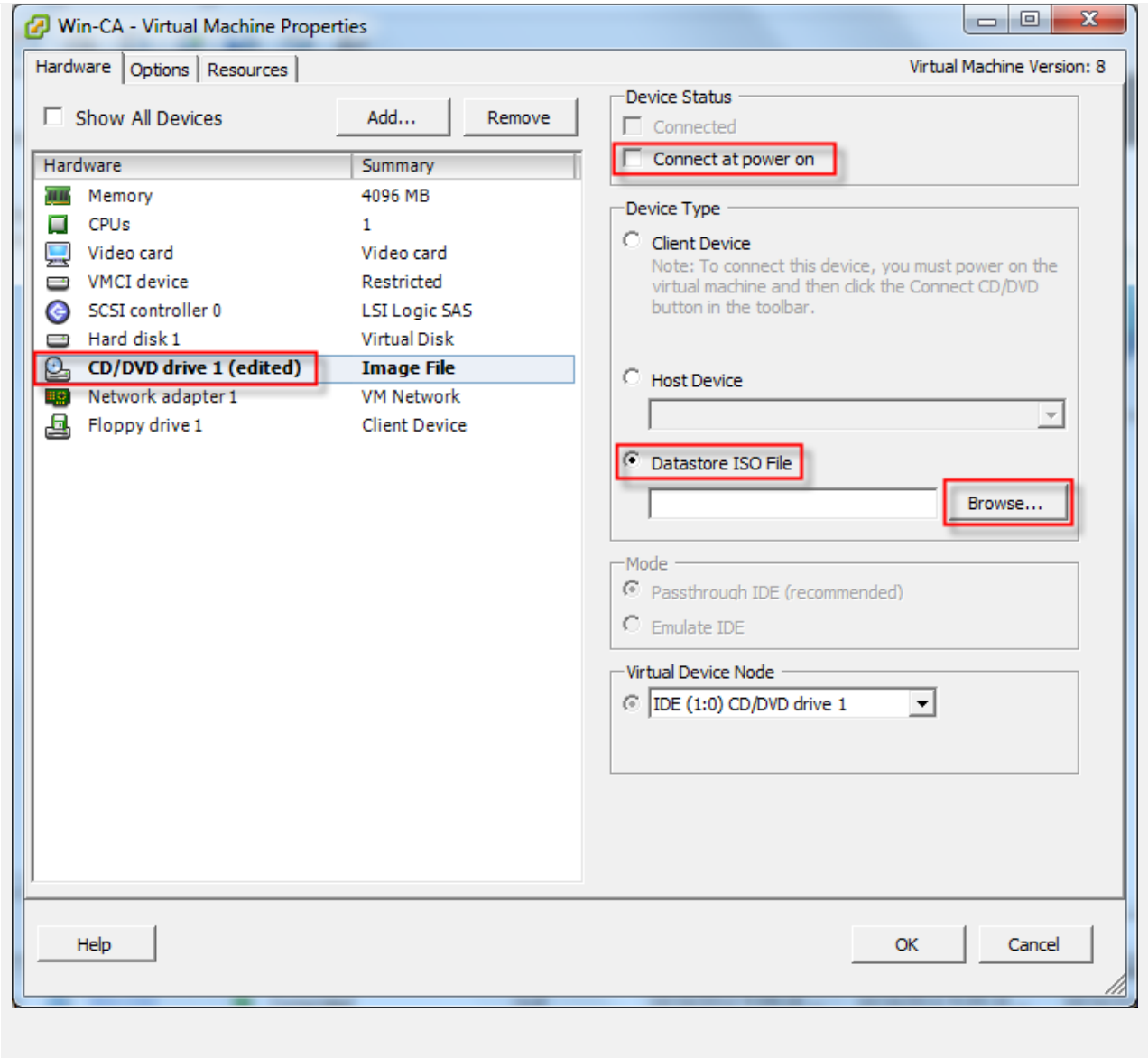
4	**Choose Thin Provision (this allows you to make more use of the available physical disk space). Click Next. Then click Finish.**


Create New Virtual Machine
Create a Disk
Specify the virtual disk size and provisioning policy
Virtual Machine Version: 8
Configuration
Name and Location
Storage
Guest Operating System
Network
Create a Disk
Ready to Complete
Datastore:
datastore1
Available space (GB):
126.3
Virtual disk size:
40
GB
Thick Provision Lazy Zeroed
Thick Provision Eager Zeroed
Thin Provision
Help
< Back
Next >
Cancel

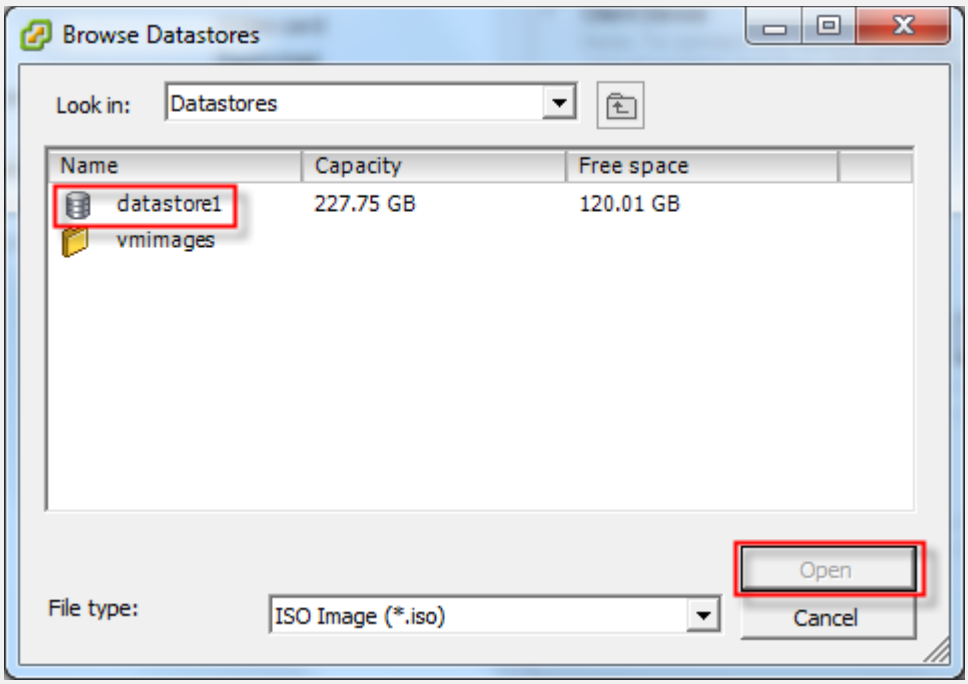


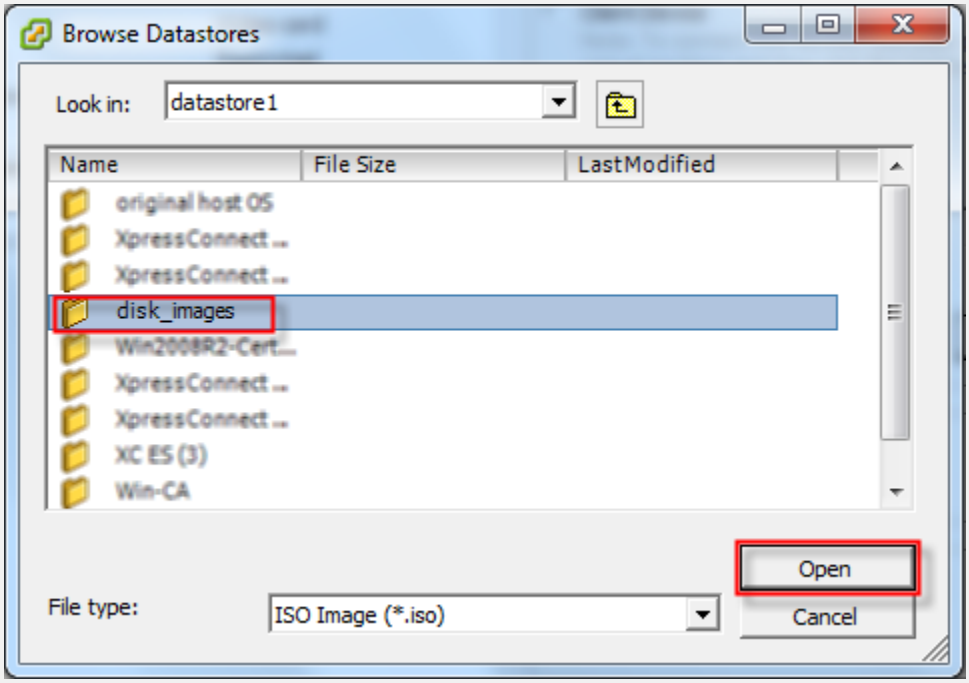
5	**Right click on the new VM and choose Edit Settings. Click on CD/DVD drive 1. Select Datastore ISO File. Check Connect at power on. Click Browse to choose the ISO image of the Windows Server setup disk.**

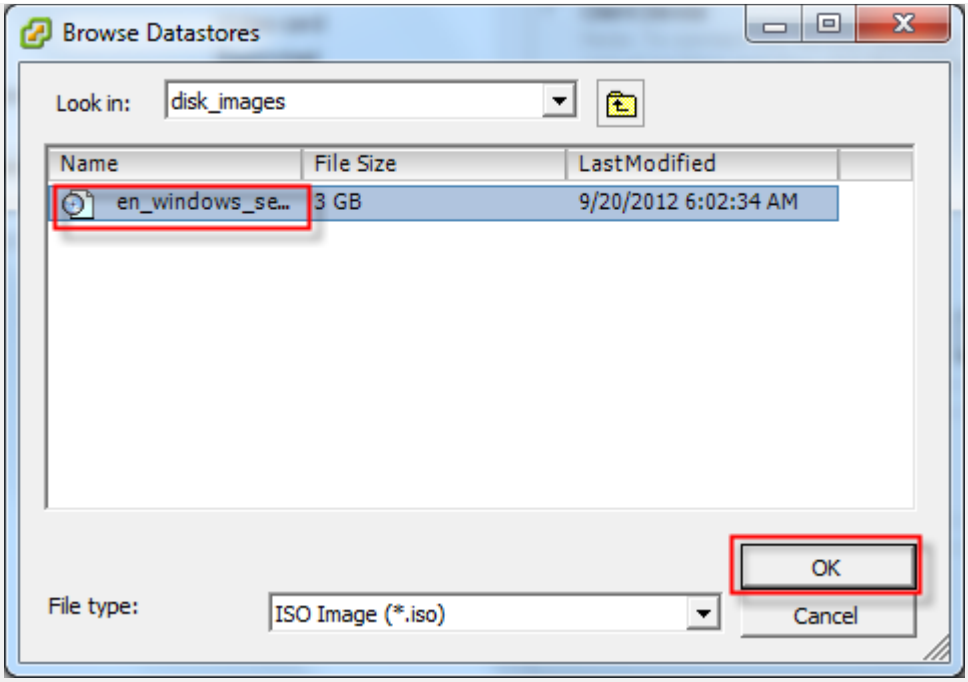

192.168.0.50 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home
Inventory
Inventory
192.168.0.50
original host OS
Win2008R2-CertificateAuth
Win-CA
Win-CA
Getting Started
Summary
Resource Allocatio
Power
Guest
Snapshot
Open Console
Edit Settings...
Add Permission... Ctrl+P
Report Performance...
Rename
Open in New Window... Ctrl+Alt+N



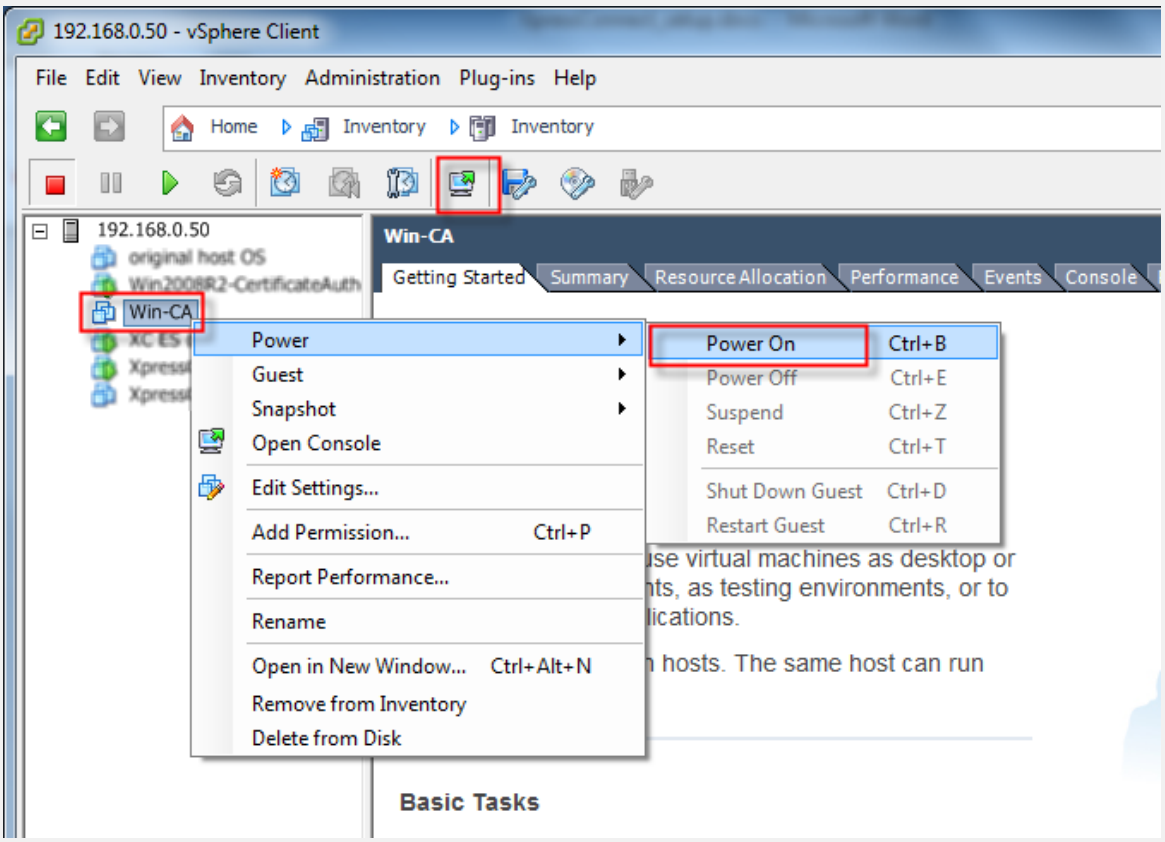
6	**Click on datastore1, then click Open. Click on your folder where you saved the ISO file and click Open. Click on the Windows Server image file and click OK. Click Ok again.**


Browse Datastores
Look in:
Datastores
Name
Capacity
Free space
datastore1
227.75 GB
120.01 GB
vmimages
Open
File type:
ISO Image (*.iso)
Cancel


Browse Datastores
Look in:
datastore1
Name
File Size
LastModified
original host OS
XpressConnect ...
XpressConnect ...
disk_images
Win2008R2-Cert...
XpressConnect ...
XpressConnect ...
XC ES (3)
Win-CA
Open
File type:
ISO Image (*.iso)
Cancel



7	**Right click on the VM in the tree, select Power, then select Power On. Click on the Launch Virtual Machine Console icon.**



8	**Proceed through the setup of Windows using the console interface.**

2.2.2 Configure Networking

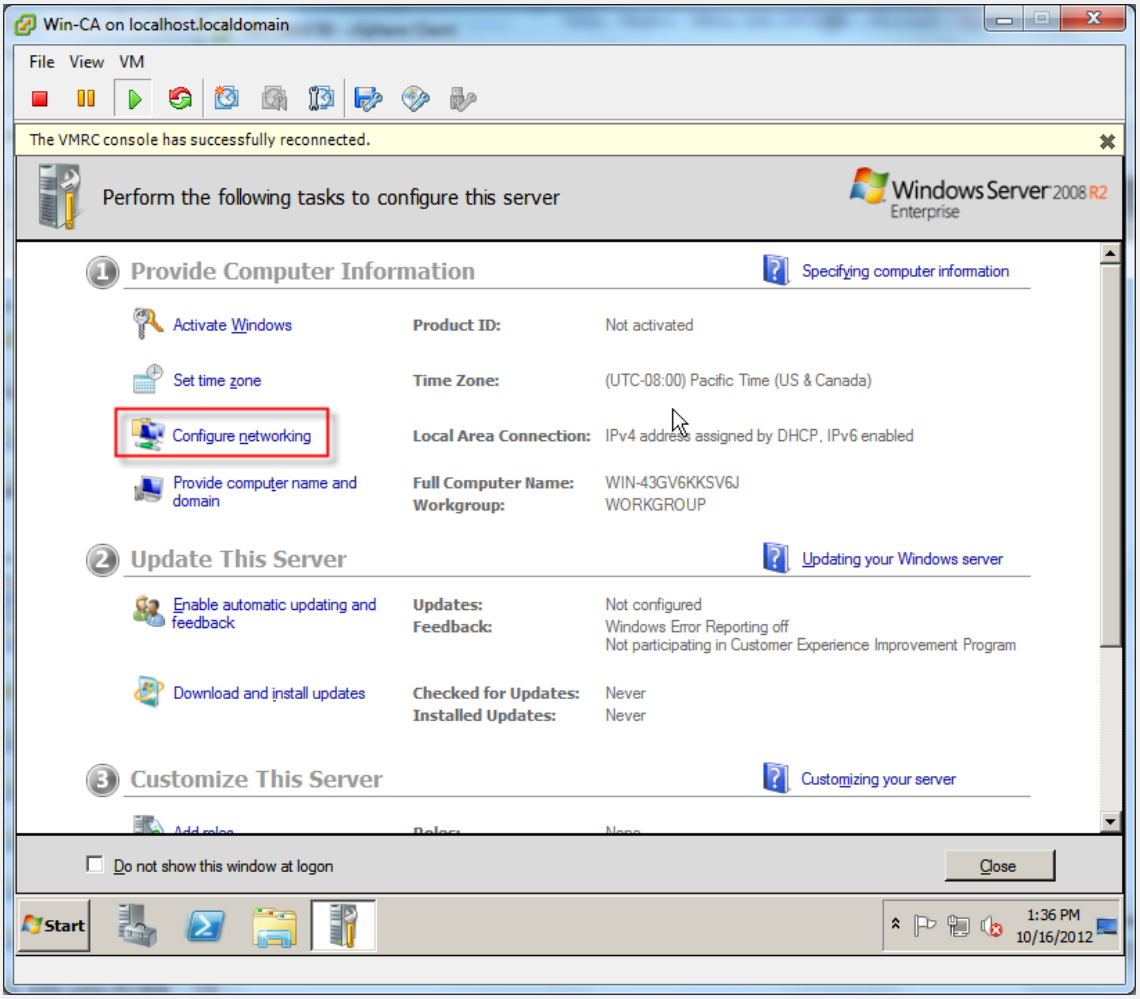
When Windows Setup is finished, it will boot up and launch the Initial Configuration Tasks application.

Note: Many of the next few sections mention launching tasks from the Initial Configuration Tasks application window. This is a convenient launch point for these next steps. If for some reason you close this window or do not see it, click Start and type “oobe” and press Enter.

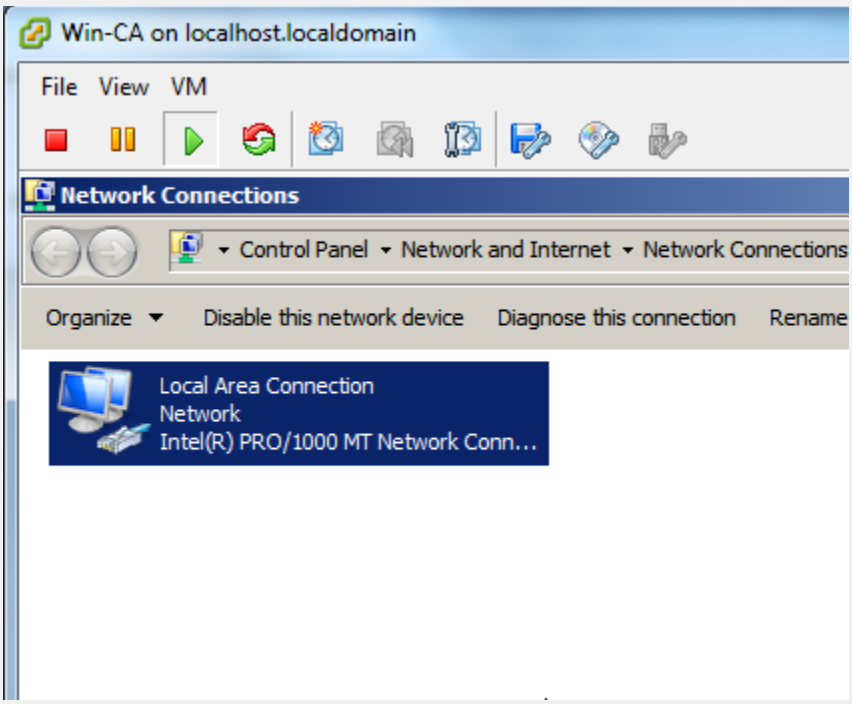
You will need to configure the server with a static IP address.

Note: The Microsoft Certificate Authority service requires a static IP address assignment for the server. In a lab demo configuration, where multiple services are installed on the same physical or virtual server, these steps are required. In a customer deployment, where services are typically installed on different physical or virtual servers, many of these steps may not be required. In addition, a customer pilot may involve integration into existing infrastructure, in which case the servers may already be setup.

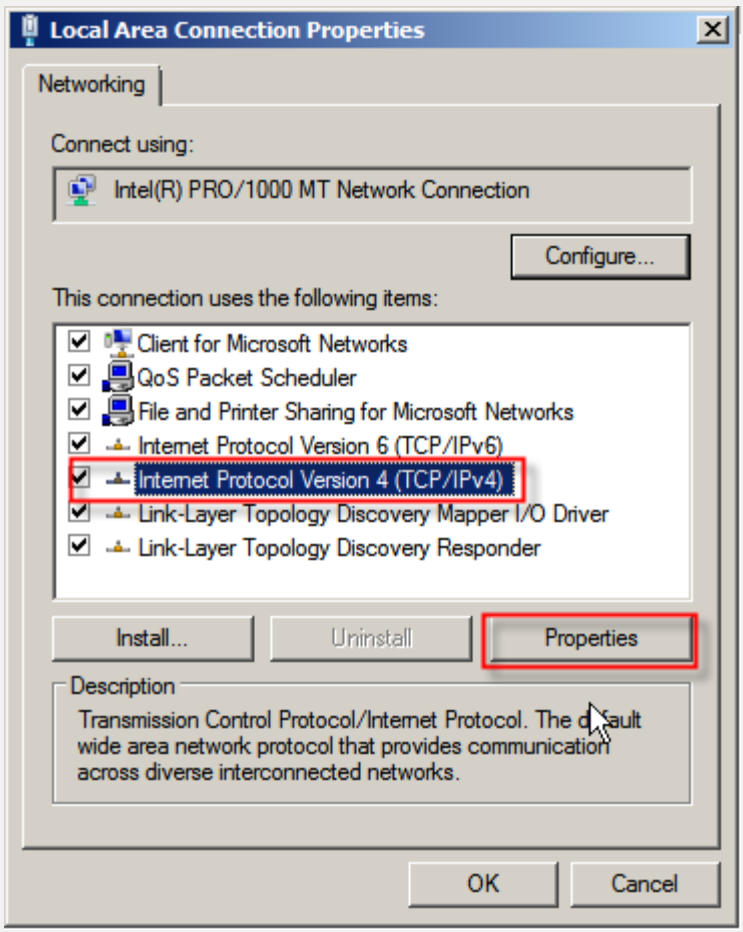
1	**From the Initial Configuration Tasks application, click Configure networking to assign a static IP to the server.**



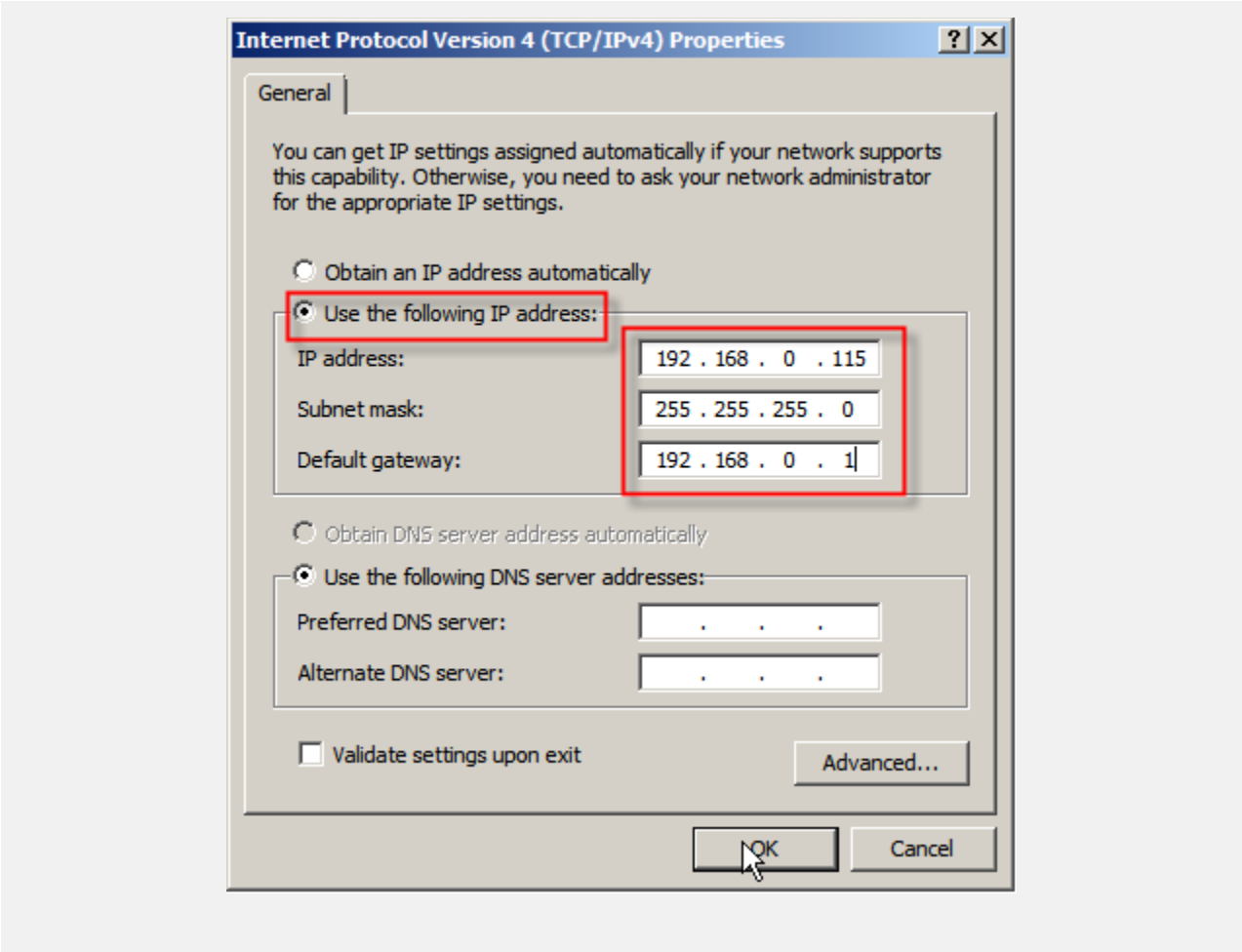
2	**Right click the network interface and choose Properties.**



3	**Click on Internet Protocol Version 4 and click Properties.**



4	**Choose Use the following IP address and fill in the respective fields. Click Ok. Click Close. Close the Network Connections window.**

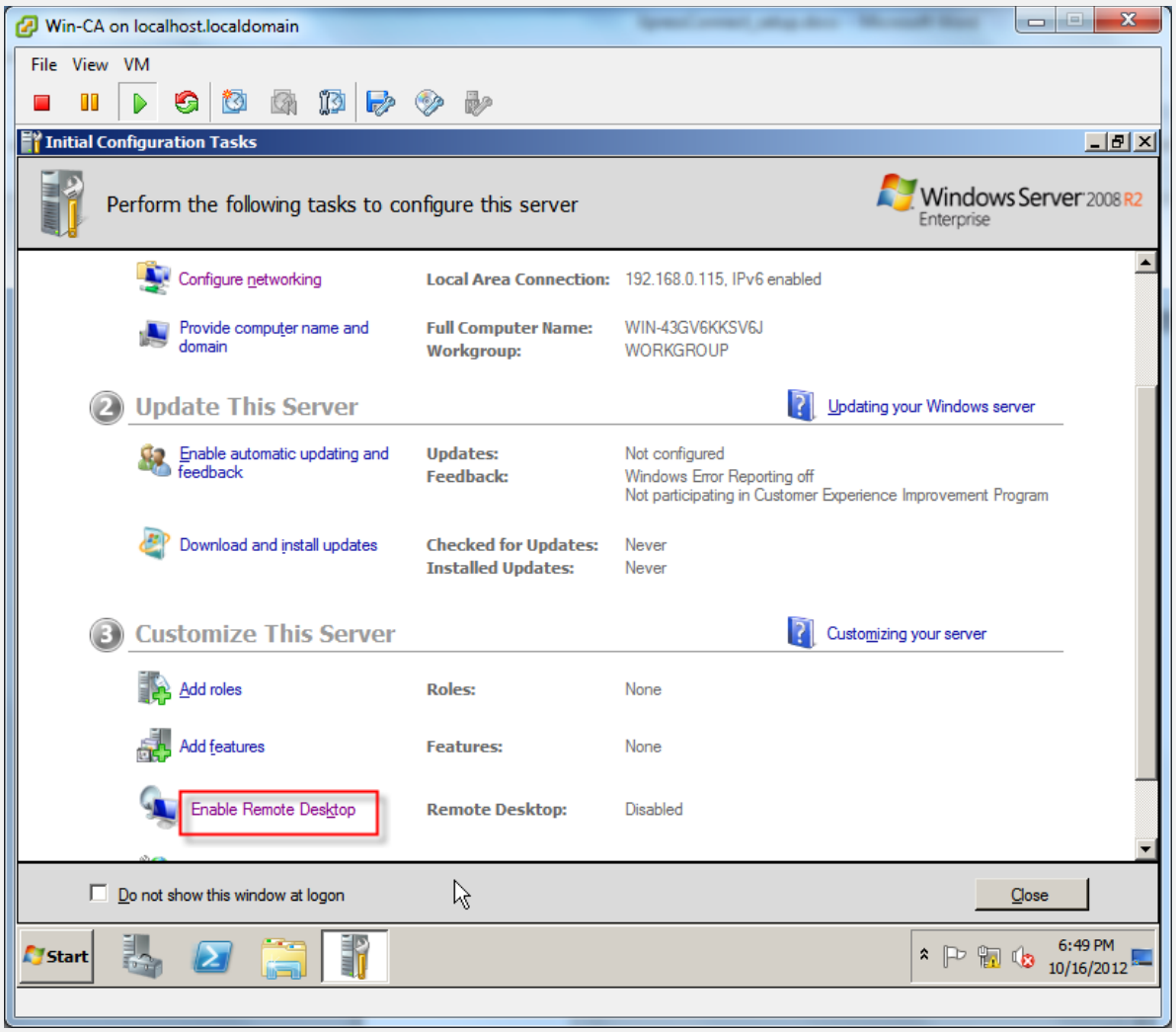


2.2.3 Configure Remote Desktop

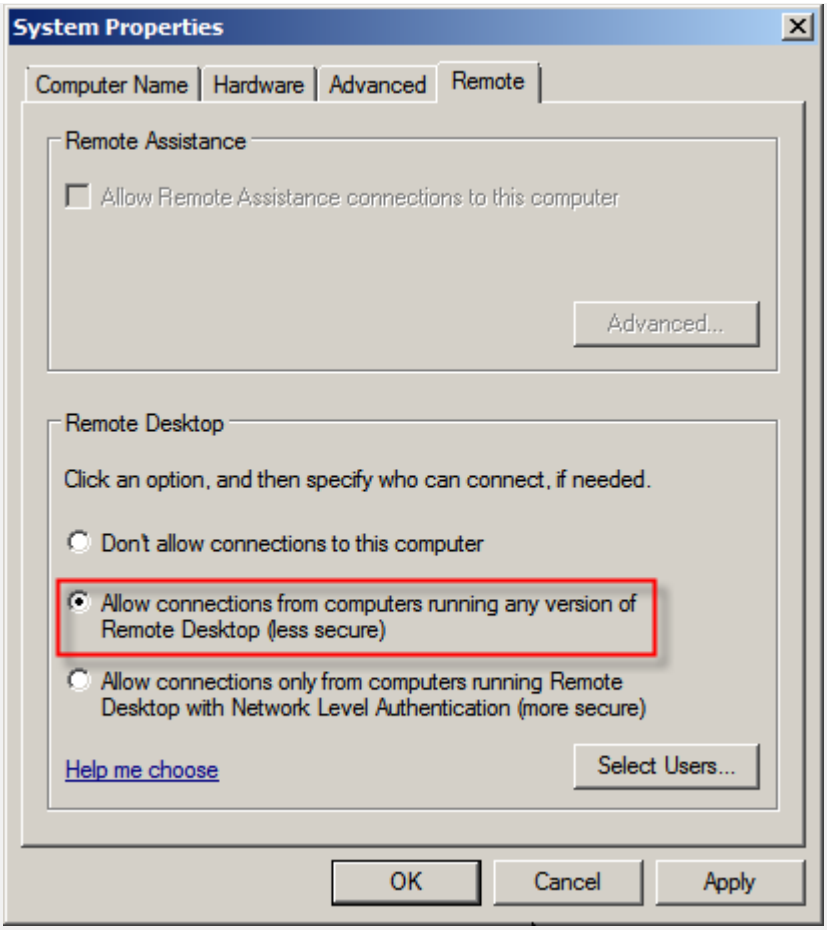
Remote Desktop will make it much easier to manage the remainder of the server setup, as well as run much faster than the vSphere virtual console interface. This is an optional step, but recommended. The easiest way to enable Remote Desktop is from the Initial Configuration Tasks application that launches at the end of Windows Server setup.

Note: Remote desktop will generally perform better than the Virtual Machine Console interface of vSphere Client.

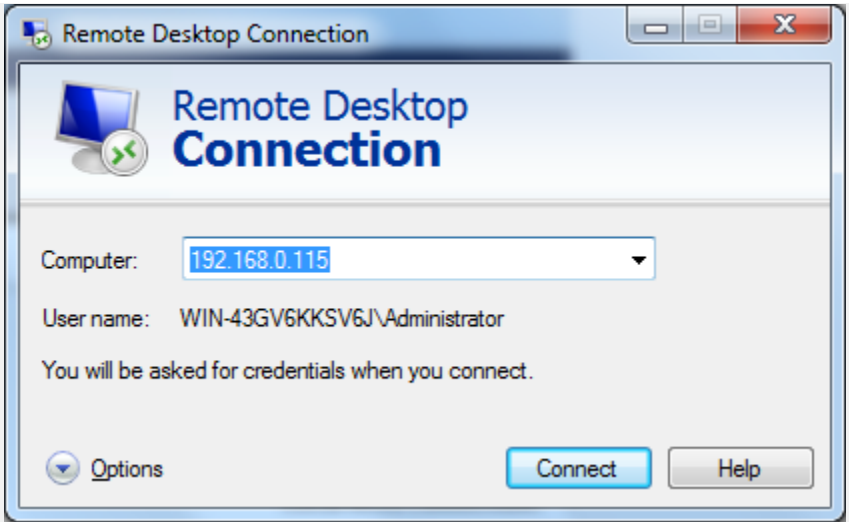
1	**From the Initial Configuration Tasks application, click Enable Remote Desktop.**



2	Choose to Allow connections. Click OK at the security pop up box. Then click OK again.



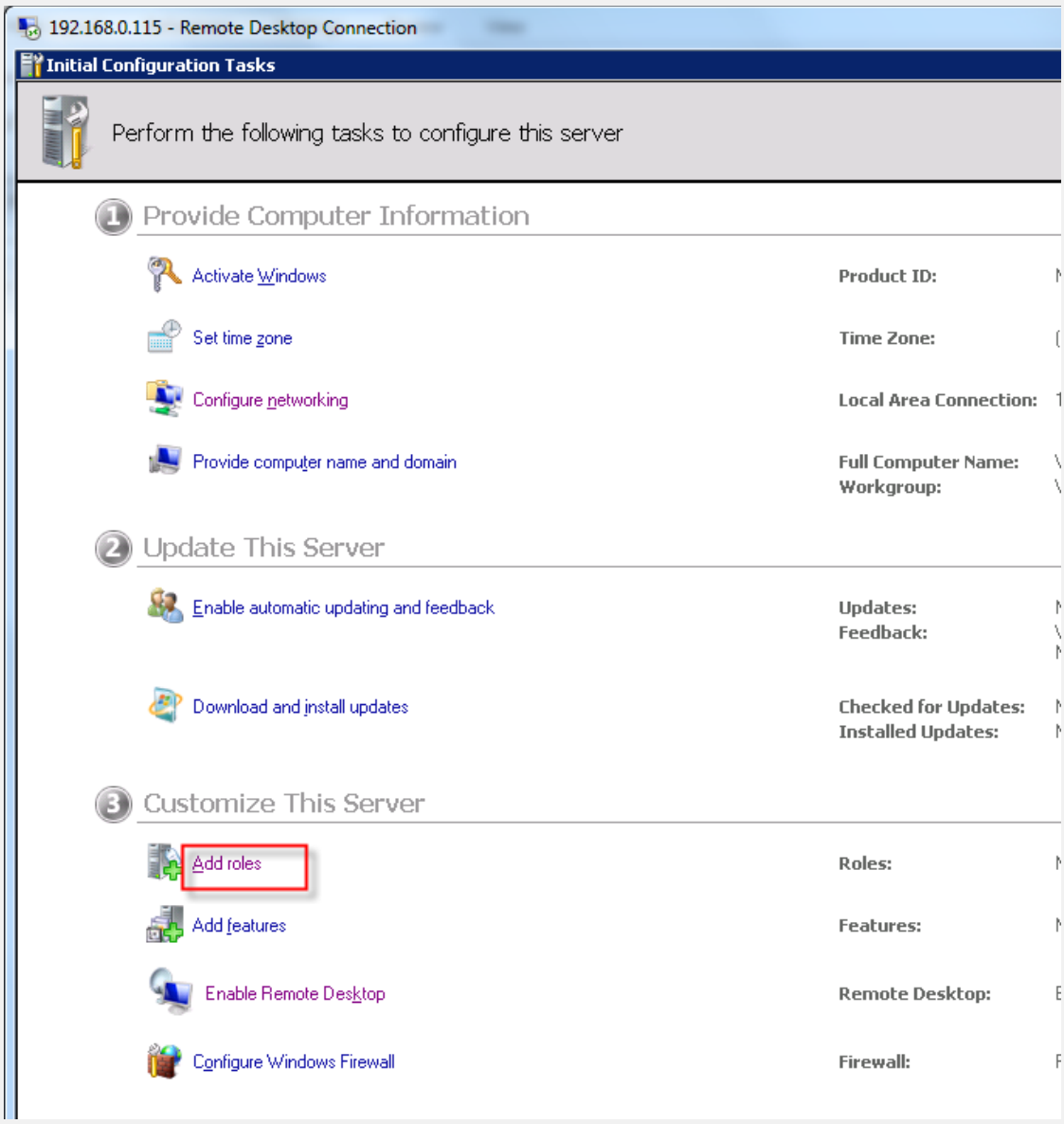
3	**Close the console window of vSphere. From your laptop, click Start, All Programs, Accessories, Remote Desktop Connection. Enter the IP address of the Windows Server, and click Connect. Enter the username (you may have to choose Use another account and type "\Administrator") and password. Click Yes at the security prompt.**

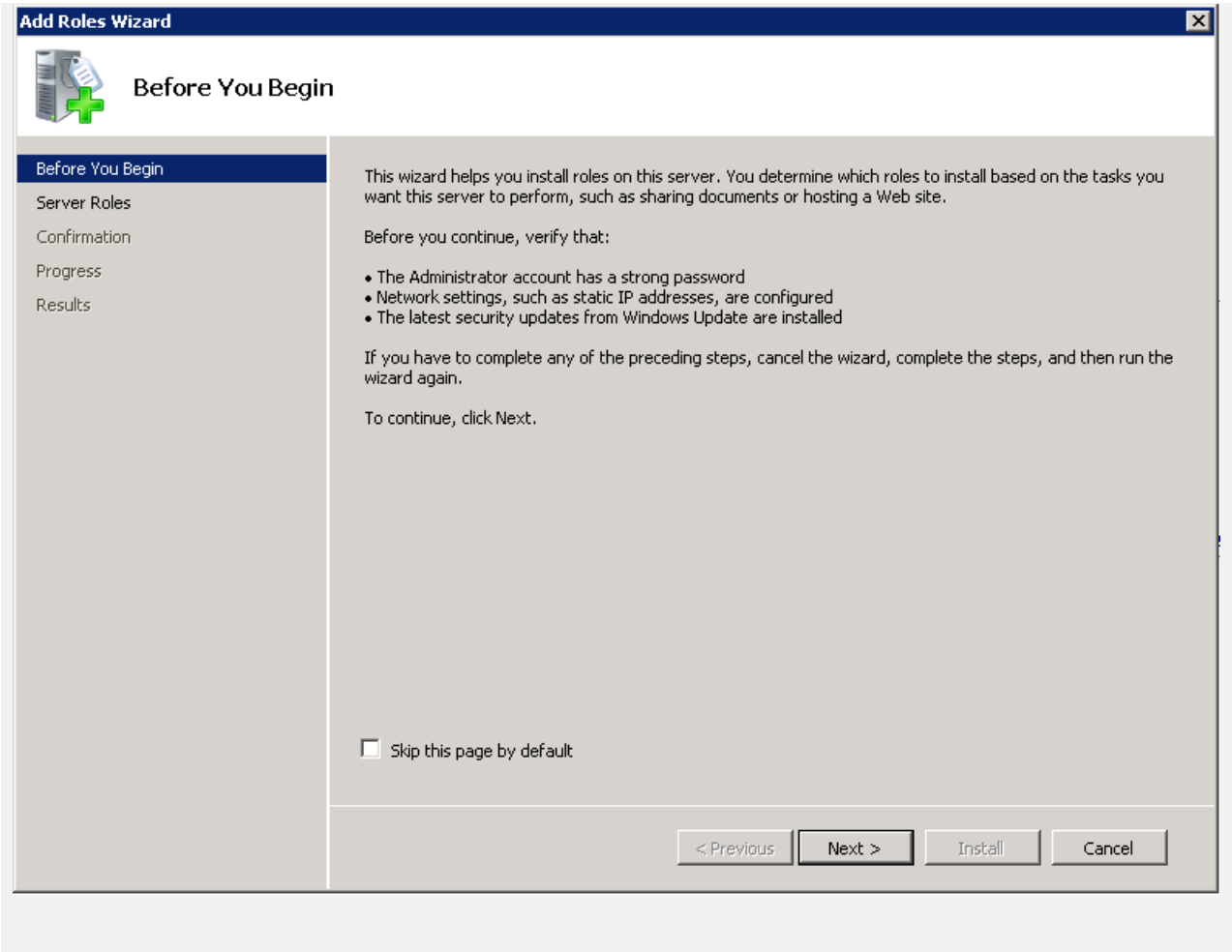


2.2.4 Configure Active Directory

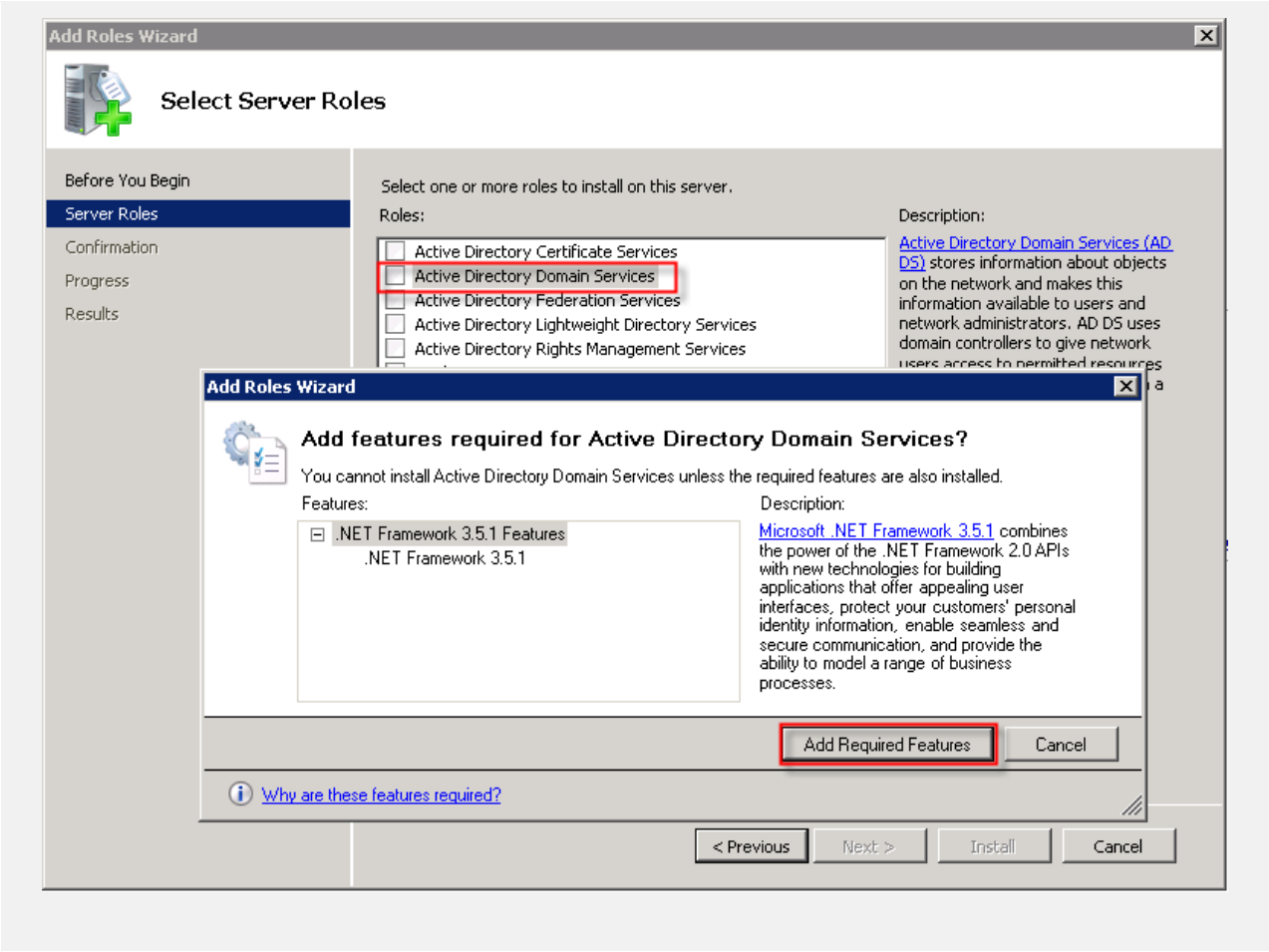
Note: When configuring Active Directory, it will ask for a domain name. You can use any name you prefer, but it typically works best in a lab environment to use ".local" as the suffix, because the ".local" DNS suffix is reserved for locally significant deployments, such as labs that may have public Internet connectivity but not a public DNS record. If you pick a ".com" suffix and the name you choose is a publicly registered DNS name, you will have DNS conflicts and DNS forwarding may not work properly. By using a ".local" suffix, you can configure name resolution in the lab and still have DNS forwarding work for public DNS names. Also, certificate hierarchies typically use DNS for things like revocation checking, so picking an appropriate domain name for Active Directory is even more important with a Secure Access demo. Alternatively, if you plan to configure everything to communicate by IP address instead of DNS name in the lab, then it doesn't really matter what domain name you choose. However, bear in mind that certificate services will be a little more difficult to setup.

