

# **Secure Access: Demo Server Configuration**

## **HOW TO GUIDE**



December 2012

Revision 0.01



# Table of Contents

Table of Contents.....	4
1. Section 1.....	<b>Error! Bookmark not defined.</b>
1.1 Section 1.1.....	<b>Error! Bookmark not defined.</b>
1.2 Section 1.2.....	<b>Error! Bookmark not defined.</b>
2. Section 2.....	<b>Error! Bookmark not defined.</b>
2.1 Section 2.1.....	<b>Error! Bookmark not defined.</b>
2.2 Section 2.2.....	133
3. Section 3.....	133
3.1 Section 3.1.....	133
3.2 Section 3.2.....	133

# 1. Overview

## 1.1 Components

## 1.2 Wizard

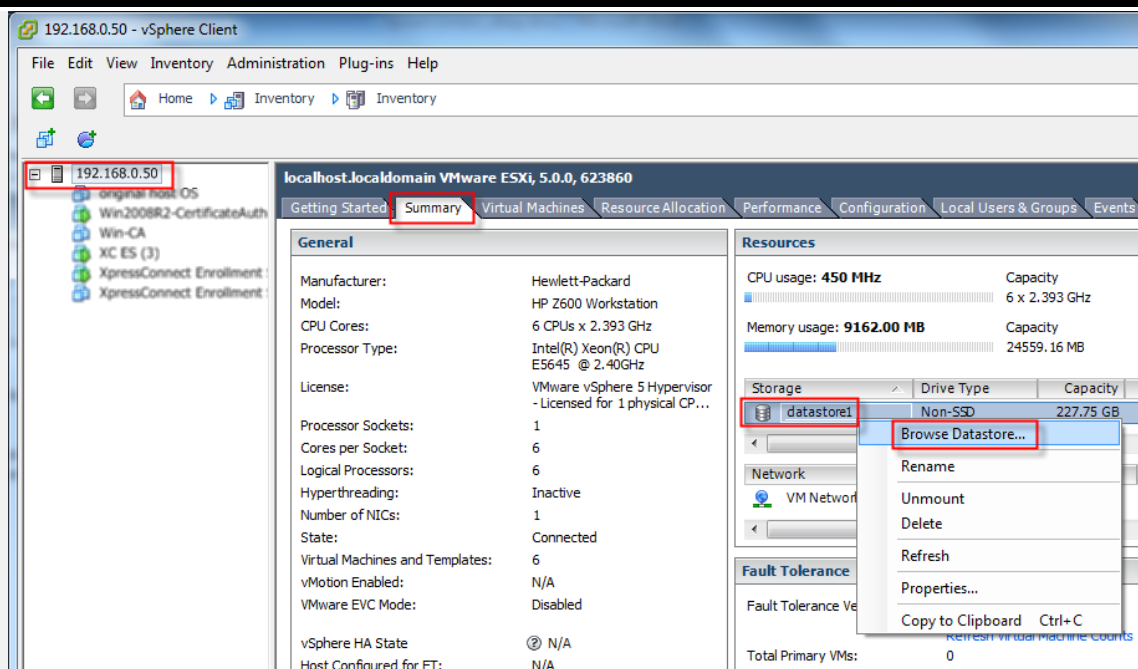
## 1.3 Enrollment Server

# 2. Demo Configuration

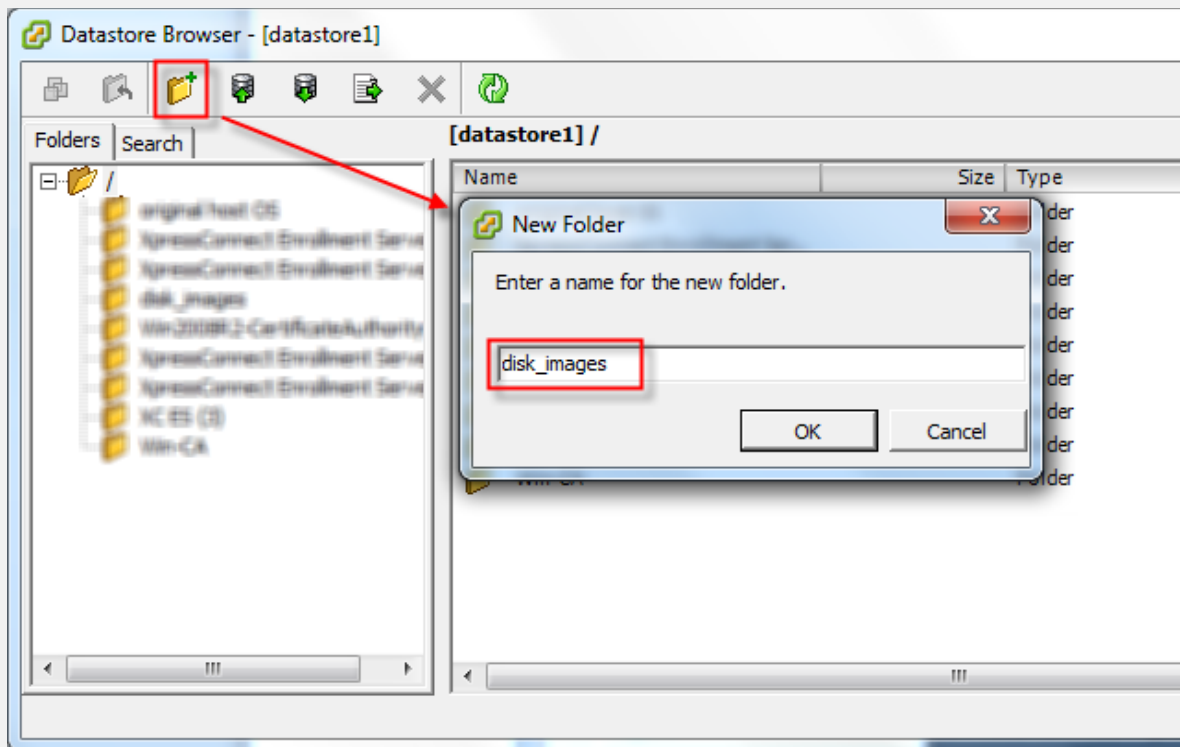
## 2.1 Initial ESXi Setup

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.

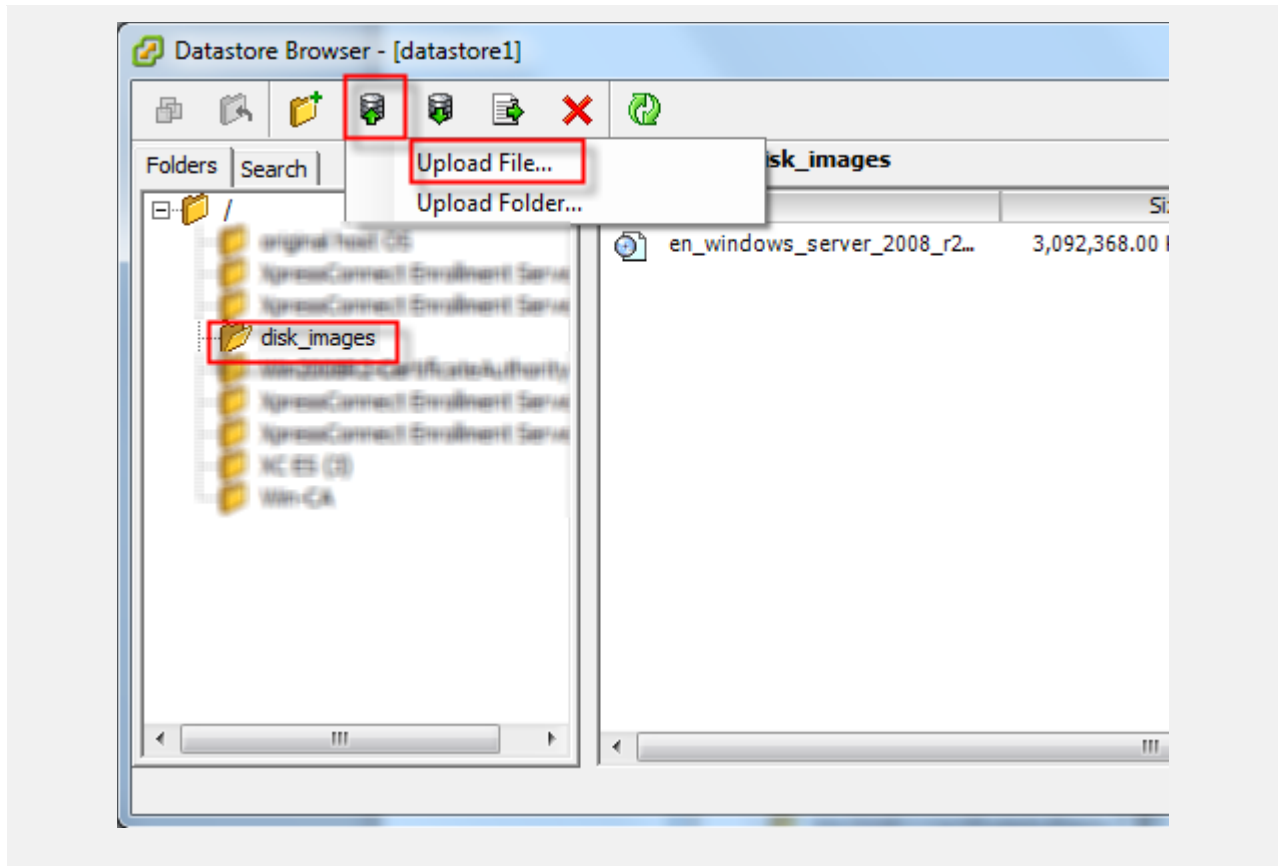
- 1 Using vSphere Client, select the VM server node. Click on the Summary tab. Right click on the datastore1 item in the right hand pane, and select Browse Datastore.



- 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.