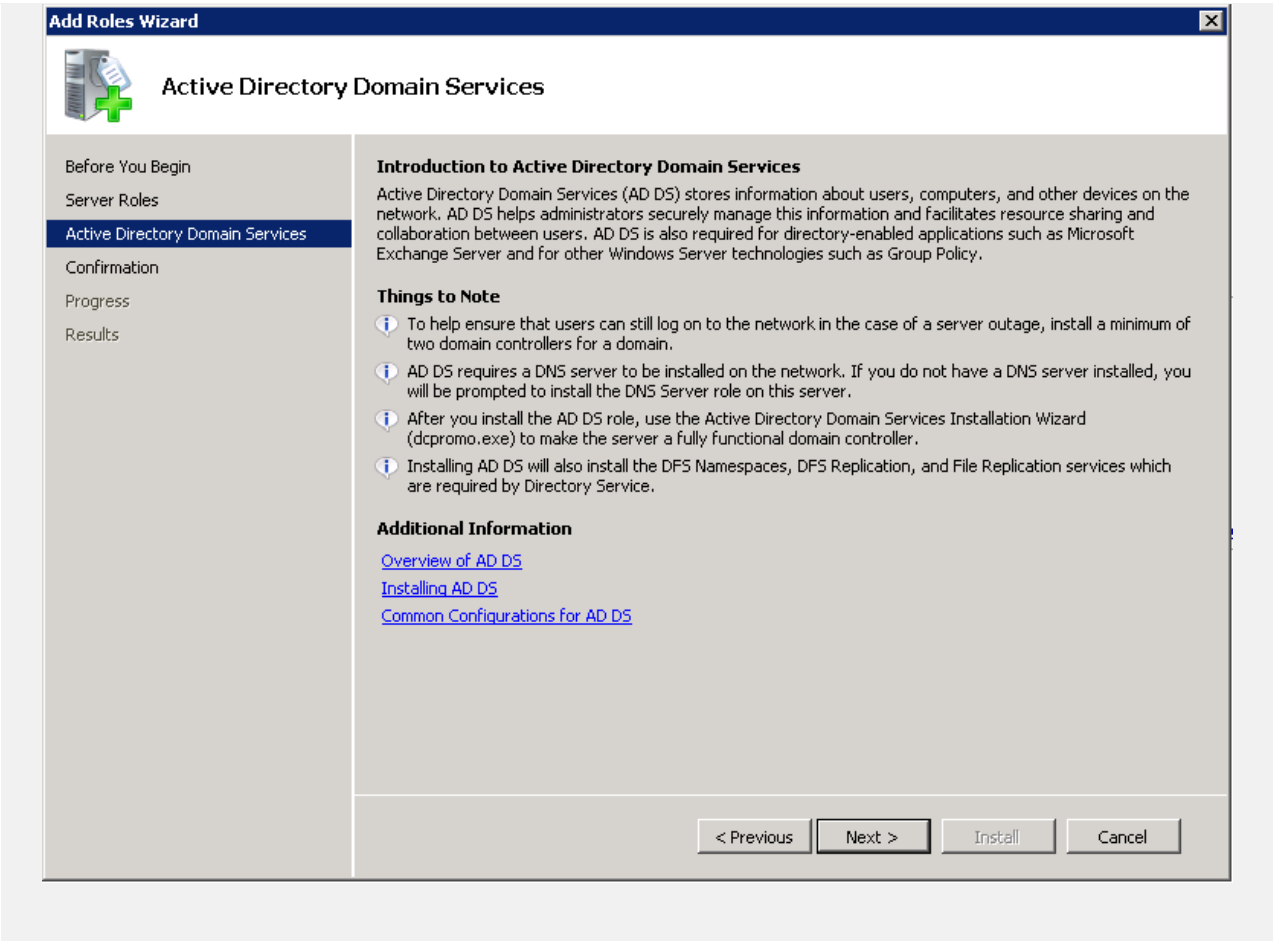
1	**From the Initial Configuration Tasks window, click Add roles. Click Next**


192.168.0.115 - Remote Desktop Connection
Initial Configuration Tasks
Perform the following tasks to configure this server
1 Provide Computer Information
Activate Windows
Product ID:
Set time zone
Time Zone:
Configure networking
Local Area Connection:
Provide computer name and domain
Full Computer Name:
Workgroup:
2 Update This Server
Enable automatic updating and feedback
Updates:
Feedback:
Download and install updates
Checked for Updates:
Installed Updates:
3 Customize This Server
Add roles
Roles:
Add features
Features:
Enable Remote Desktop
Remote Desktop:
Configure Windows Firewall
Firewall:

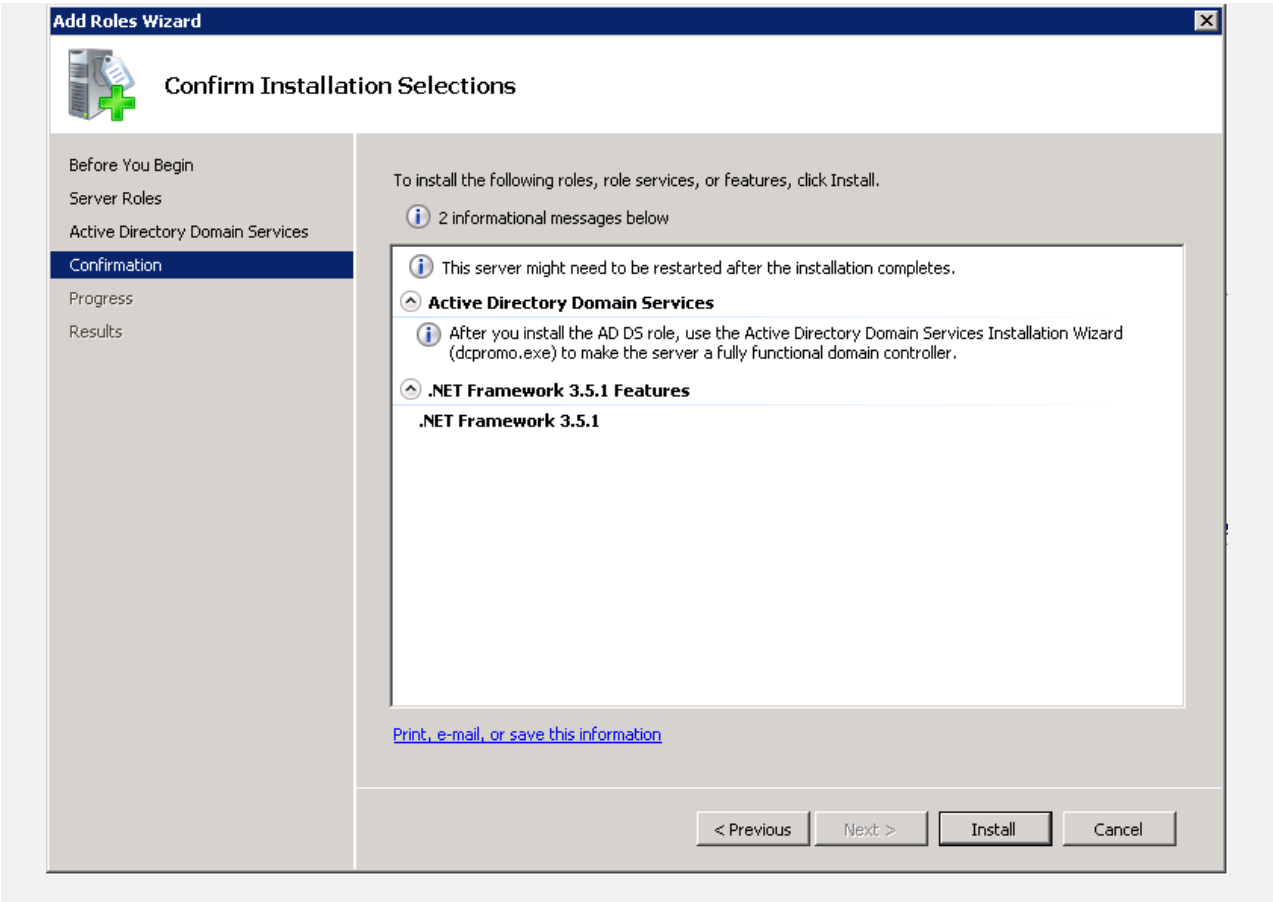


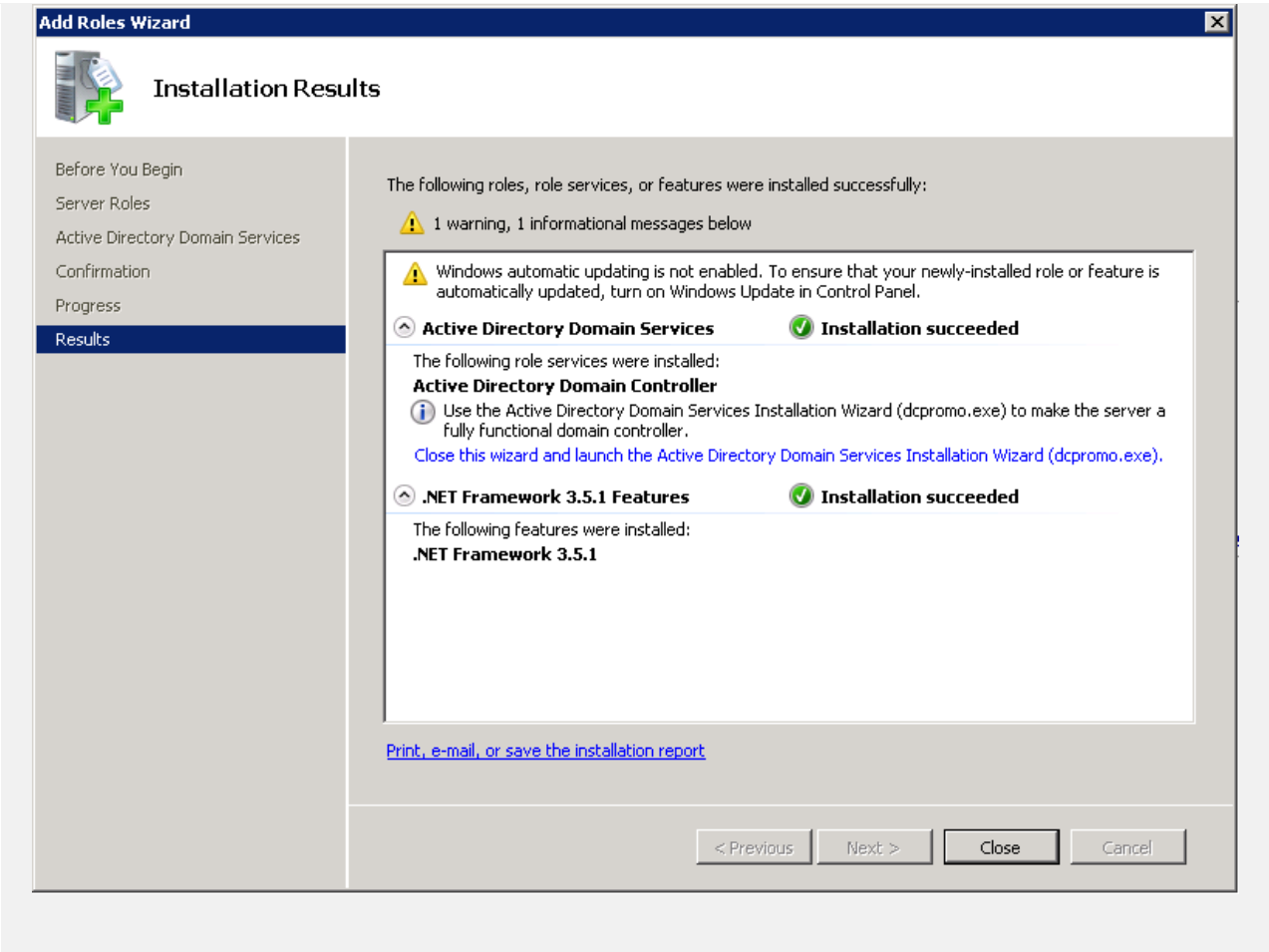
2	**Check Active Directory Domain Services. When the pop up appears click Add Required Features. Click Next. Then click Next again.**


Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
Confirmation
Progress
Results
Select one or more roles to install on this server.
Roles:
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Description:
Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network
Add Roles Wizard
Add features required for Active Directory Domain Services?
You cannot install Active Directory Domain Services unless the required features are also installed.
Features:
.NET Framework 3.5.1 Features
.NET Framework 3.5.1
Description:
Microsoft .NET Framework 3.5.1 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
Add Required Features
Cancel
Why are these features required?
< Previous
Next >
Install
Cancel

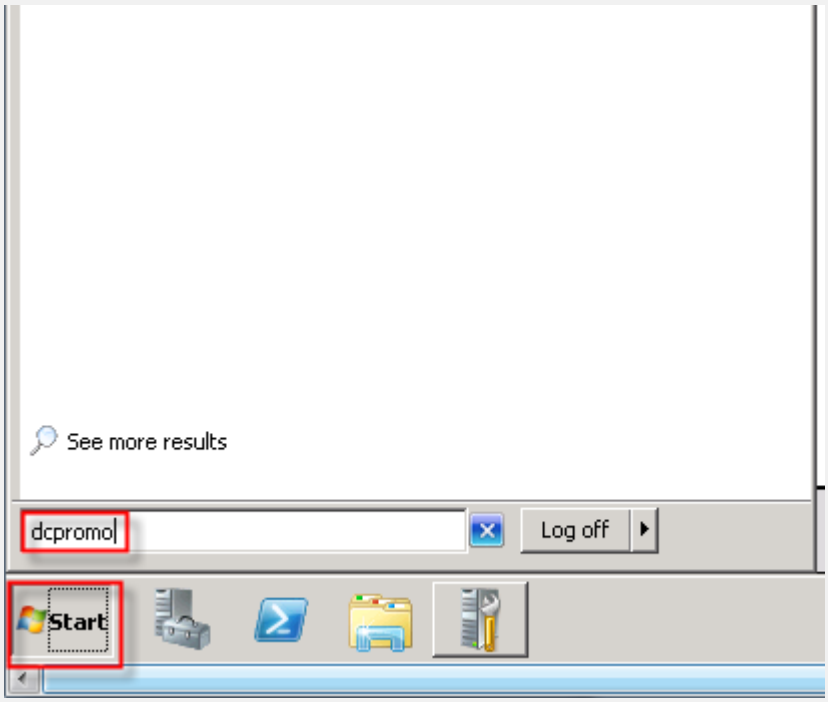


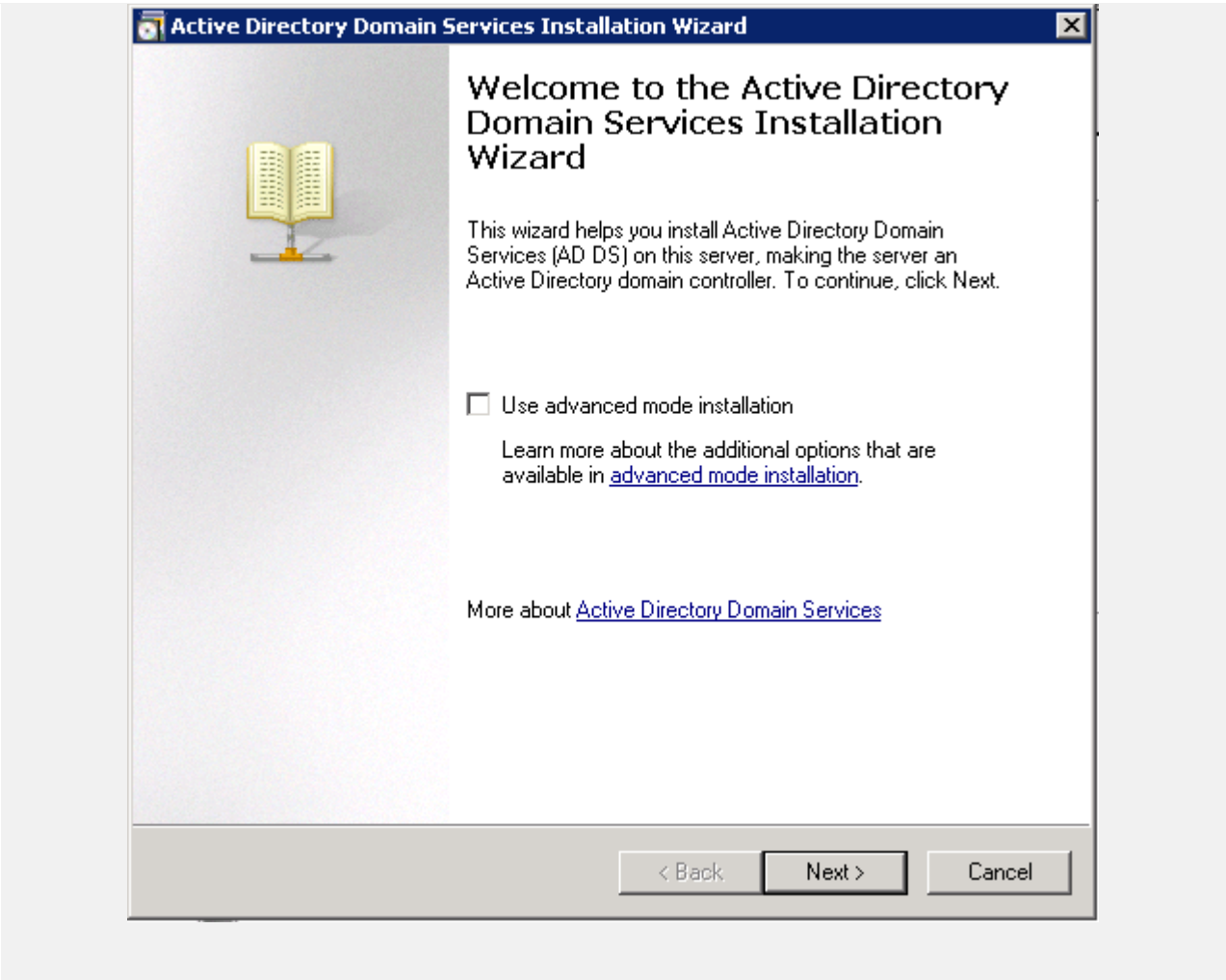
3	**Click Install.** Click Close after it finishes installing.

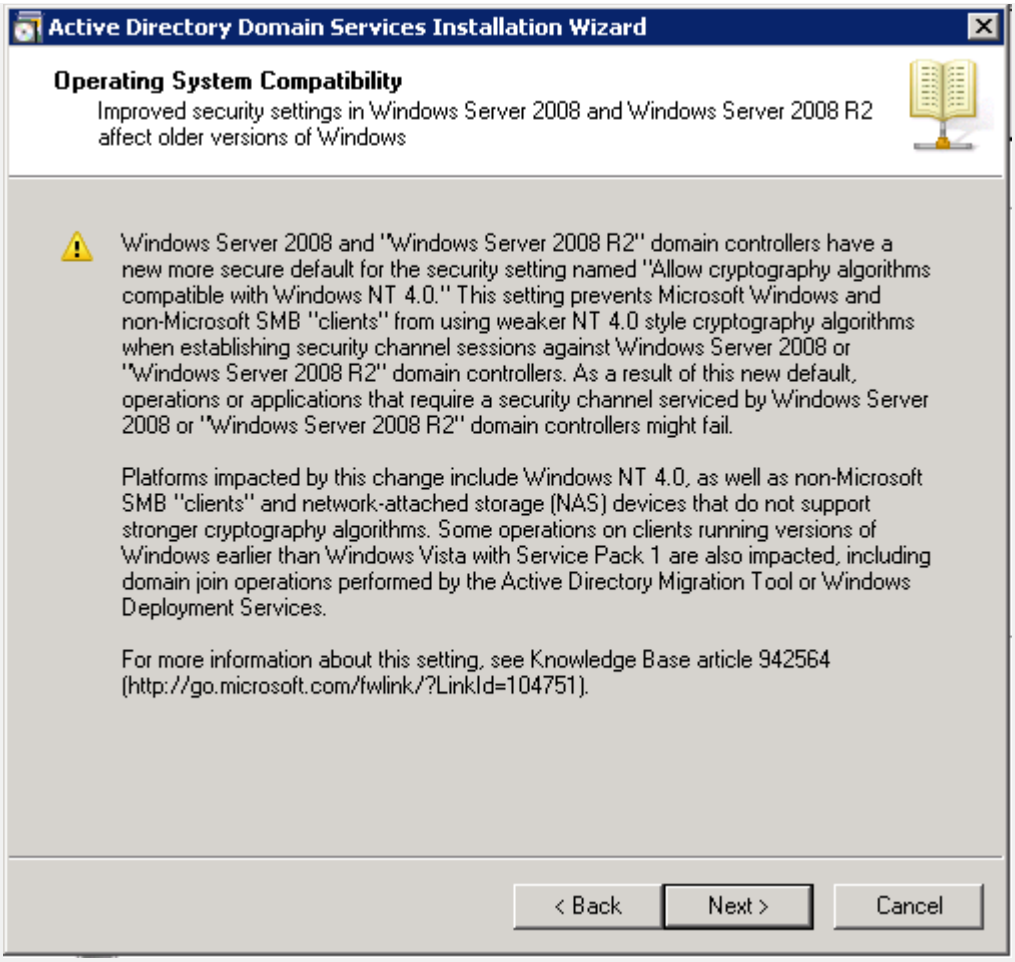

Add Roles Wizard
Confirm Installation Selections
Before You Begin
Server Roles
Active Directory Domain Services
Confirmation
Progress
Results
To install the following roles, role services, or features, click Install.
2 informational messages below
This server might need to be restarted after the installation completes.
Active Directory Domain Services
After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller.
.NET Framework 3.5.1 Features
.NET Framework 3.5.1
Print, e-mail, or save this information
< Previous
Next >
Install
Cancel



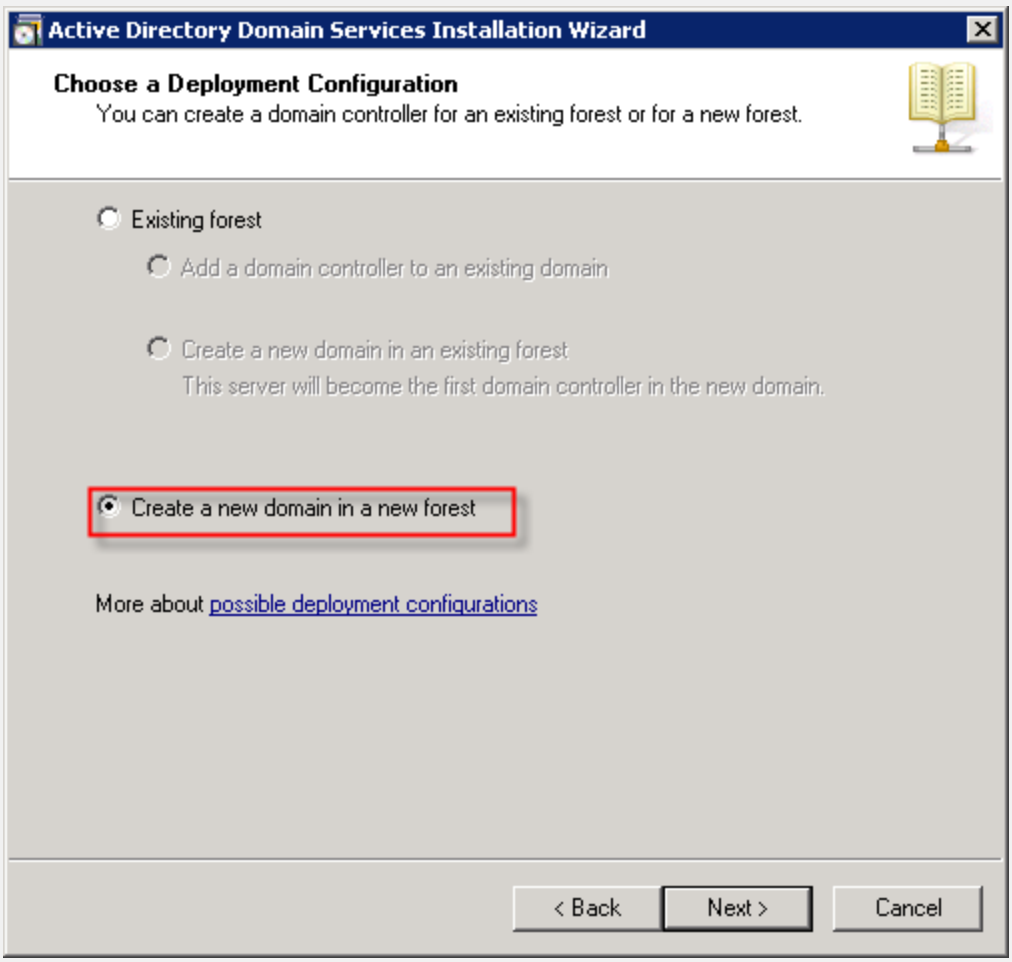
4	**Click Start. Type dcpromo in the box and press Enter. Click Next to begin the Wizard. Click Next again.**


See more results
dcpromo
Log off
Start

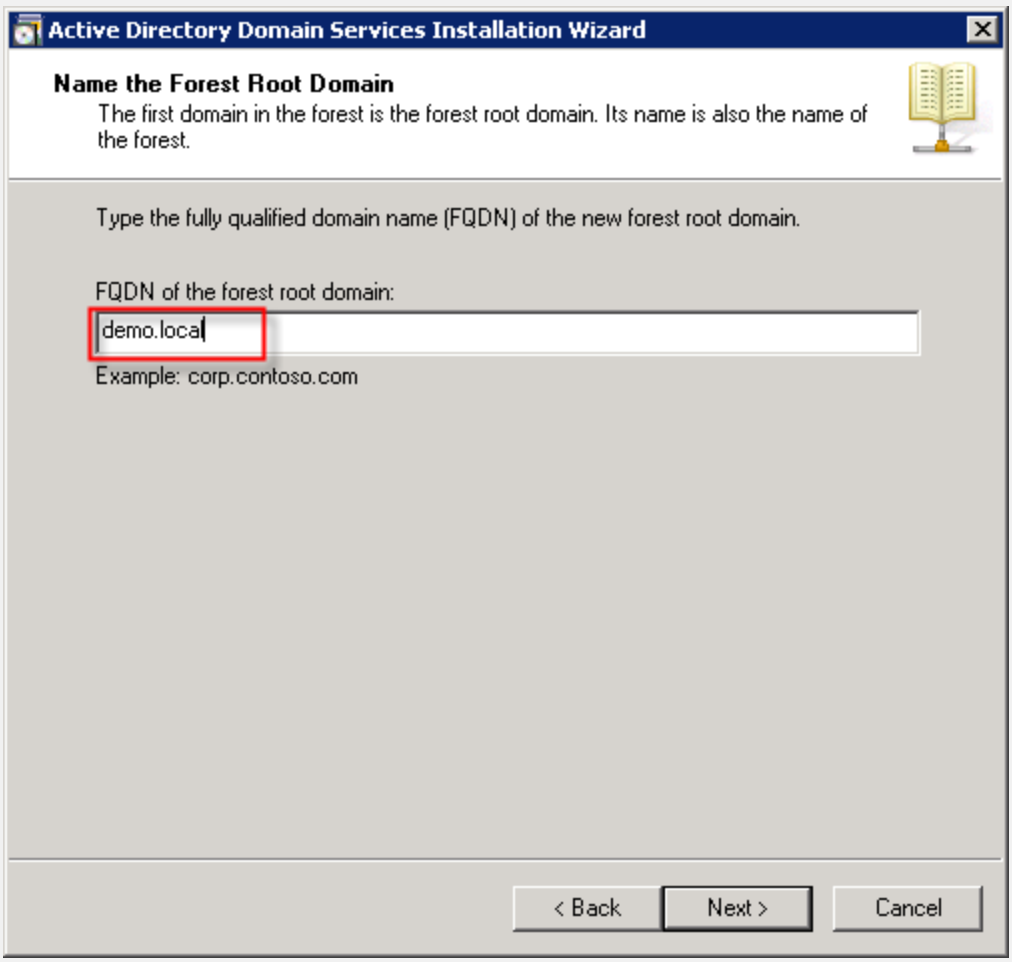

Active Directory Domain Services Installation Wizard
Welcome to the Active Directory Domain Services Installation Wizard
This wizard helps you install Active Directory Domain Services (AD DS) on this server, making the server an Active Directory domain controller. To continue, click Next.
Use advanced mode installation
Learn more about the additional options that are available in advanced mode installation.
More about Active Directory Domain Services
< Back
Next >
Cancel



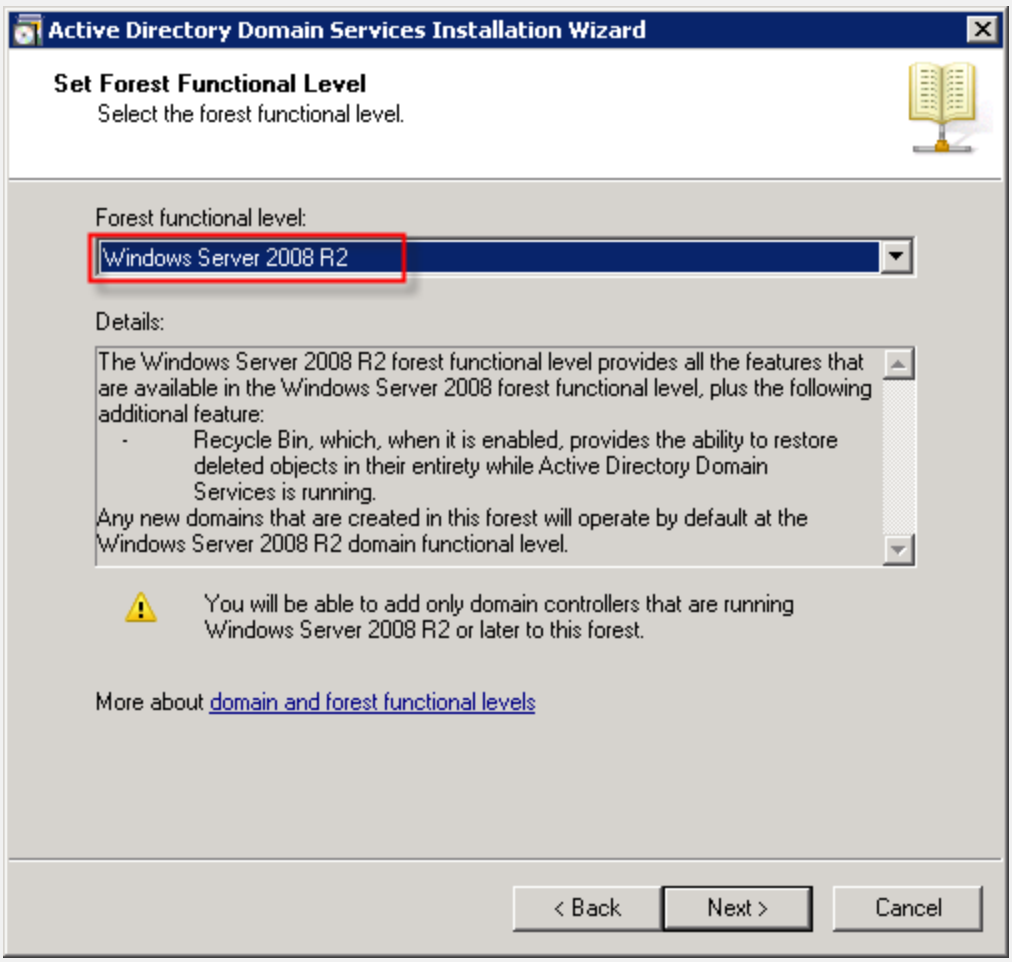
5	**Select Create a new domain in a new forest. Click Next.**



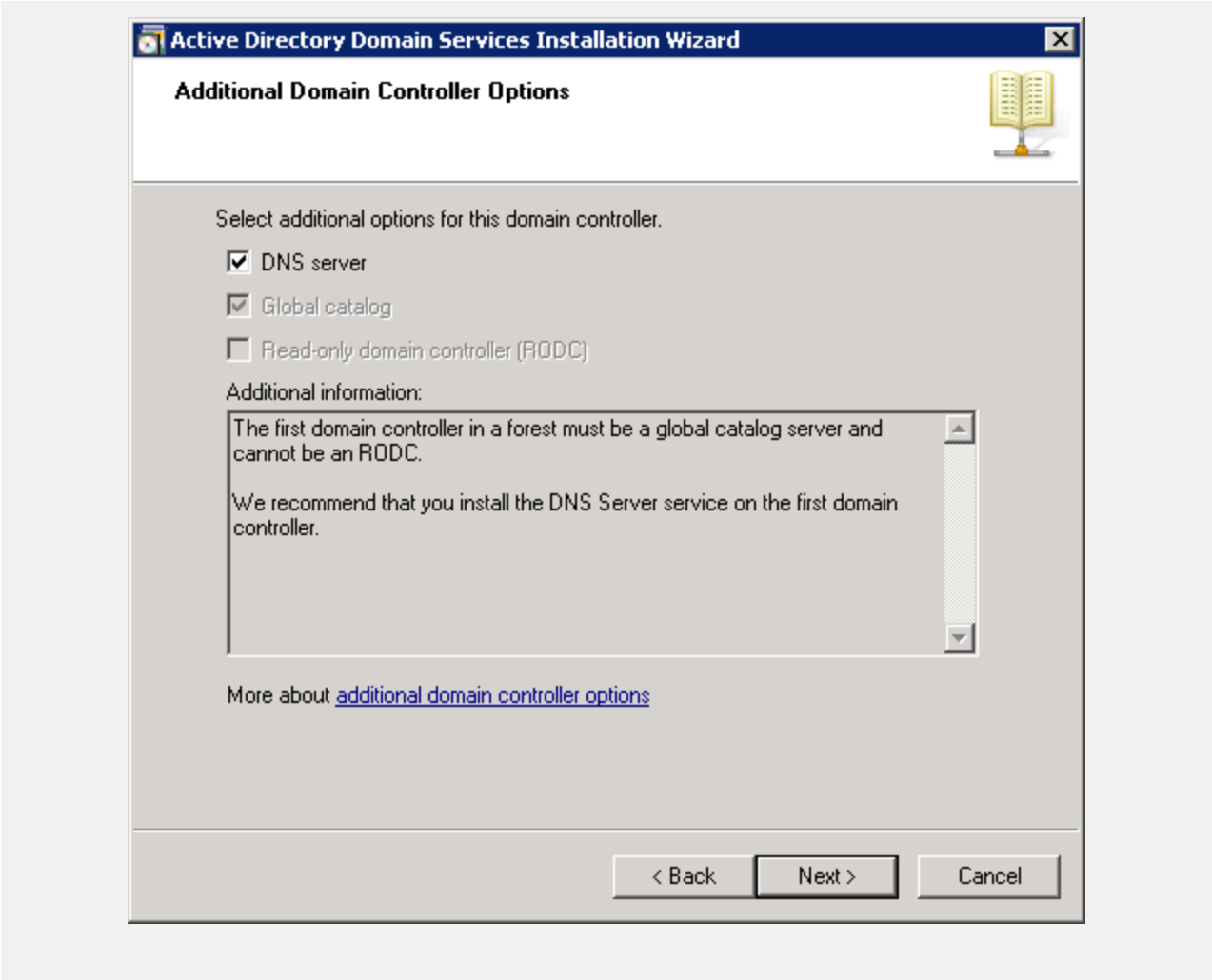
6	**Create a domain name such as “demo.local”. Click Next.**

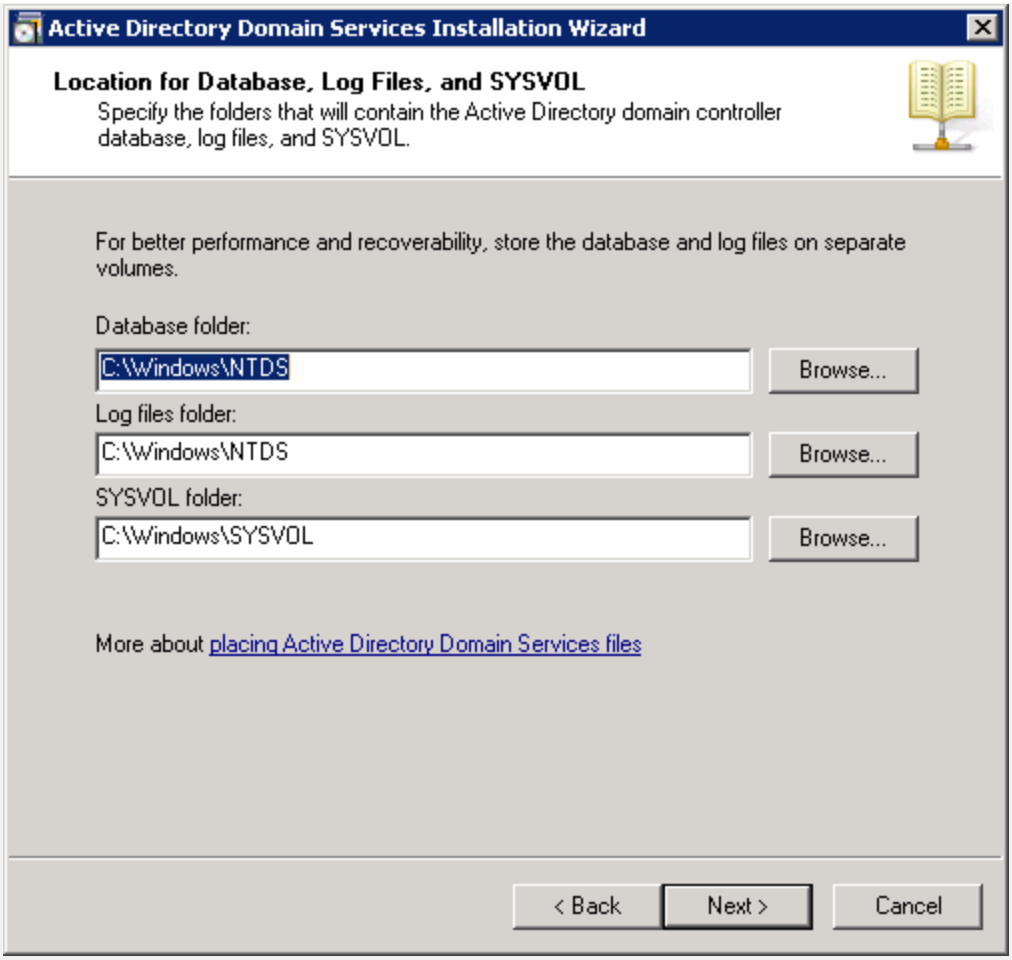


7	**Select Windows Server 2008 R2. Click Next. At the warning dialog box, click Yes.**

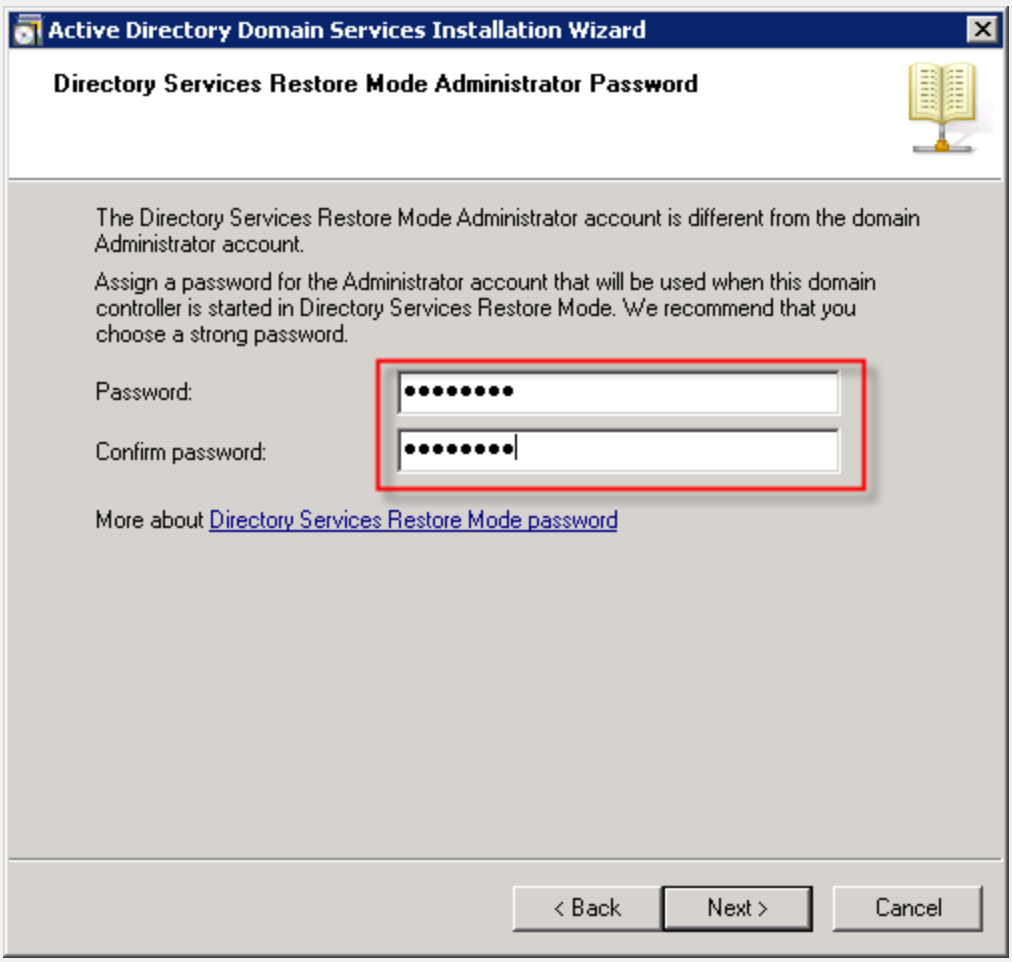


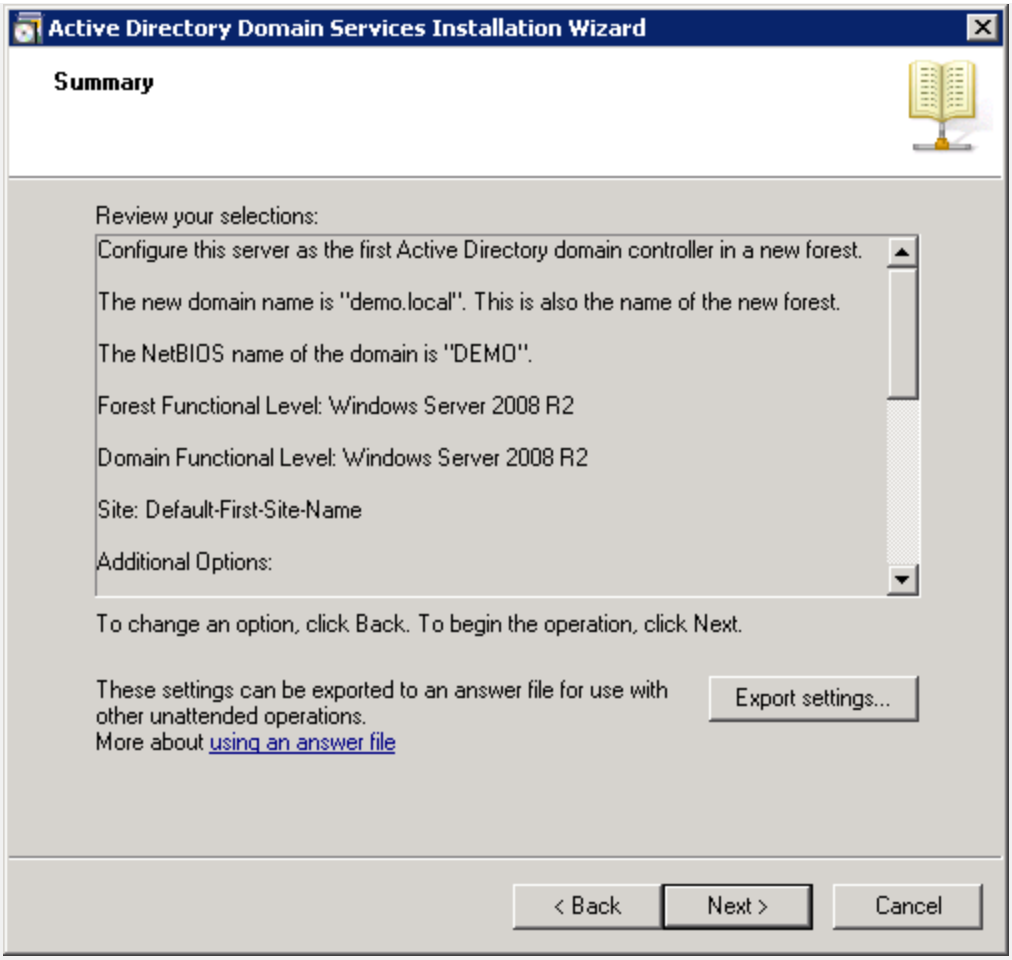
8	**Check DNS server and click Next. Click Next again.**


Active Directory Domain Services Installation Wizard
Additional Domain Controller Options
Select additional options for this domain controller.
DNS server
Global catalog
Read-only domain controller (RODC)
Additional information:
The first domain controller in a forest must be a global catalog server and cannot be an RODC.
We recommend that you install the DNS Server service on the first domain controller.
More about additional domain controller options
< Back
Next >
Cancel

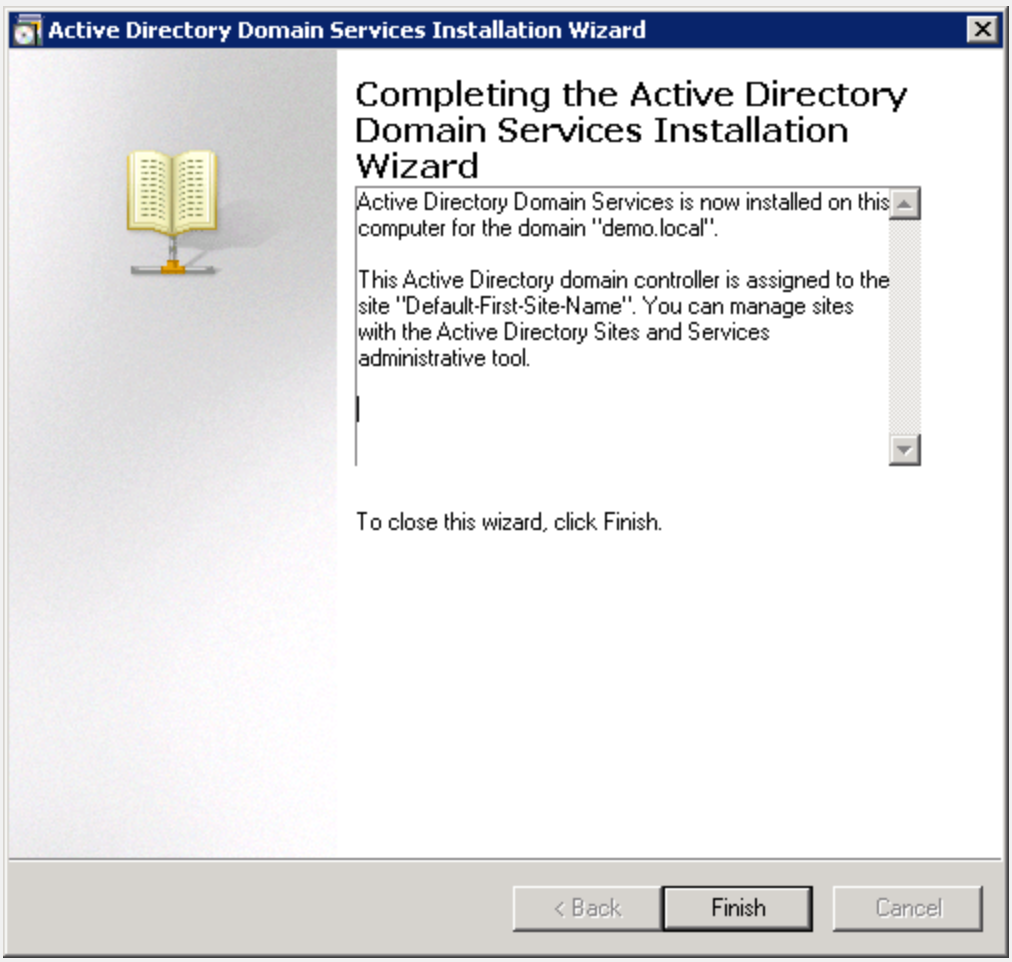


9	**Type and confirm a domain Administrator account. Click Next. Click Next again at the Summary screen.**


Active Directory Domain Services Installation Wizard
Directory Services Restore Mode Administrator Password
The Directory Services Restore Mode Administrator account is different from the domain Administrator account.
Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.
Password:
Confirm password:
More about Directory Services Restore Mode password
< Back
Next >
Cancel

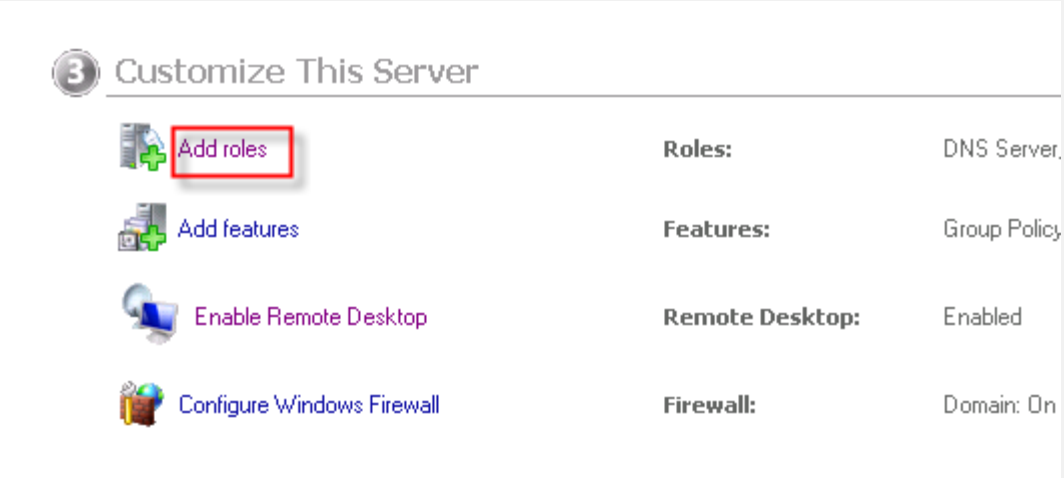


10	**After the installation completes, click Finish. Click Restart now at the prompt. After the server finishes rebooting, reconnect with Remote Desktop. Choose Use other account to login (demo\administrator), and click OK.**

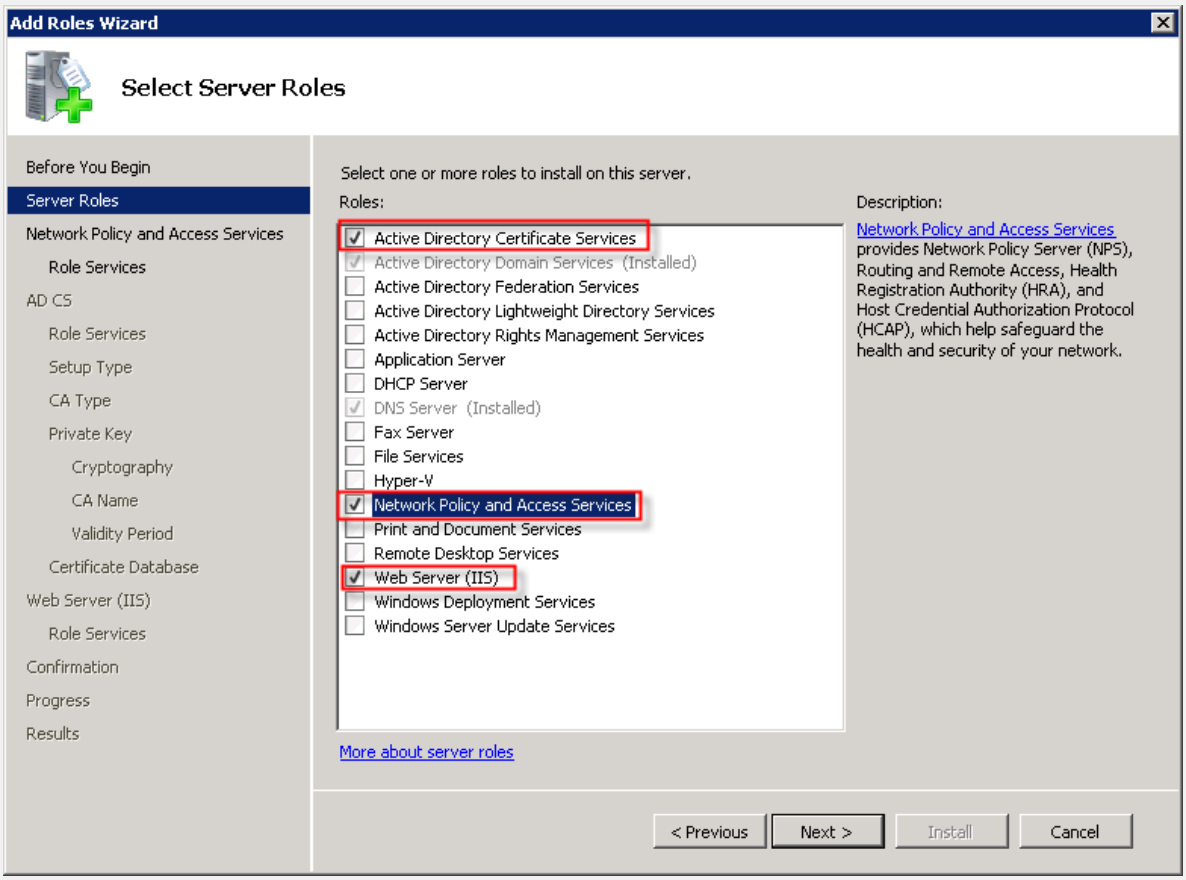


2.2.5 Add Windows Server Roles

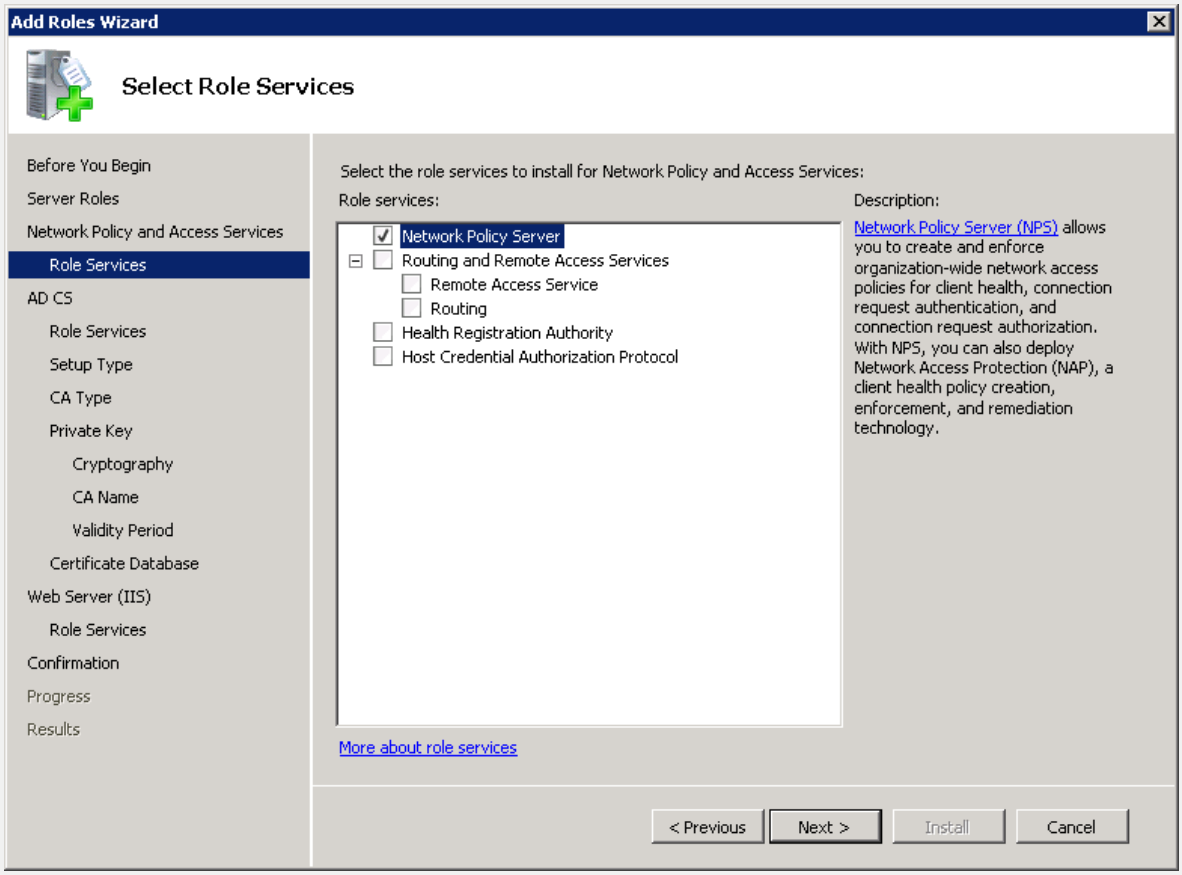
1	**In the Initial Configuration Tasks window, click Add roles. Click Next.**

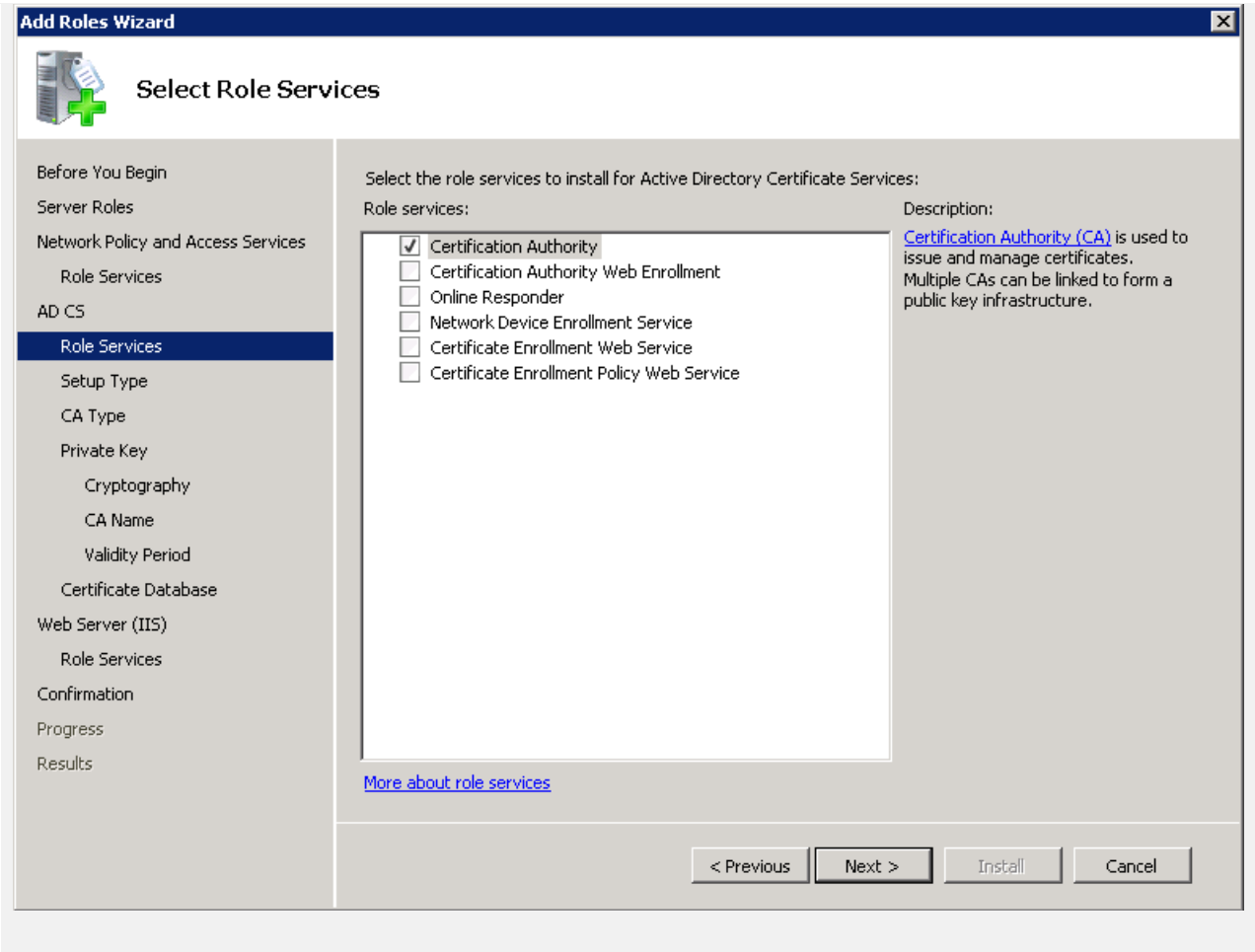


2	**Check Active Directory Certificate Services, Network Policy and Access Services, and Web Server (IIS). Click Next. Click Next again.**

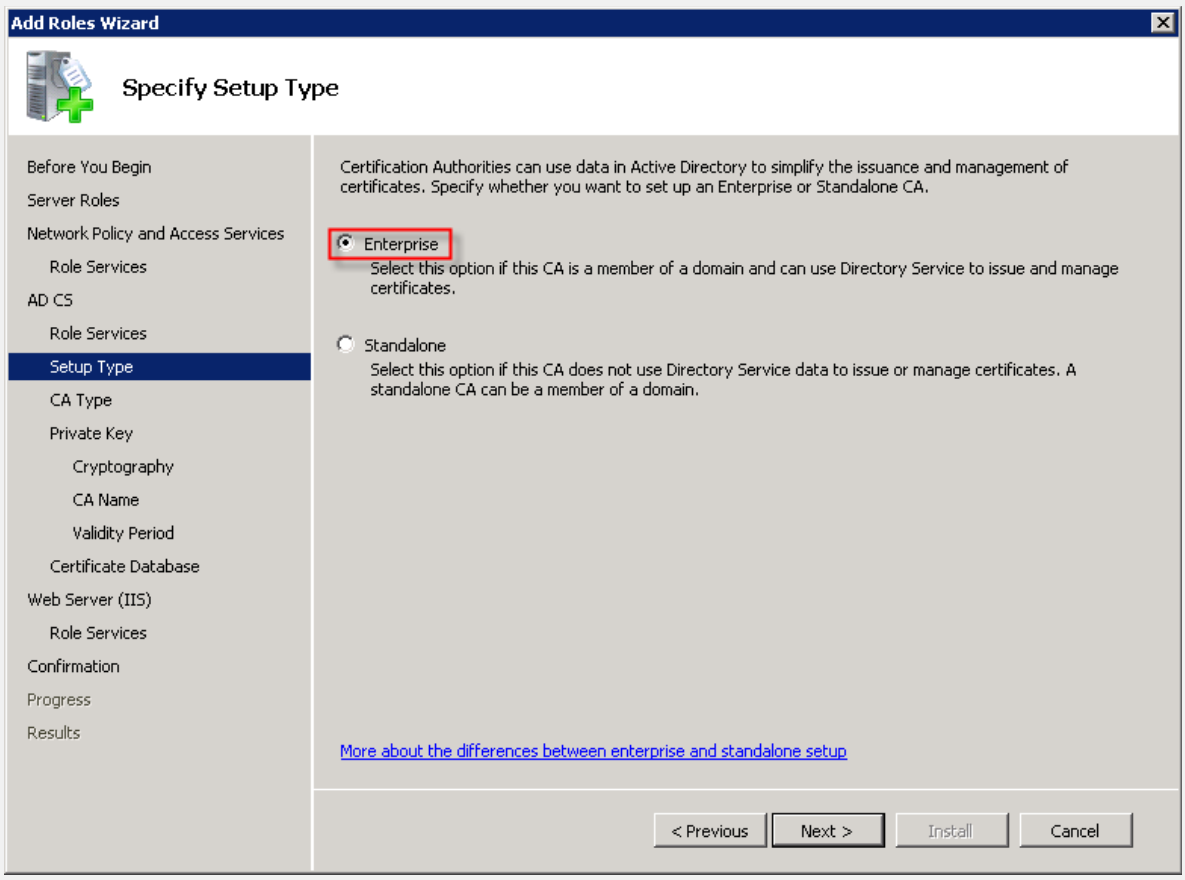


3	Check Network Policy Server. Click Next. Click Next. Click Next again.

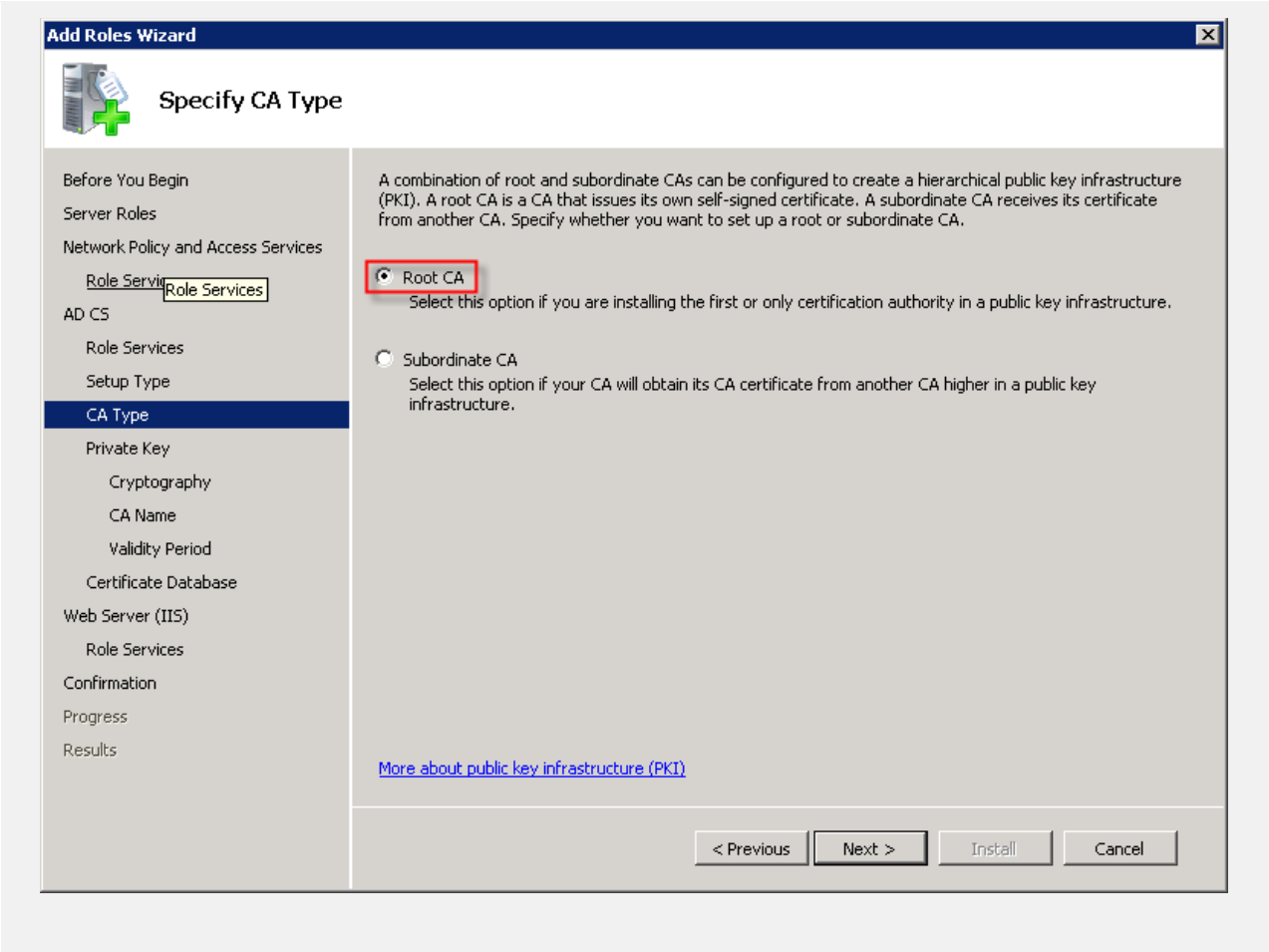




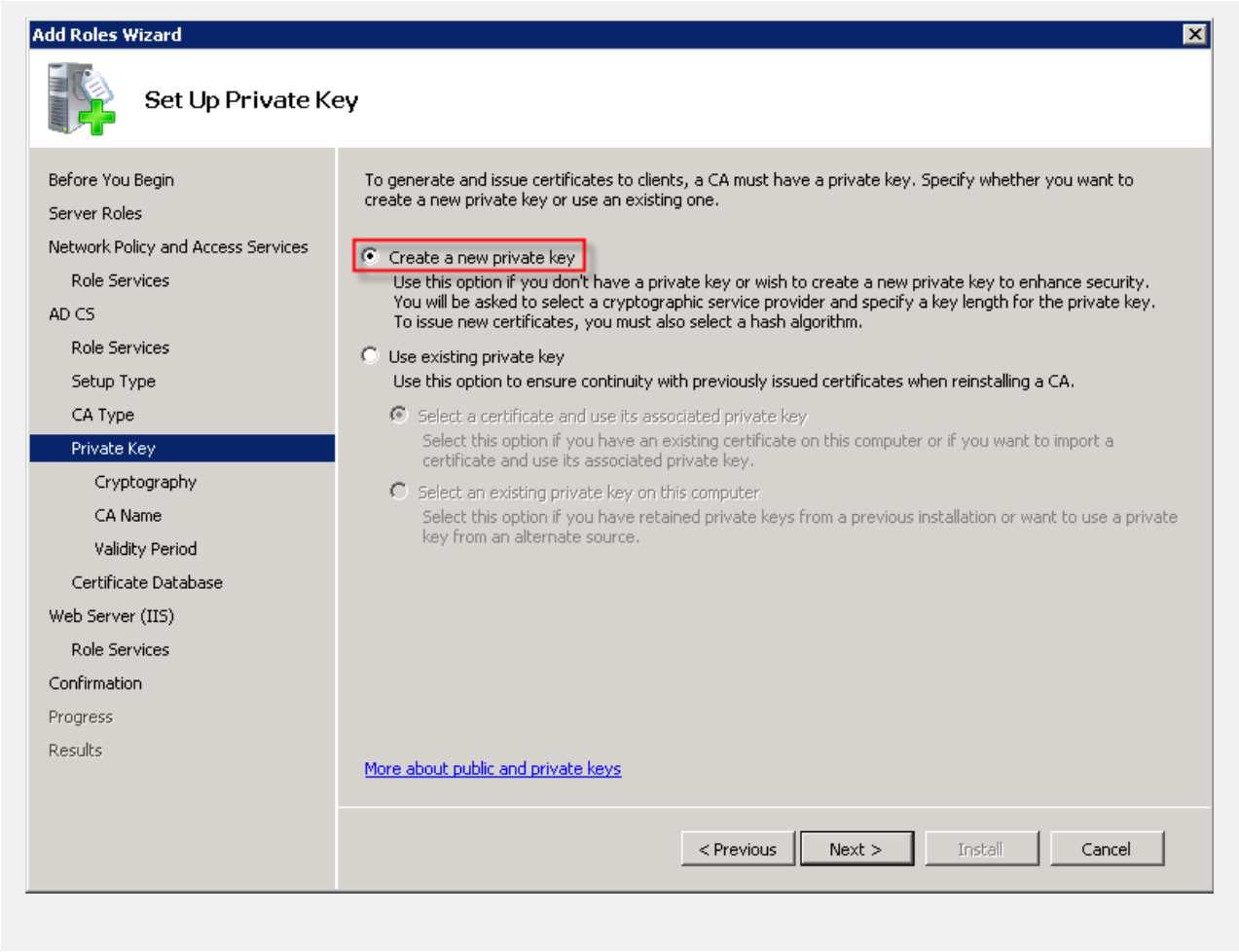
4	**Make sure Enterprise is selected. Click Next.**



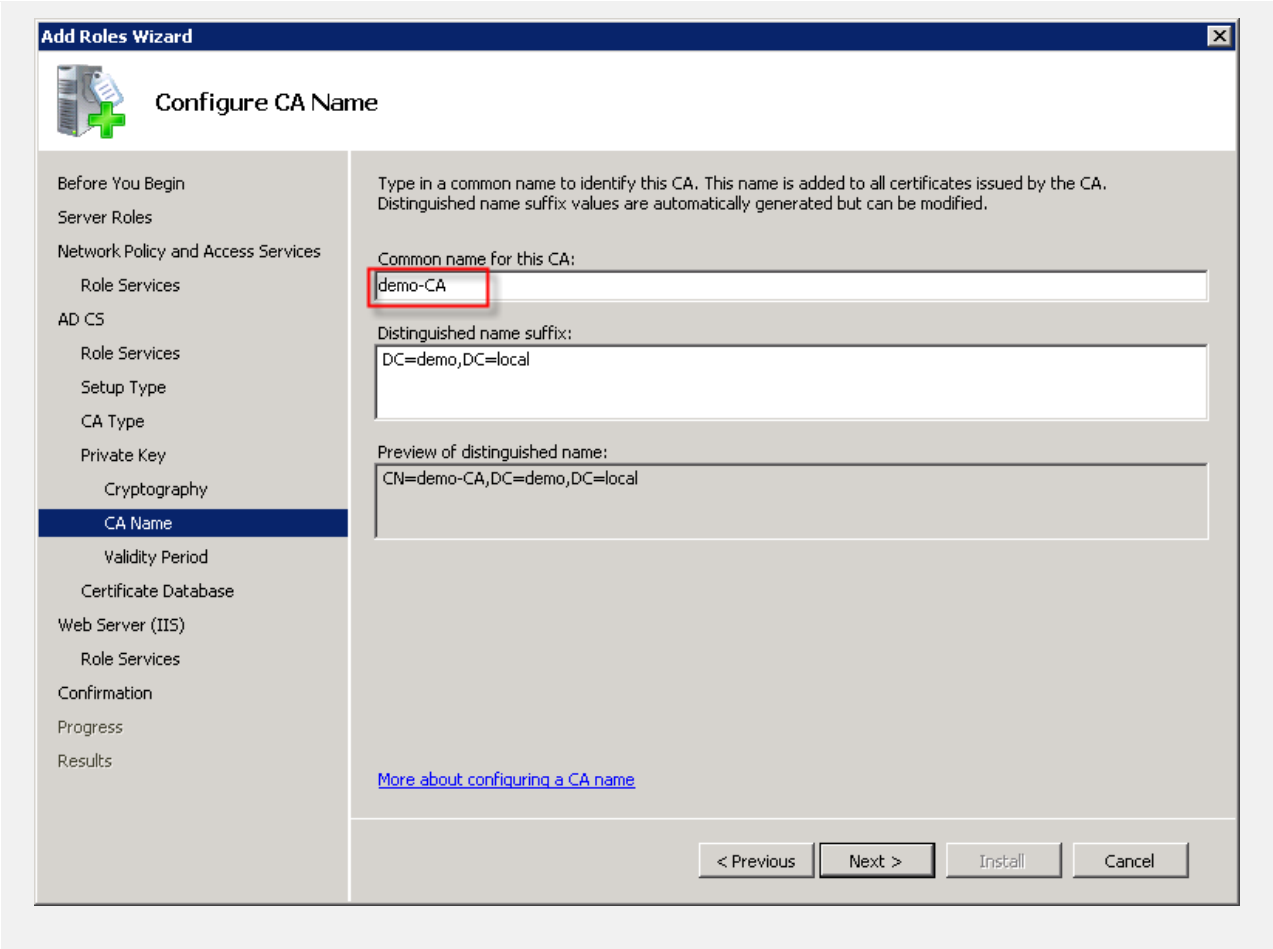
5	**Ensure Root CA is selected and Click Next.**



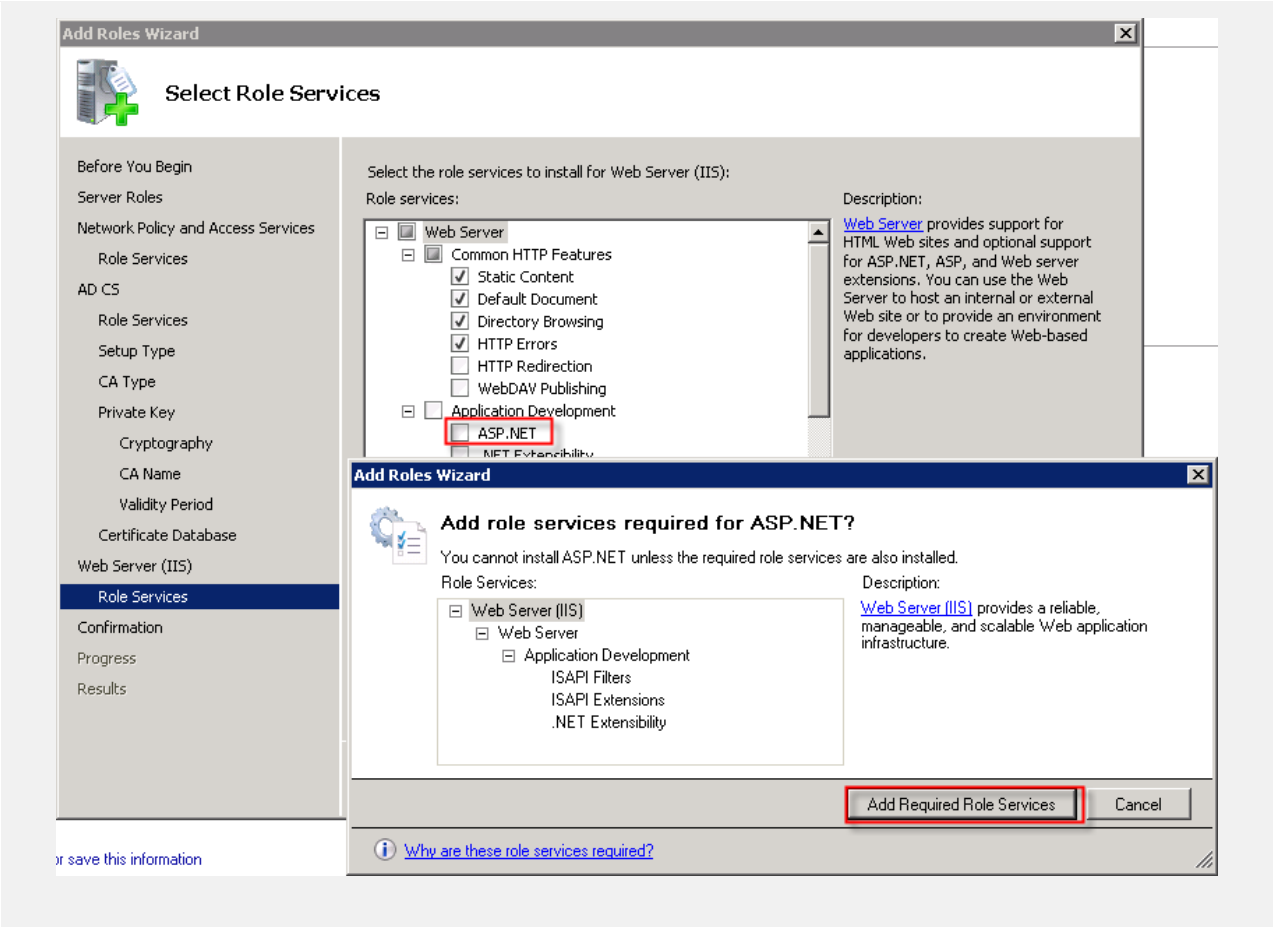
6	**Ensure Create a new private key is selected and click Next. Click Next again.**



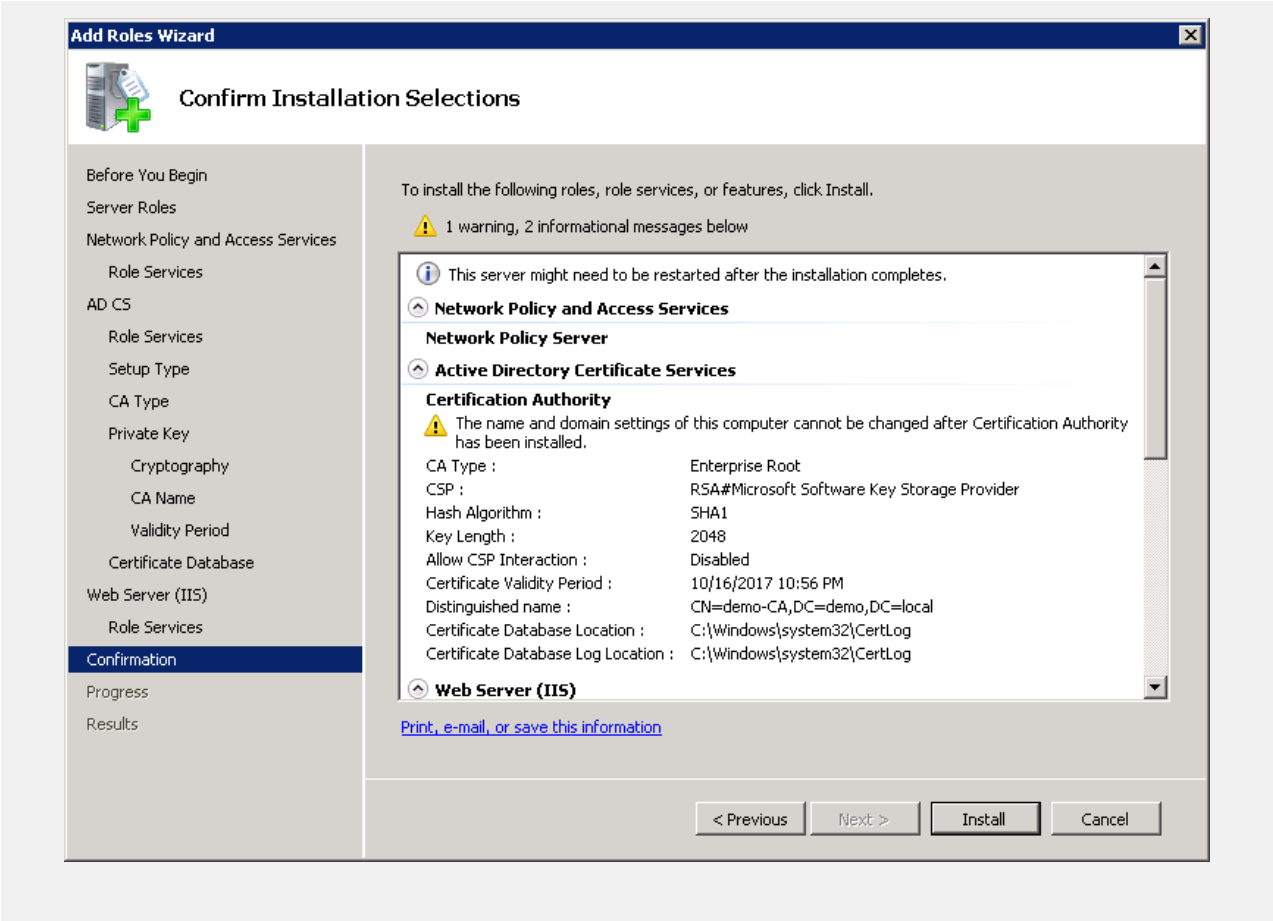
7	**Set the common name to something such as “demo-CA” and click Next. Click Next three more times through the next screens.**



8	**Check ASP.NET. When the pop up window appears, click Add Required Role Services. Click Next.**



9	**Click Install. After the installation finishes, click Close.**

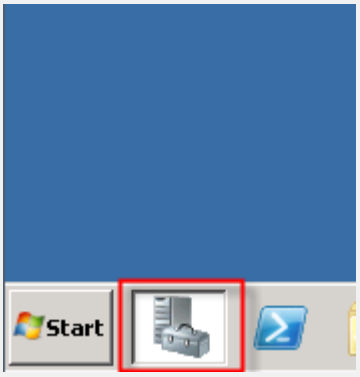


2.2.6 Configure DNS

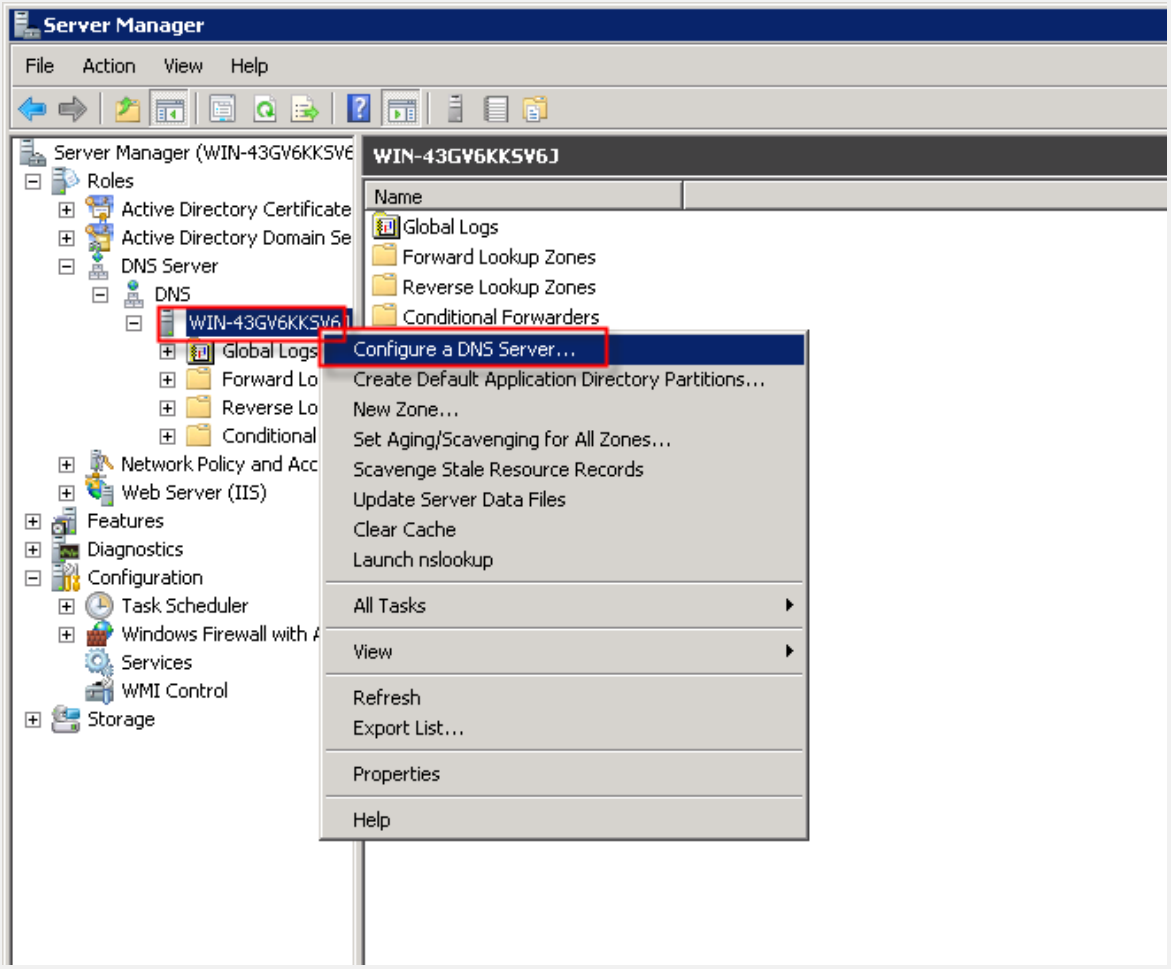
This will setup the DNS service to resolve any names in the ".local" hierarchy and forward any unknown queries to other public DNS servers. This will allow use of DNS names within the lab configuration and allow the certificate hierarchy to function with minimal extra configuration, while still allowing Internet access using name resolution from public DNS servers via the forwarding service of the Windows Server.

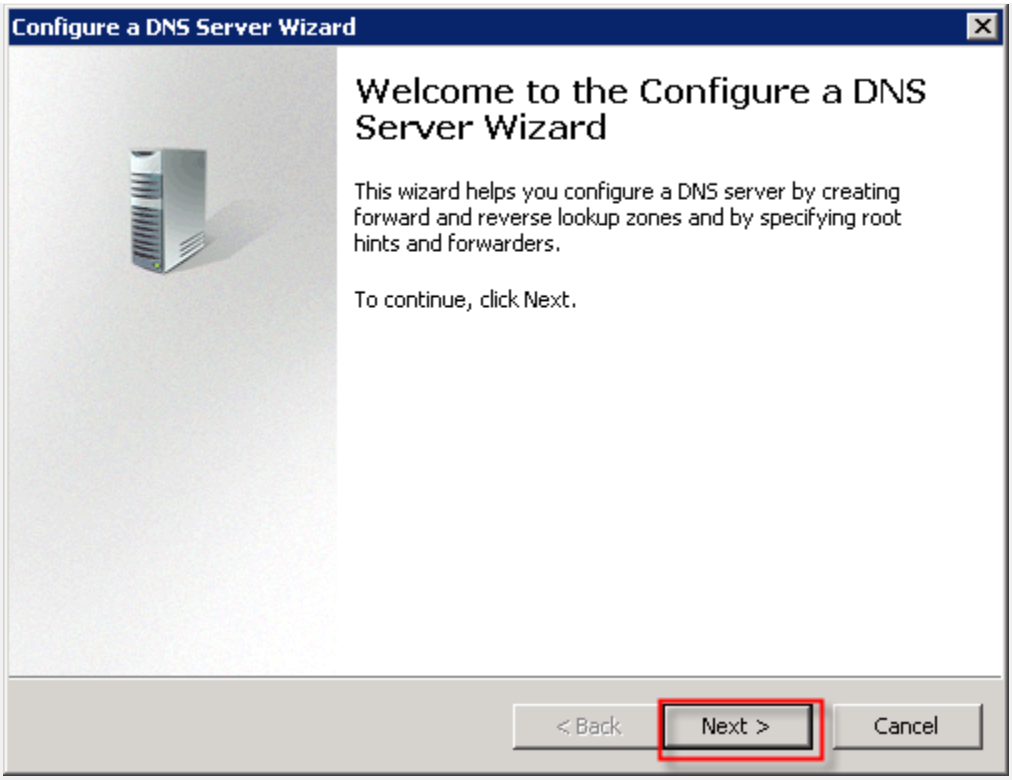
For the demo environment to work properly and clients or servers in the lab that are part of the demo, should be assigned to use this Windows Server as the DNS server. For example, if this server has an IP address of 192.168.0.115, then a DHCP server would need to be configured with the option for DNS servers set to "192.168.0.115" when assigning IP addresses to clients. Likewise any other servers should also be configured to use this server for DNS.

1	**Click on the Server Manager icon in the task bar, or alternatively, click Start, type "servermanager.msc" and press Enter.**

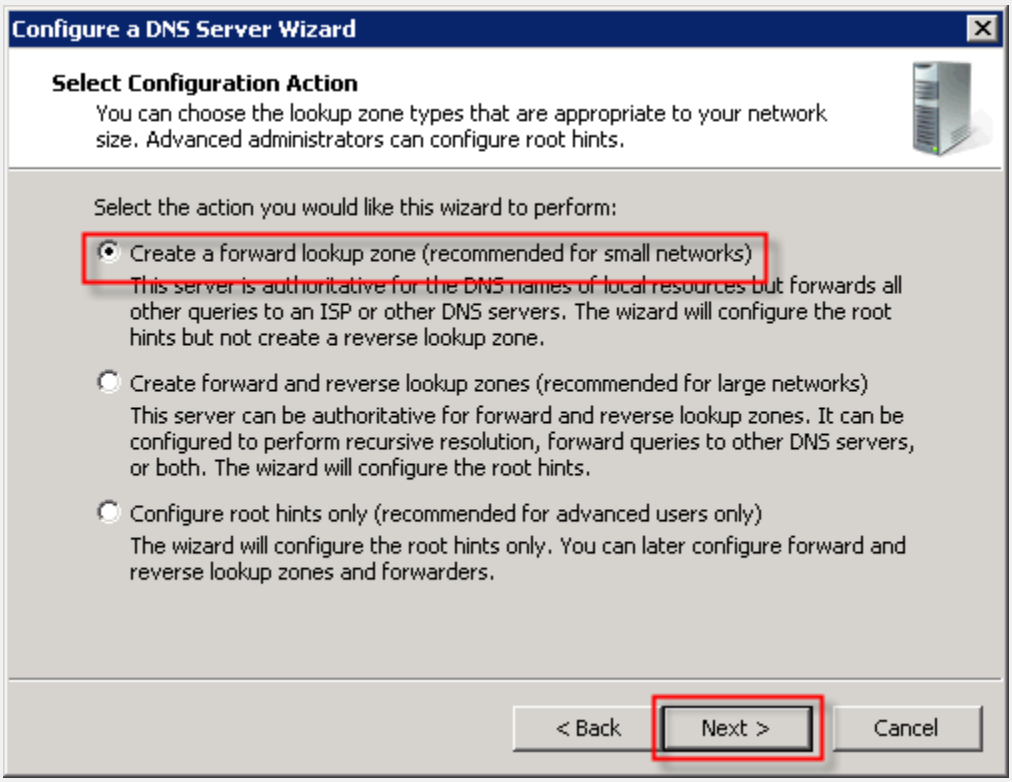


2	**Expand Roles → DNS Server → DNS. Right click on the name of the server and choose Configure a DNS Server. Click Next.**

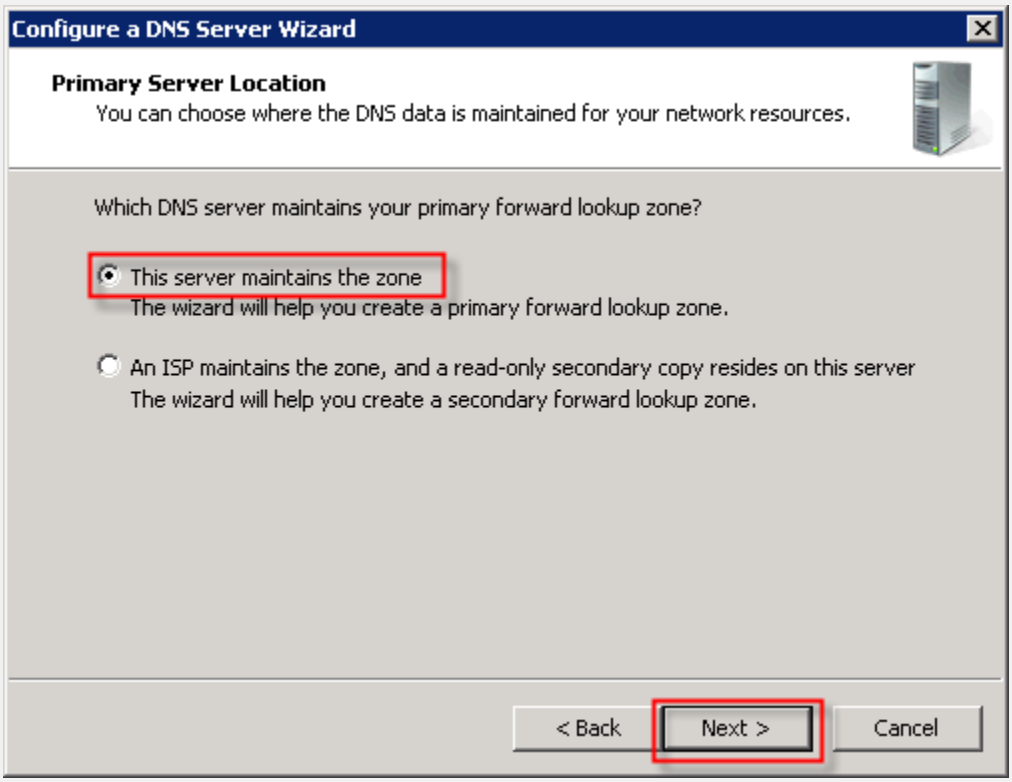




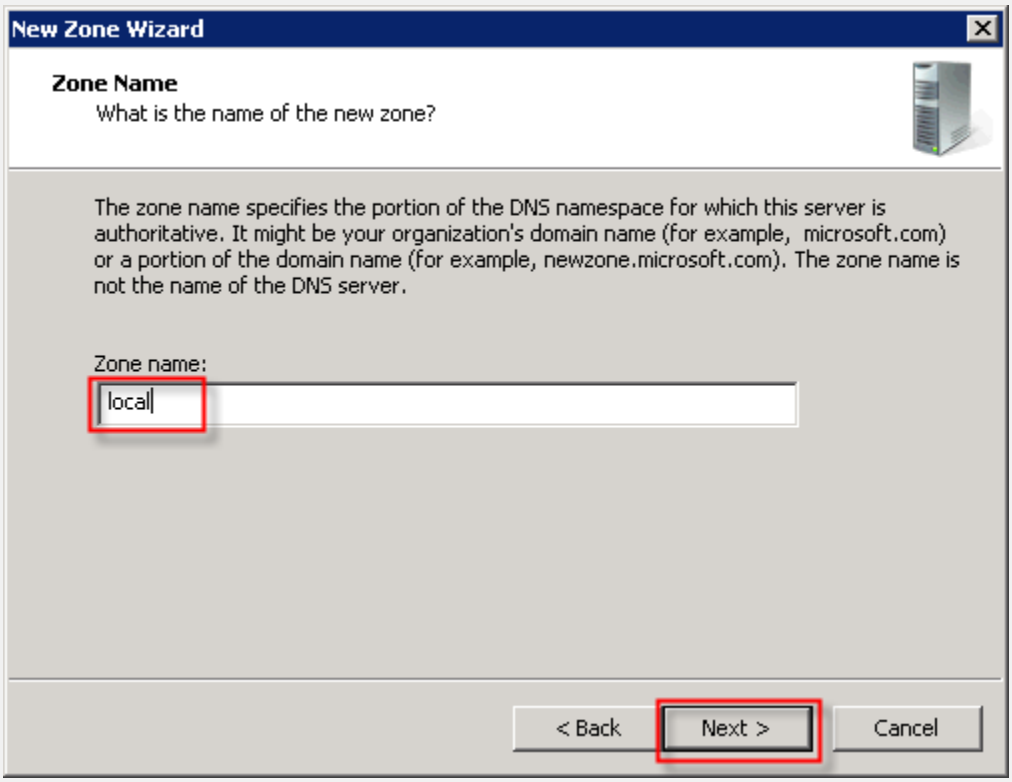
3	**Choose Create a forward lookup zone and click Next.**



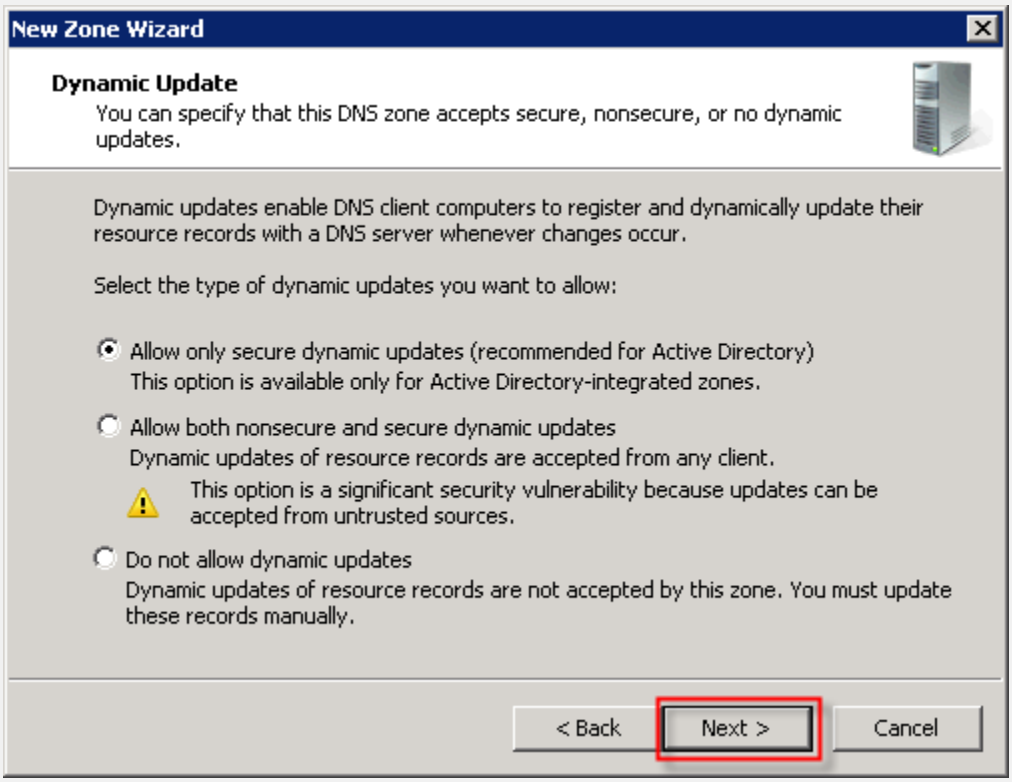
4	**Choose This server maintains the zone and click Next.**



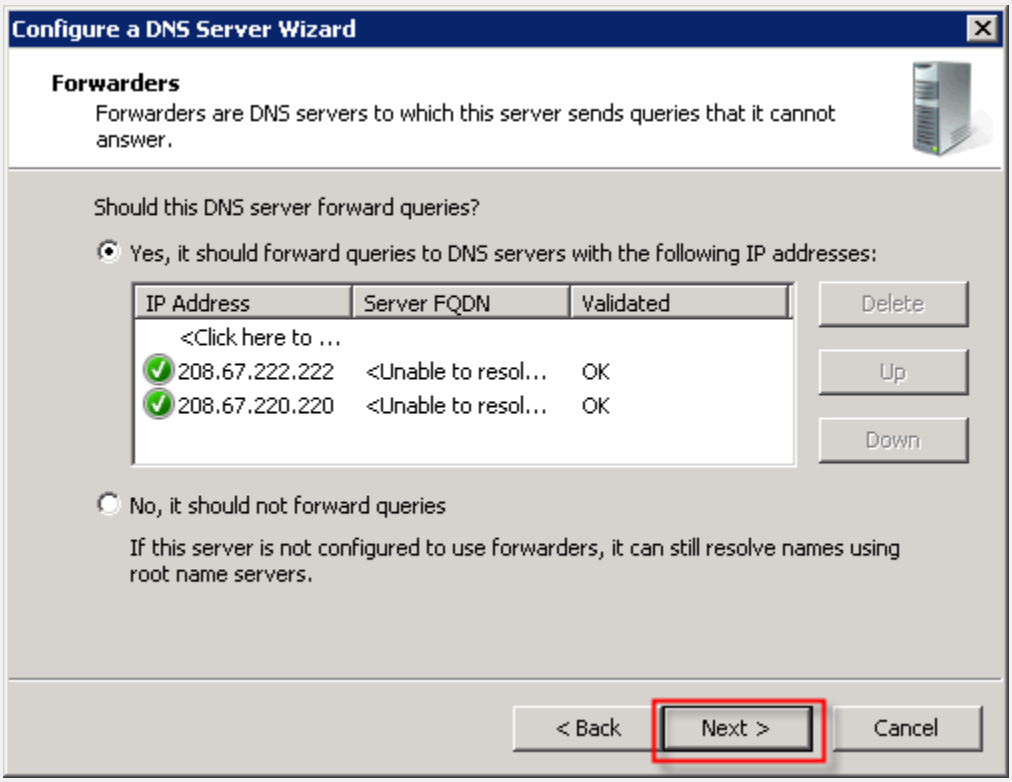
5	**Type “local” as the zone name. If you used a different DNS name for your Active Directory domain name, then enter that name instead. Click Next.**

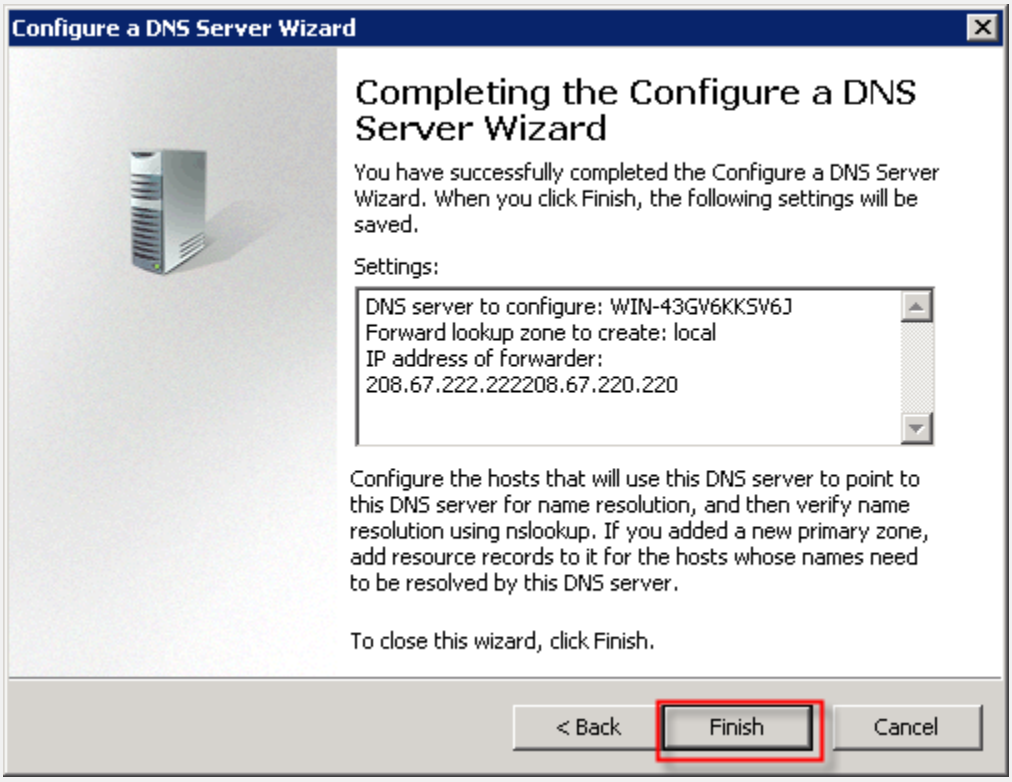

New Zone Wizard
Zone Name
What is the name of the new zone?
The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.
Zone name:
local
< Back
Next >
Cancel

6	**Click Next.**



7	**Choose Yes, it should forward queries to DNS servers with the following IP addresses. Click in the box to add your ISP's DNS server address. Shown below are Open DNS server addresses. When finished adding servers, click Next. Then click Finish.**


Configure a DNS Server Wizard
Forwarders
Forwarders are DNS servers to which this server sends queries that it cannot answer.
Should this DNS server forward queries?
Yes, it should forward queries to DNS servers with the following IP addresses:
IP Address
Server FQDN
Validated
<Click here to ...
208.67.222.222
<Unable to resol...
OK
208.67.220.220
<Unable to resol...
OK
Delete
Up
Down
No, it should not forward queries
If this server is not configured to use forwarders, it can still resolve names using root name servers.
< Back
Next >
Cancel

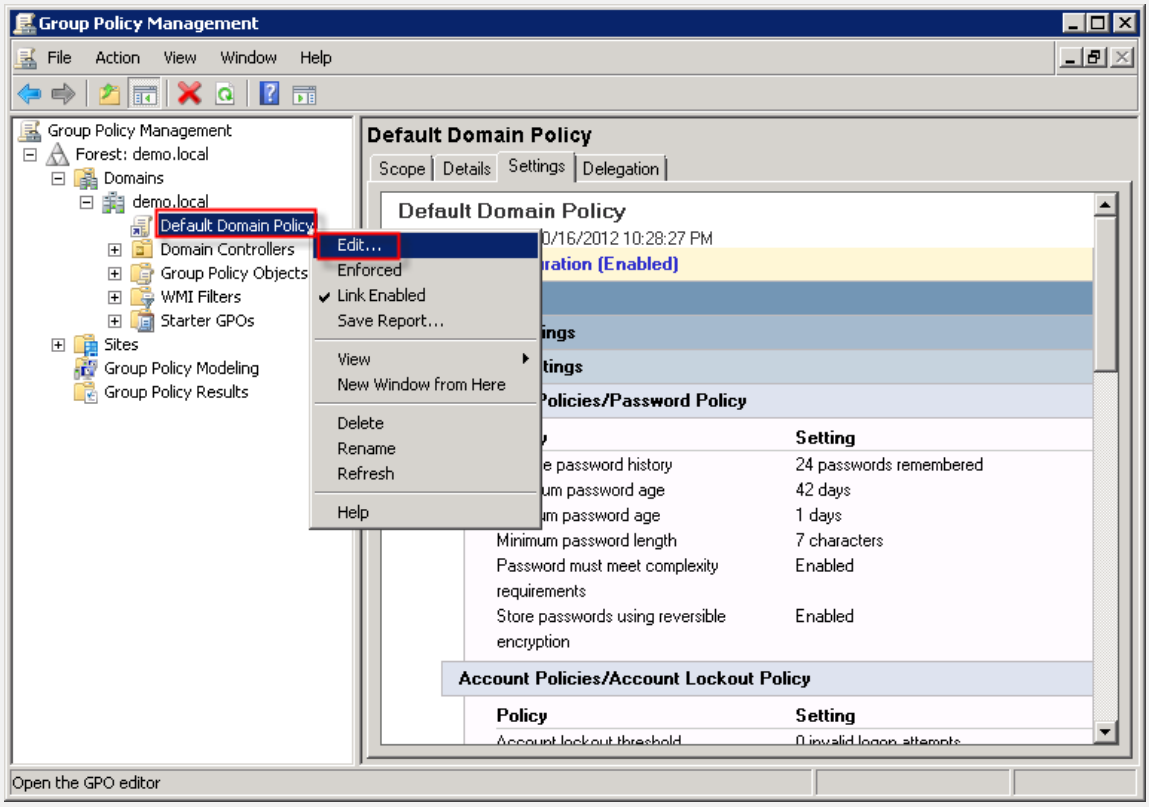

Configure a DNS Server Wizard
Completing the Configure a DNS Server Wizard
You have successfully completed the Configure a DNS Server Wizard. When you click Finish, the following settings will be saved.
Settings:
DNS server to configure: WIN-43GV6KKSV6J
Forward lookup zone to create: local
IP address of forwarder:
208.67.222.222208.67.220.220
Configure the hosts that will use this DNS server to point to this DNS server for name resolution, and then verify name resolution using nslookup. If you added a new primary zone, add resource records to it for the hosts whose names need to be resolved by this DNS server.
To close this wizard, click Finish.
< Back
Finish
Cancel

2.2.7 Configure Windows Server Password Policy

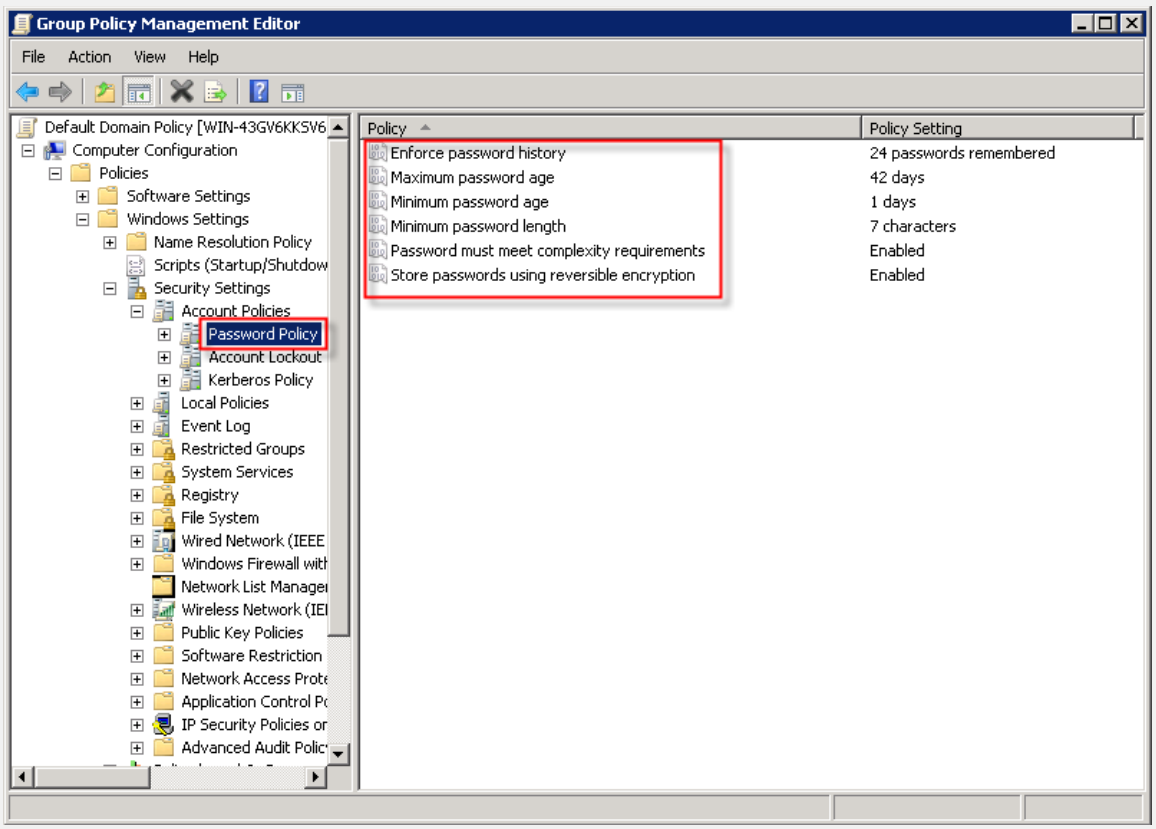
You may want to edit the password policy for this demo server to eliminate complexity and expiration limits on passwords. This will make it simpler when creating test accounts in Active Directory. This is not a required step.

Note: Making changes to the group policy may take a few minutes to take effect because of Active Directory synchronization. If the password policy does not appear to have taken effect after steps 1-2 are performed, then follow step 3.

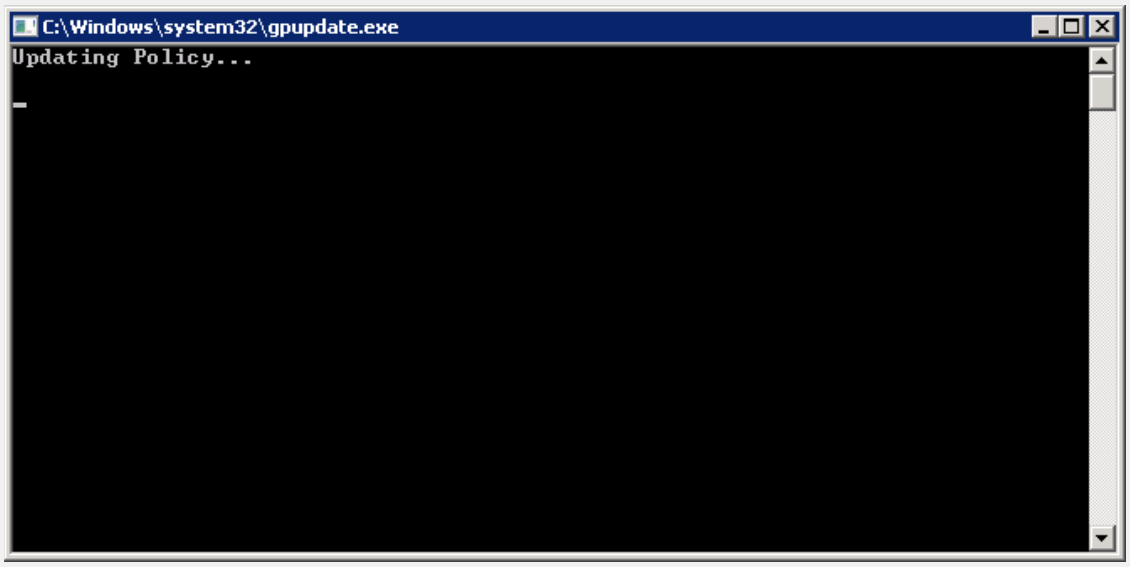
1 **Click Start, type gpmc.msc and press Enter. Expand the Forest: <domain name> → Domains → <domain name>, then right-click on Default Domain Policy and select Edit.**



2 **Expand Computer Configuration → Policies → Windows Settings → Security Settings → Account Polices, and then click on Password Policy. Change each parameter on the right side to your preferences, by double-clicking each item and changing the values. Note that unchecking Define this policy setting may not actually change the enforced value. You should explicitly set each parameter.**



3 **After each parameter is unset, close the Editor window and close the Group Policy Management window. Click Start and type “gpupdate /force” and press Enter.**



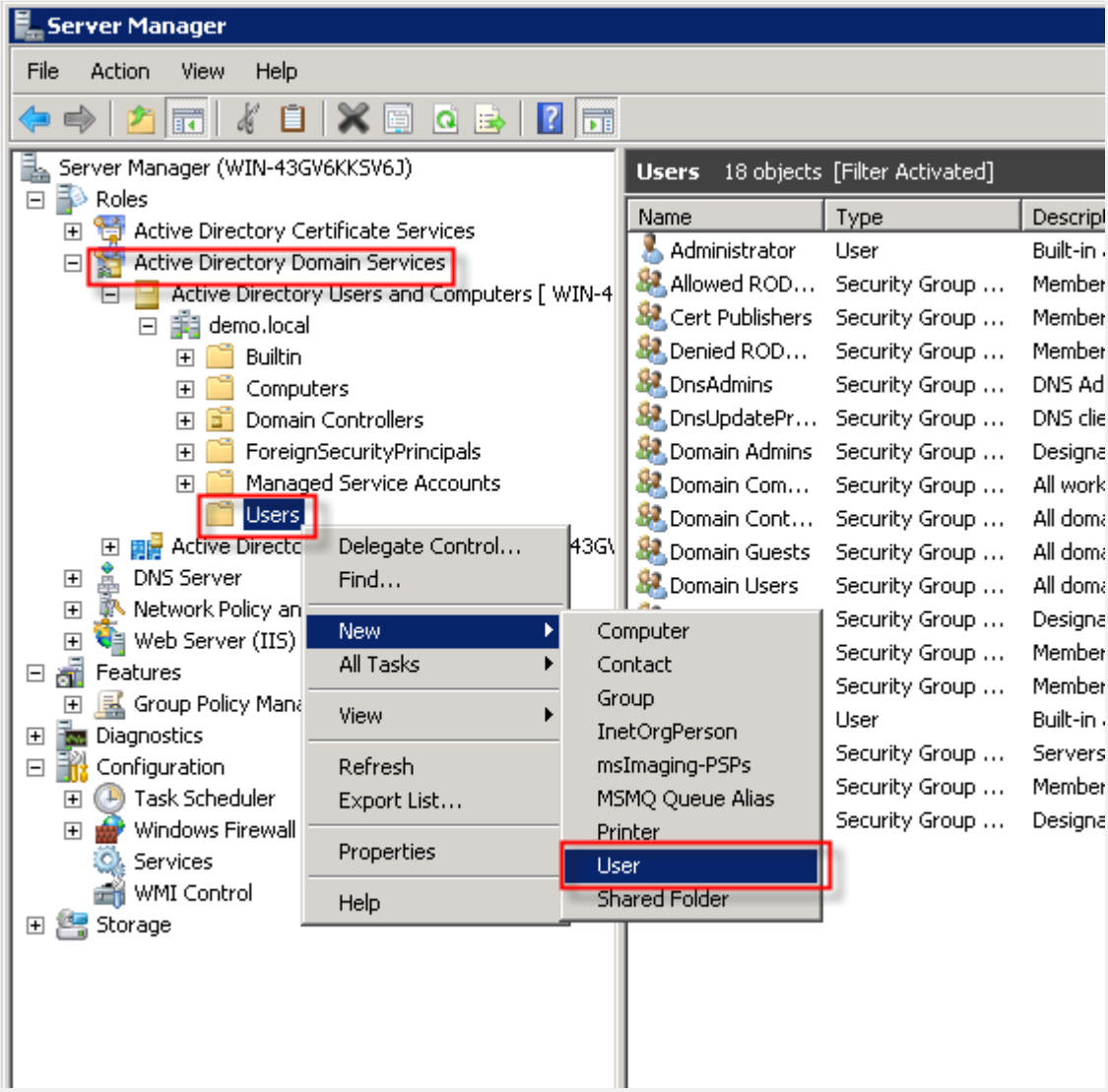
2.2.8 Configure User Accounts in Active Directory

You will need to add a few user accounts and groups for testing onboarding and certificate generation. The group will be used for checking permission to onboard. In a future step, you will configure the enrollment server which has a default regex that matches the group string “BYOD APP*”. The group name below is deliberately chosen to match this regex, so that users that are group members will be allowed to continue to the onboarding a BYOD step. You should configure a user that is a member of this group as well as a user that is not a member in order to demonstrate users that are denied permission to onboard as well as users that are permitted.

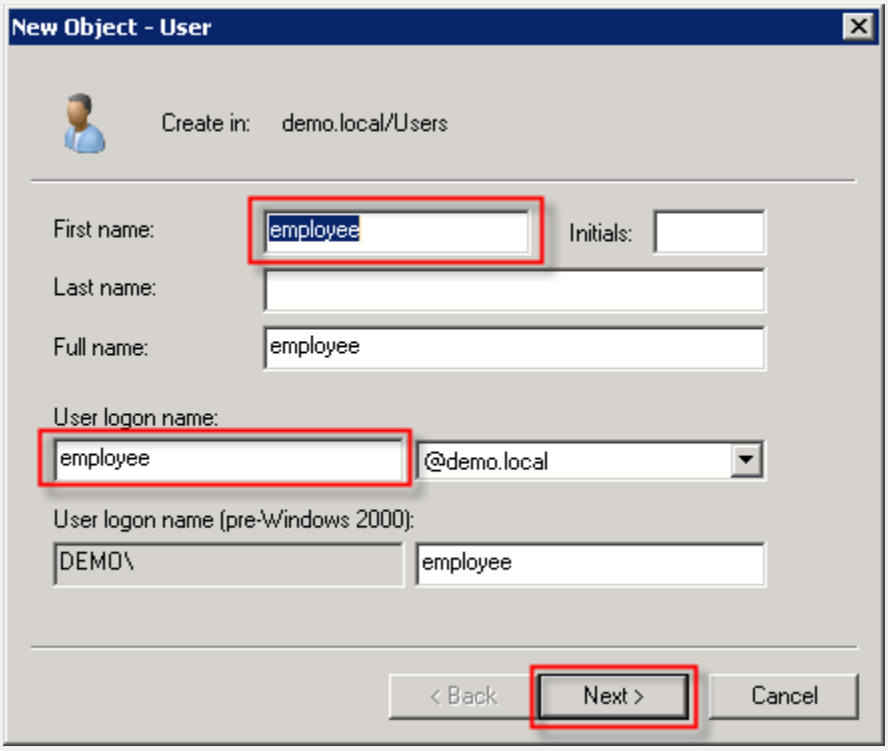
Note: Step 7 below shows adding the user to the “Print Operators” group. This is to avoid an issue that arises in lab environments that does not typically occur in a customer deployment. The Secure Access Microsoft Certificate Integration Module requires a local login privilege on the IIS server it is installed on. Domain users have this permission by default on most non-Domain Controllers. But in the lab, all services are running on the same virtual server, including both Domain Controller and IIS. By default, Domain Controllers have modified server permissions that restrict local login privileges to Domain users. The easiest way to resolve this without granting Administrator privileges to users is to make them a member of the Print Operators group. By doing so, this will avoid the issue where employees cannot get a certificate when onboarding their BYOD.

This step of adding the users to the Print Operators group is not necessary when the IIS server that is hosting the Integration Module is not on a server that is also a Domain Controller.

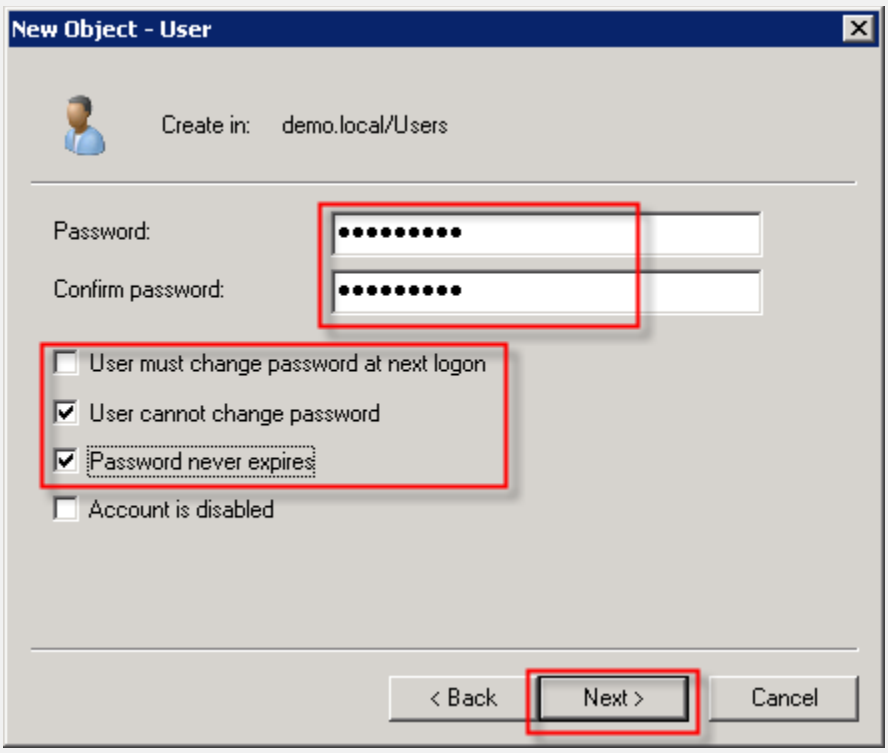
1	**From Server Manager, expand Roles → Active Directory Domain Services → Active Directory Users and Computers → <domain_name>, and then right click on Users and select New → User.**

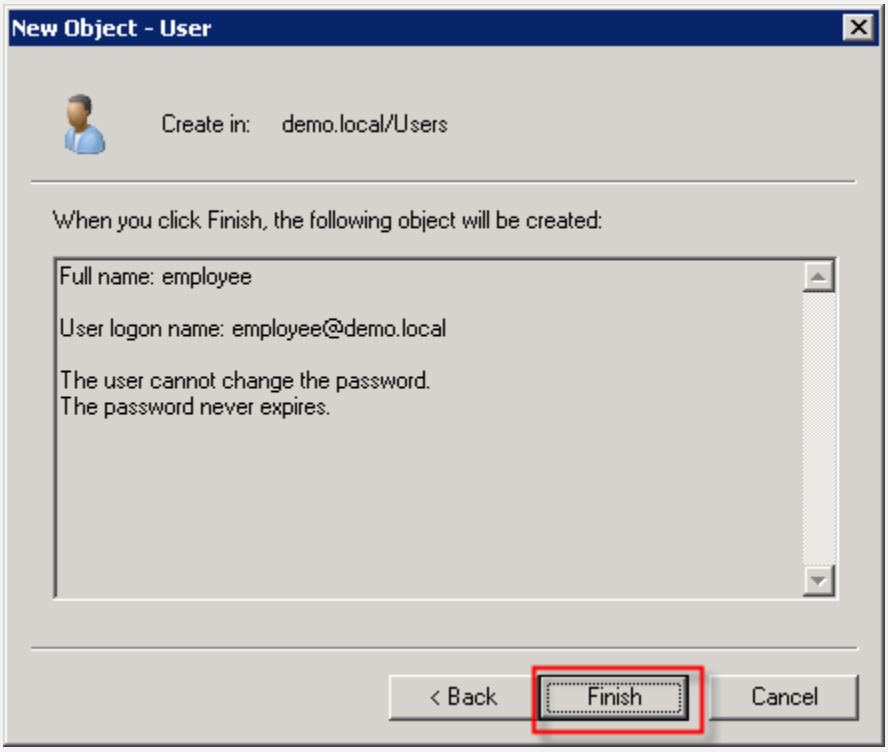


2	Type “employee” or some other name. Click Next.

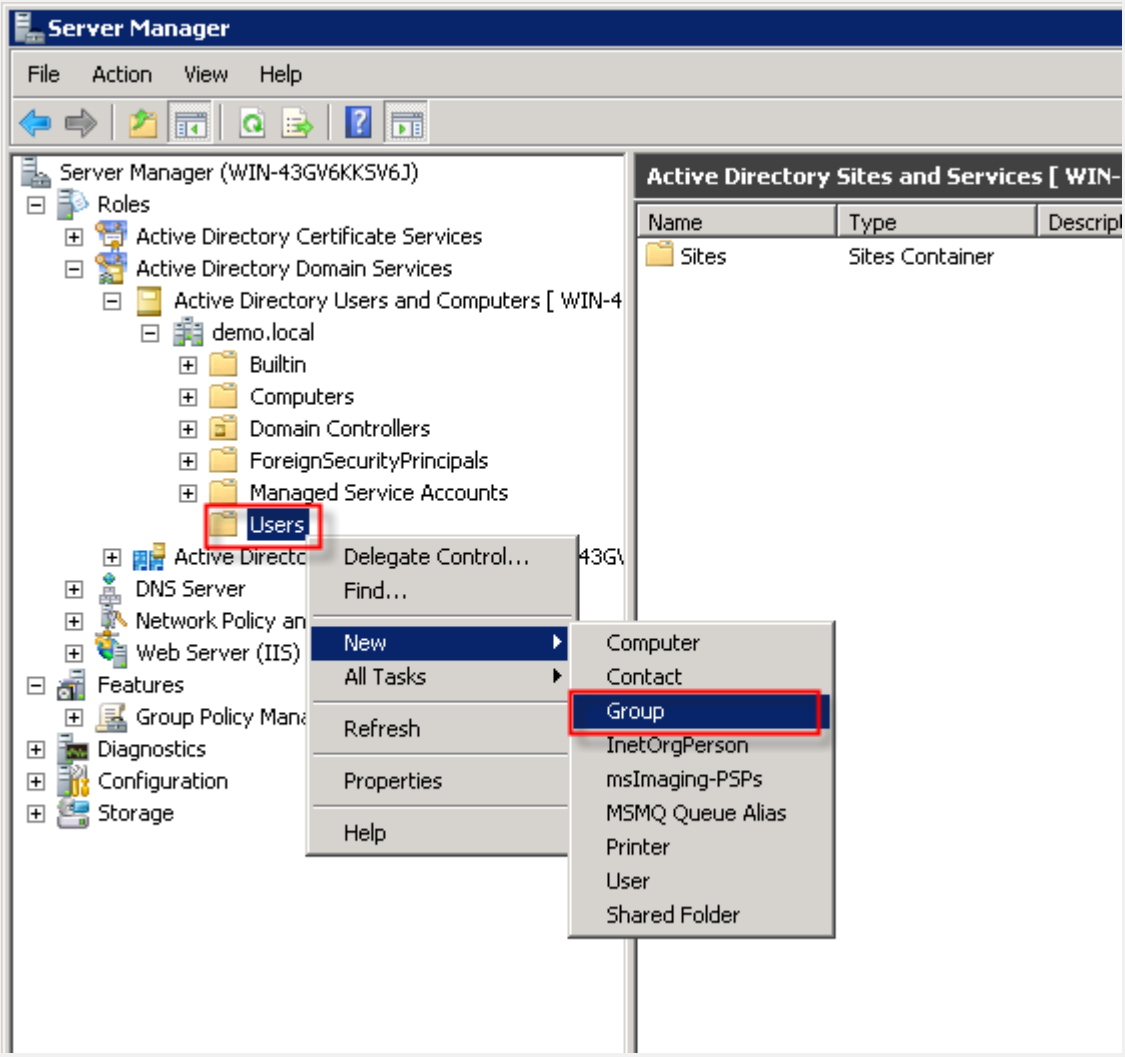


3	**Set the password. Uncheck User must change password at next login, check User cannot change password, and Password never expires. Click Next. Then click Finish.**

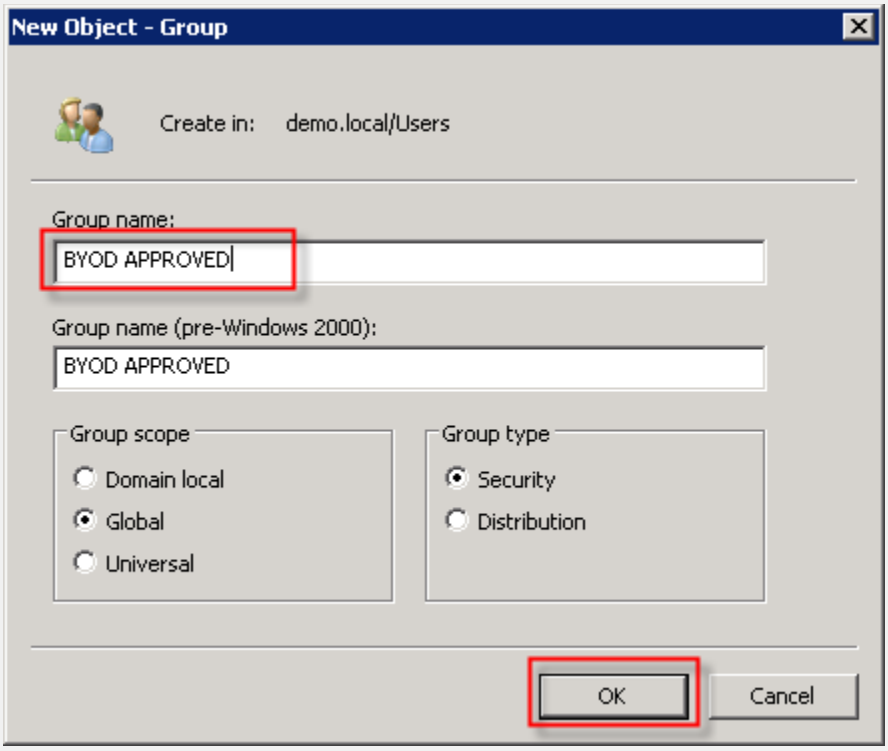

New Object - User
Create in: demo.local/Users
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel


New Object - User
Create in: demo.local/Users
When you click Finish, the following object will be created:
Full name: employee
User logon name: employee@demo.local
The user cannot change the password.
The password never expires.
< Back
Finish
Cancel

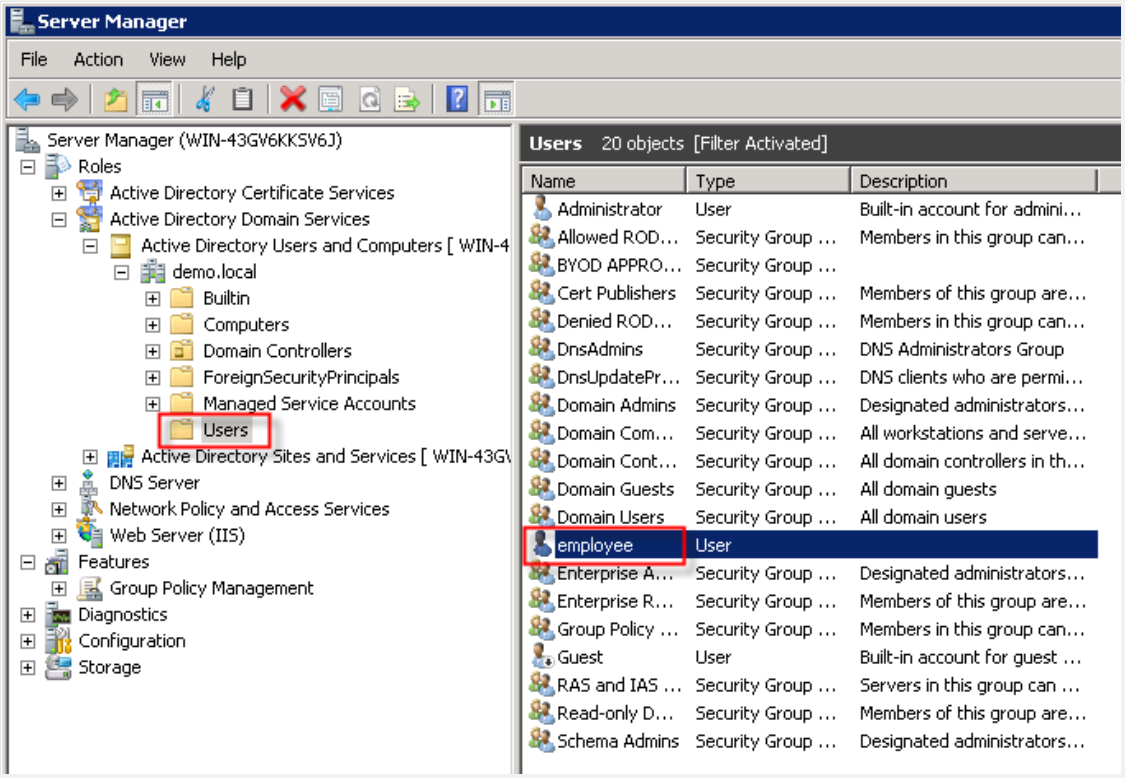
4	**From Server Manager, expand Roles → Active Directory Domain Services → Active Directory Users and Computers → <domain_name>, and then right click on Users and select New → Group.**



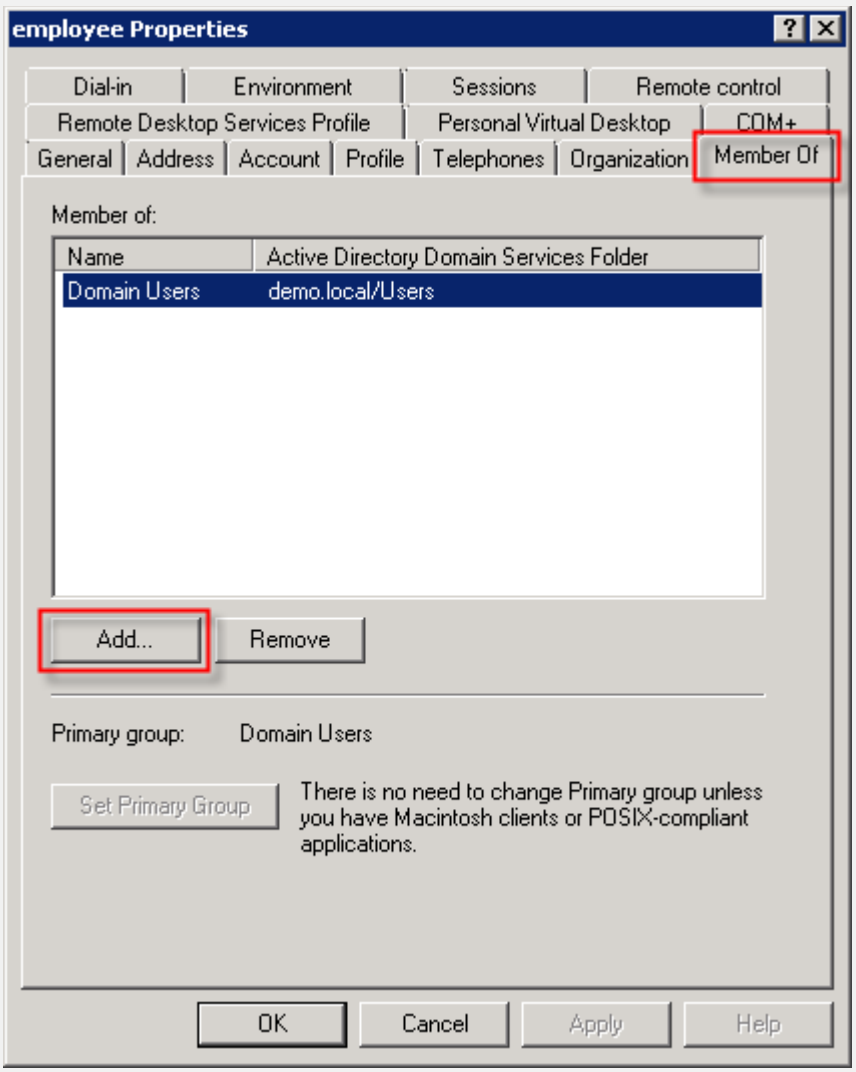
5	**Type "BYOD APPROVED" for the group name and click OK.**

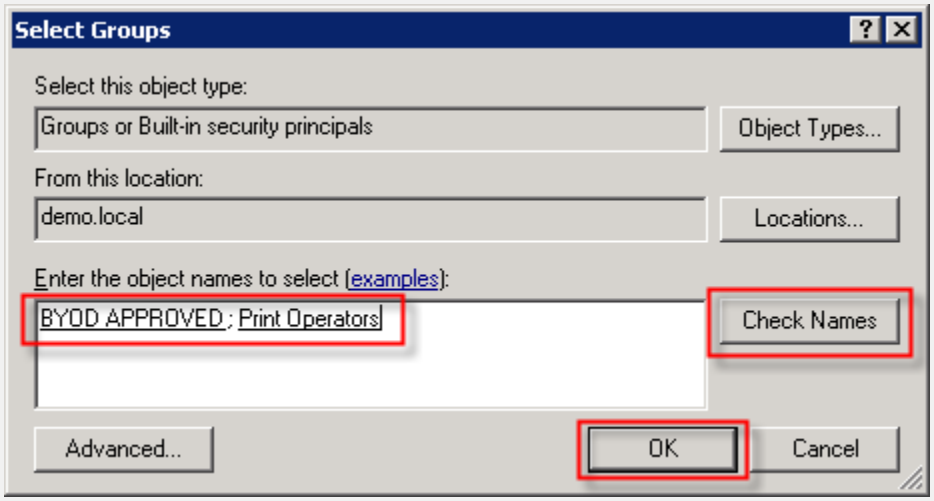


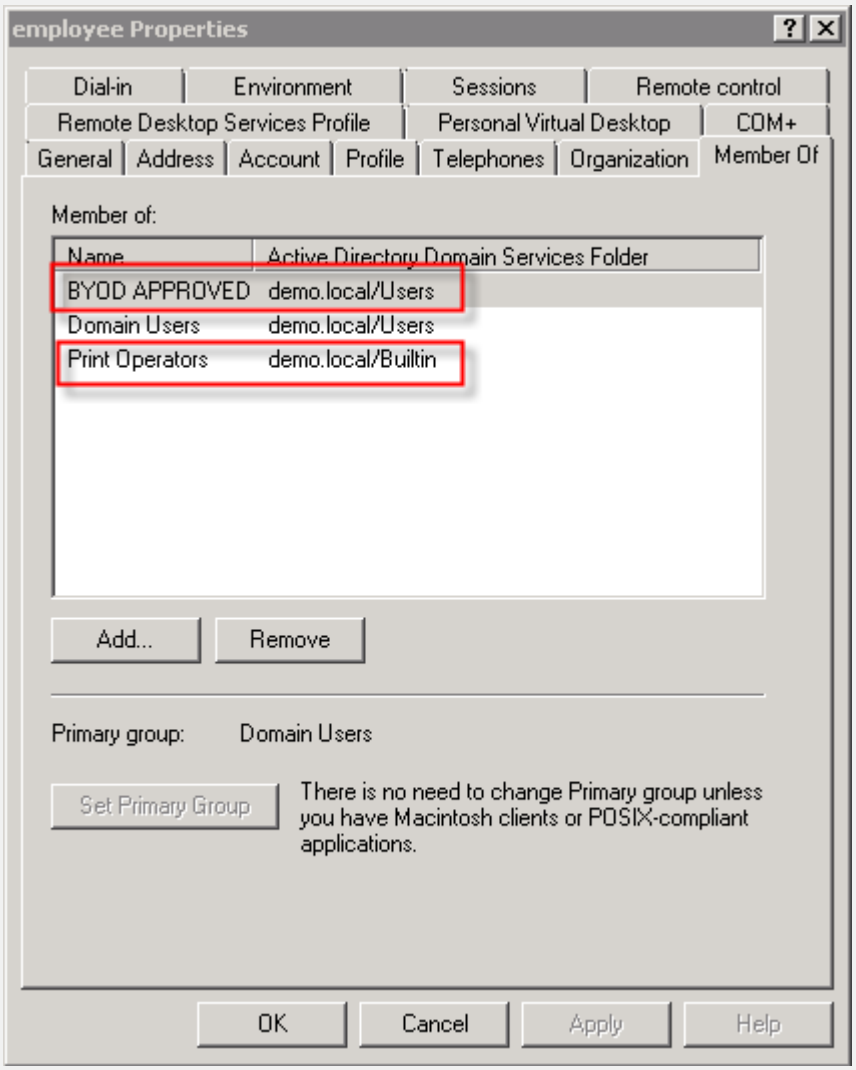
6	**From Server Manager, expand Roles → Active Directory Domain Services → Active Directory Users and Computers → <domain_name>, and then click on Users. In the right hand window double-click "employee" (or the username configured previously).**



7	**Click on the Member Of tab and click Add. Type “BYOD APPROVED” and “Print Operators” and then click Check Names. Click OK when finished, and then click OK again.**


employee Properties
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
Personal Virtual Desktop
COM+
General
Address
Account
Profile
Telephones
Organization
Member Of
Member of:
Name
Active Directory Domain Services Folder
Domain Users
demo.local/Users
Add...
Remove
Primary group:
Domain Users
Set Primary Group
There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.
OK
Cancel
Apply
Help

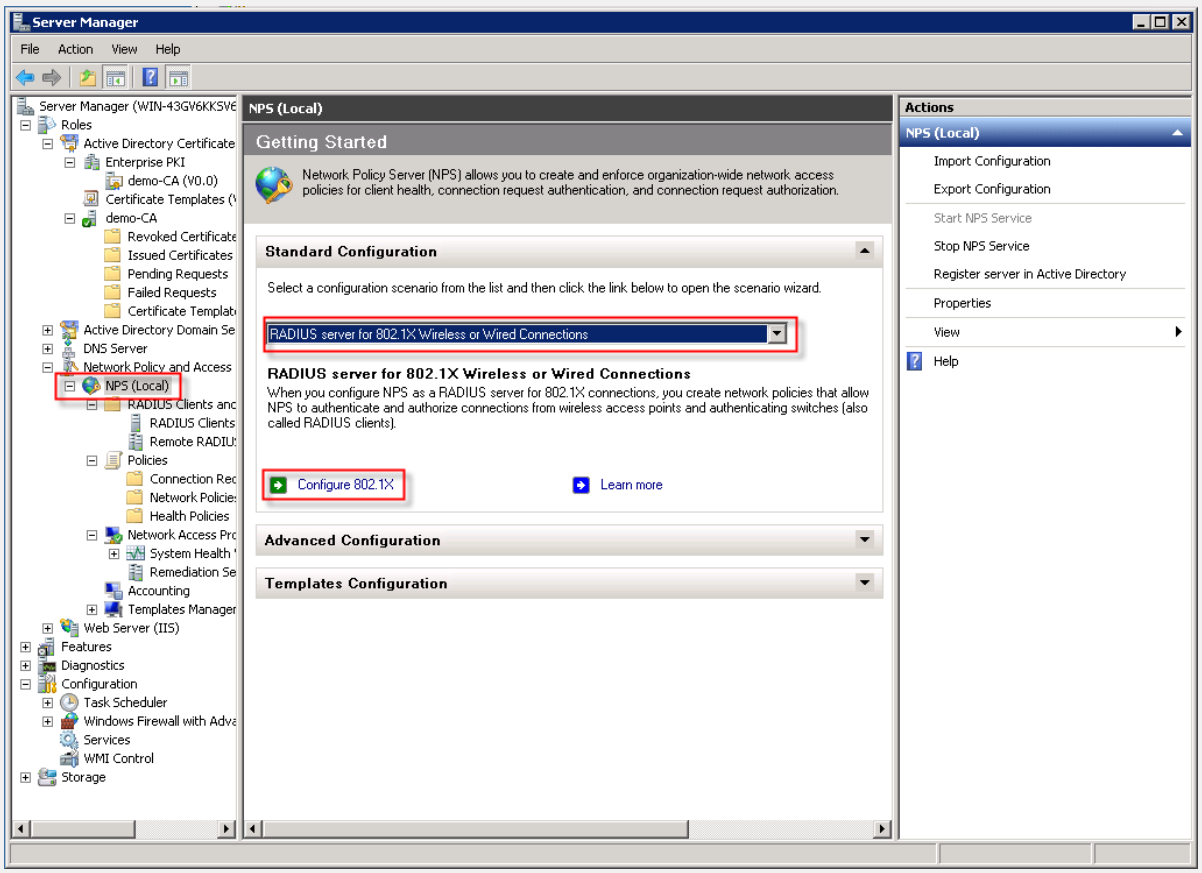

Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
demo.local
Locations...
Enter the object names to select (examples):
BYOD APPROVED ; Print Operators
Check Names
Advanced...
OK
Cancel



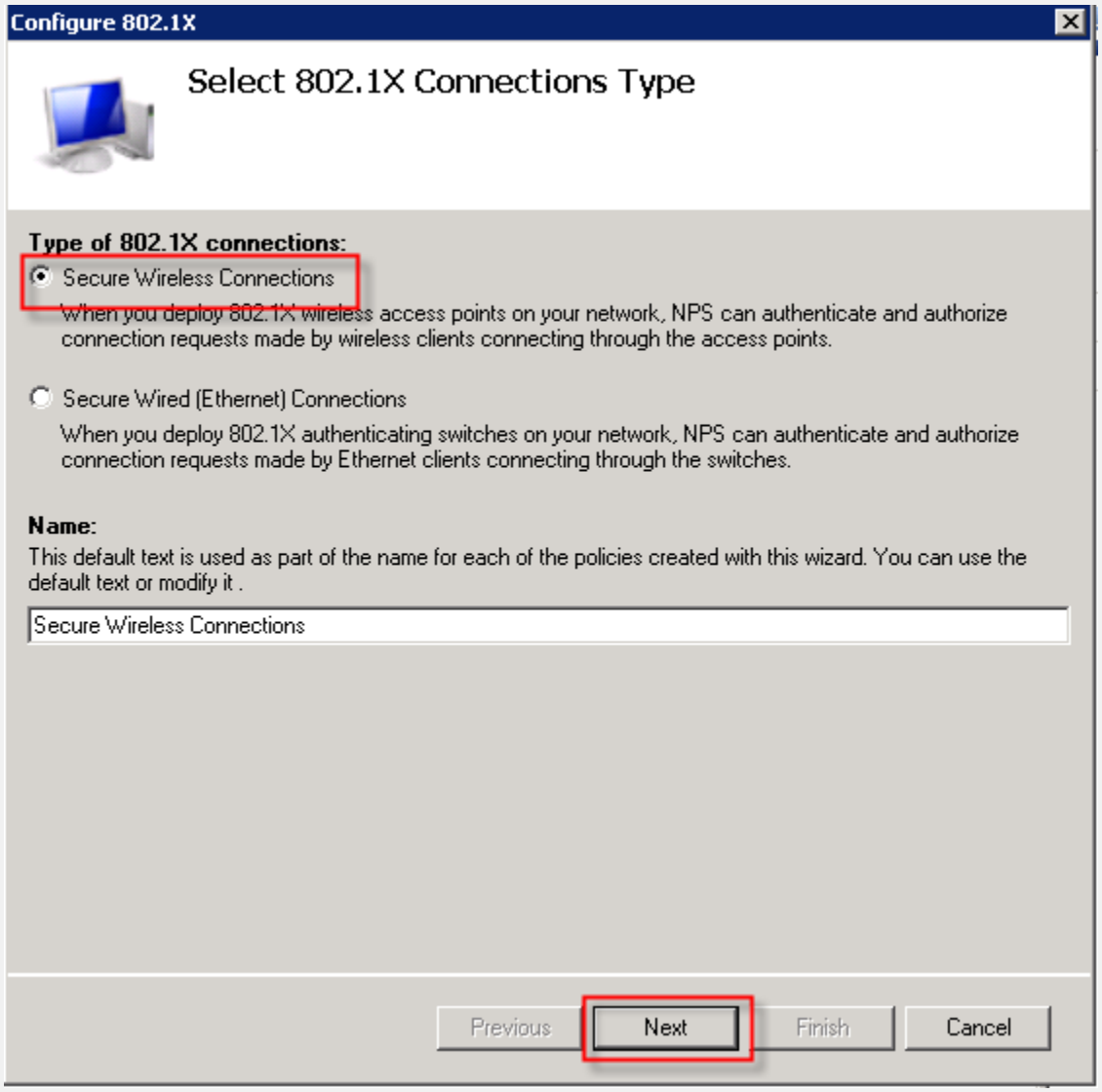
8	**Create a second demo employee account, but this time DO NOT add it to the group "BYOD APPROVED". Make sure to also add it to the Print Operators group.**

2.2.9 Configure Network Policy Server

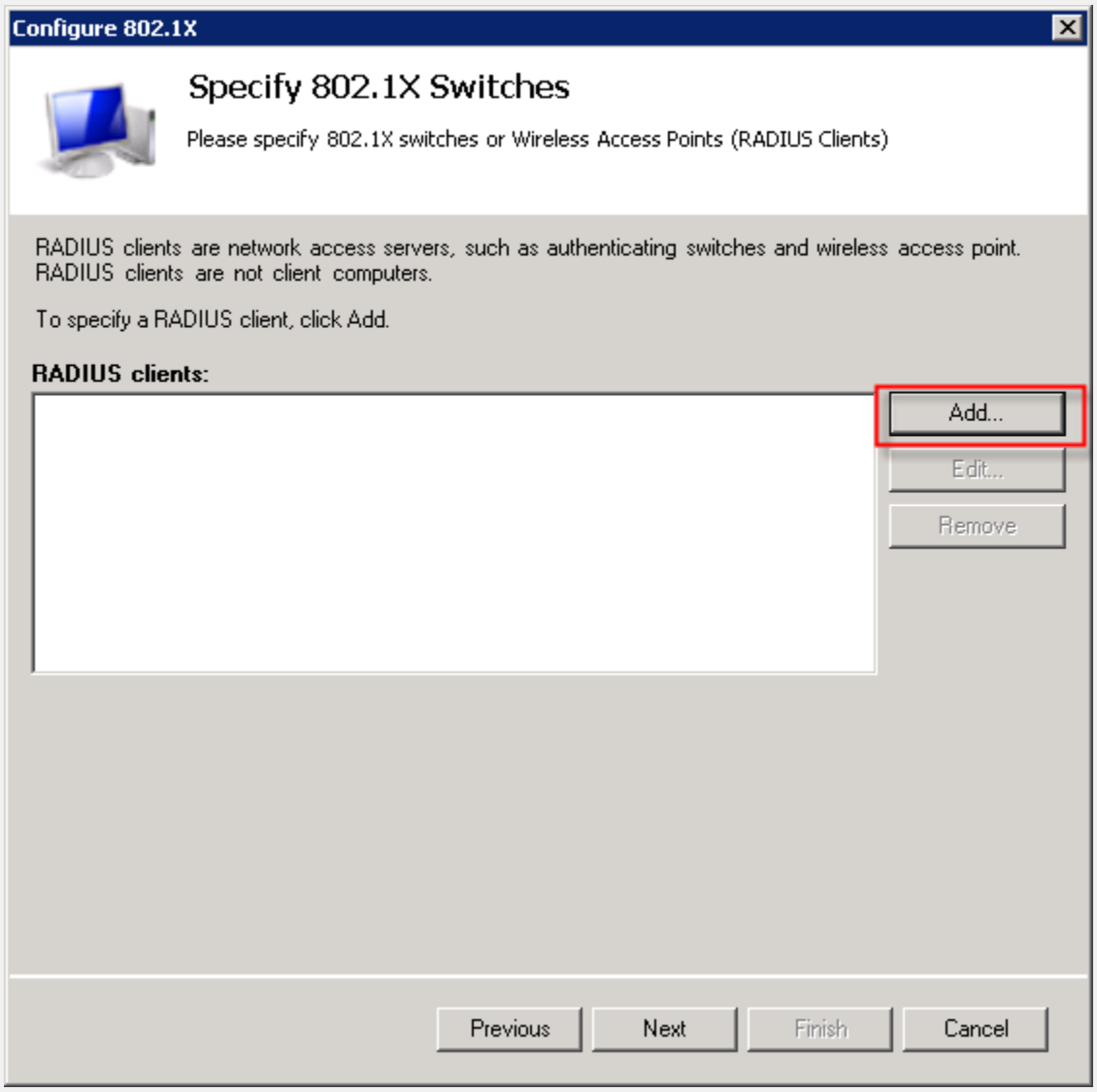
1	**From Server Manager, expand Roles → Network Policy and Access Services, and then click on NPS (local). In the right-hand window pane, select RADIUS server for 802.1X Wireless or Wired Connections. Then click on Configure 802.1X.**



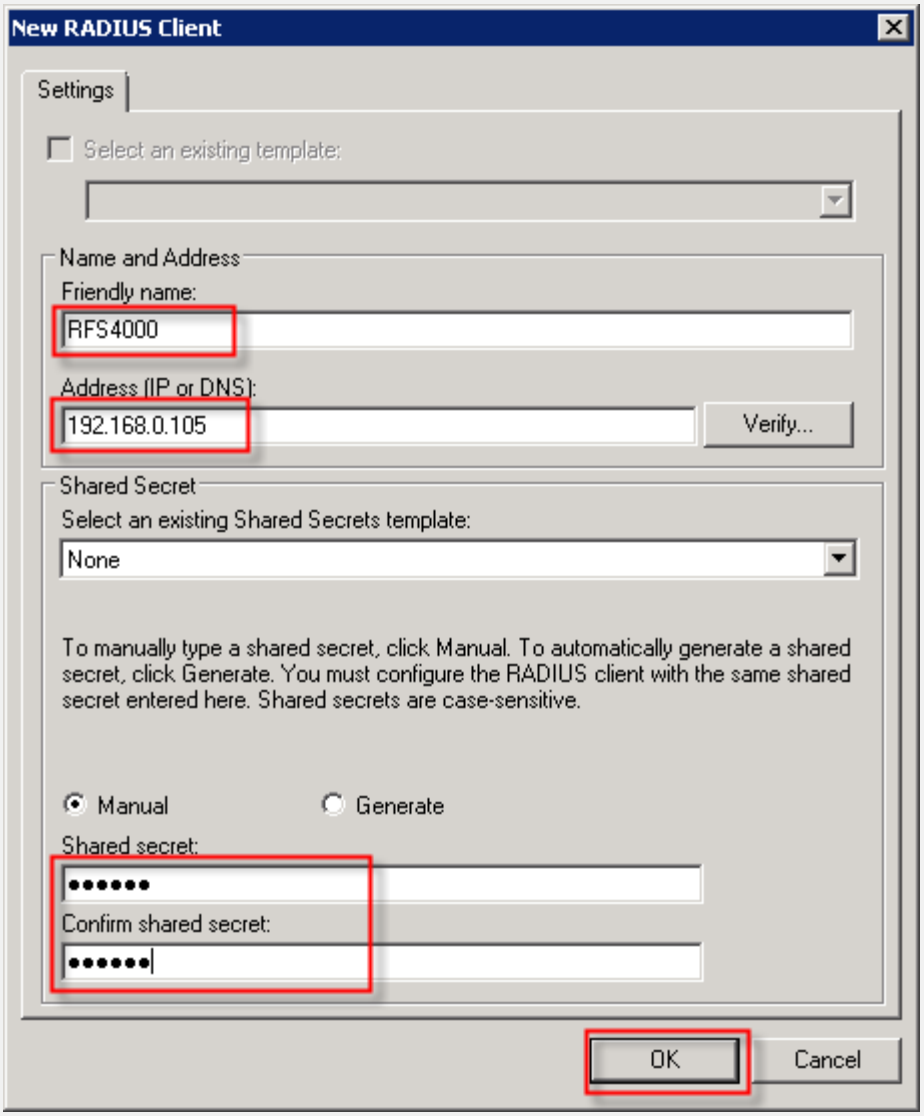
2	Choose Secure Wireless Connections, optionally name the policy, and click Next.



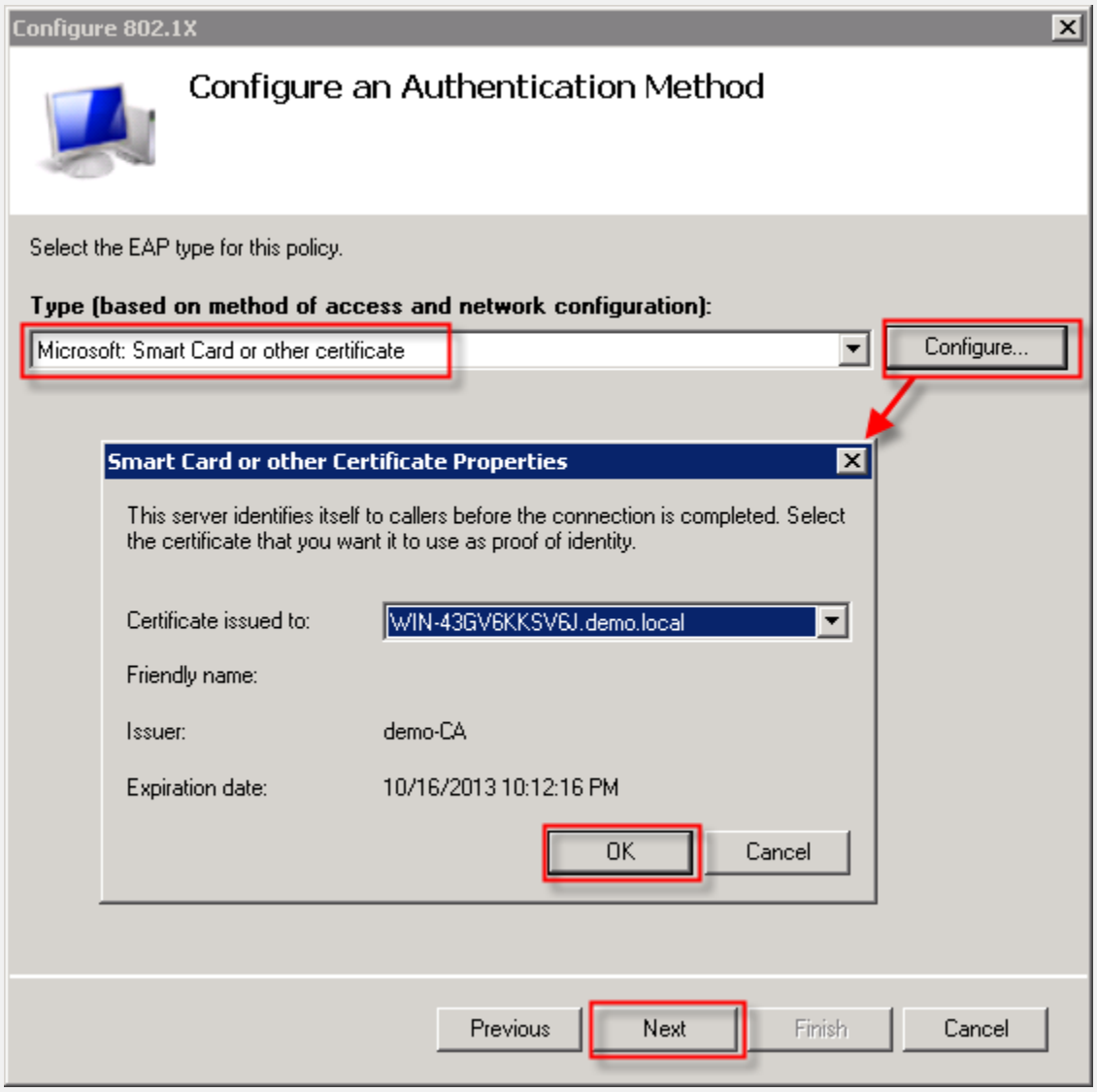
3	**Click Add to add a RADIUS Client.**



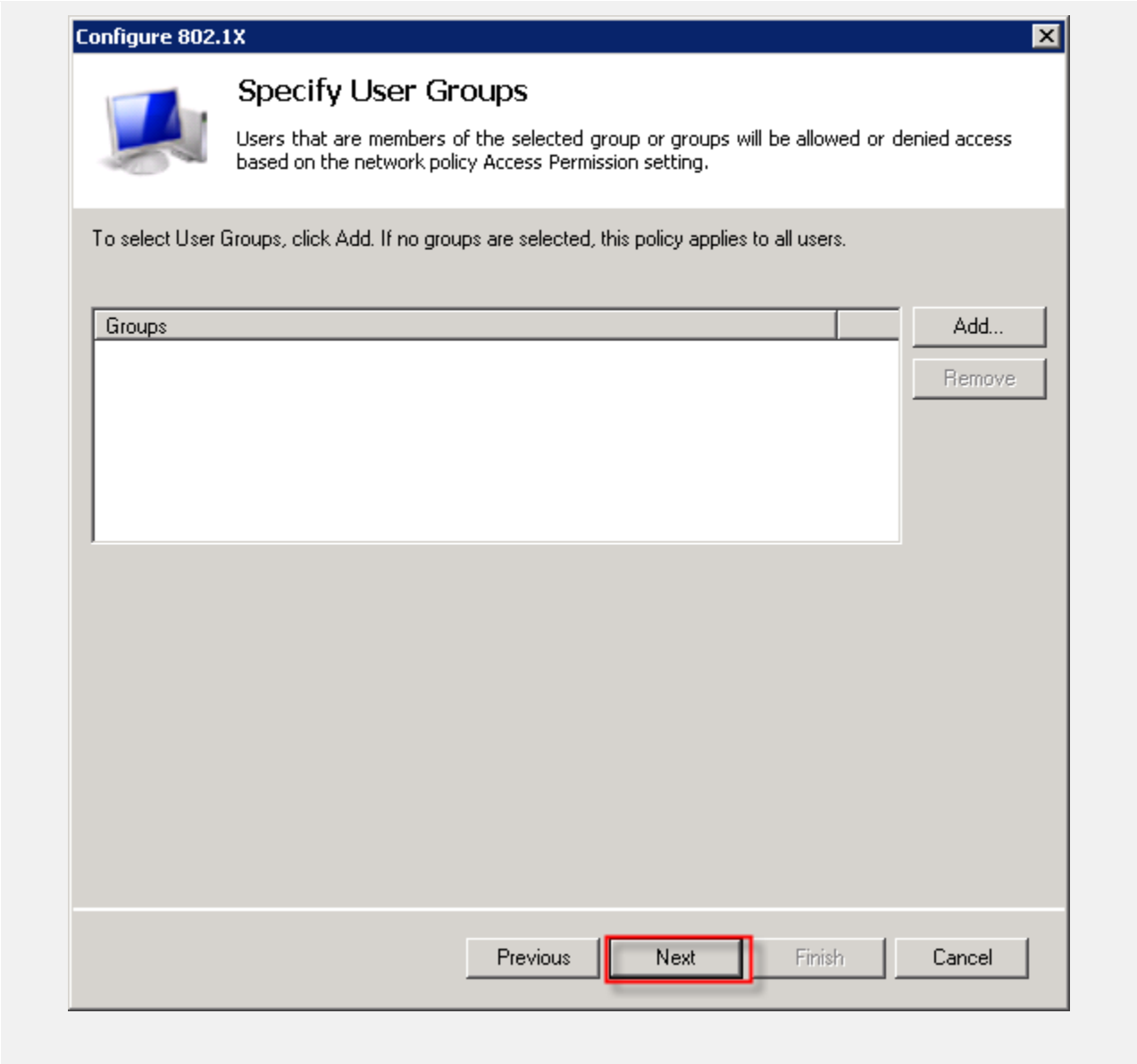
4	**Type the Name, IP address of your RFS, type the shared secret as “secret”. Click OK. Then click Next.**

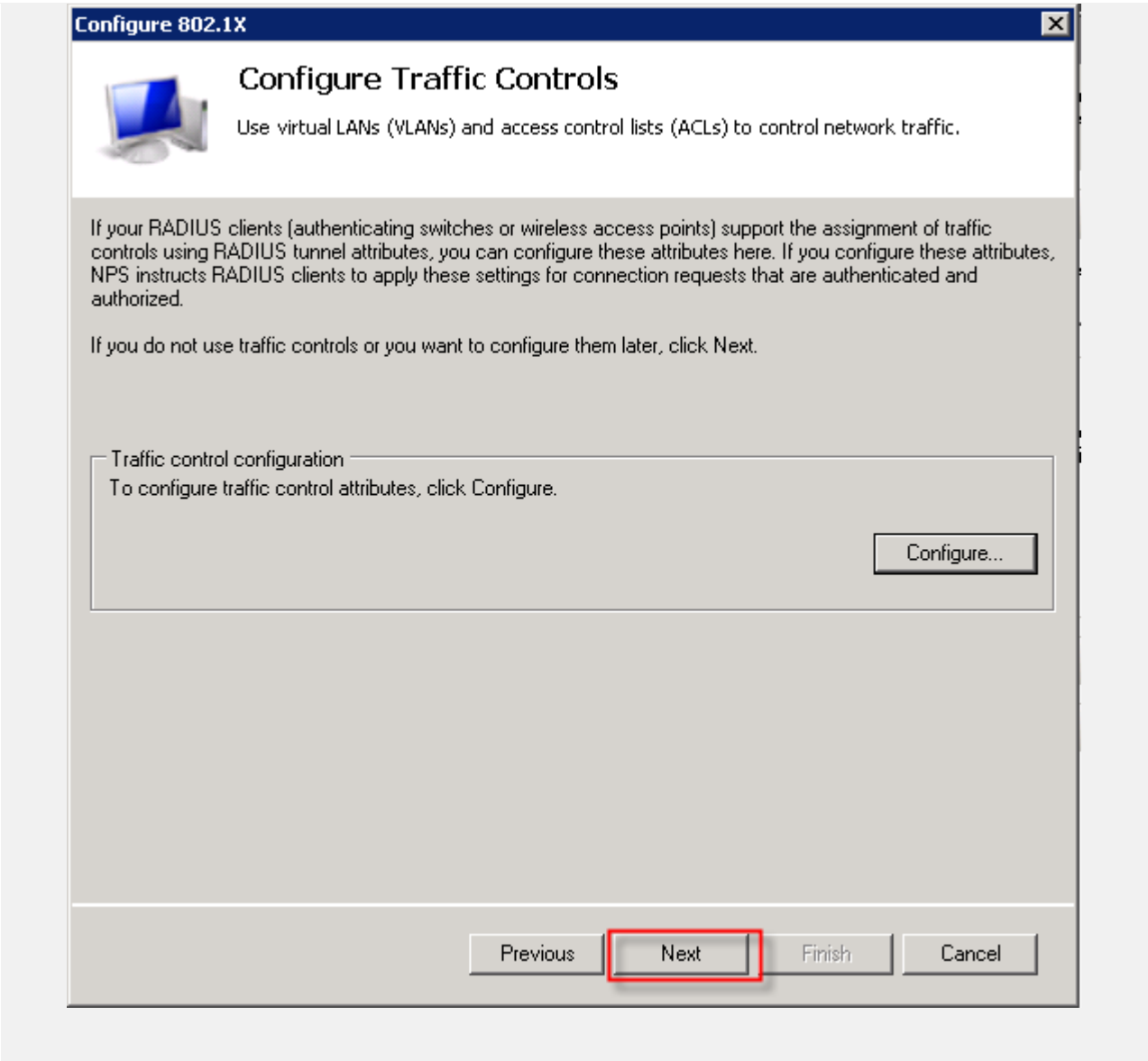


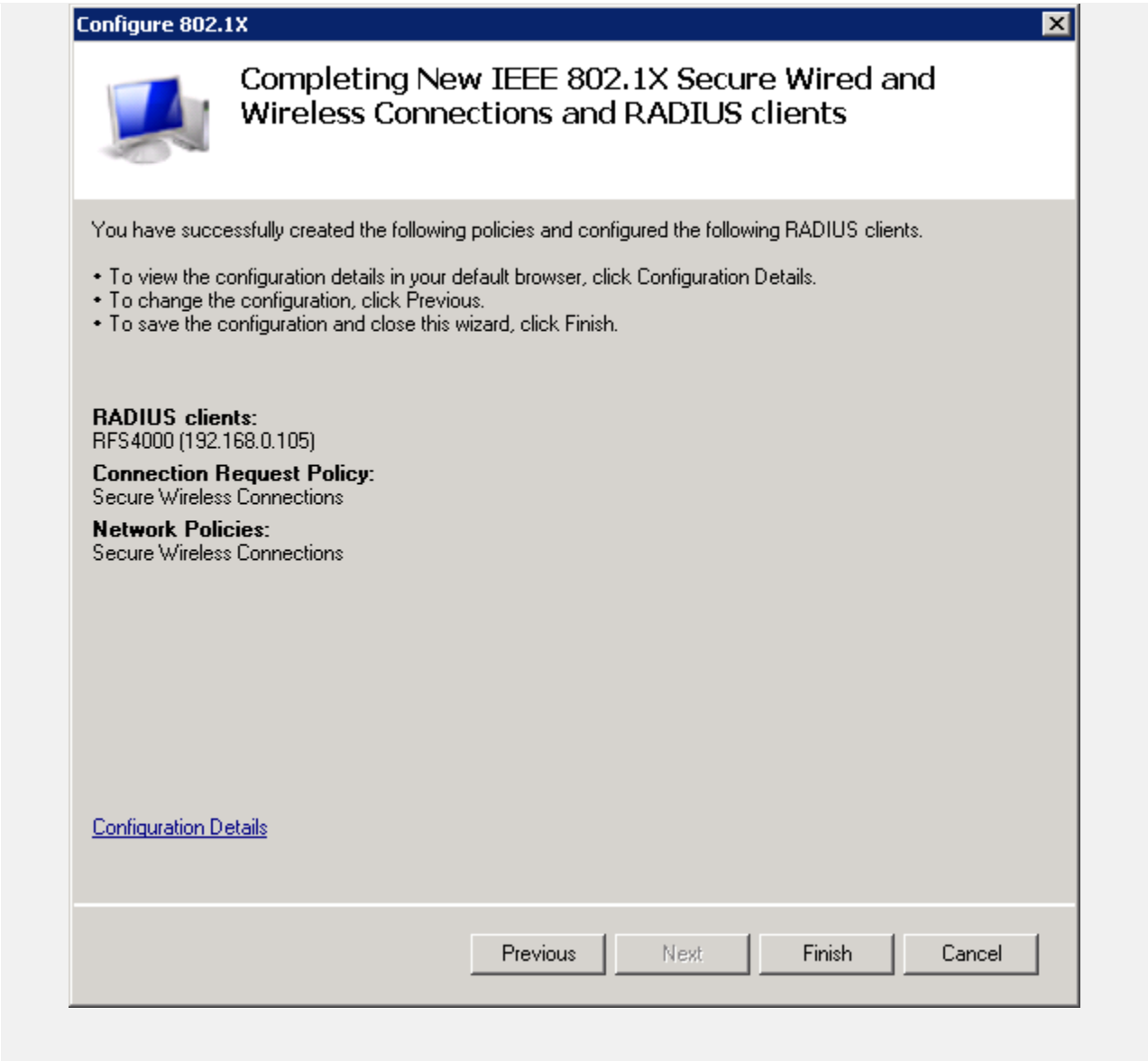
5	**Select Microsoft: Smart Card or Certificate and click Configure. Note the name of the certificate assigned to the computer. Click OK and then click Next.**



6	**Click Next. Then click Next again. Click Finish.**


Configure 802.1X
Specify User Groups
Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.
To select User Groups, click Add. If no groups are selected, this policy applies to all users.
Groups
Add...
Remove
Previous
Next
Finish
Cancel


Configure 802.1X
Configure Traffic Controls
Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.
If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. If you configure these attributes, NPS instructs RADIUS clients to apply these settings for connection requests that are authenticated and authorized.
If you do not use traffic controls or you want to configure them later, click Next.
Traffic control configuration
To configure traffic control attributes, click Configure.
Configure...
Previous
Next
Finish
Cancel

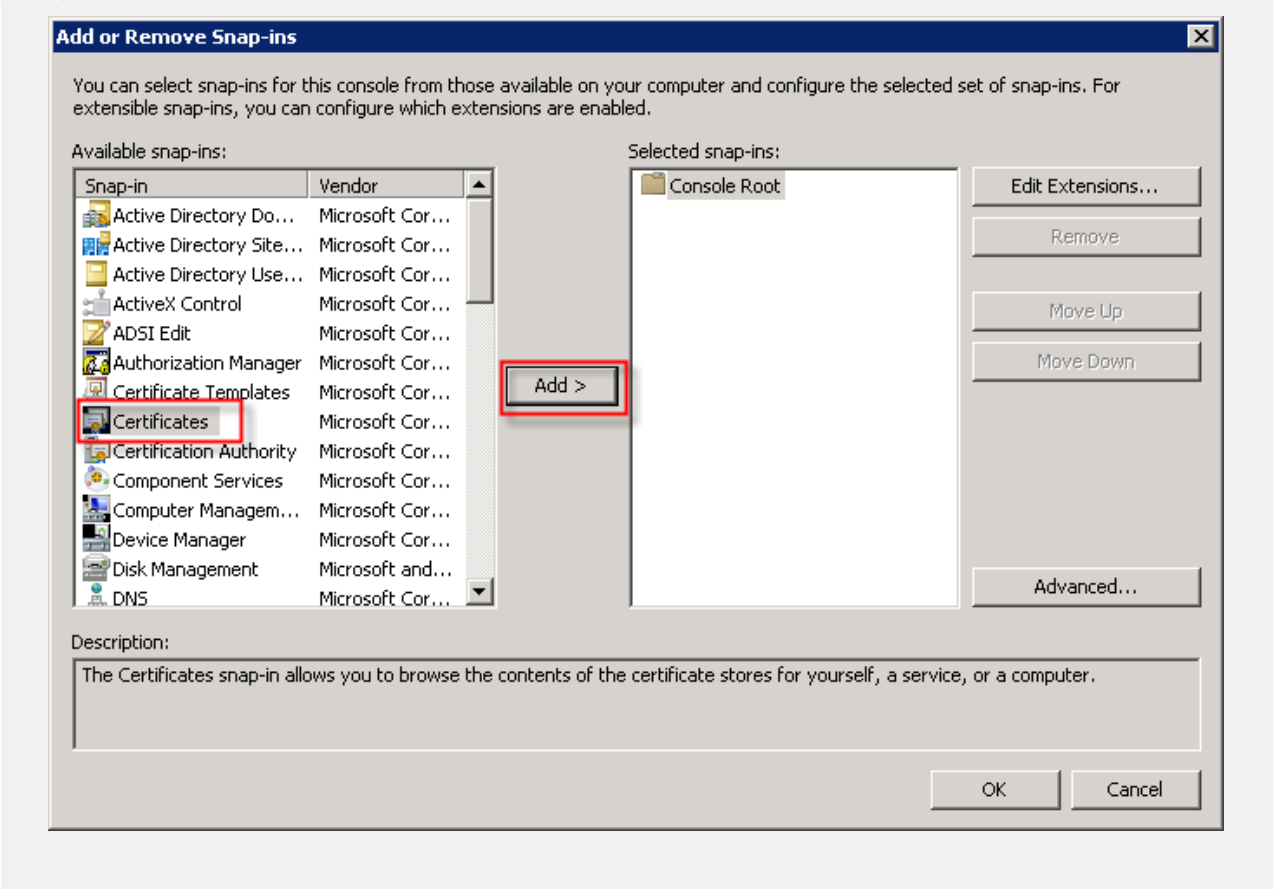


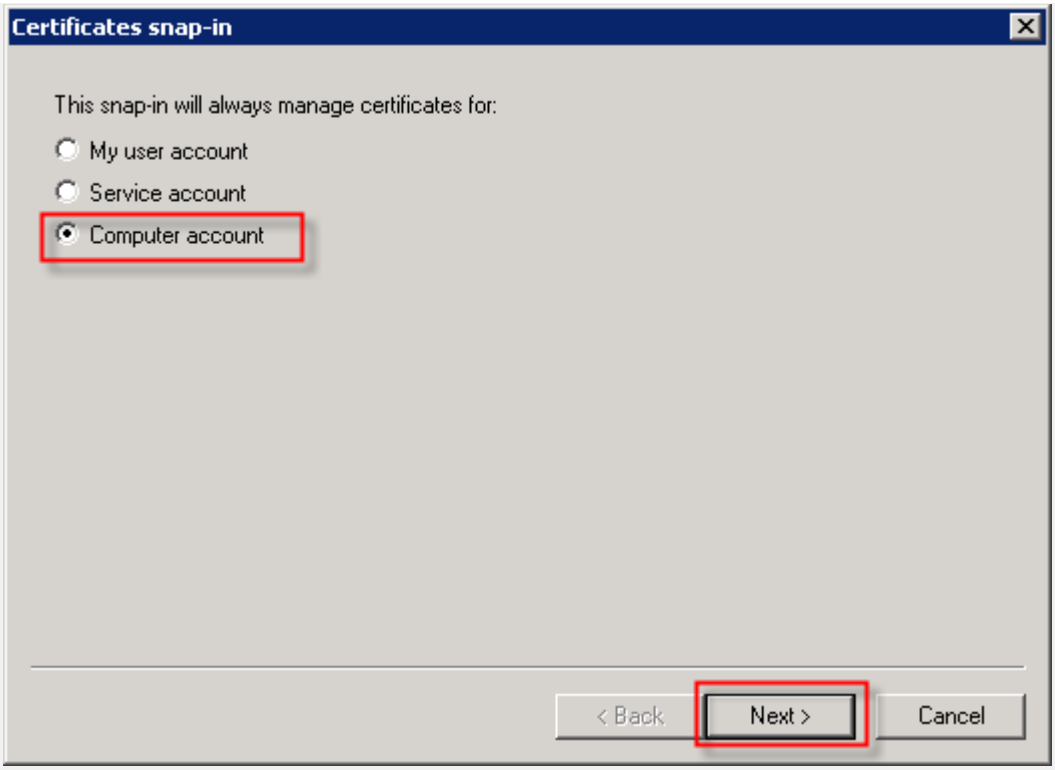
2.2.10 Export Root CA Certificates

You will need to export the root CA from the Microsoft server so it can be imported to the Admin Console. There will be two certificates on the server. The first will be the root CA certificate, and the other will be a certificate issued to the local server. This certificate is used by other server services, such as NPS (RADIUS) and IIS. You will export both certificates for use with the Admin Console in a later step.

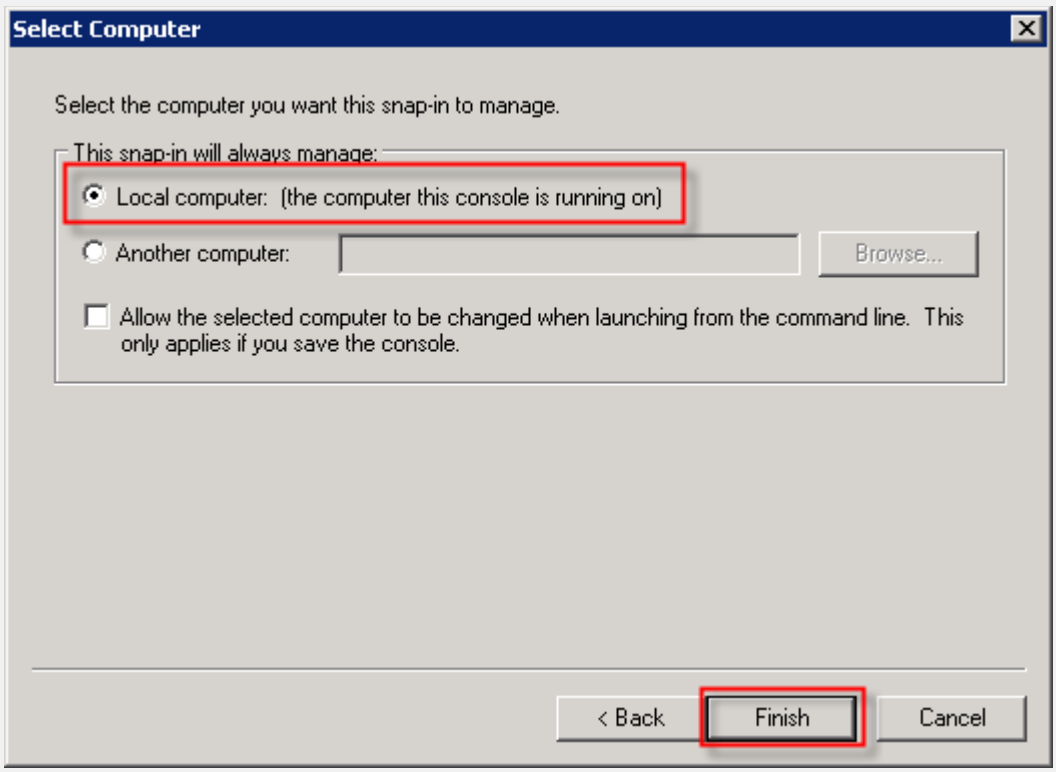
Note: The root CA certificate will be installed on clients as a trusted root certificate so that they don't generate security warnings about untrusted servers. The NPS (RADIUS) certificate will be installed on clients and selected as the expected RADIUS server certificate, which allows clients to authenticate the server in order to thwart possible honeypot networks pretending to be the corporate SSID.

1	**Click Start, type mmc and press Enter to launch the Microsoft Management Console. Click File → Add/Remove Snap-in. Choose Certificates. Click Add. Choose Computer account. Click Next.**

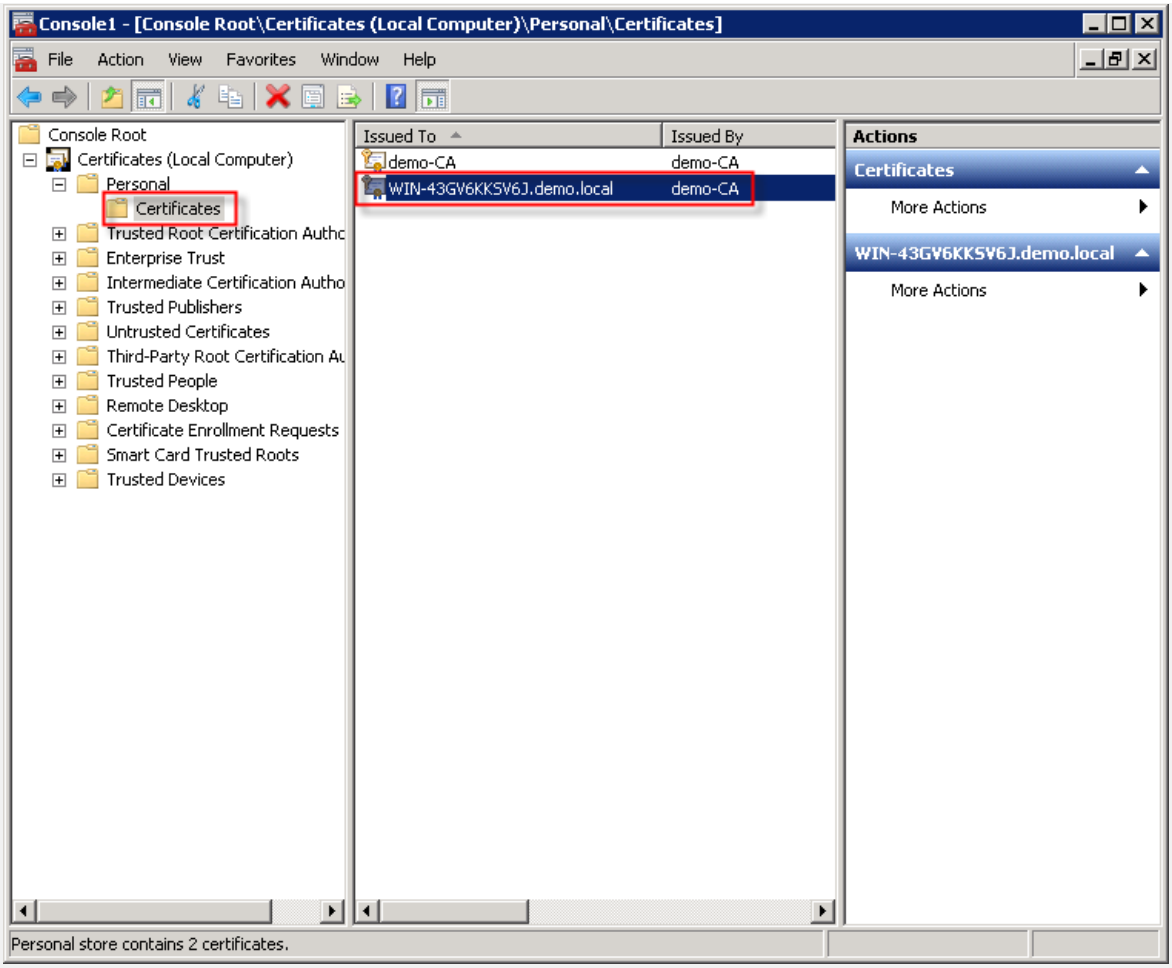




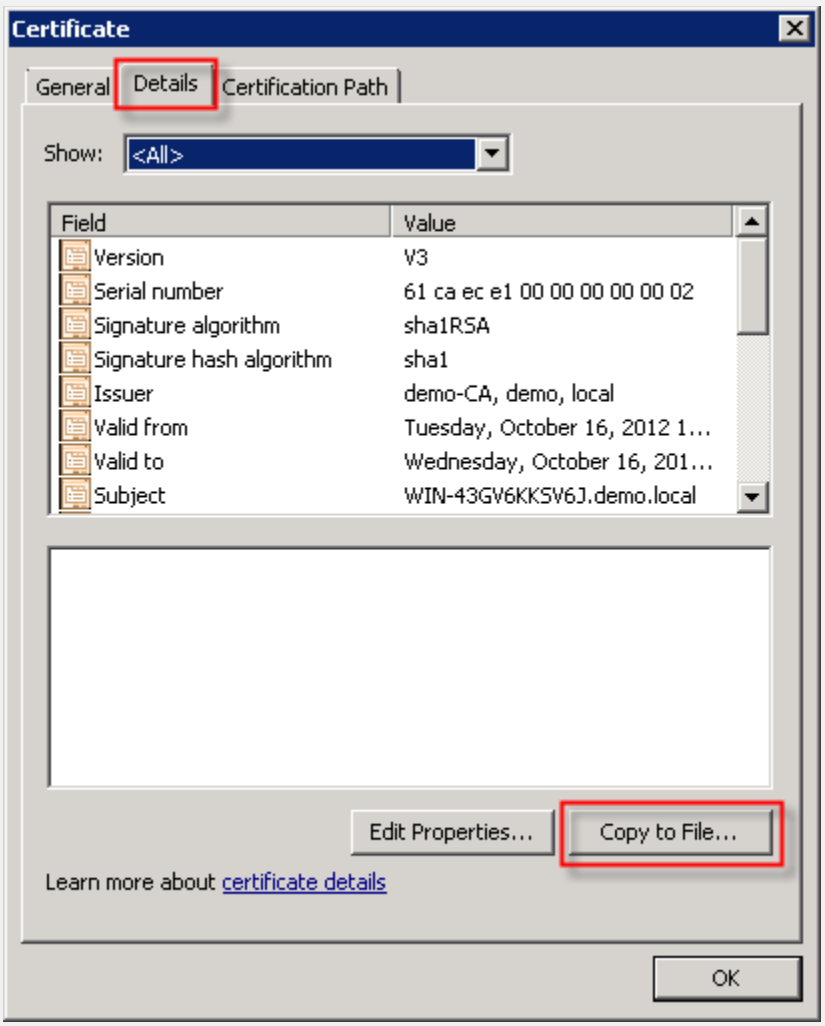
2	**Click Finish and then click OK.**



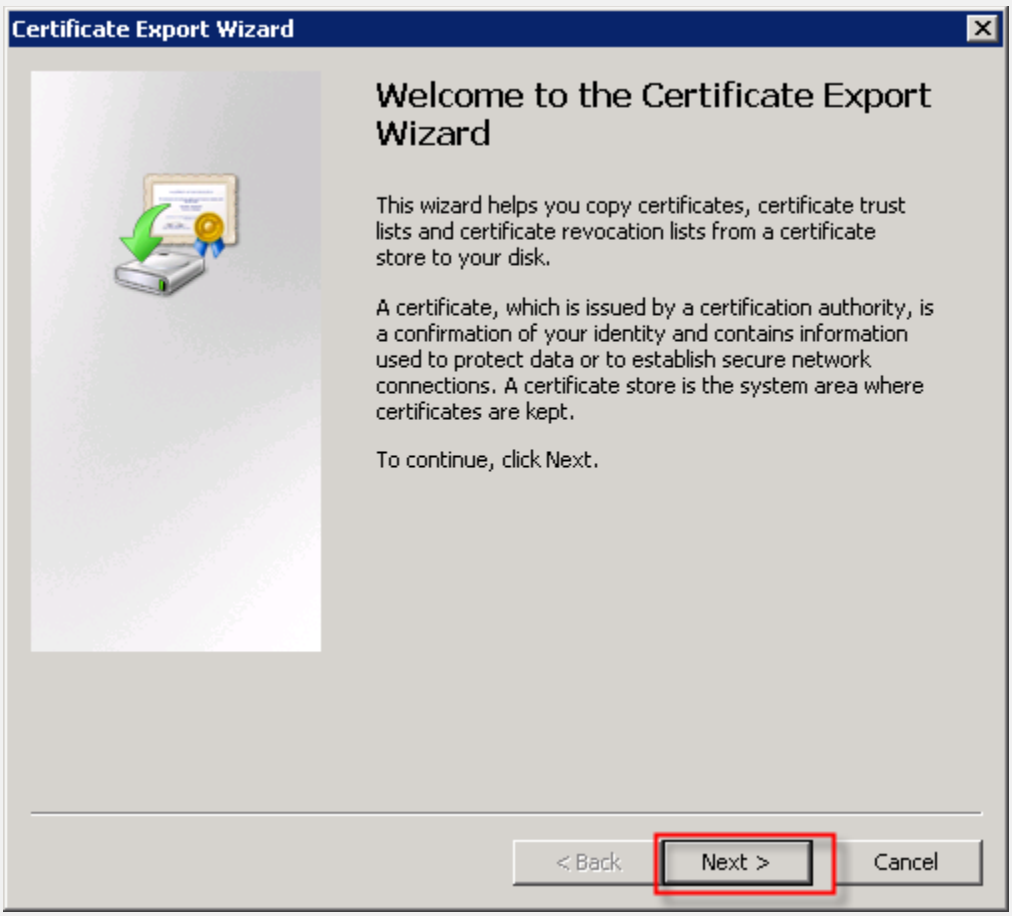
3	**Expand Certificates → Personal and click on Certificates. In the right-hand window pane, double click the server certificate you noted from the NPS configuration section. This is the certificate assigned to the NPS (RADIUS) server.**

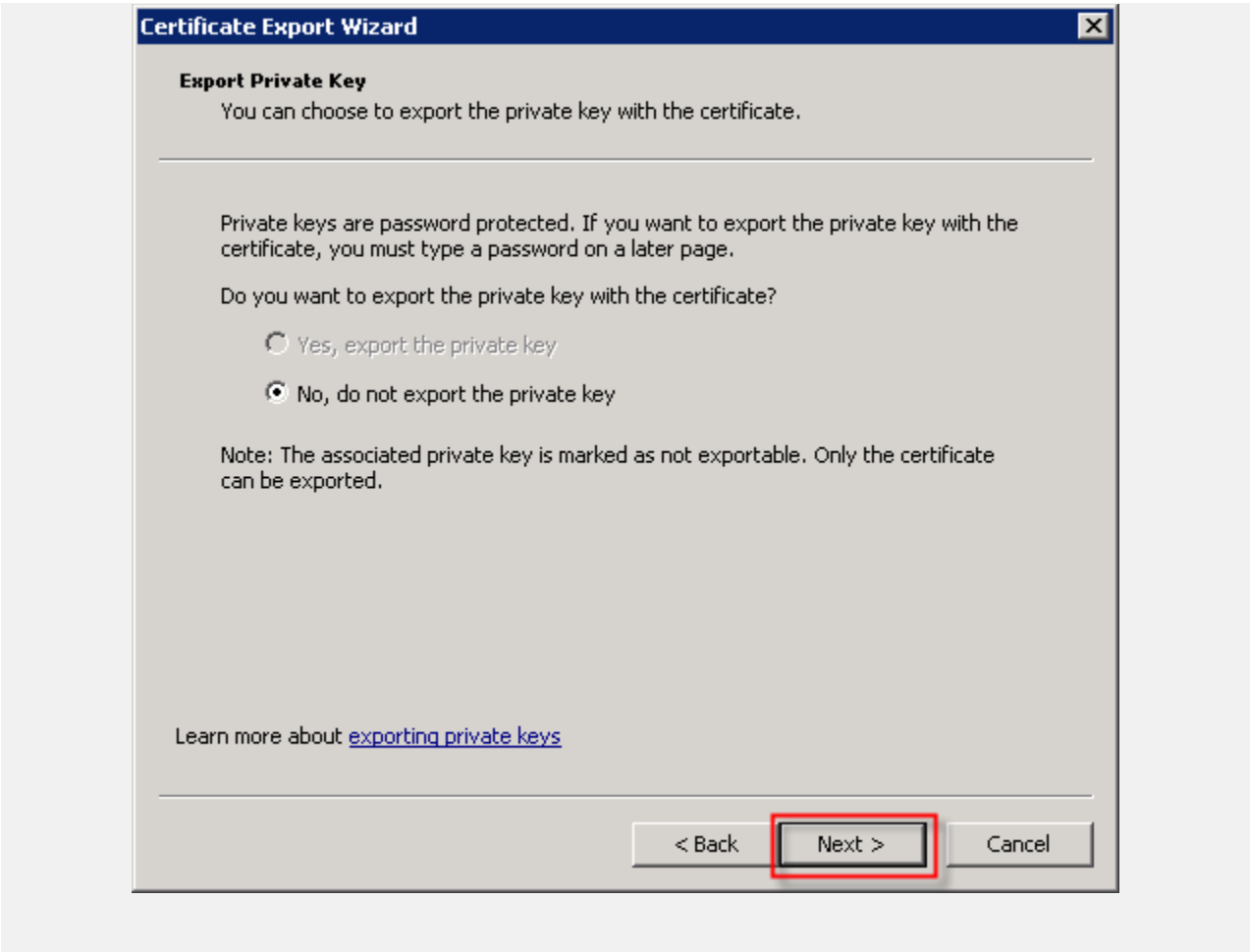


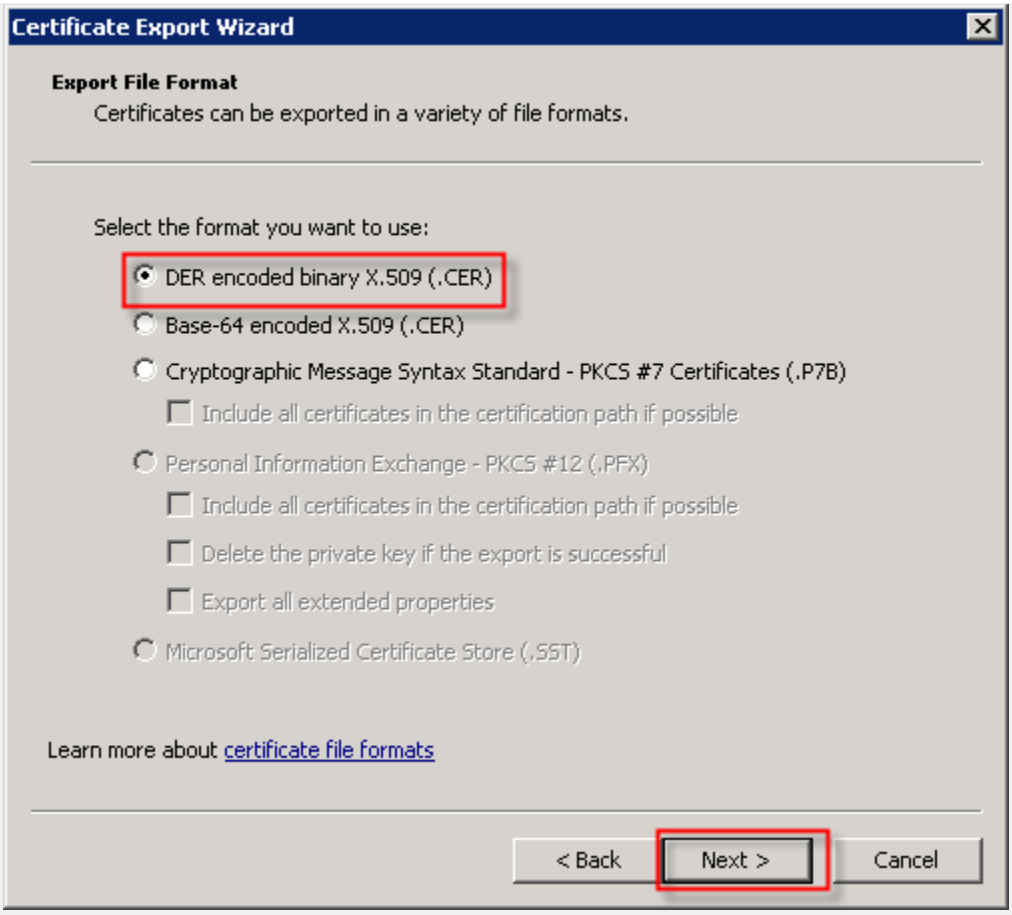
4	**Click the Details tab and click Copy to File.**



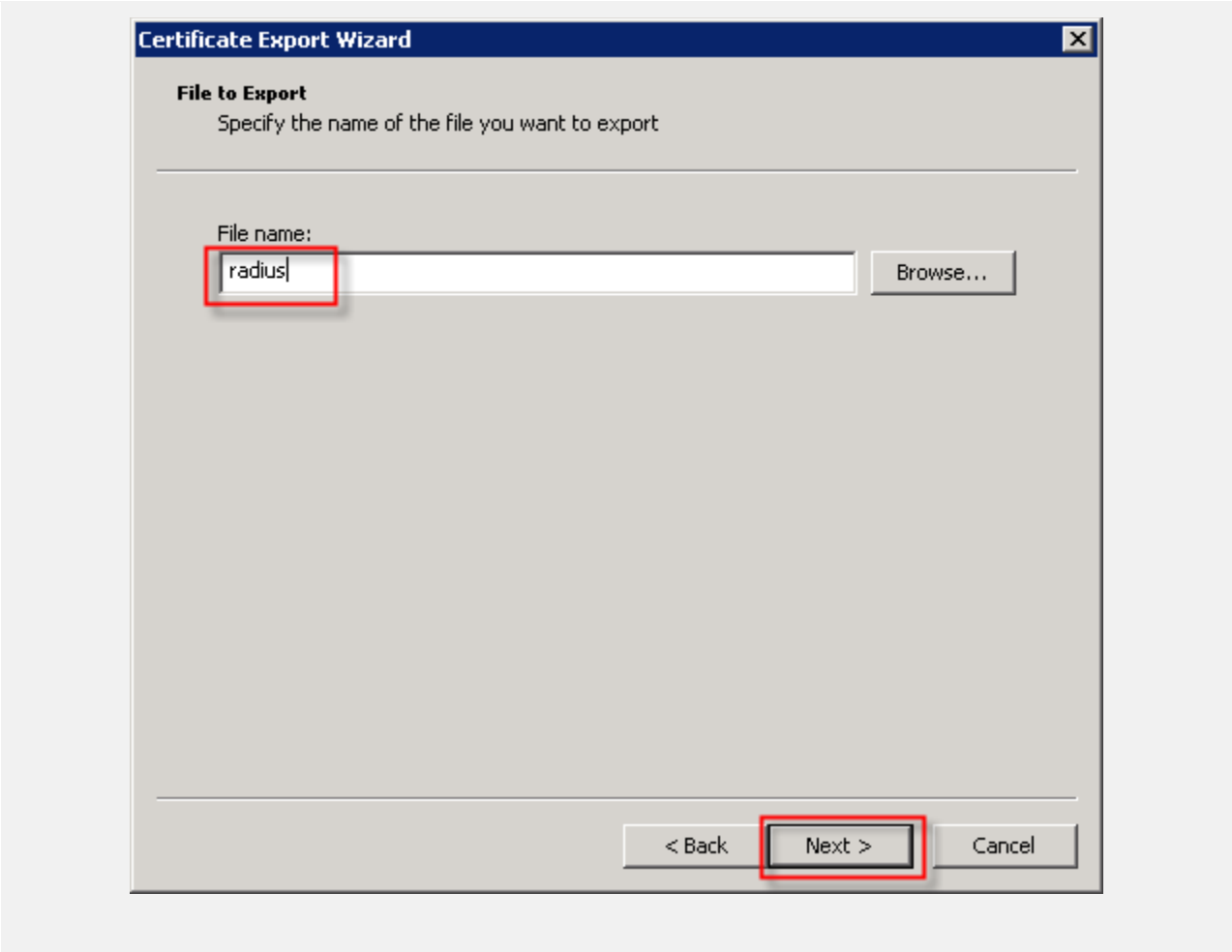
5	**Click Next to begin the export wizard. Click Next again. Select DER format and click Next.**

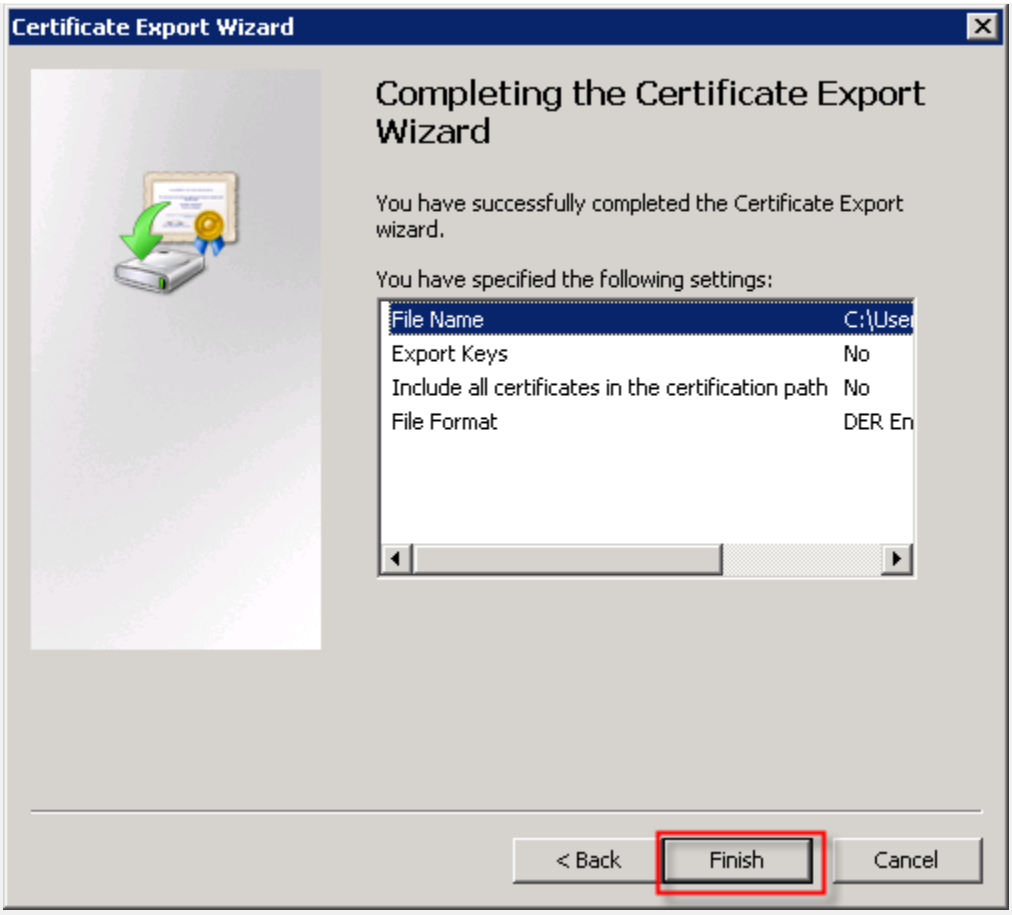

Certificate Export Wizard
Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel


Certificate Export Wizard
Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
Yes, export the private key
No, do not export the private key
Note: The associated private key is marked as not exportable. Only the certificate can be exported.
Learn more about exporting private keys
< Back
Next >
Cancel



6	**Type a filename for the export certificate file and click Next. Click Finish**


Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
radius
Browse...
< Back
Next >
Cancel



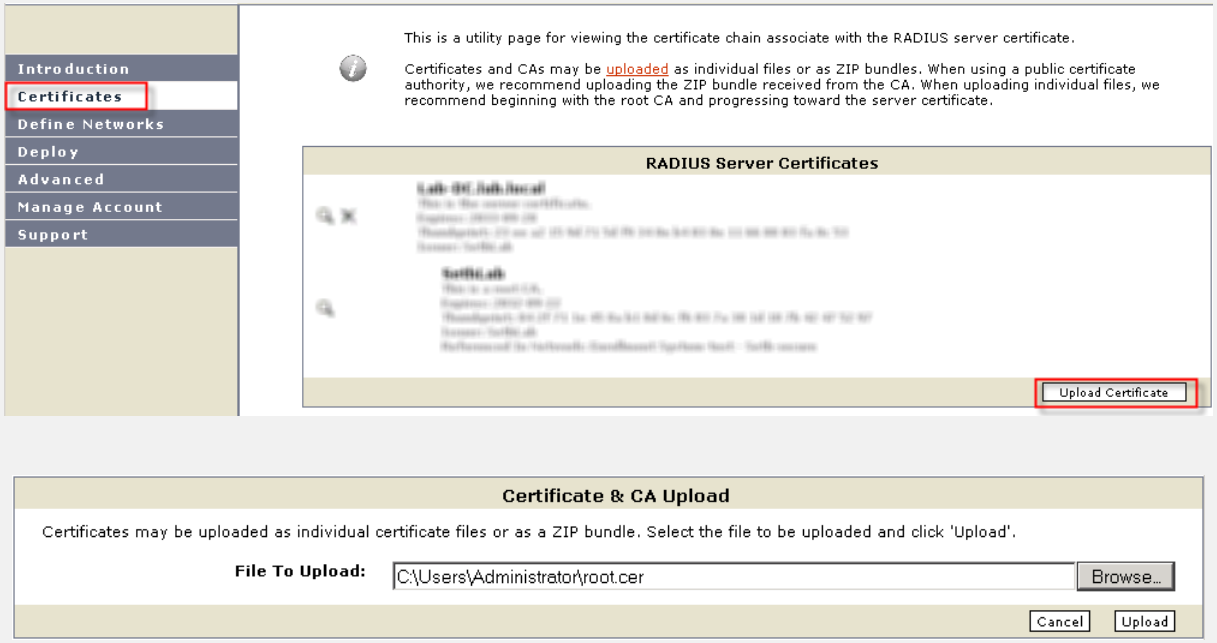
7	**Repeat this same process to export the root certificate, making sure to choose the other certificate in the certificate store.**

2.3 Admin Console Configuration

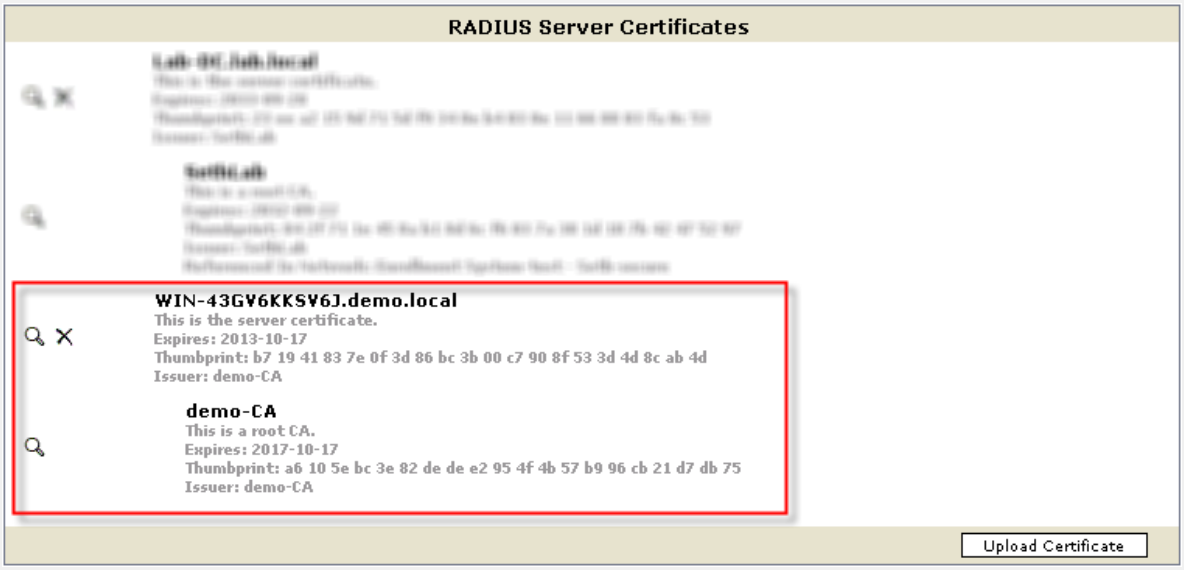
The next set of tasks will be performed on the Admin Console in the “cloud”. Go to http://byod.motorolasolutions.com and login.

2.3.1 Import Microsoft CA Certificates

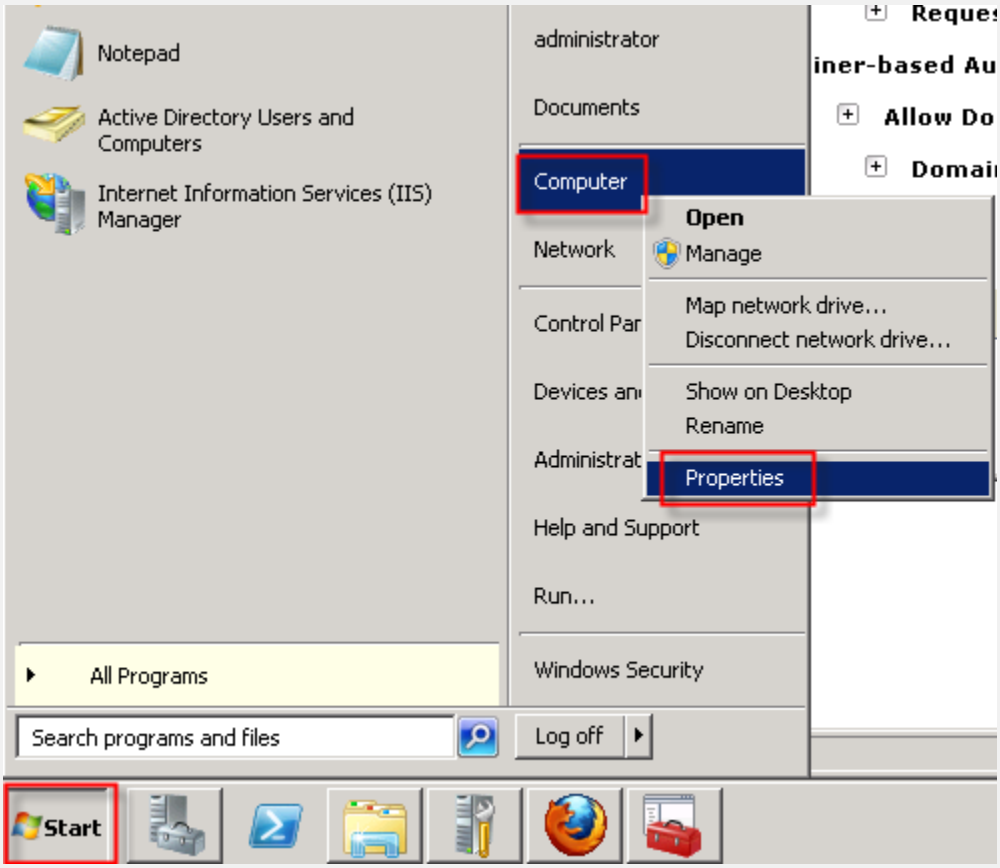
1	**Click Certificates, then click Upload Certificates. Click Browse and locate the certificate file you previously exported. Click Upload.**

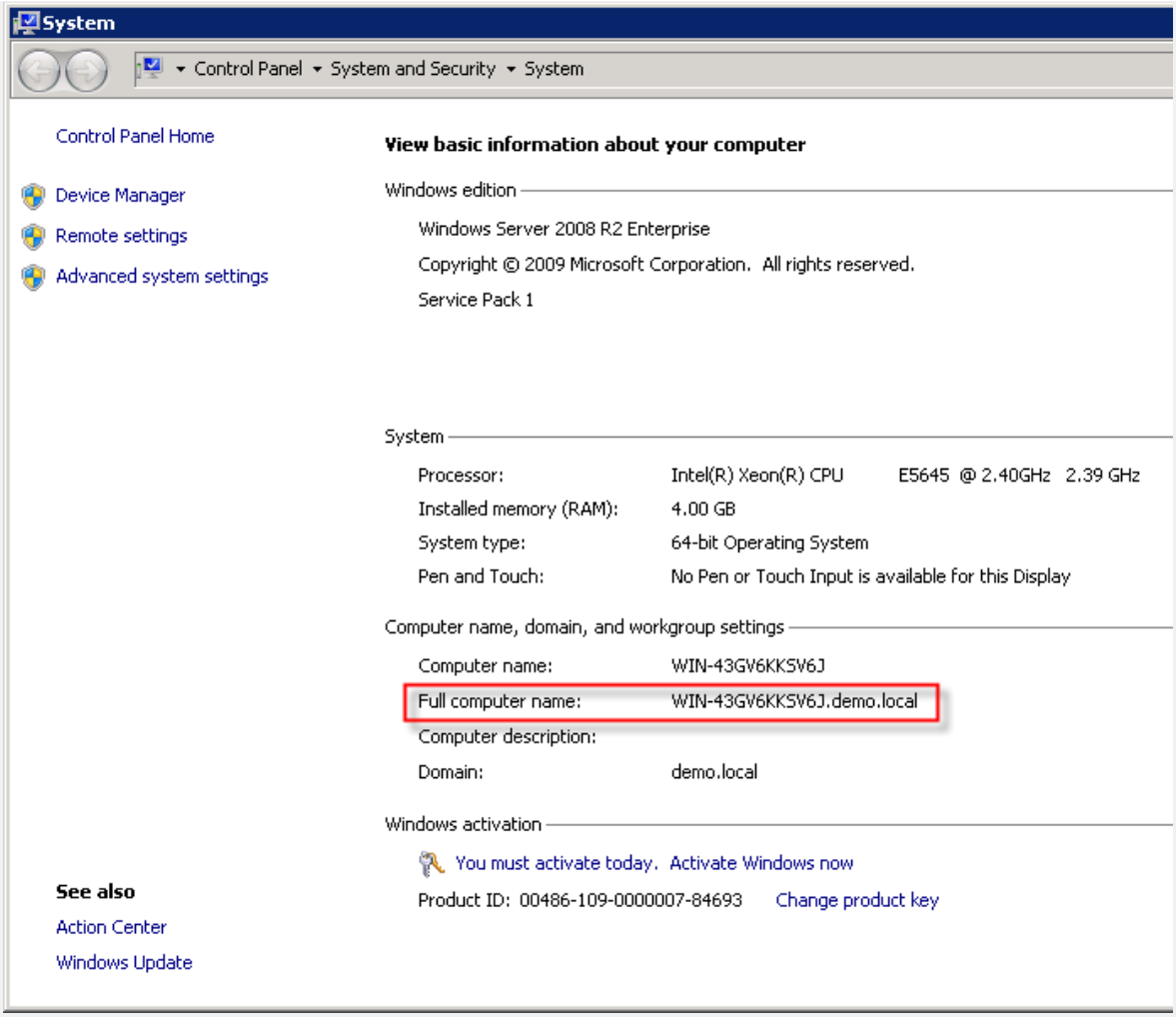


2	Repeat for the server certificate.

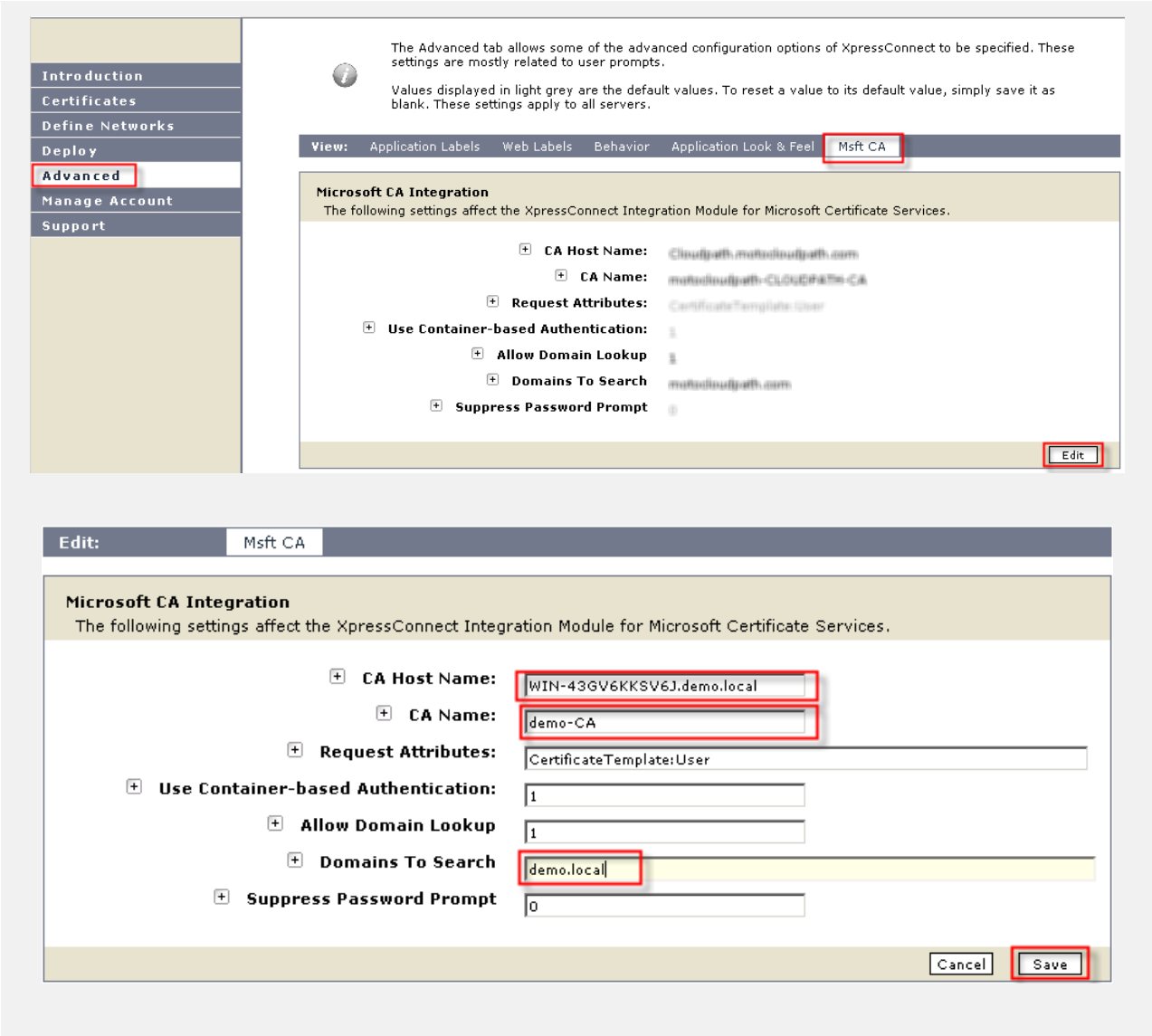


3	Identify the Windows Server name. Click Start, and right-click on Computer and select Properties. Copy the Full computer name. Close the window.


Notepad
Active Directory Users and Computers
Internet Information Services (IIS) Manager
All Programs
Search programs and files
administrator
Documents
Computer
Network
Control Par
Devices an
Administrat
Help and Support
Run...
Windows Security
Log off
Open
Manage
Map network drive...
Disconnect network drive...
Show on Desktop
Rename
Properties
Start

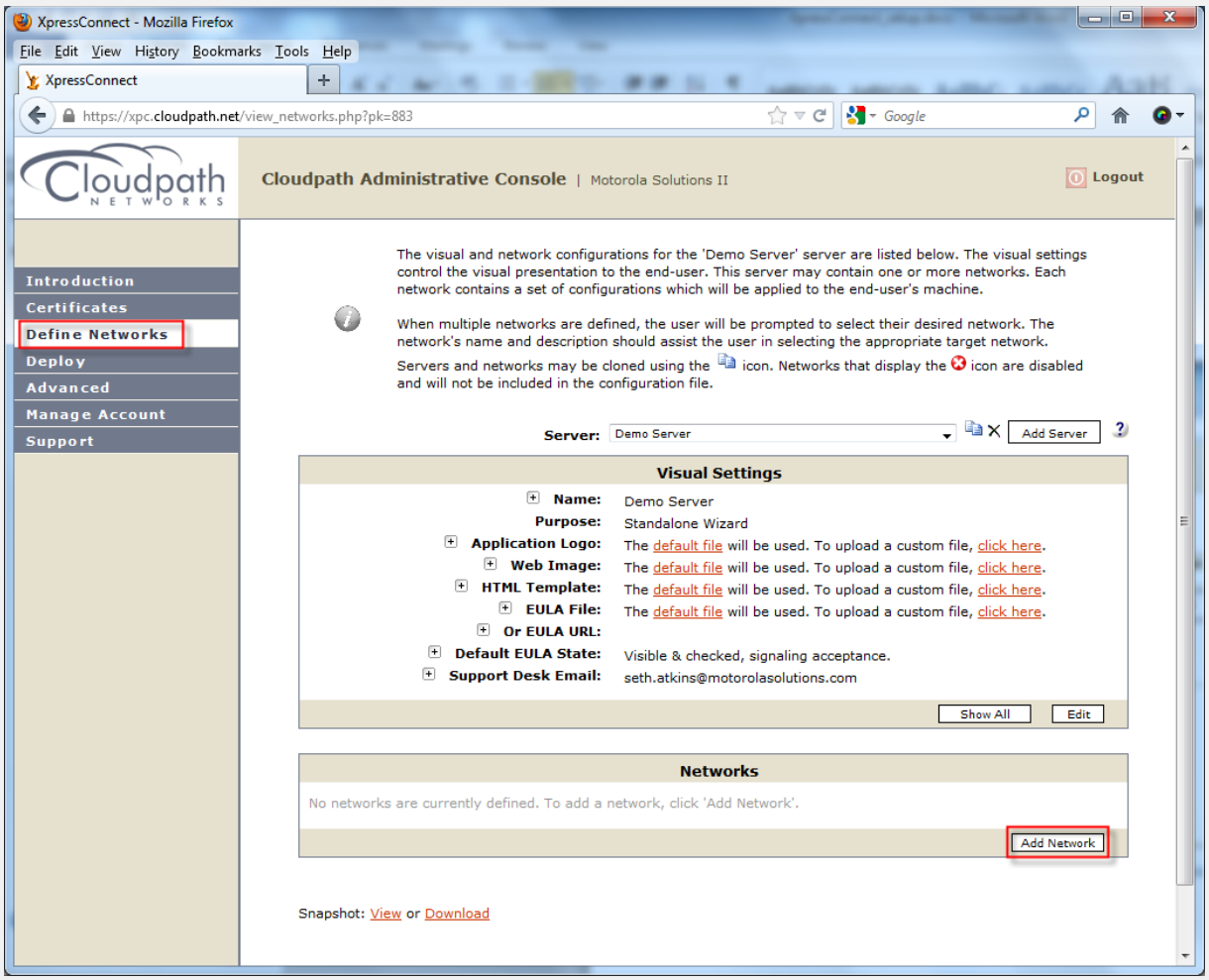


4	**Click Advanced → Msft CA. Click Edit. Fill in the CA Host Name, CA Name, and Search Domain fields with the information from the Windows Server setup in previous sections.**

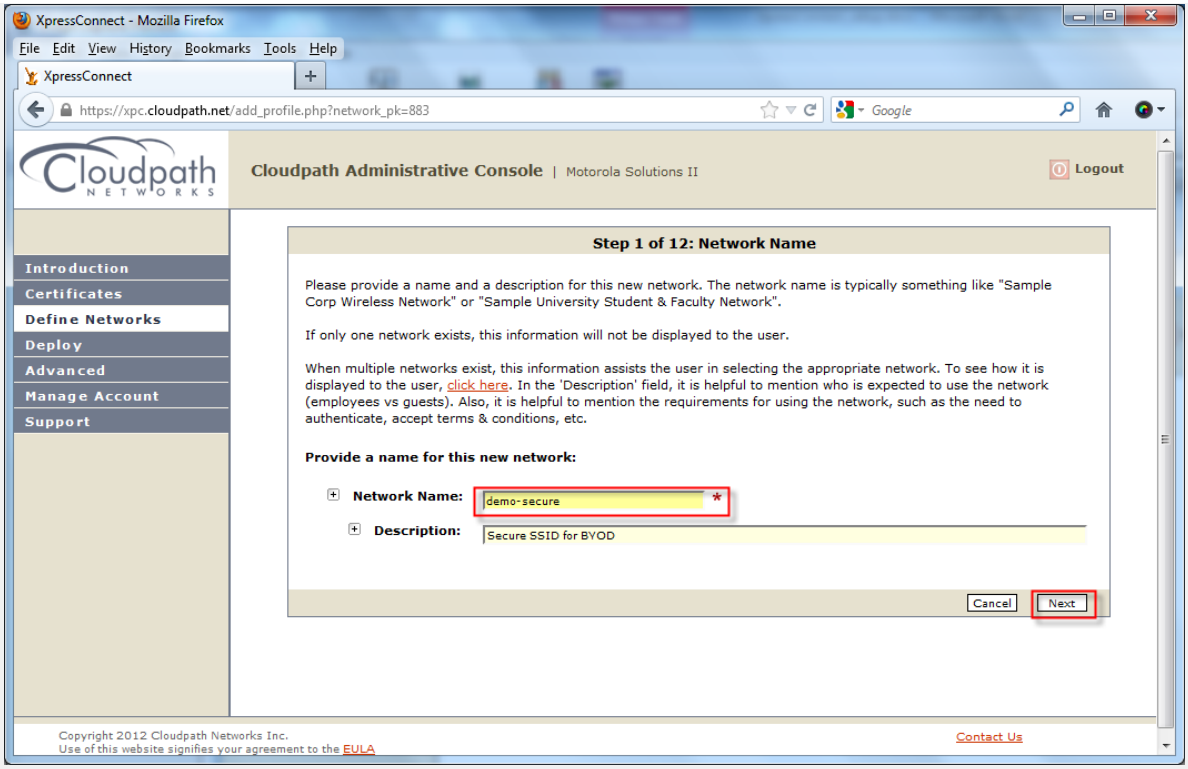


2.3.2 Configure a Network

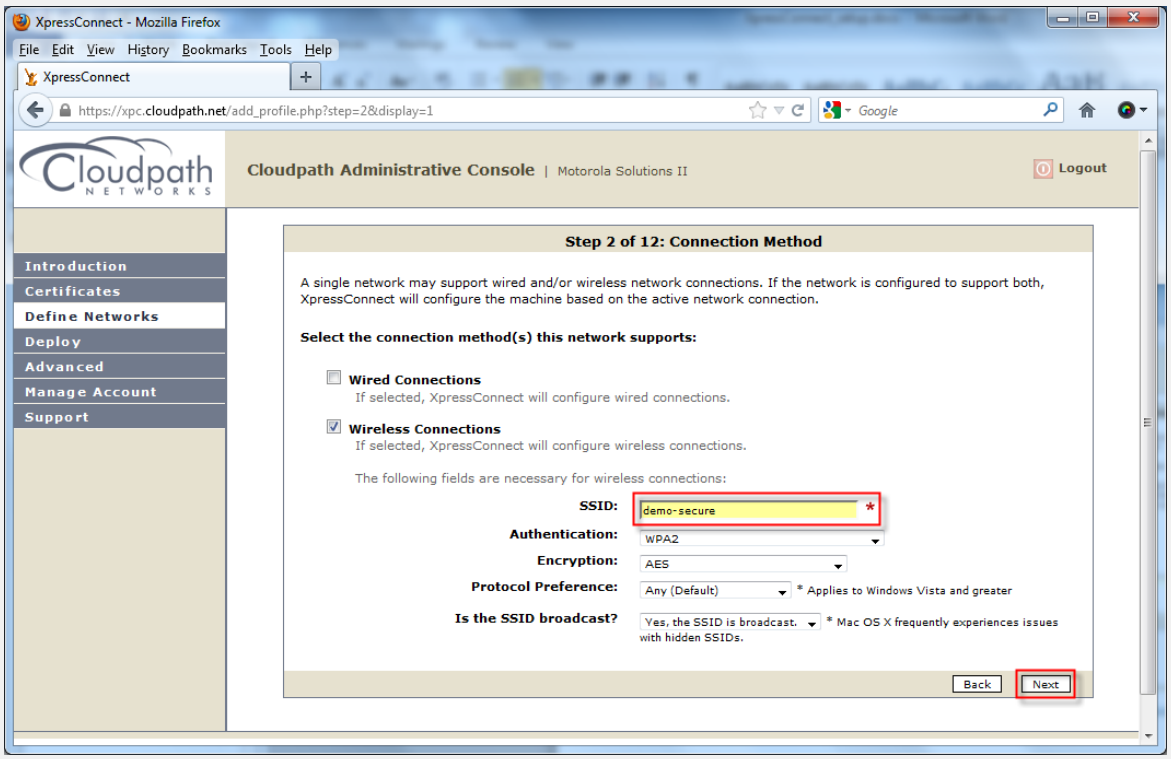
1	Select Define Networks and click Add Network.



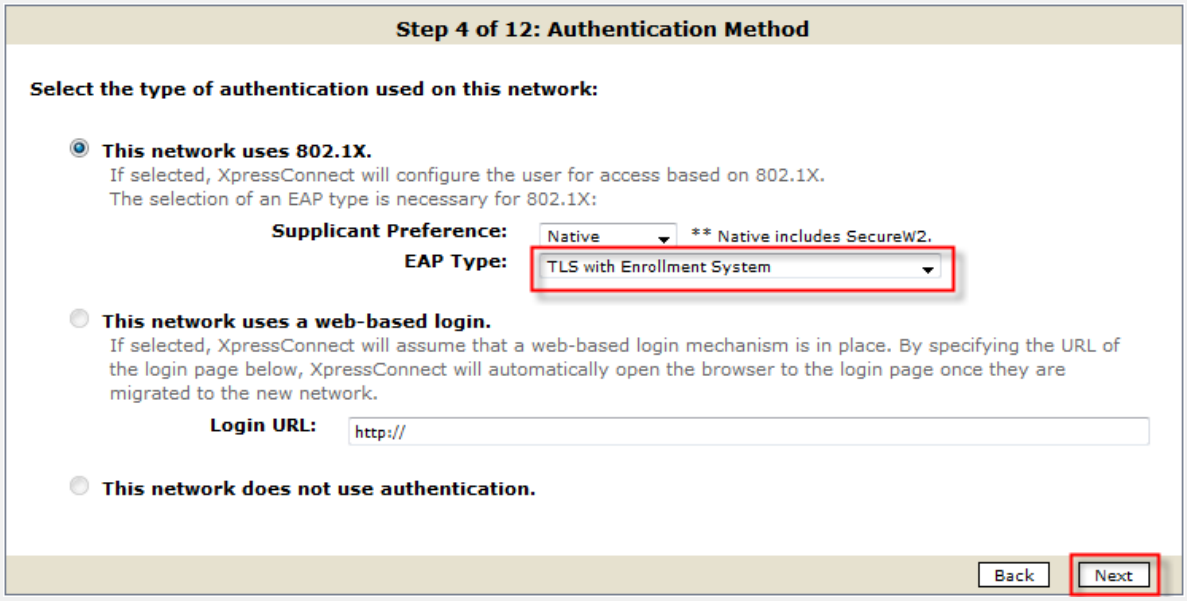
2 **Type a name for the network. Click Next.**

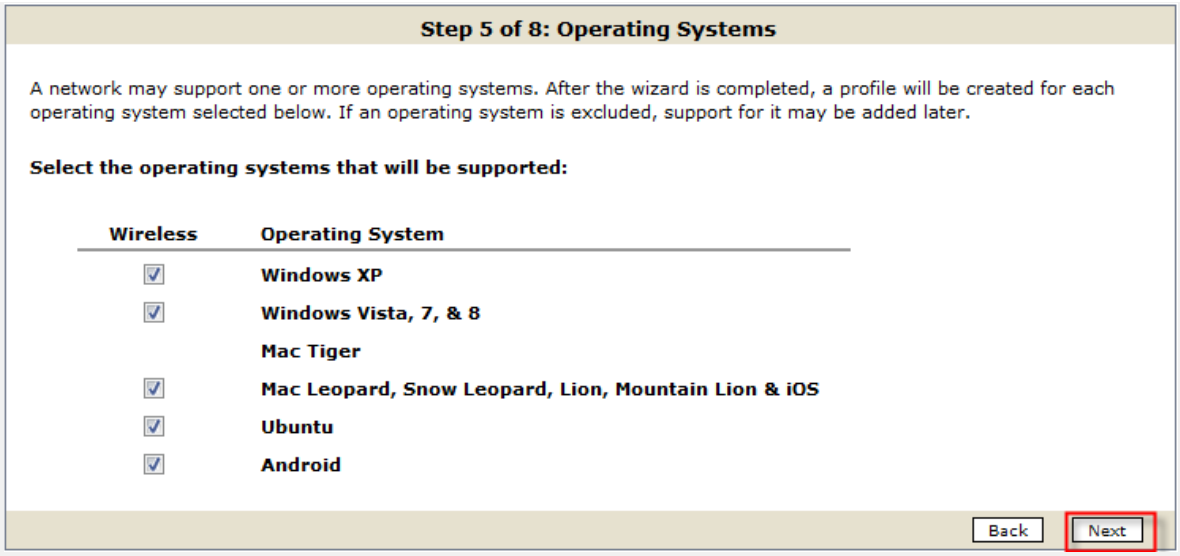


3	Type “demo-secure” for the SSID. Click Next. Click Next again.

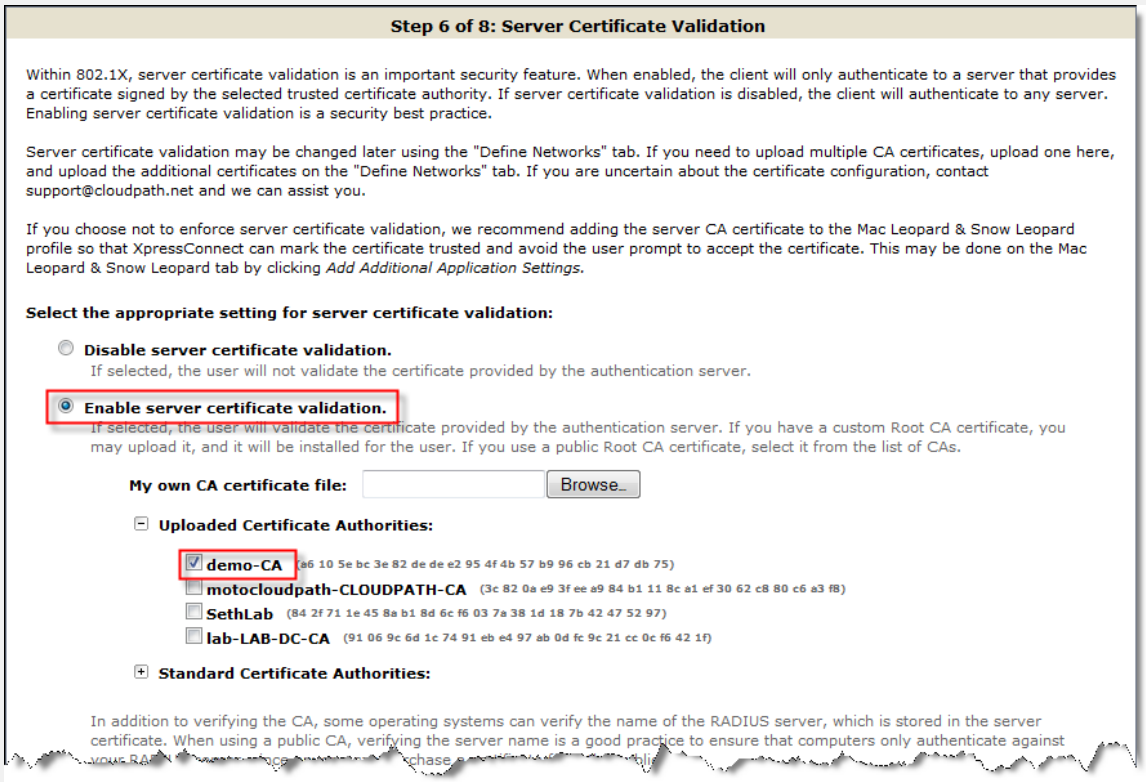


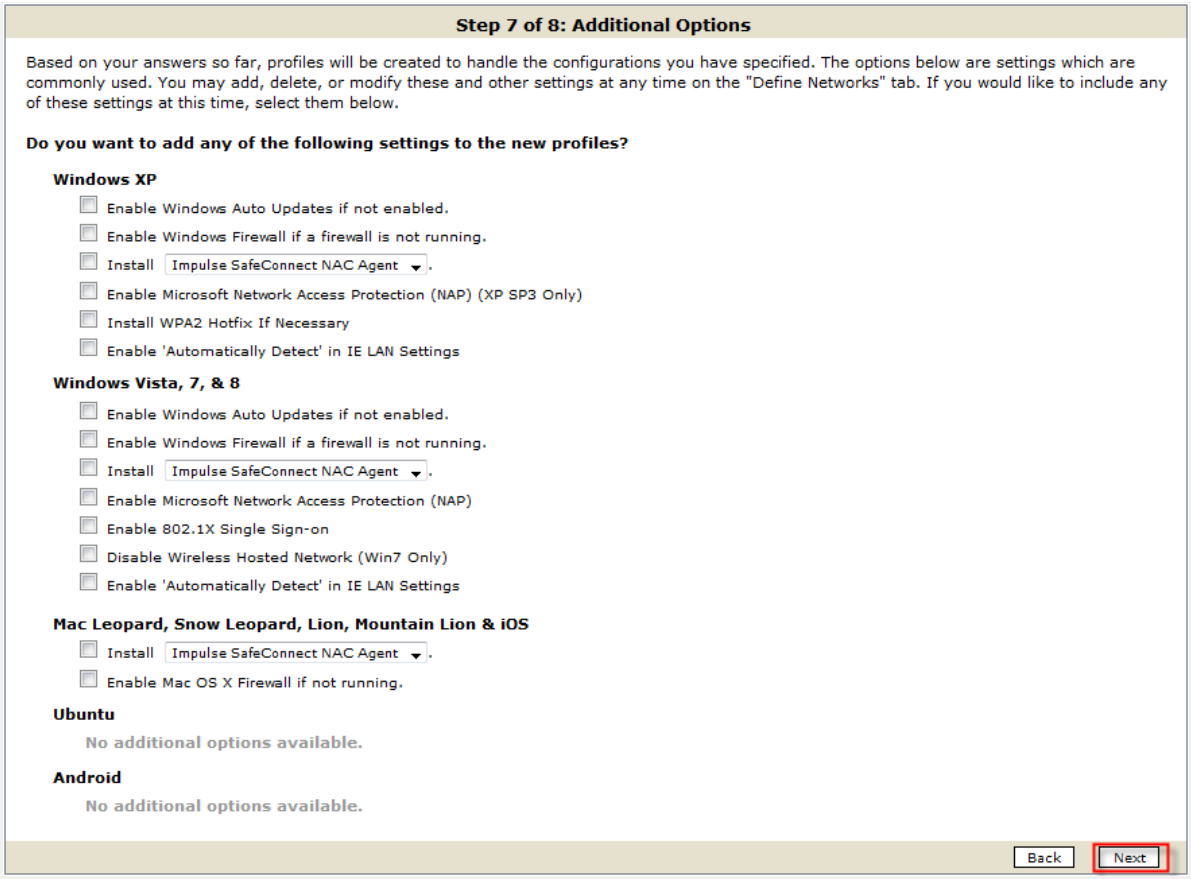
4 Select TLS with Enrollment System. Click Next. Click Next again.



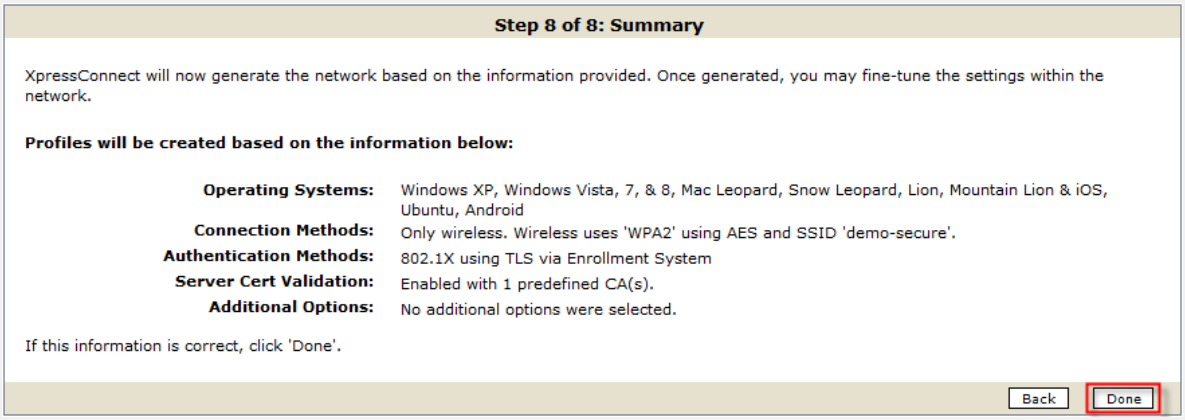


5 **Choose Enable server certificate validation and check the CA you imported previously. Click Next. Click Next again.**



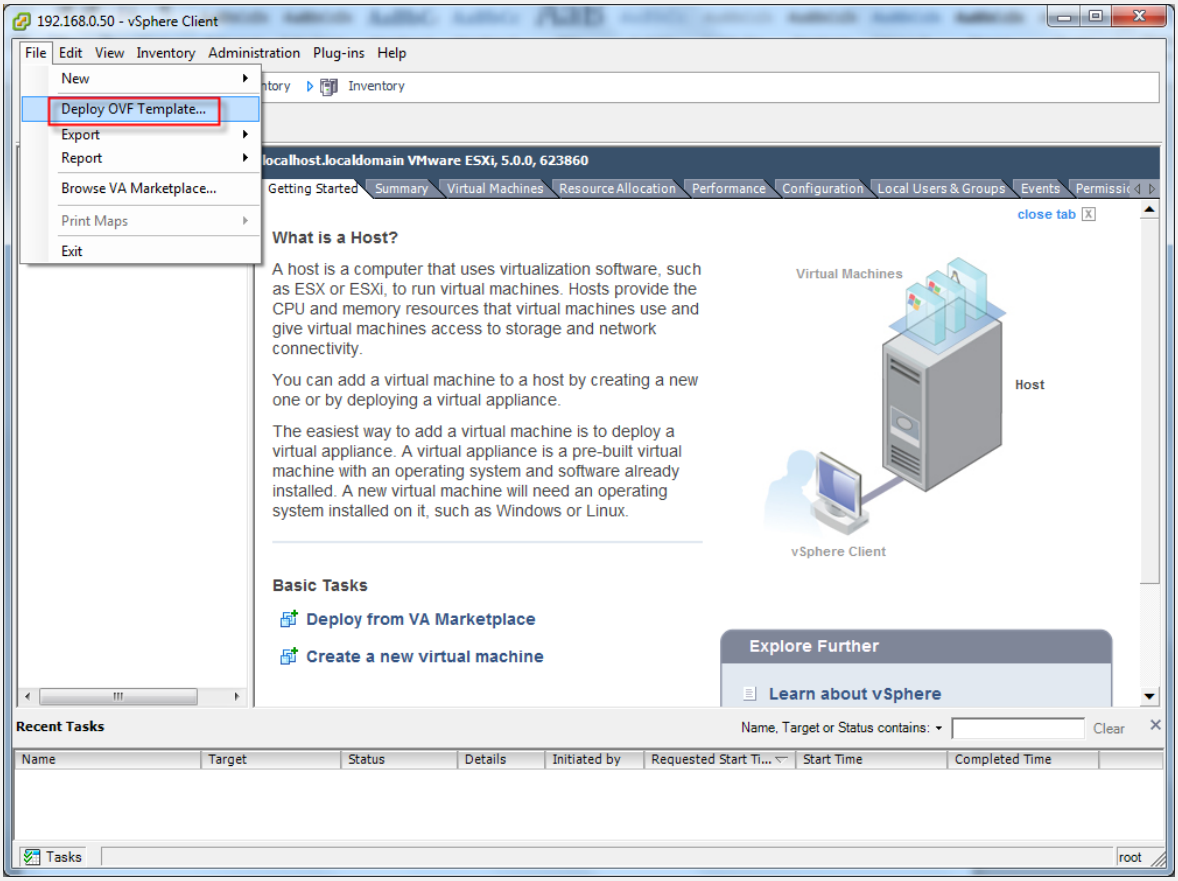


6 **Click Done.**

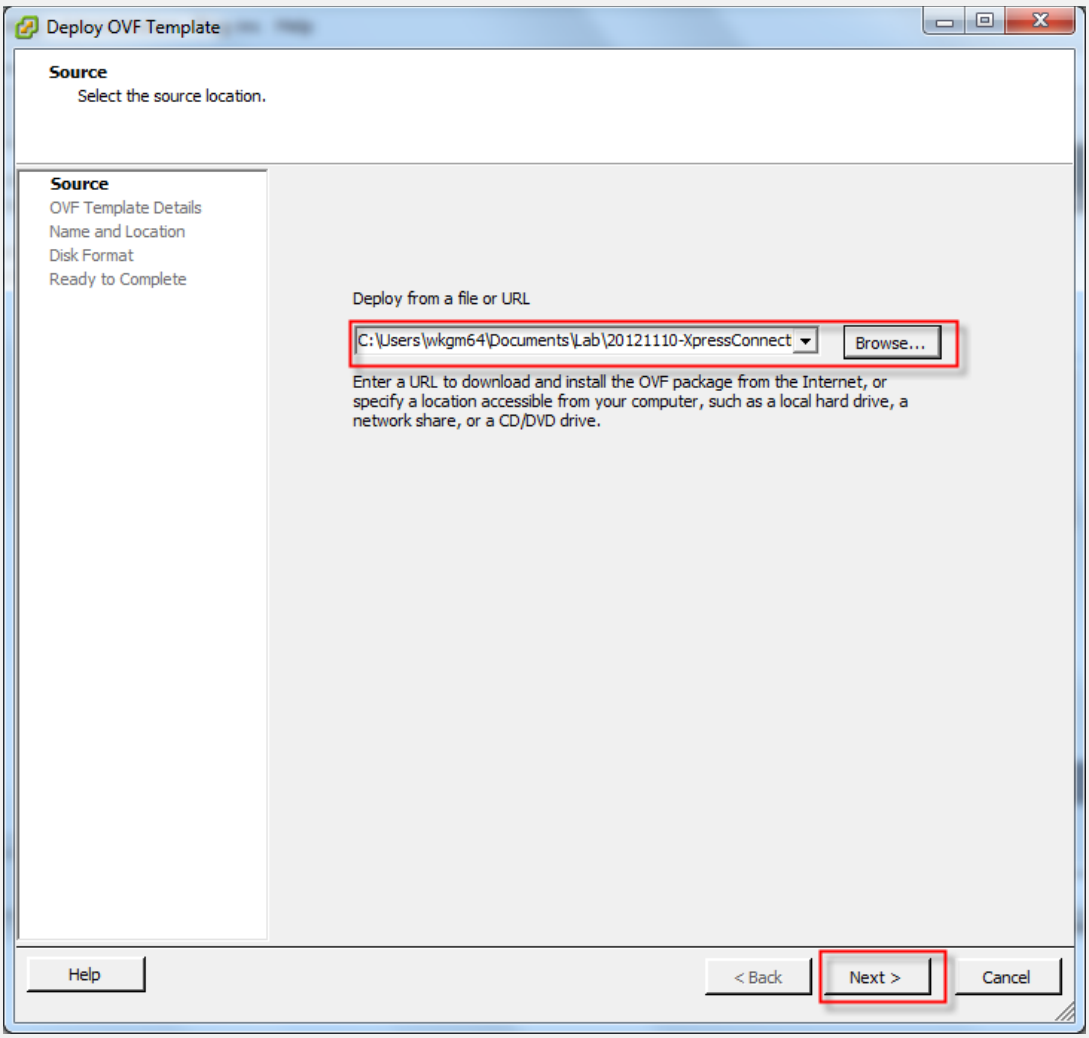


2.4 Configure the Enrollment Server Virtual Machine

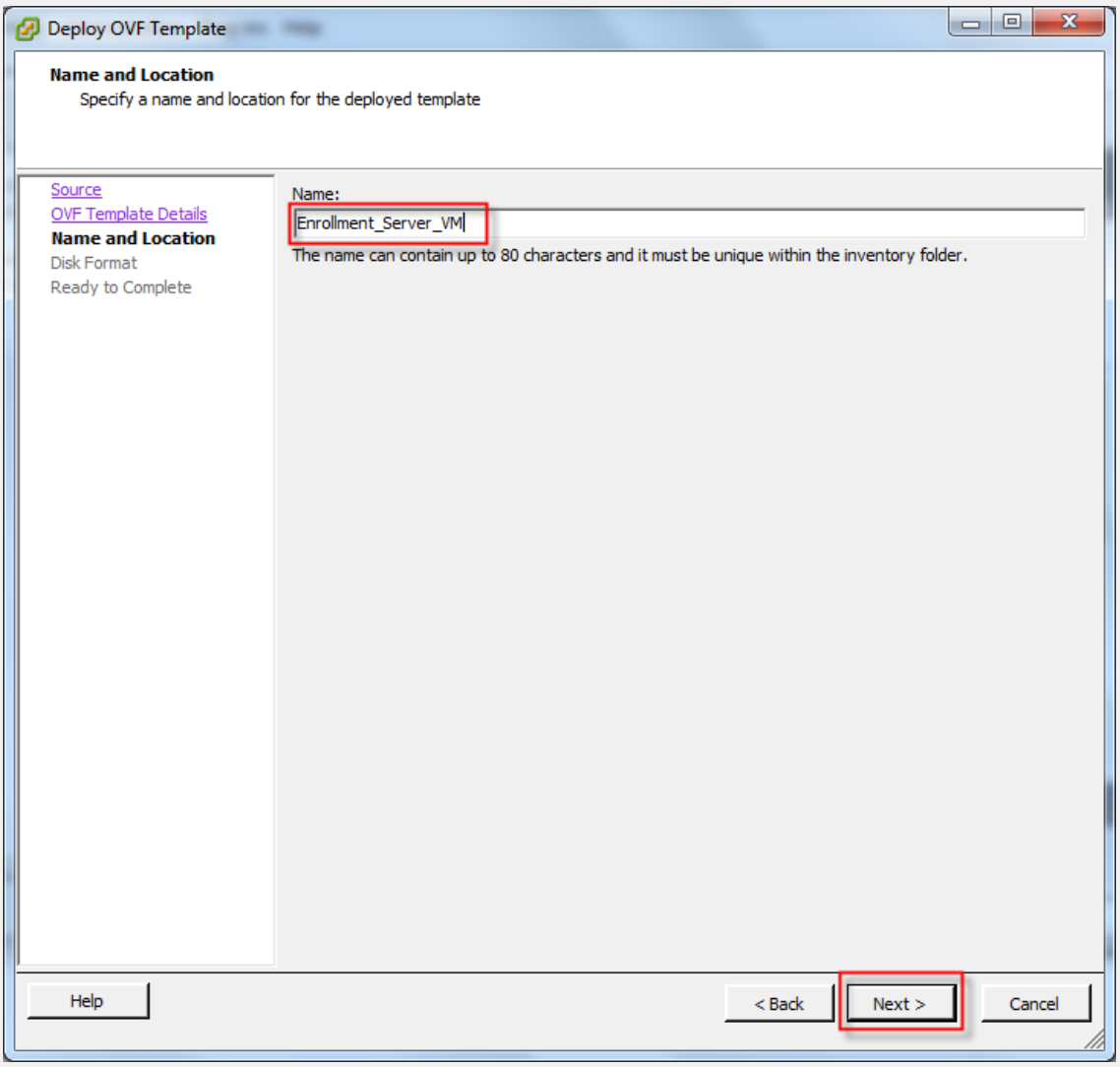
1	In vSphere Client click File → Deploy OVF Template.



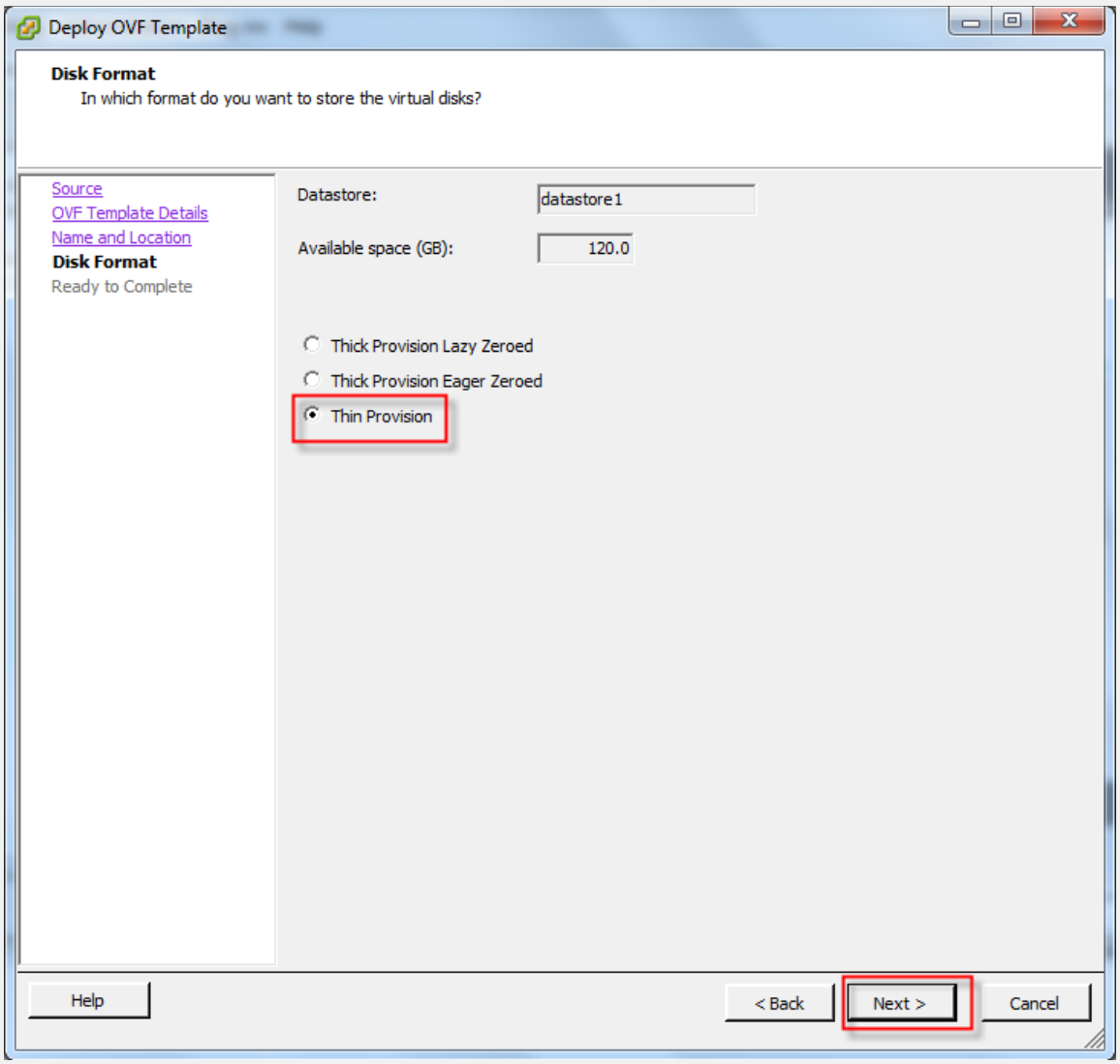
2	Click Browse and select the OVA file for the Enrollment Server VM. Click Next. Click Next again.



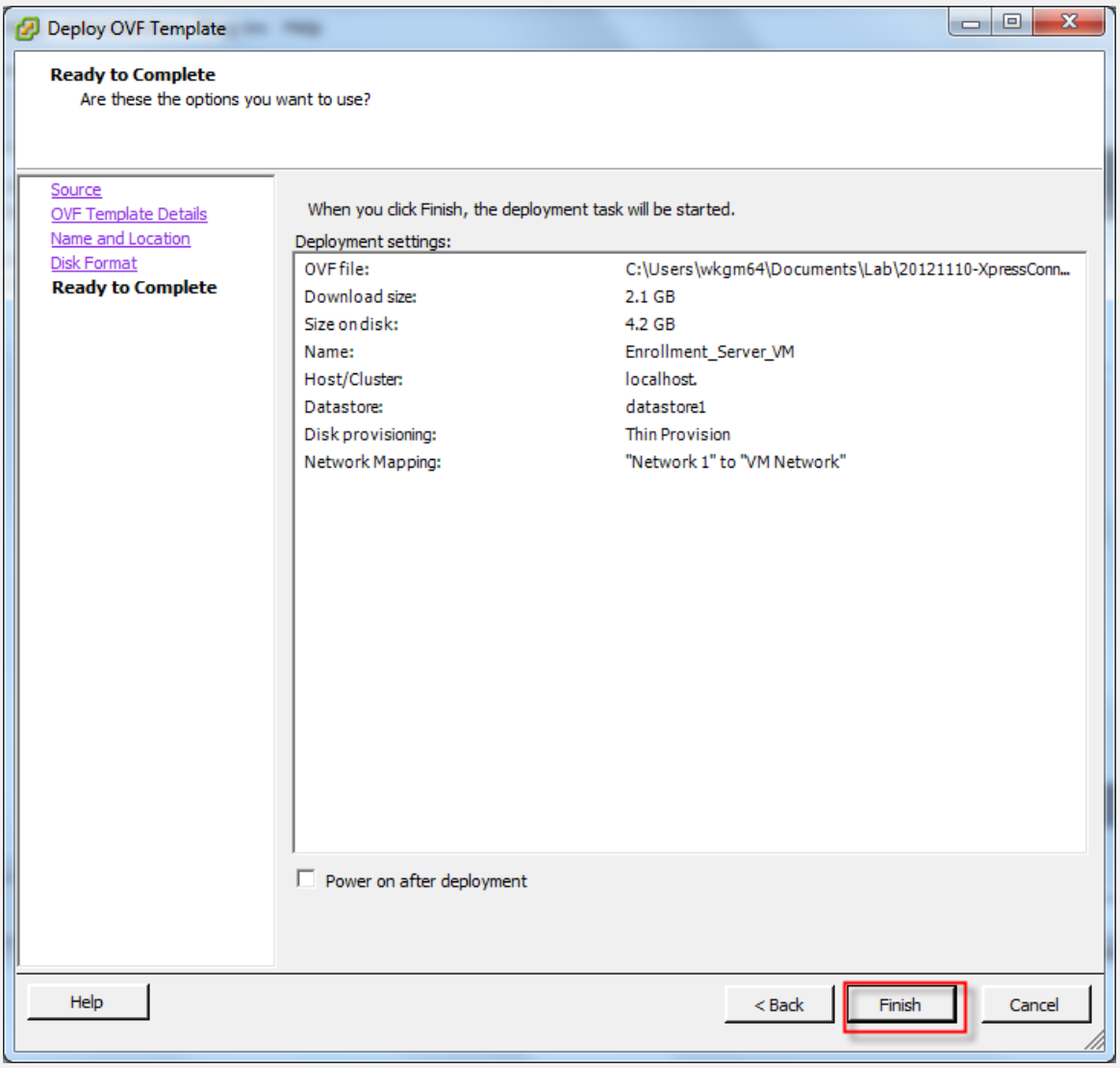
3	Give the VM a name and click Next.



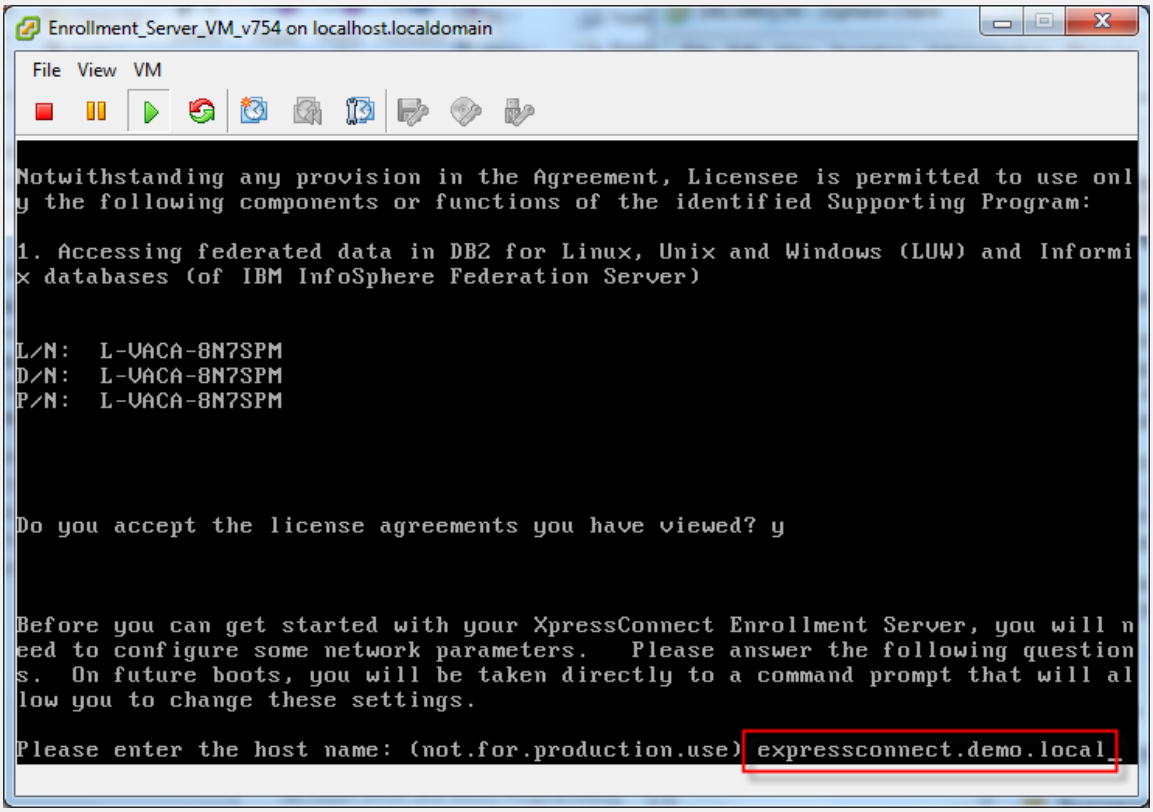
4	**Select Thin Provision, and click Next.**



5	**Click Finish.**

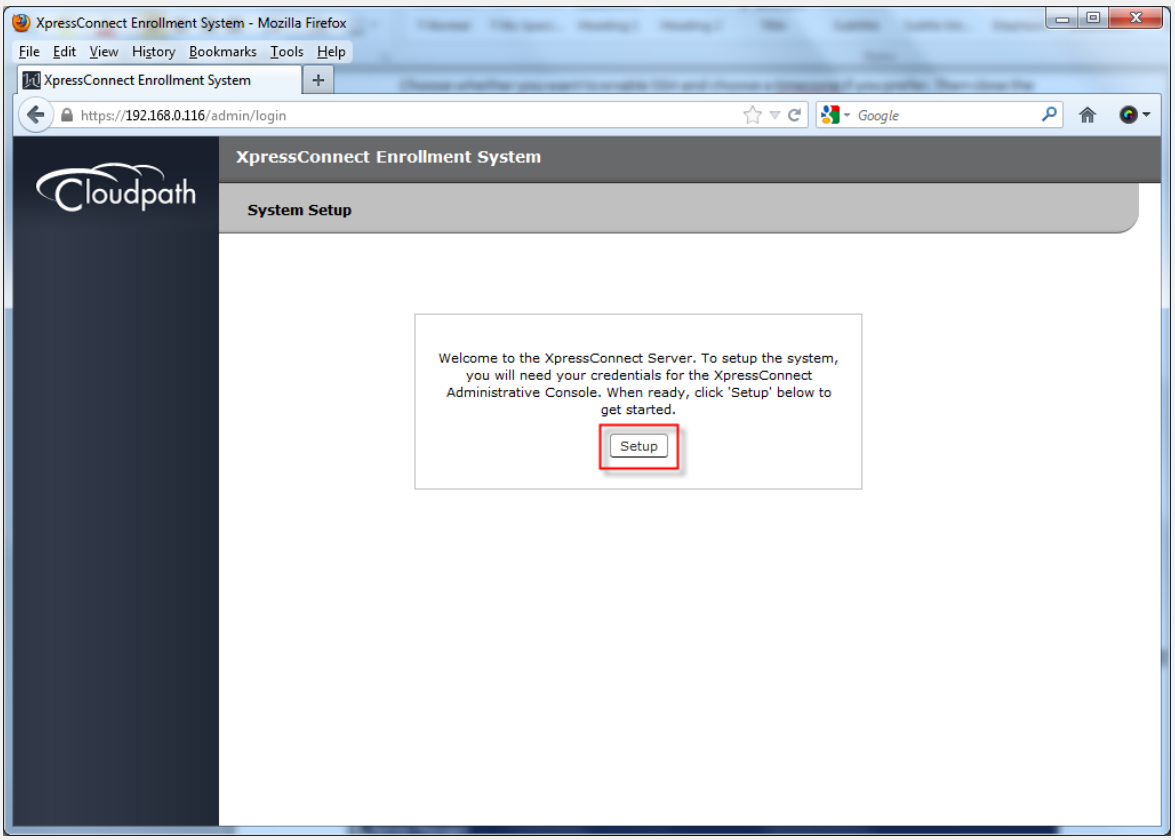


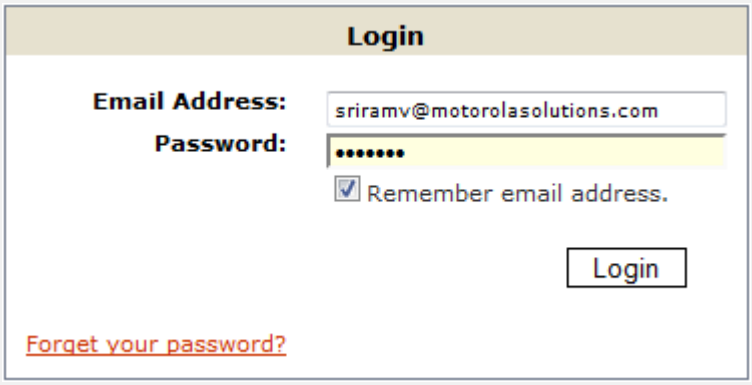
6	**Start the VM and click Launch Virtual Machine Console. Accept the license agreements. Give the server a hostname such as xpressconnect.demo.local. Note if you want to be able to ping this by DNS name, you will need to configure a record in the DNS server. Configure IP address, mask, gateway, and DNS server. Note: the DNS server should be the Windows server configured in previous steps.**



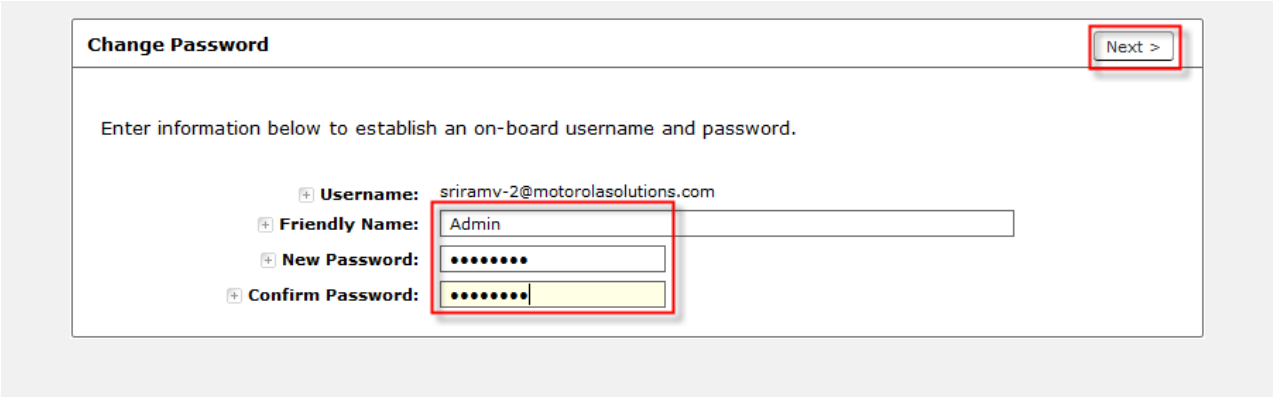
7	**Choose whether you want to enable SSH and choose a timezone if you prefer. Then close the virtual console window.**

8	**Open a web browser and point it to the IP address of the xpressconnect server. For example, http://192.168.0.116/. You will be prompted to begin setup. Click Setup. Click Next. Enter credentials and click Login.**

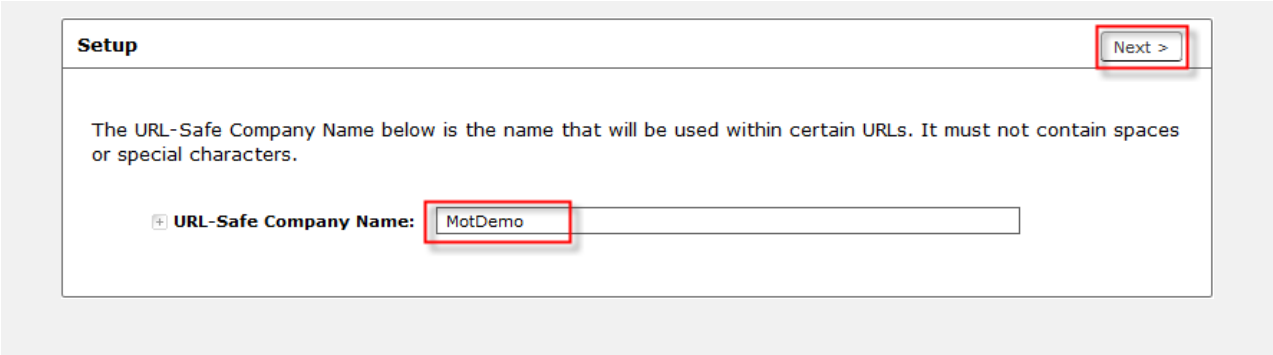




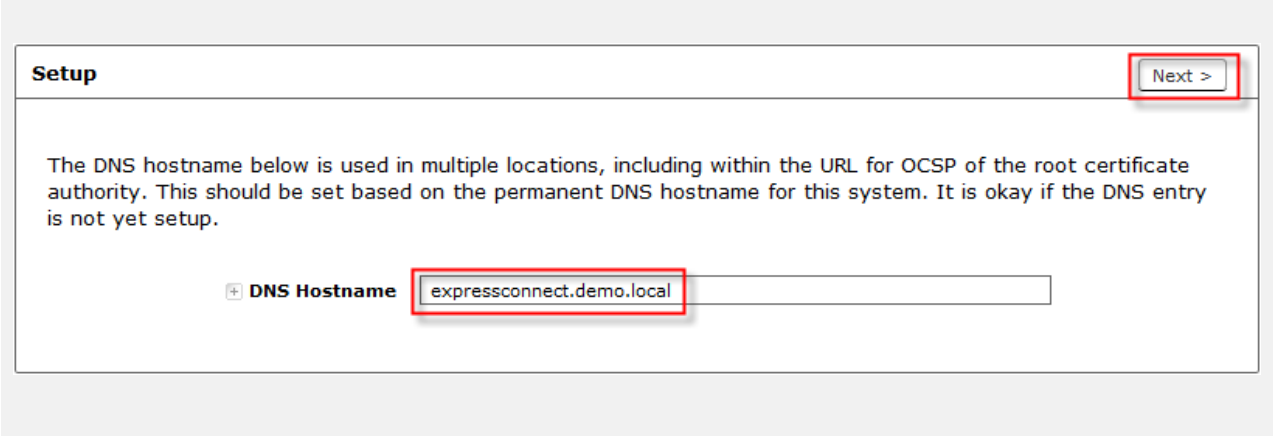
9	Type a Name and new password. Click Next.



10	Type a name with no spaces that will be used in the onboarding URL. Click Next.

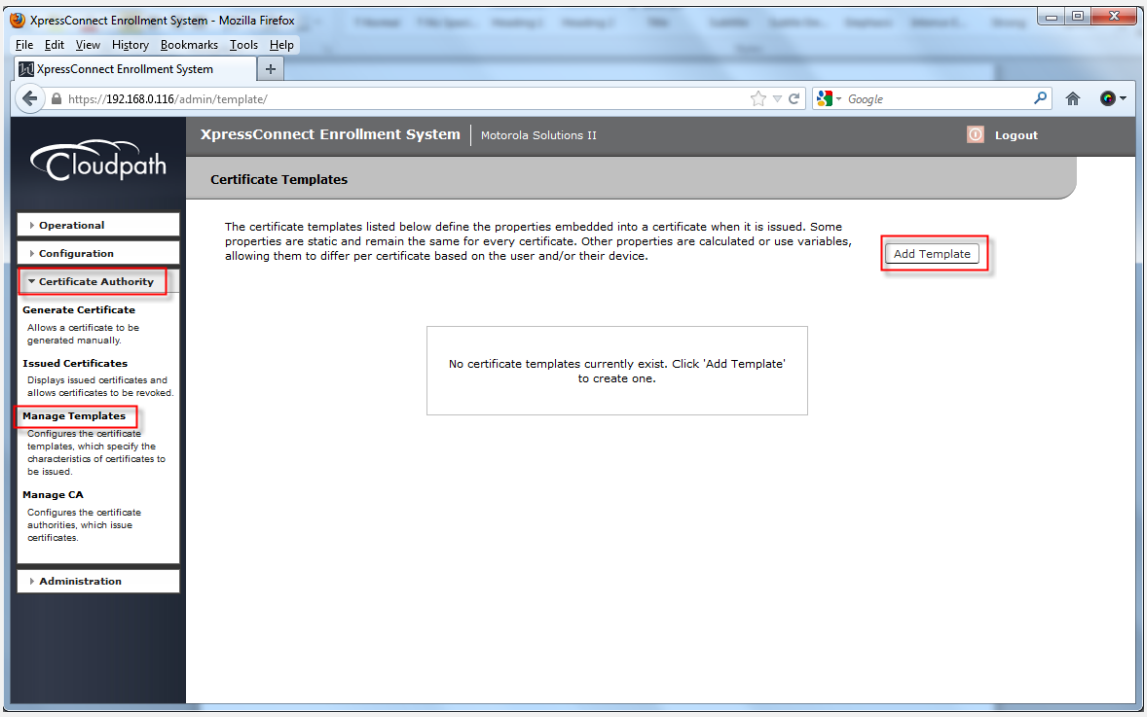


11	Confirm DNS hostname. Click Next.

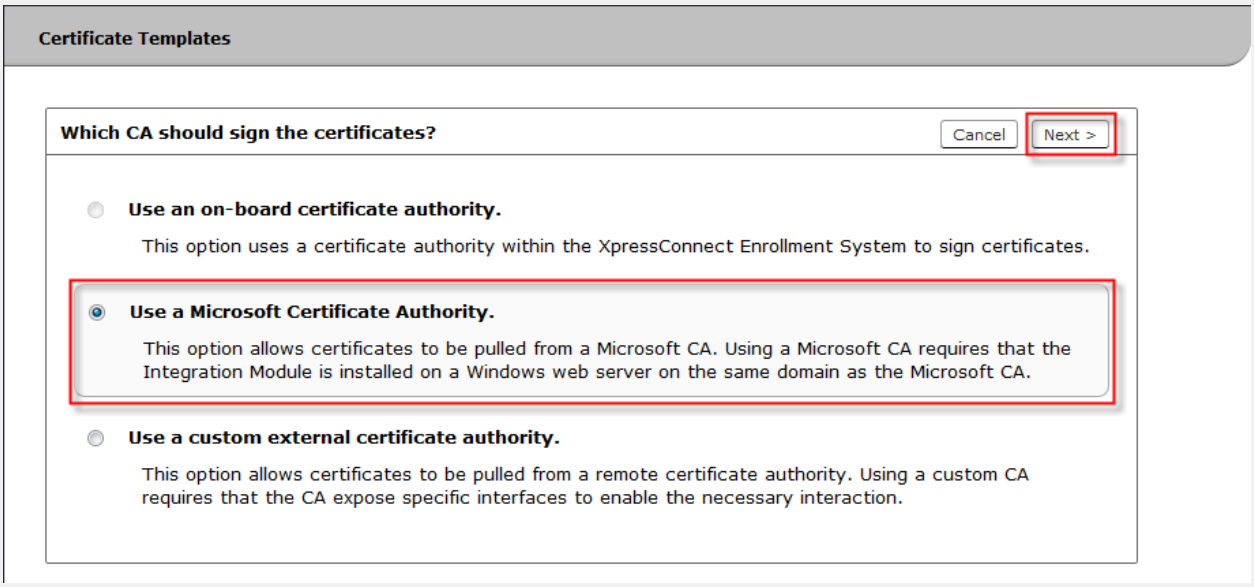


2.5 Configure Integration Module on Windows Server

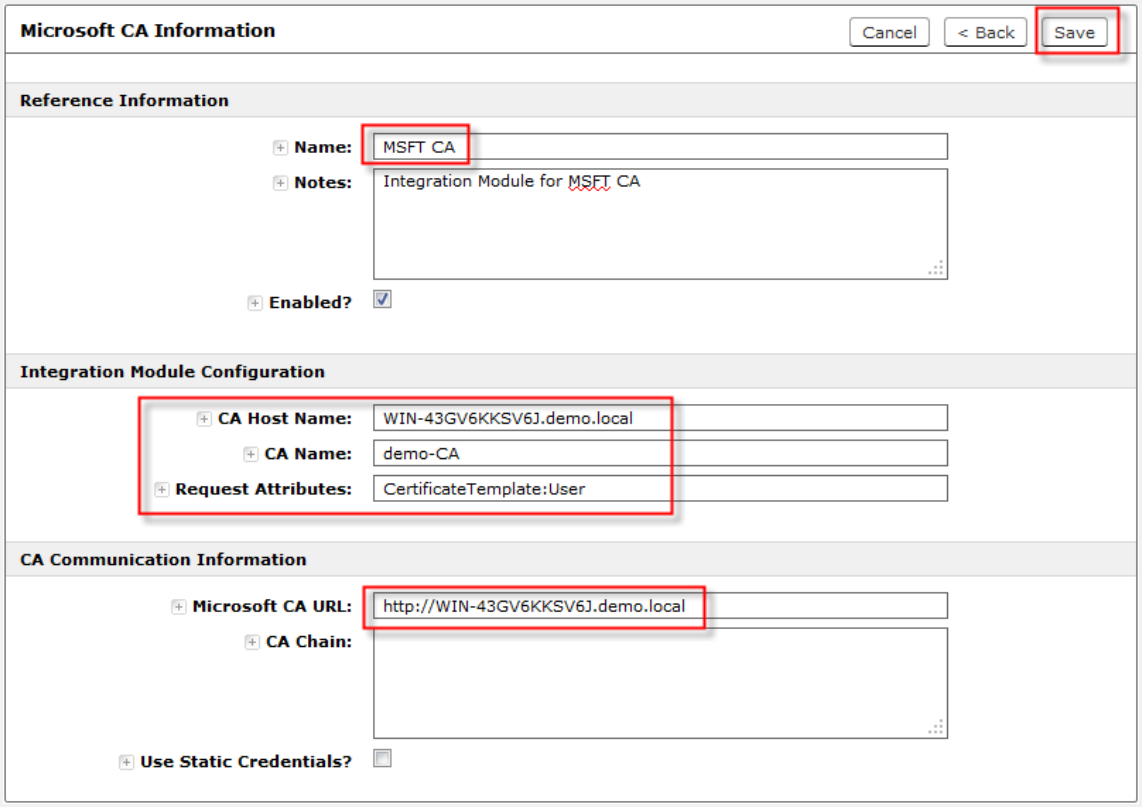
1	In the web interface of the Enrollment Server, go to Certificate Authority → Manage Templates. Click Add Template.



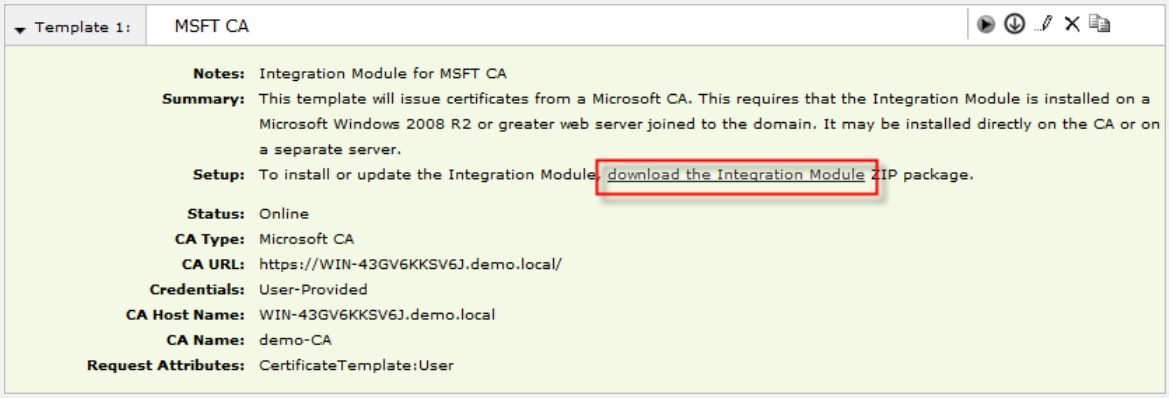
2	Choose Use a Microsoft Authority. Click Next.

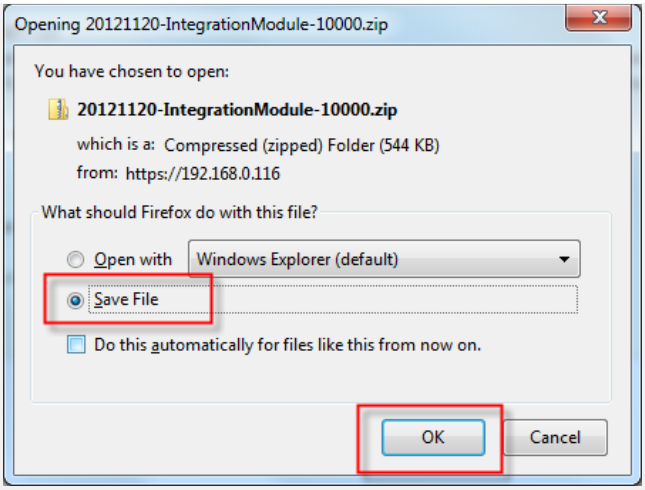


3	Type “MSFT CA” for the Name, and type the CA Host Name and CA Name from previous steps. In the Request Attribute text box, type “CertificateTemplate:User”. This must be exact. Fill in the CA URL field corresponding to the DNS name of the Windows Server. Click Save.

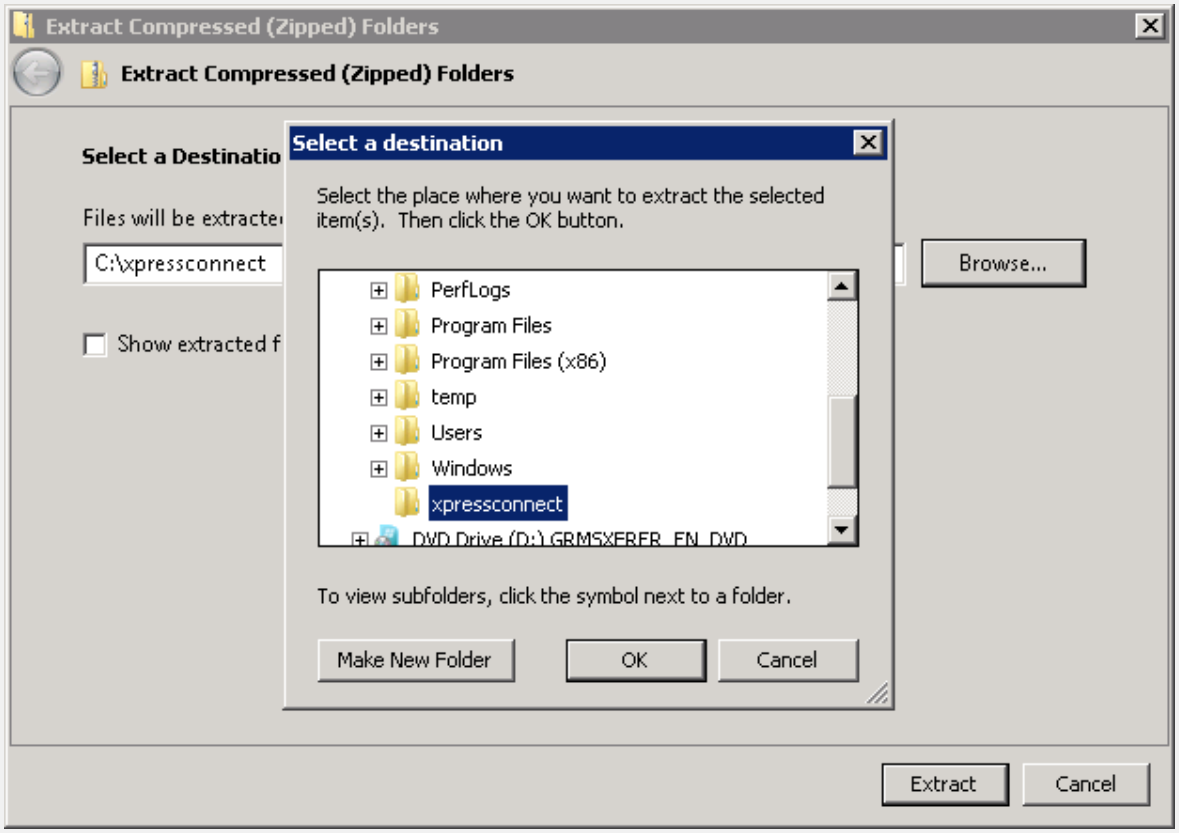


4	**Click download the Integration Module URL. Save the ZIP file to the Windows Server. This step is simpler if you are using a browser on the Windows Server to access the Enrollment Server so the package is saved to the local hard drive.**



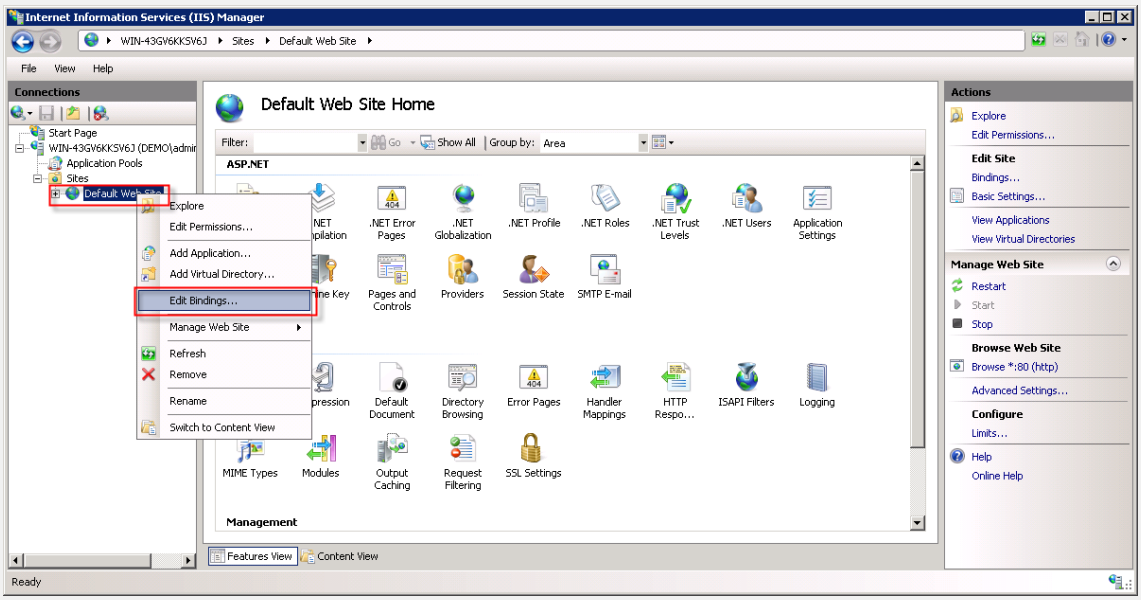


5	**Extract the contents of the ZIP file to a local folder. Create a new folder named SecureAccess, and unzip into that folder. Click OK. Click Extract.**

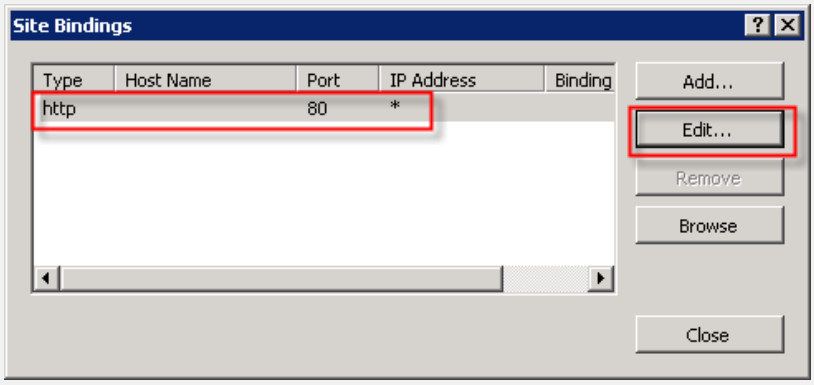


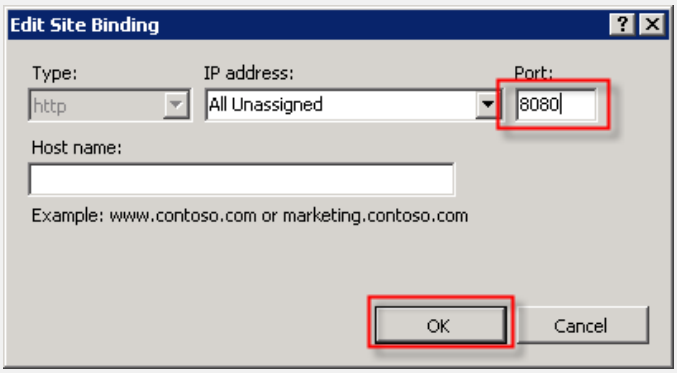
6	**Start IIS Manager by clicking Start and typing inetmgr in the search box, and press Enter. In IIS Manager, expand <server_name> → Sites, and right-click Default Web Site and select Edit**

Bindings.

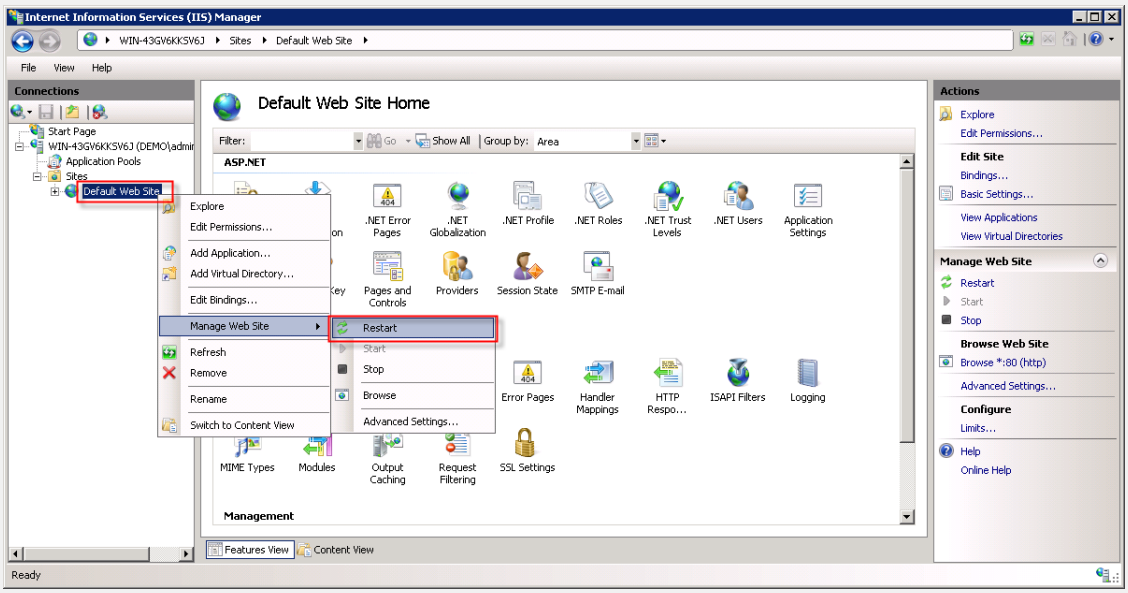


7 **Click Edit. Change the port number from 80 to something else, such as 8080. Click OK. Click Close.**

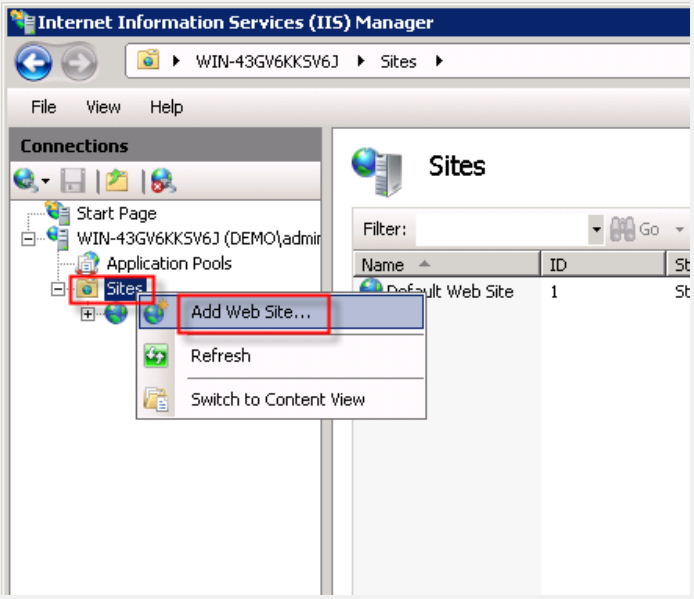




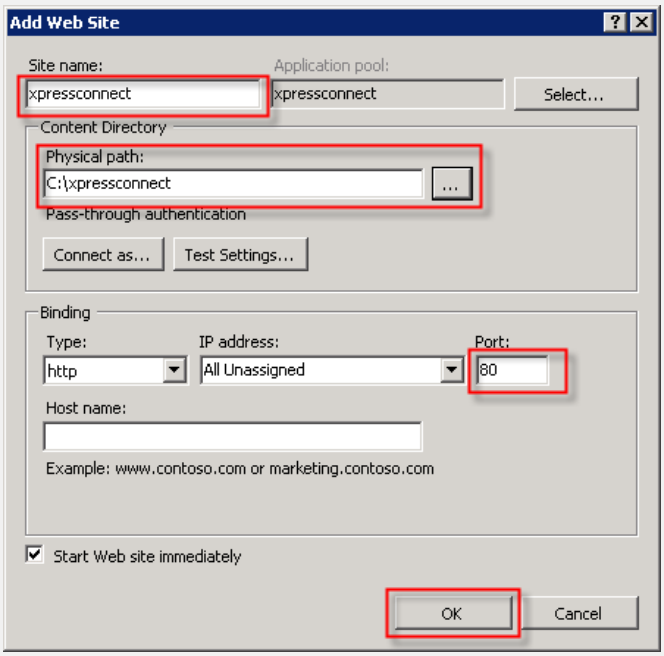
8	Right-click Default Web Site, select Manage WebSite → Restart to restart the site.



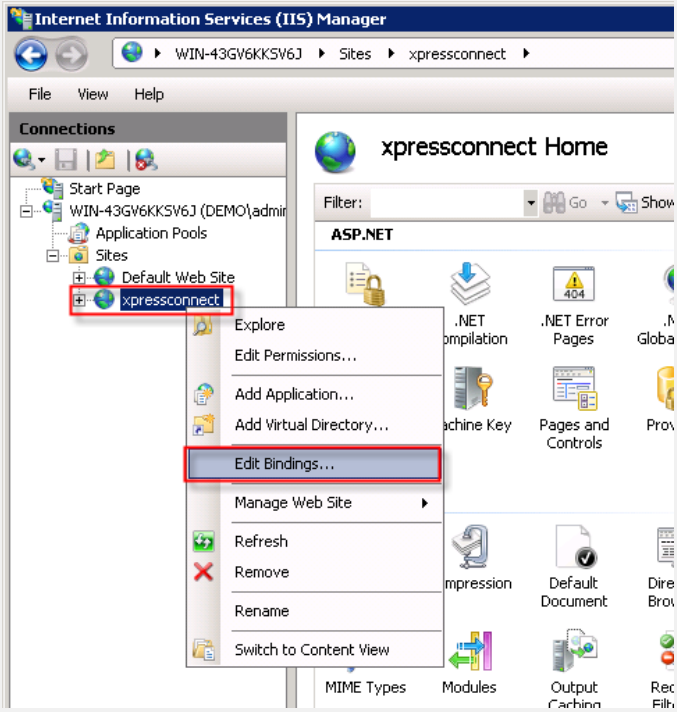
9	Right-click Sites and select Add Web Site.



10	Name the site SecureAccess, and set the path to the location where you extracted the ZIP file previously. Set the port to 80. Click OK.

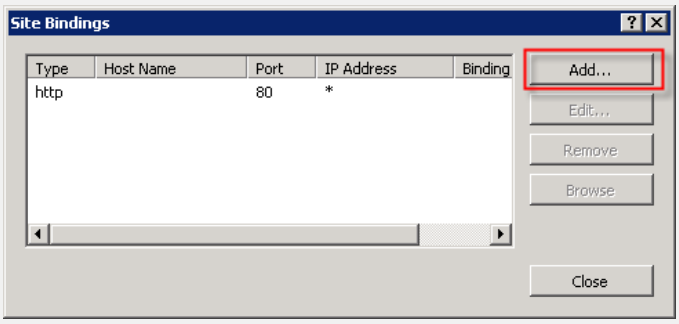


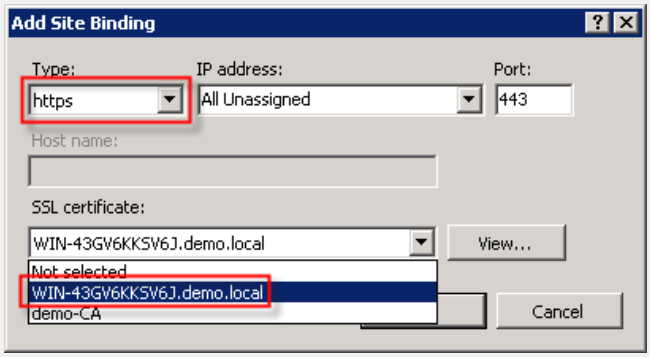
11 **Right-click the new SecureAccess site, and select Edit Bindings.**



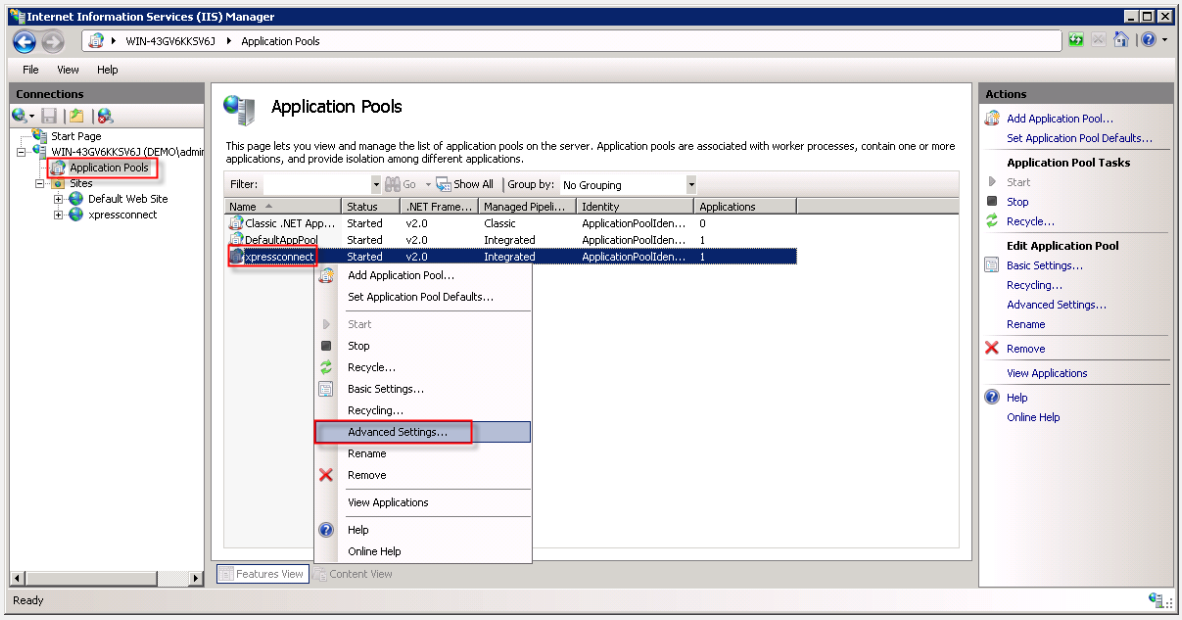
12 **Click Add. Select https. Select the SSL server certificate to be the same certificate used by**

NPS previously (not the root CA certificate). Click OK. Click Close.

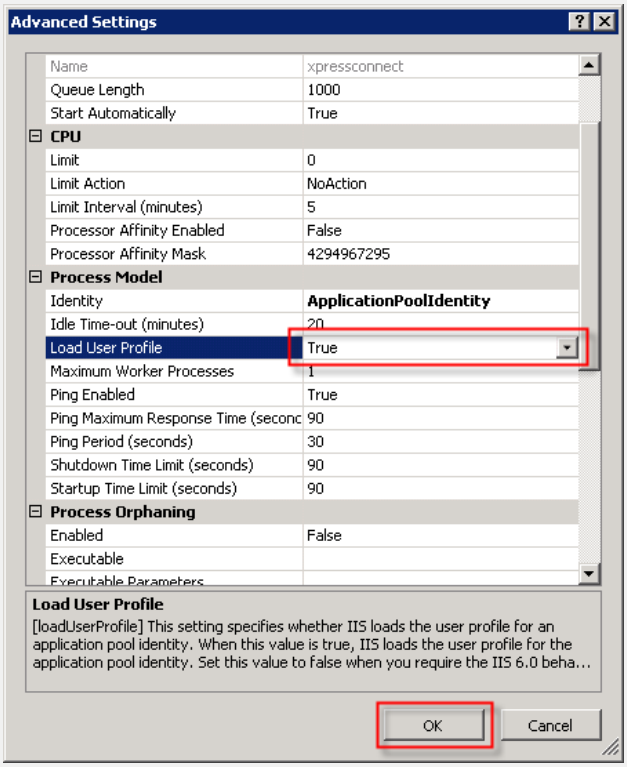




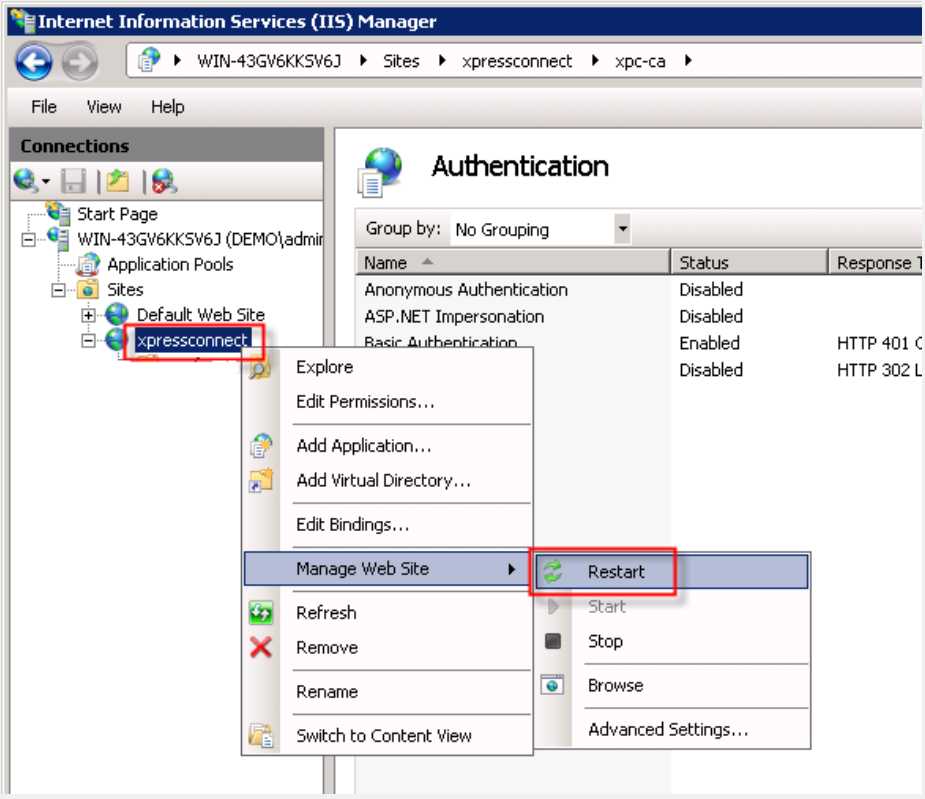
13 Click Application Pools. In the right-hand window pane, right click SecureAccess and select Advanced Settings.



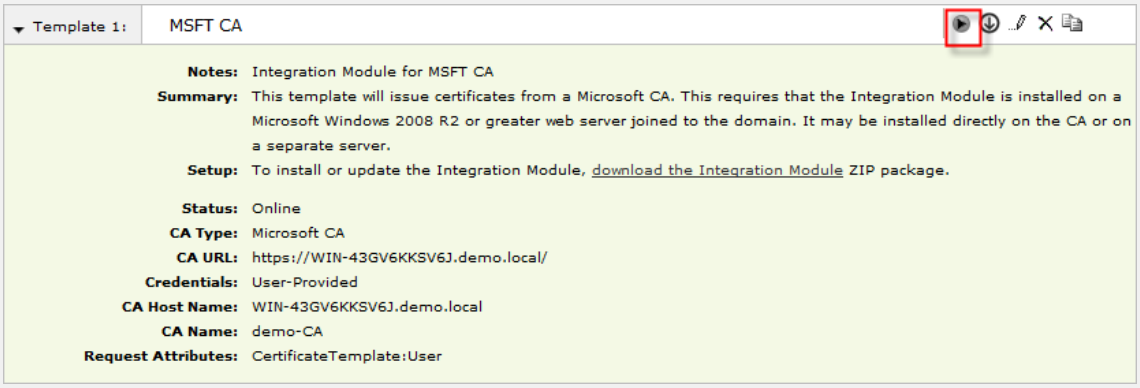
14 Change the Load User Profile parameter to True. Click OK.

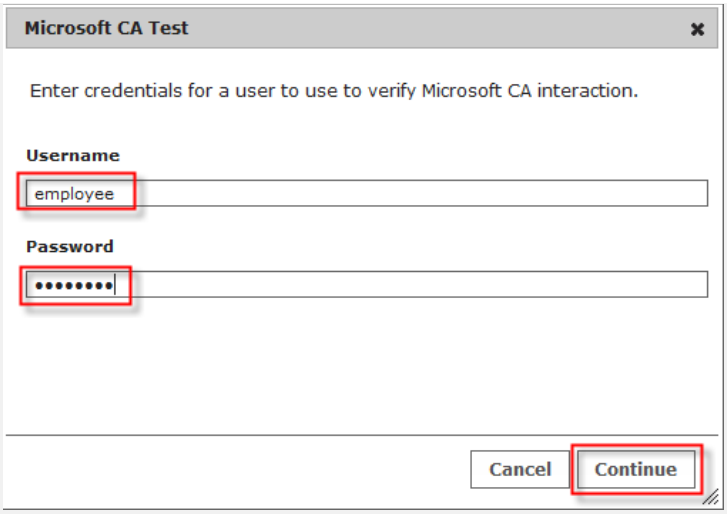


15 Right-click the SecureAccess site and select Manage Web Site → Restart.



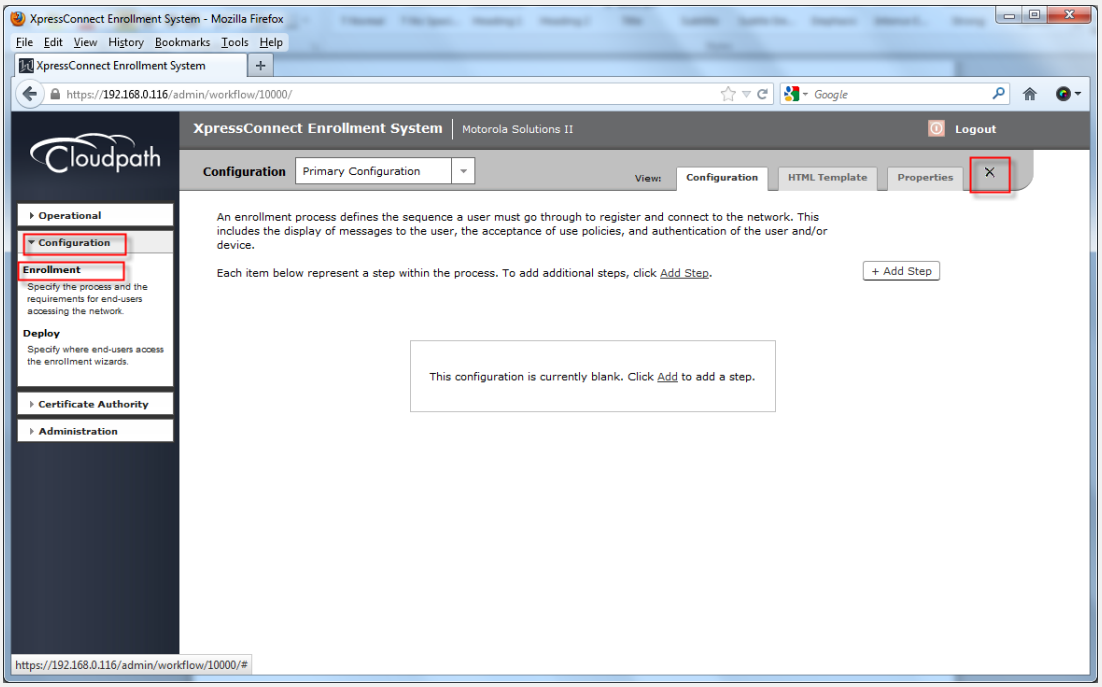
16 **On the Enrollment Server, click the play button on the template to test the configuration. Provide user credentials and click Continue. You should see success information as well as a certificate in the results screen.**

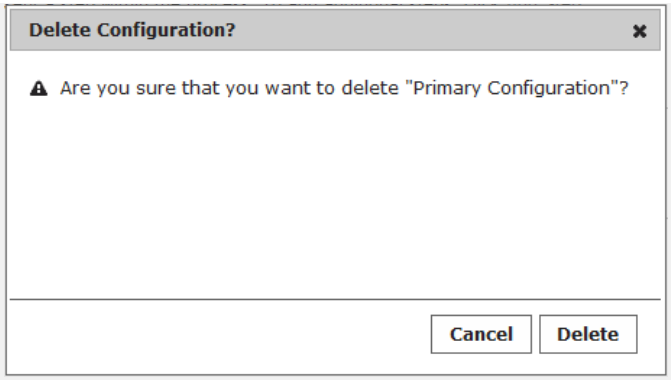




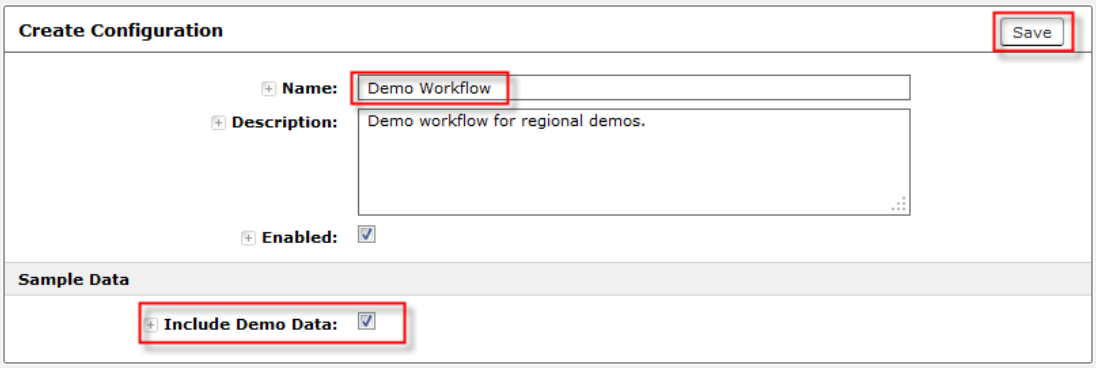
2.6 Configure Workflows on the Enrollment Server

1	In the web interface of the Enrollment Server, go to Configuration → Enrollment. Click on the X in the upper right corner. Confirm by clicking Delete.

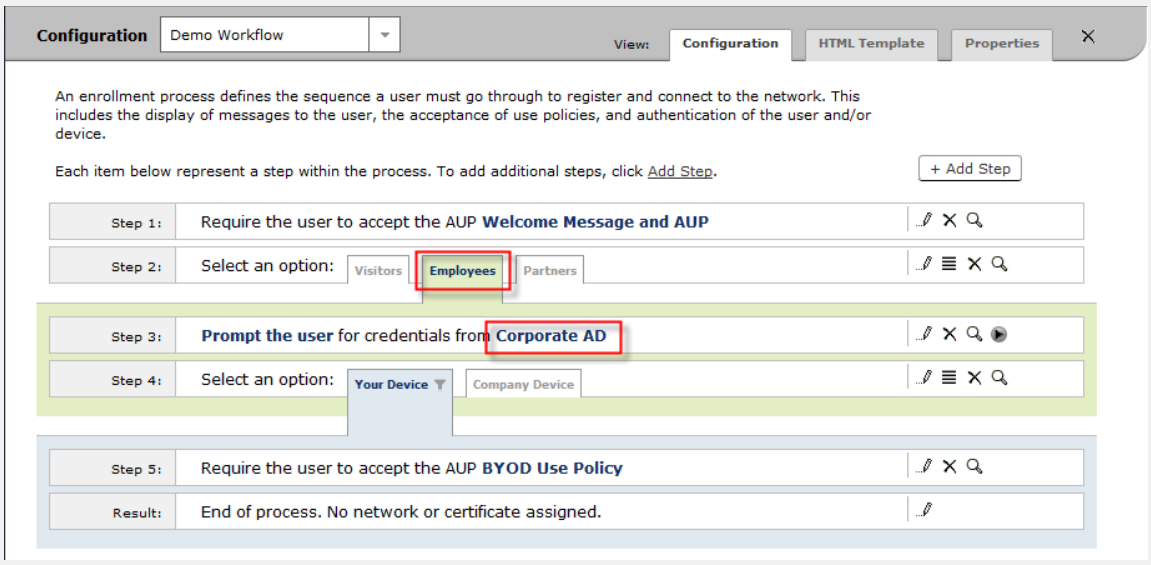




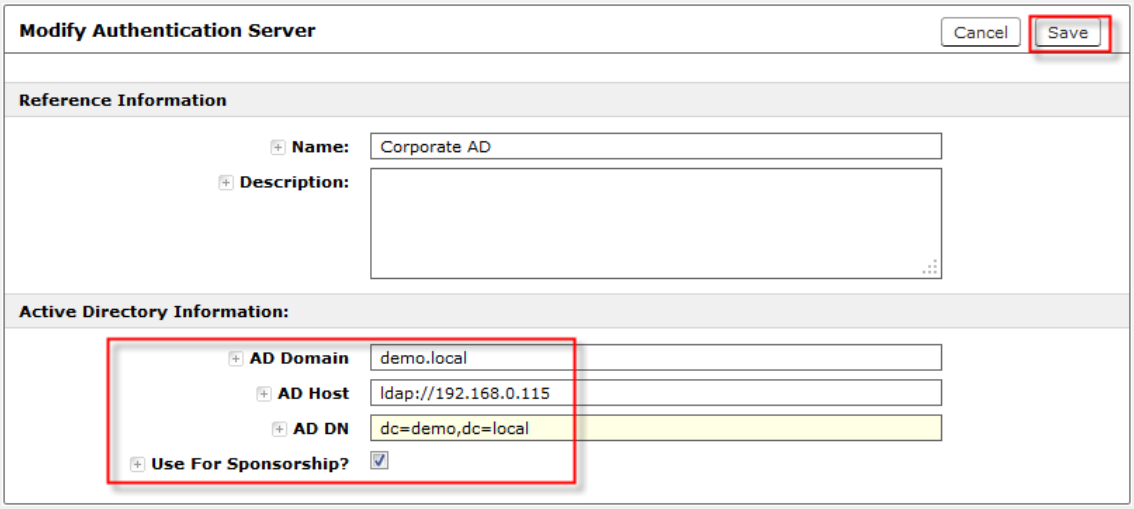
2	Click the “click here” URL. Name the configuration Demo Workflow. Check Include Demo Data, and click Save.



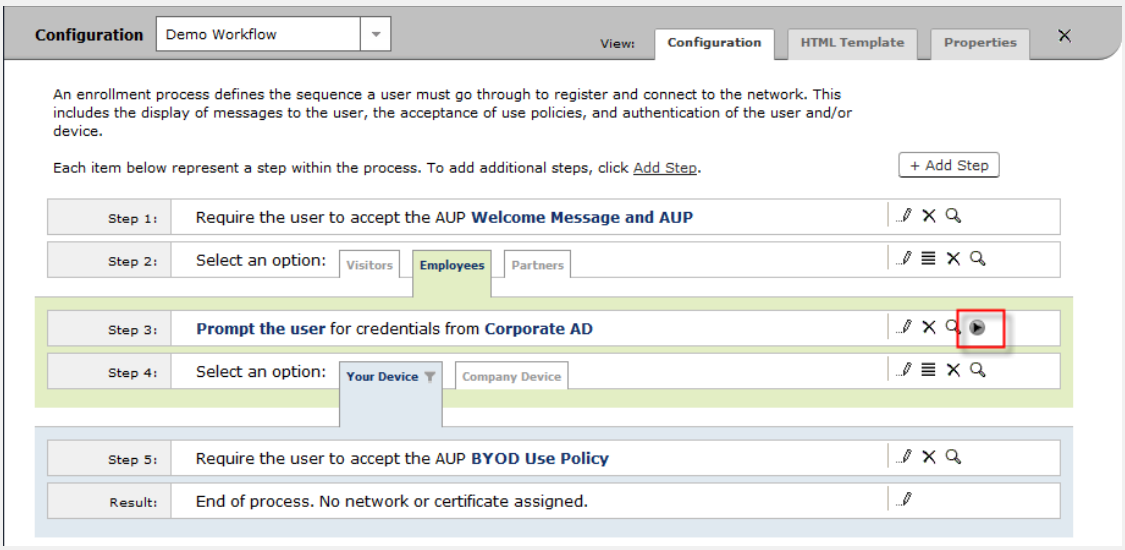
3	In the new workflow, click Employees → Corporate AD



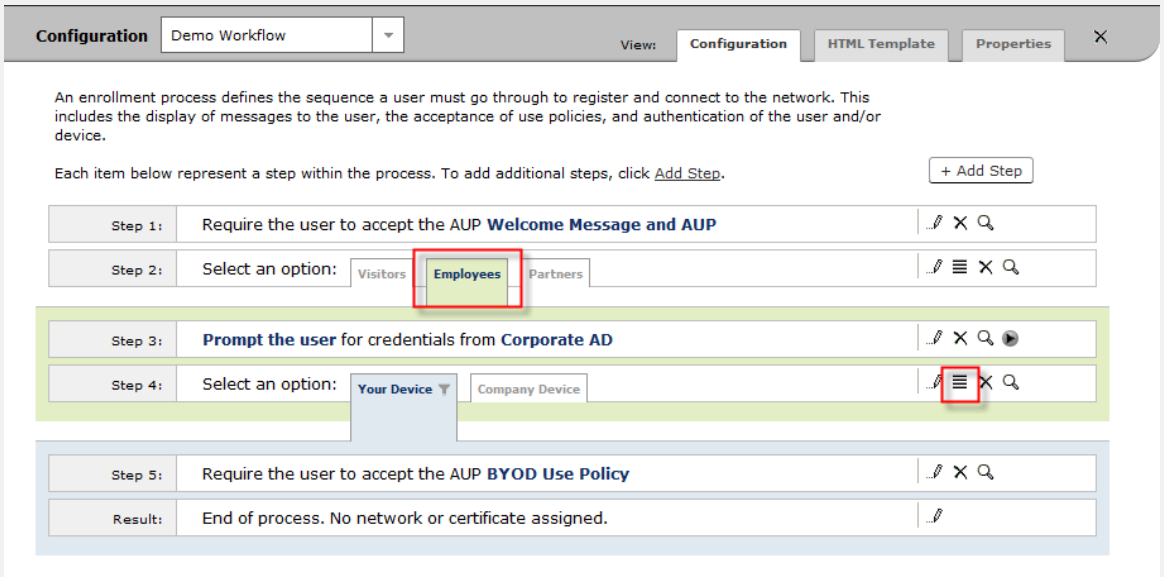
4	**Type the AD Domain, AD Host, and DN information. Check User For Sponsorship. Click Save.**

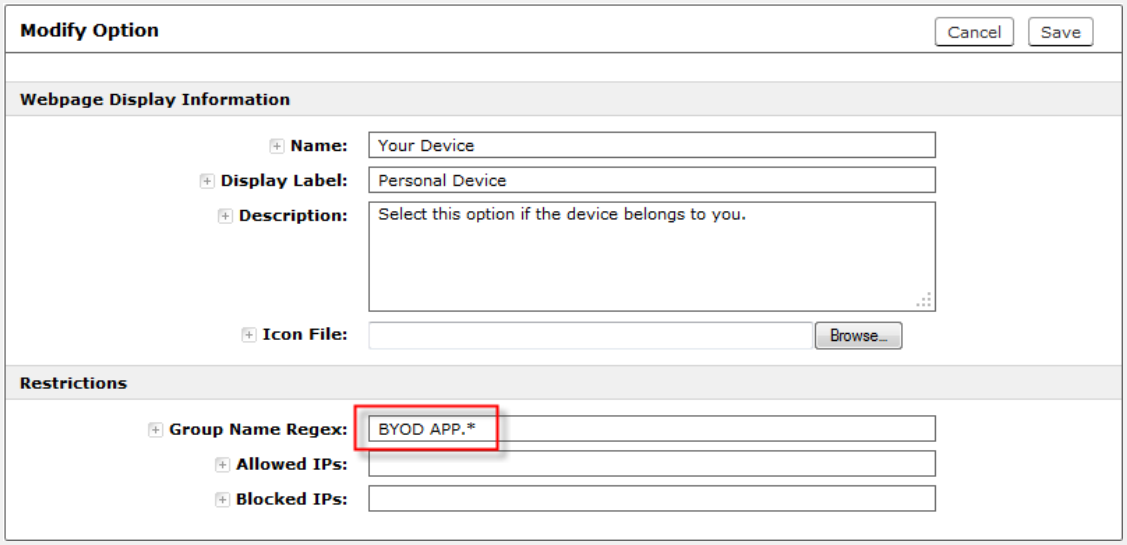


5	**Test the Active Directory login by clicking the play icon. Verify the group Regex for self onboarding by trying the two different employee accounts you created previously. This will make sure the BYOD option is always available for specific users.**

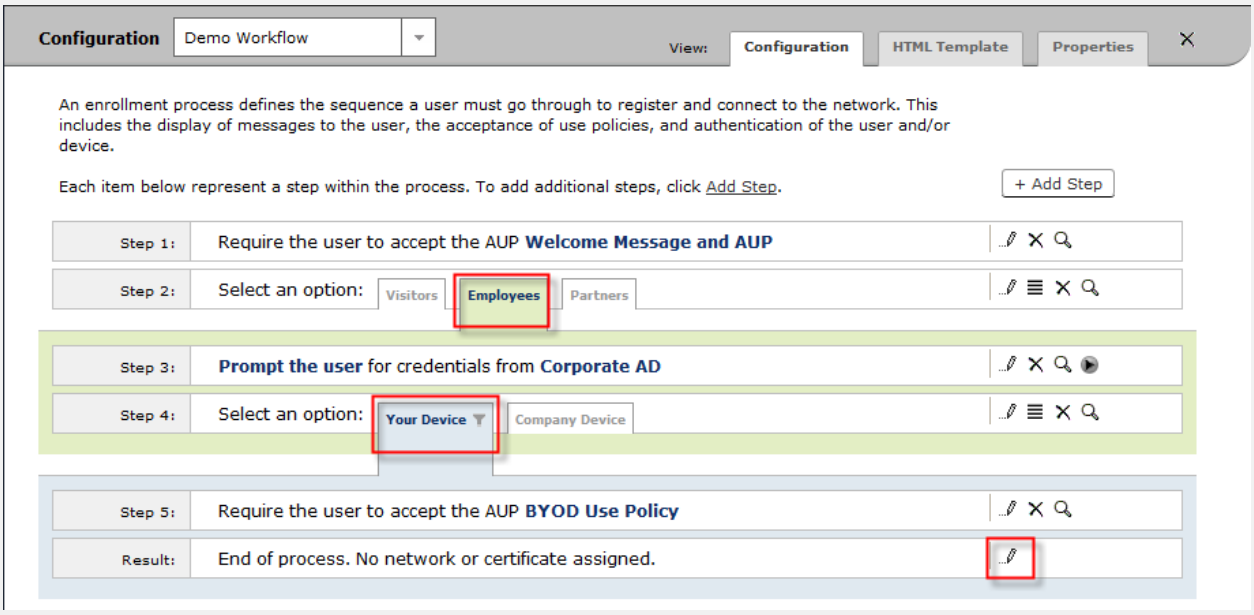


6	**Verify the AD group permission check, by clicking on the Edit List icon of Step 4. Click the configure icon for Option 1. Notice the Group Name Regex. Click Cancel and navigate back to the main workflow page.**

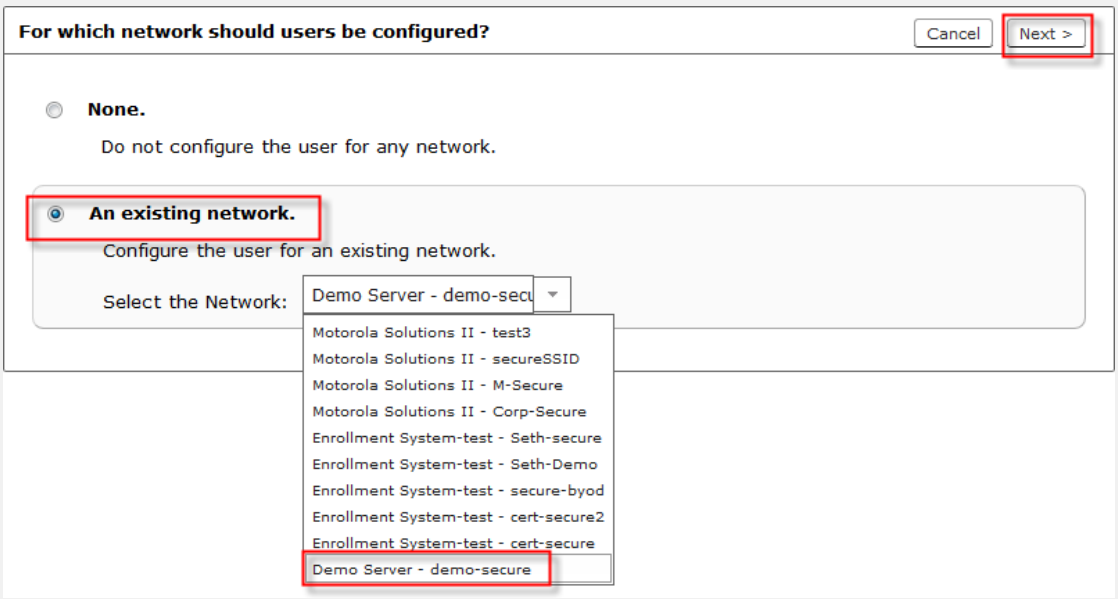




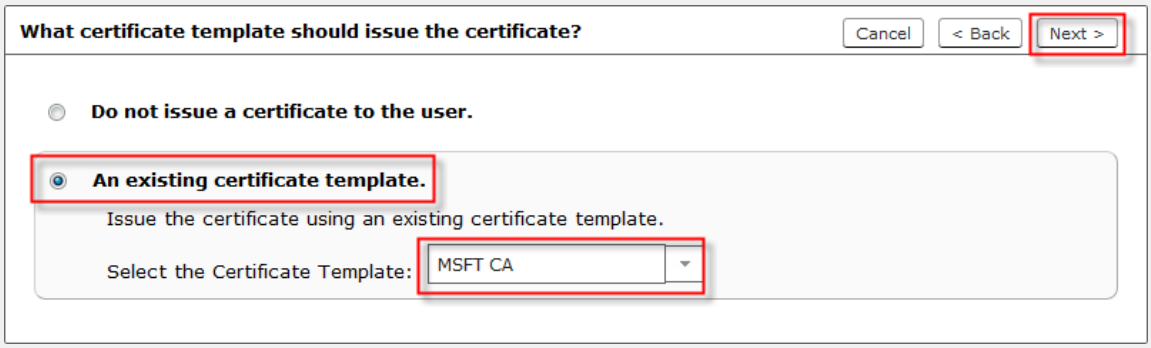
7 **Choose Employees → Your Device, and click the configure icon.**

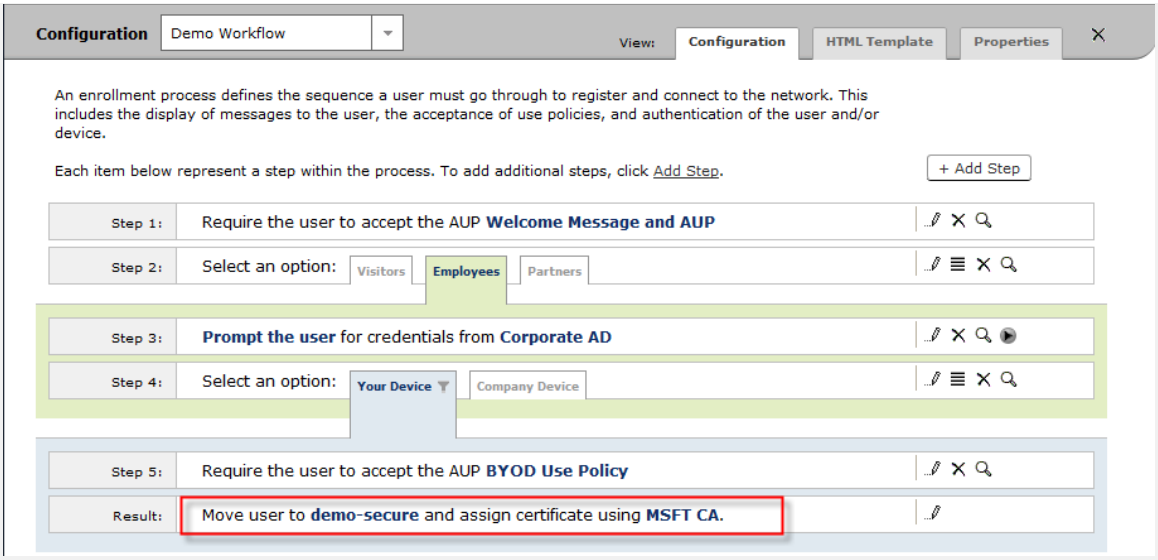


8 **Select An existing network. If necessary, select the server from the Network pick list. Click Next.**

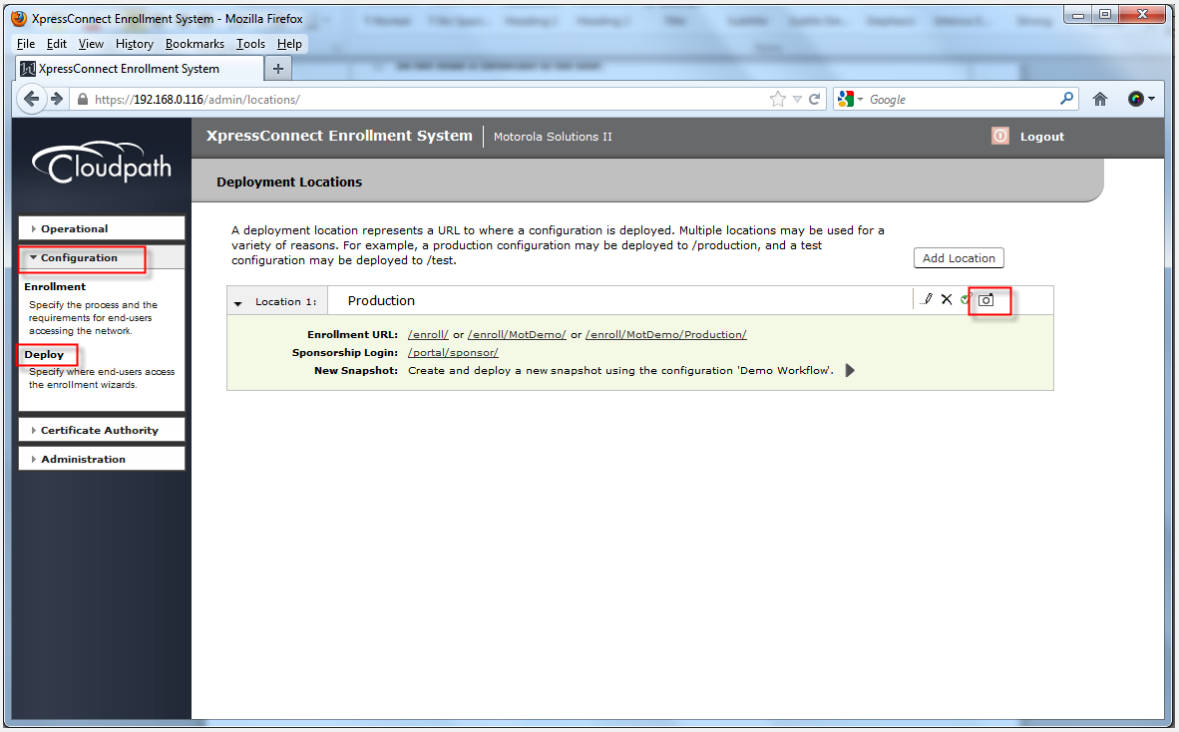


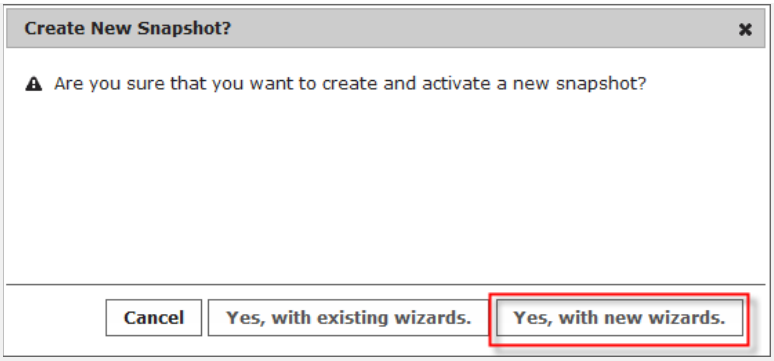
9	**Select An existing certificate template, and choose the MSFT CA option you configured earlier. Click Next.**





10	**Navigate to Configuration → Deploy, and click the snapshot icon. Click Yes, with new wizards.**



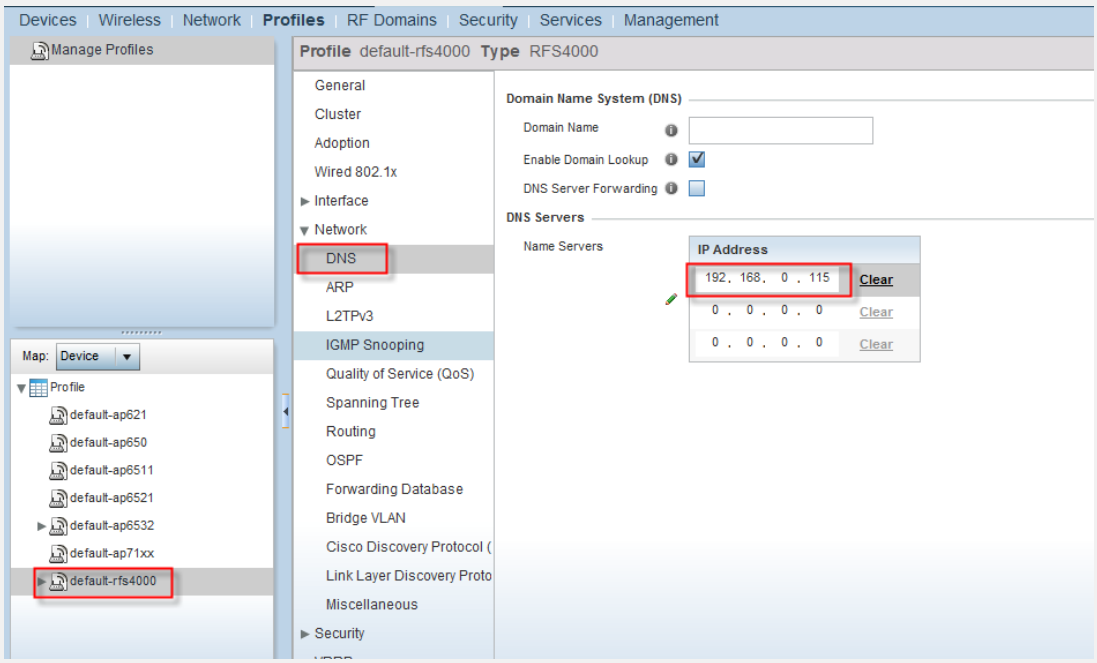


11	**Point your browser to http://<server_name>/enroll (or alternatively use the IP address of the server instead of name) to see the onboard webpage. Verify it is working.**

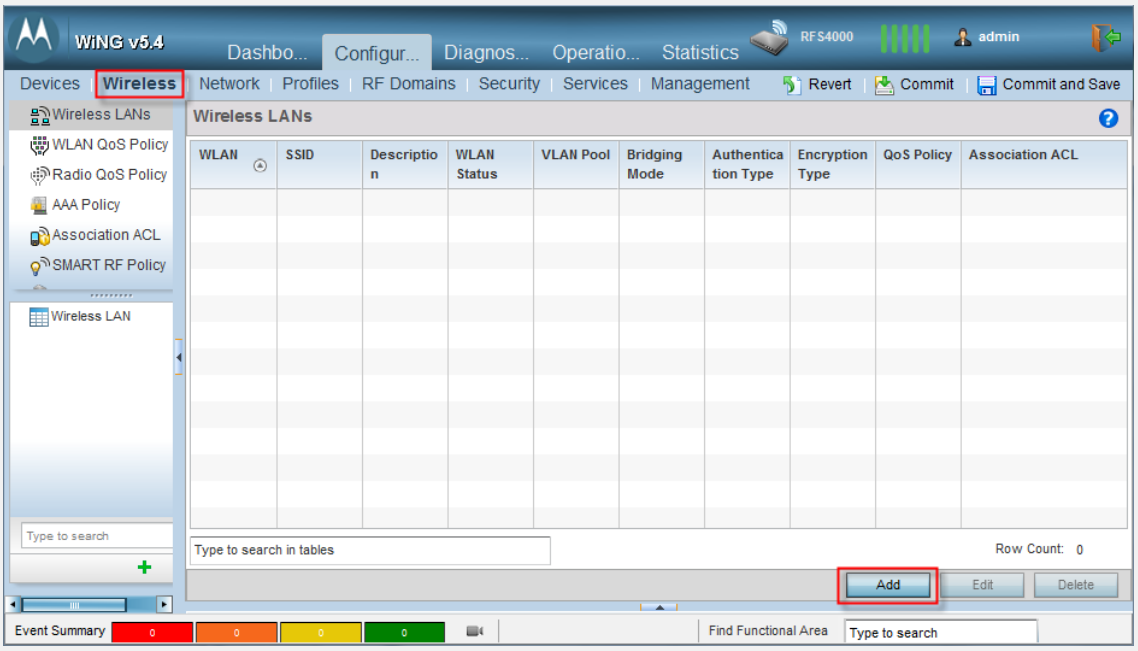
2.7 Configure RFS and Access Point

It is assumed that you have an RFS and/or AP with basic connectivity and management established. The AP is managed by an RFS and a VLAN is configured for client traffic, either tunneled or local, whichever is preferred. These steps will detail how to setup an open on-boarding SSID and secure SSID for secure access. You don't have to have different VLANs for the two, but it would be recommended if you are demonstrating the basics of a secure solution.

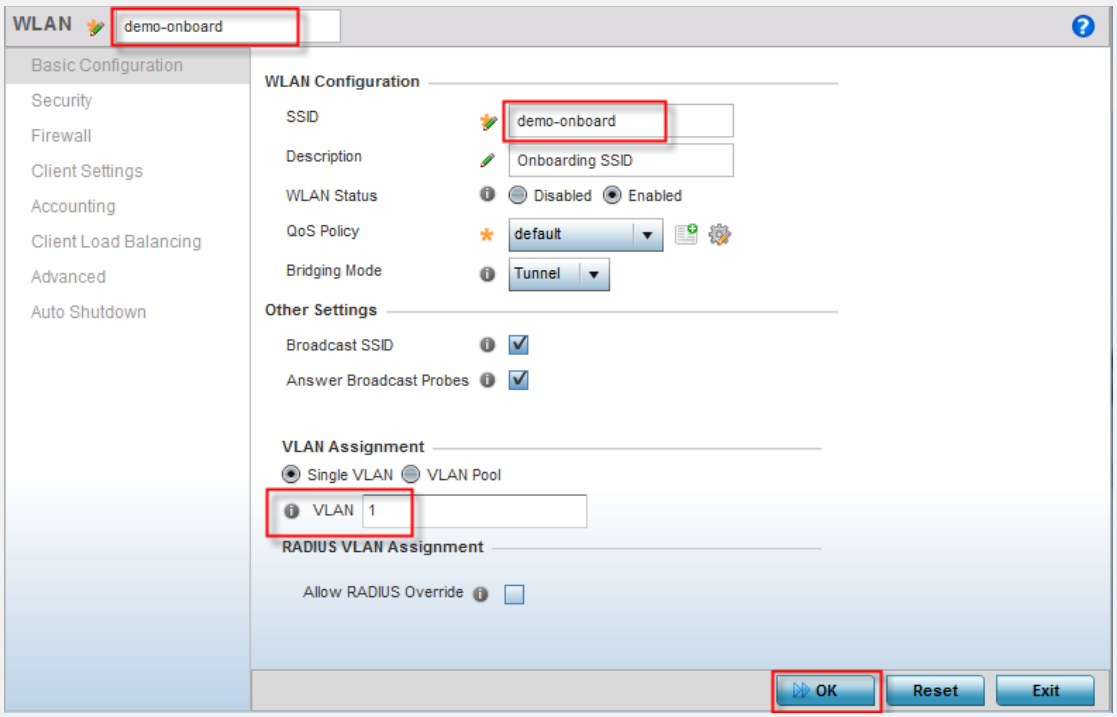
1	**Using the Web-UI select *Configuration → Profiles → <rfs-profile-name> → DNS.* Enter the IP address of the Windows Server. Click Ok.**



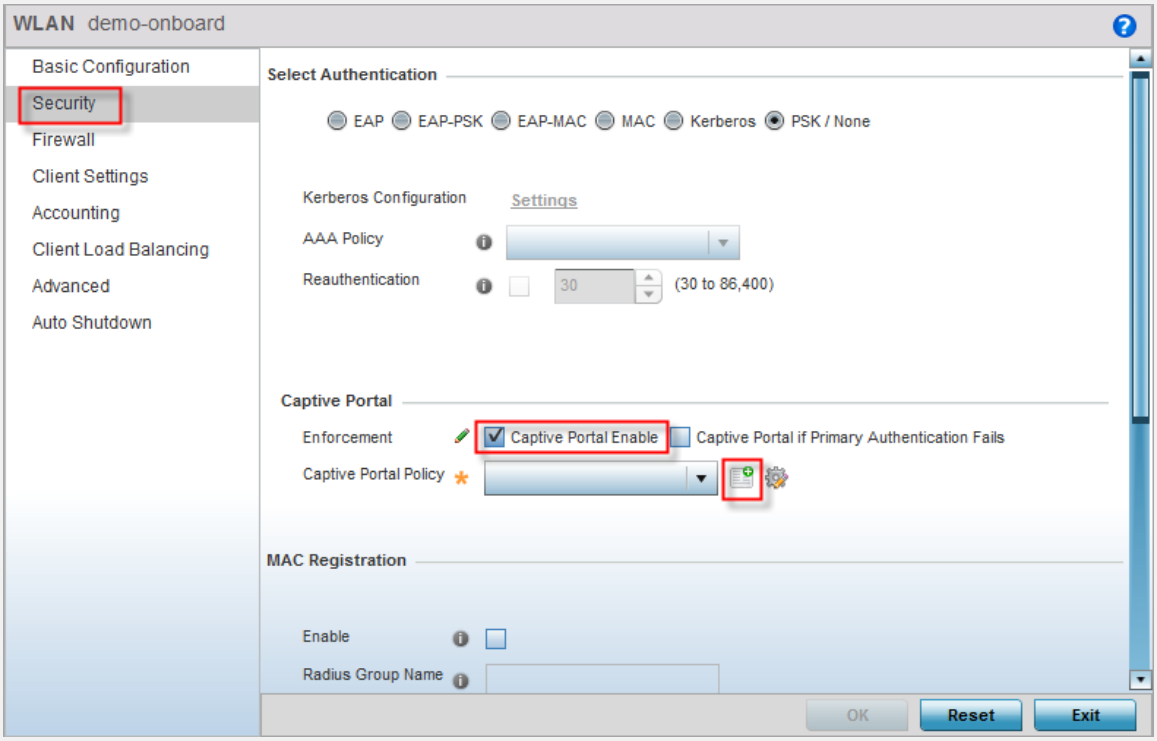
2	**Select *Configuration* → *Wireless*. Click Add.**



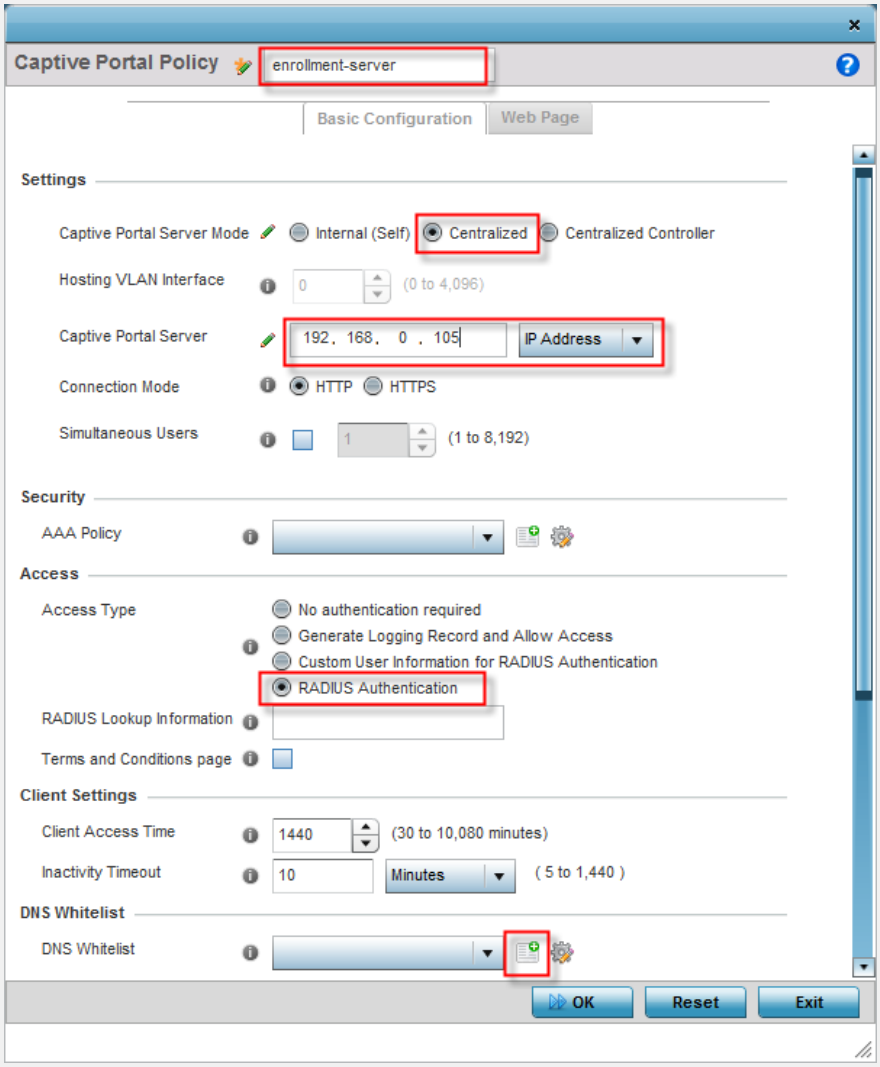
3	**Name the WLAN demo-onboard and also type demo-onboard for the SSID. Use VLAN 1. Click OK.**



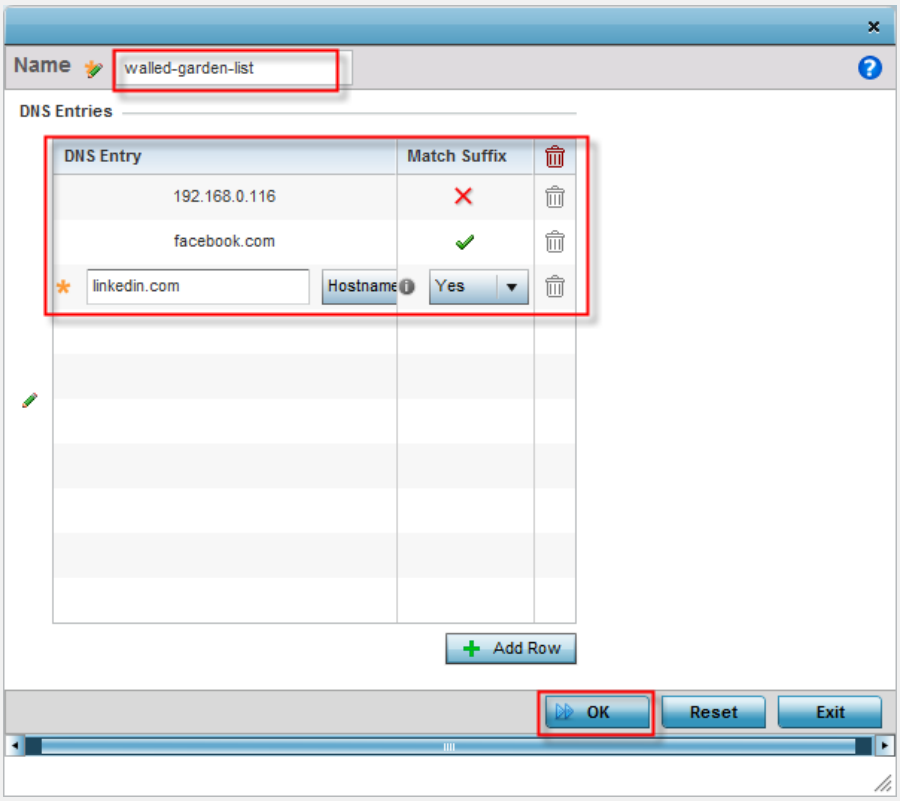
4	**Click Security. Check Captive Portal Enable. Click the Add button.**



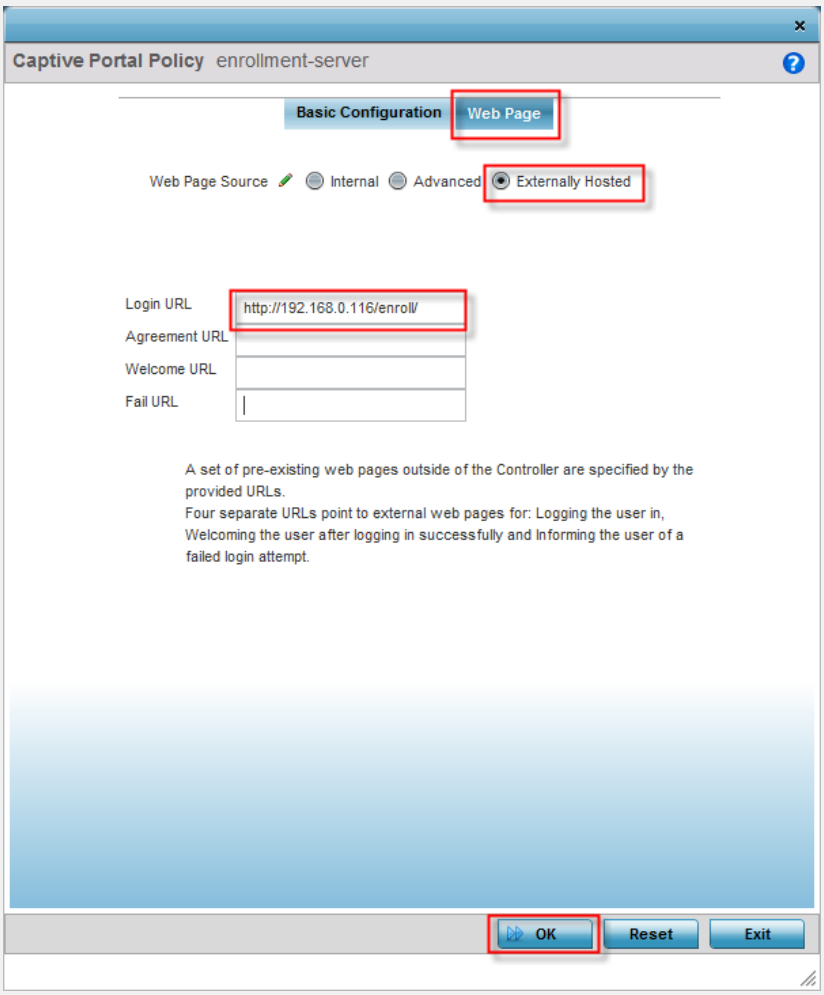
5	**Select Centralized, and enter the IP address of the RFS. Choose RADIUS Authentication. Click the Add button next to DNS Whitelist.**



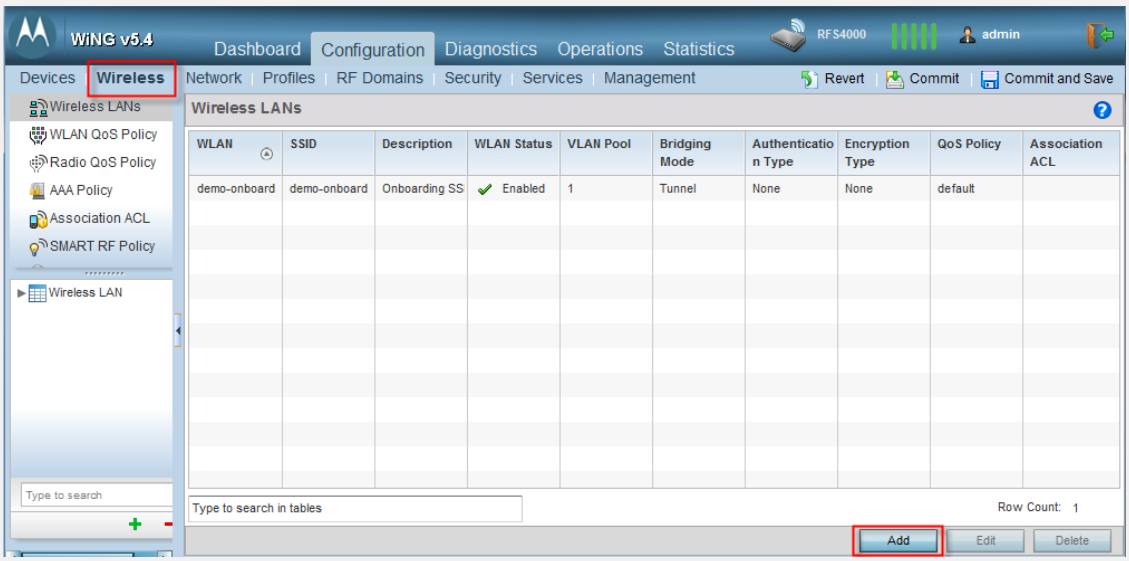
6	**Name the list walled-garden-list. Add facebook.com and linkedin.com as suffix entries. Add the IP address of the Enrollment Server. Click OK. Then click Exit. Now click OK, but don't click exit.**



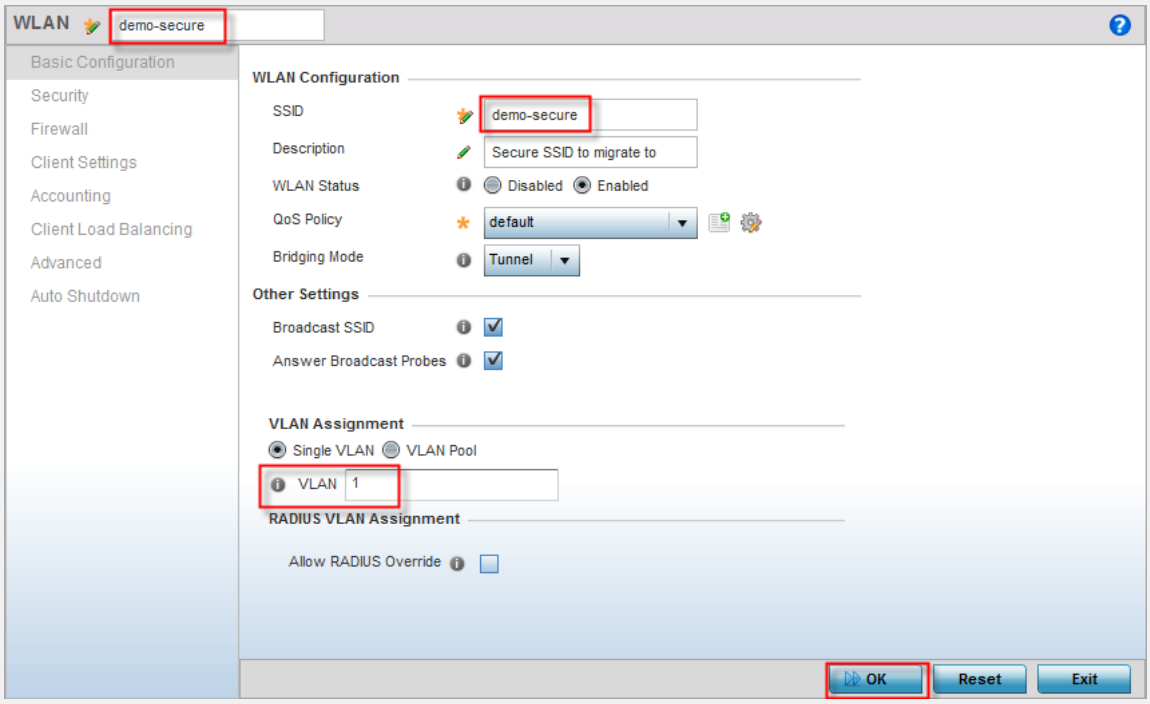
7	**Click the Web Page tab. Select Externally Hosted. In the login URL field, type the either http://<enrollment_server_name>/enroll/ (or use the IP address instead of DNS name). Click Exit. Then click OK and click Exit again.**



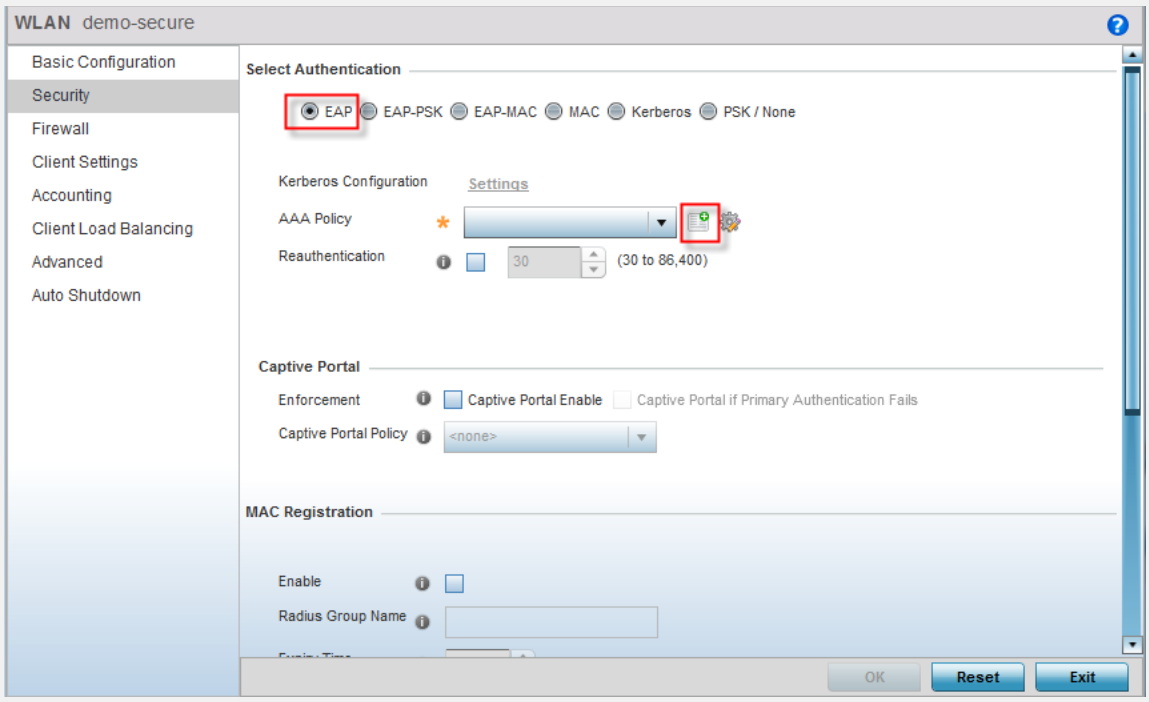
8	**Select *Configuration* → *Wireless*. Click Add.**



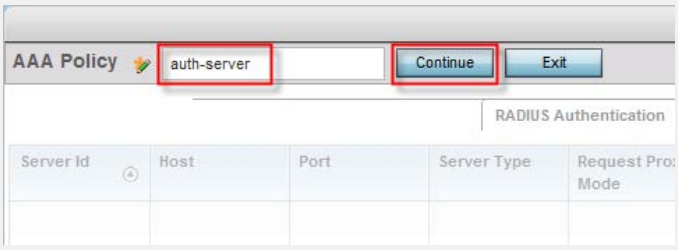
9	Name the WLAN demo-secure and also type demo-secure for the SSID. Use VLAN 1. Click OK.



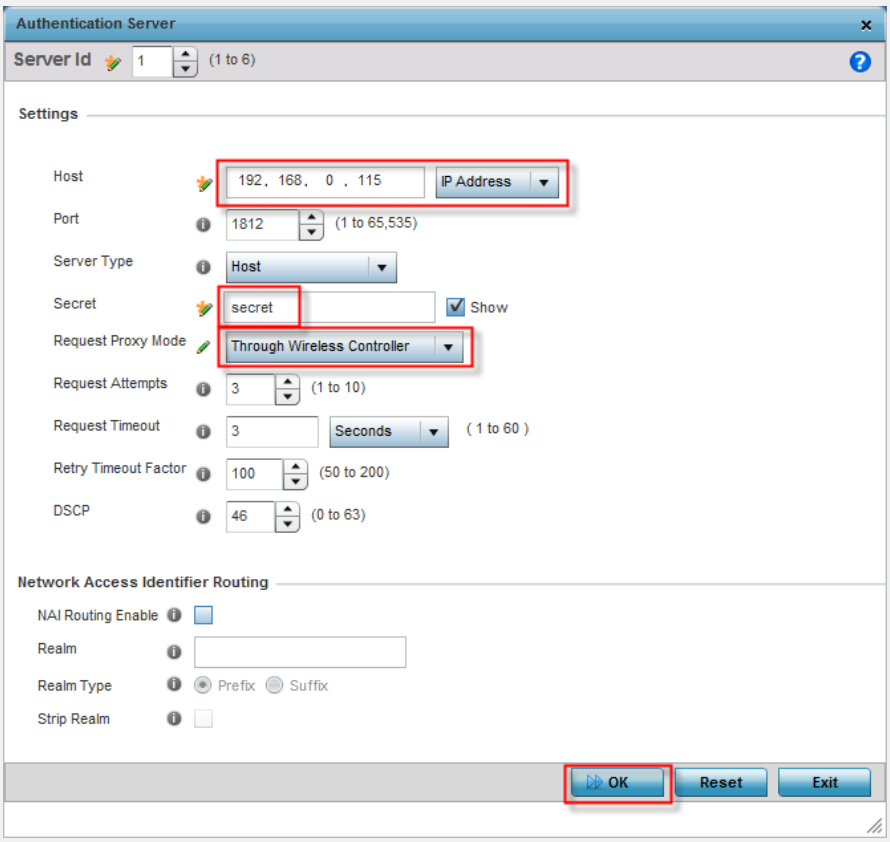
10	Click Security. Select EAP. Click the Add button next to AAA Policy.



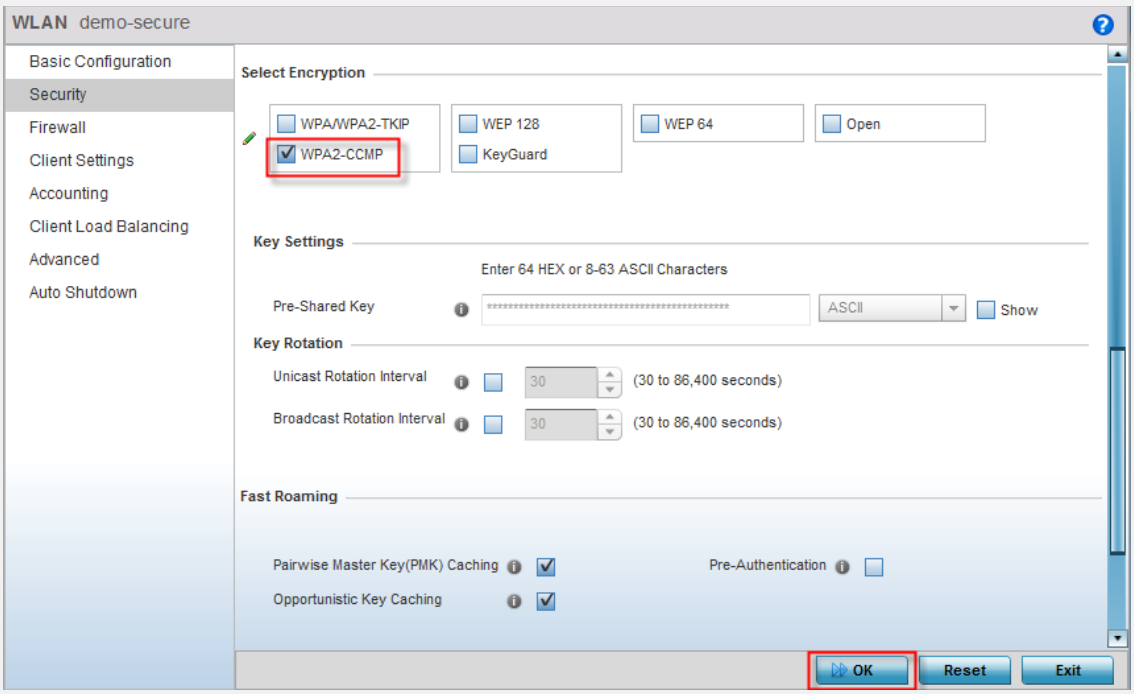
11	Type auth-server for the policy name. Click Continue. Click Add.



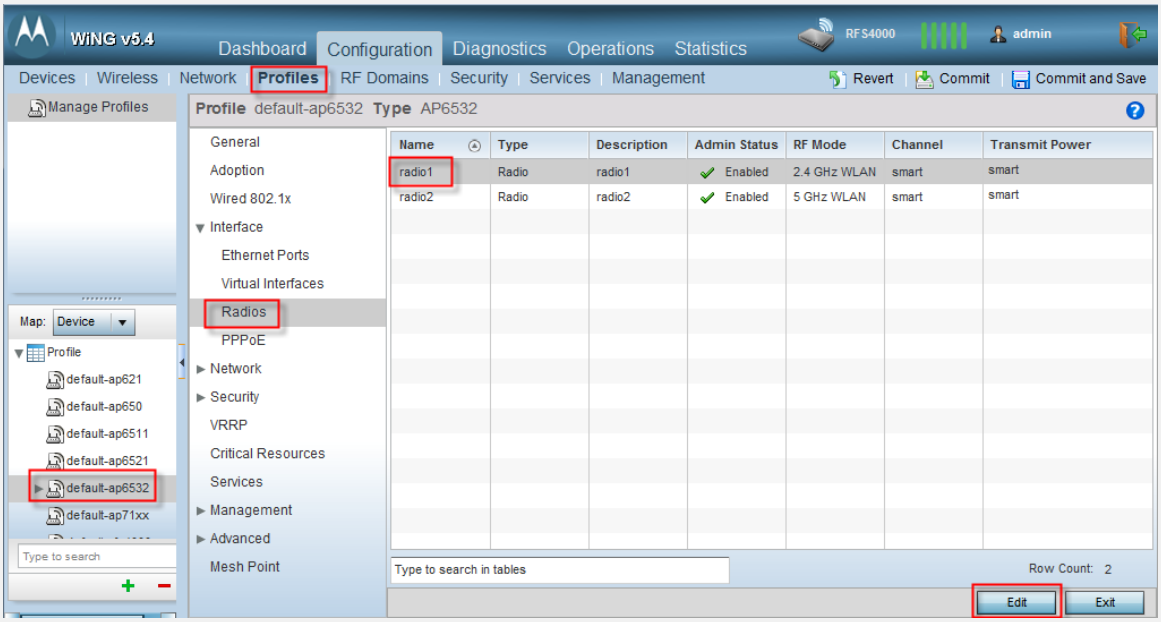
12	Type the IP address of the Windows Server. Type “secret” for the Secret. Select Through Wireless Controller. Click OK. Click Exit. Click Exit again.



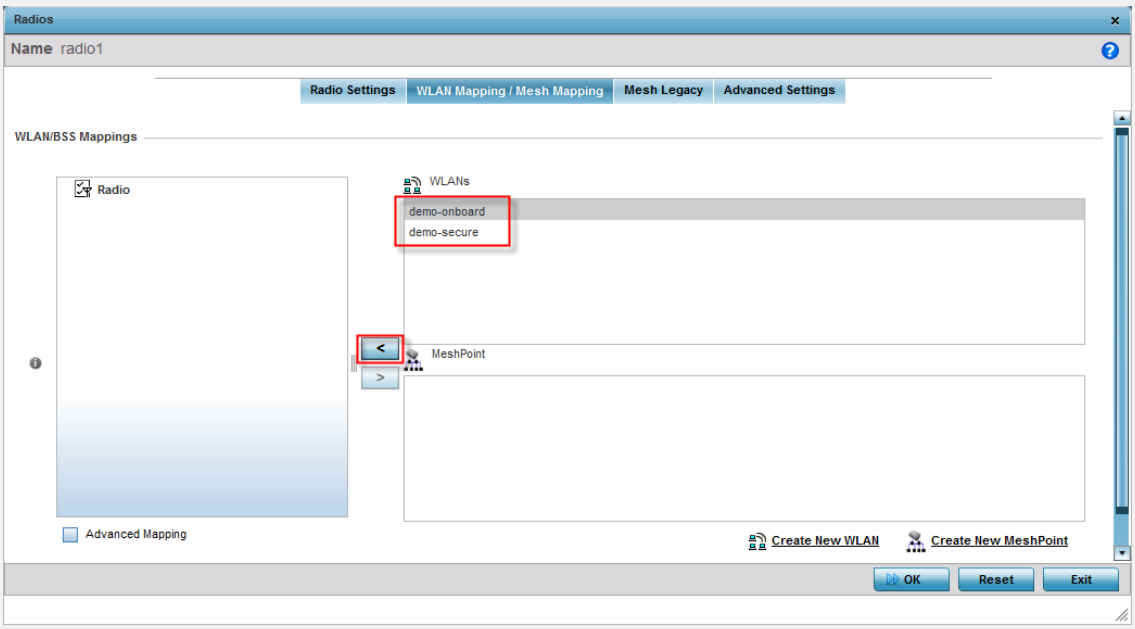
13	Check WPA2-CCMP. Click OK. Click Exit.



14	**Select *Configuration* → *Profiles* → *<ap-profile-name>* → *Radios* → *radio1.* Click Edit.**

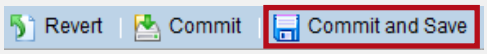


15	**Click on the WLAN Mapping tab. Select each WLAN and click the arrow button to map them to the radio. Click OK and click Exit.**



16	Repeat previous step for the other radio.

17	Commit and Save the changes:



2.8 Section 2.2

3. Section 3

3.1 Section 3.1

3.2 Section 3.2

1	Using

2	Click
3	Click
4	From
5	Give
6	Select
7	Choose
8	Right
9	Click
10	Right
11	Proceed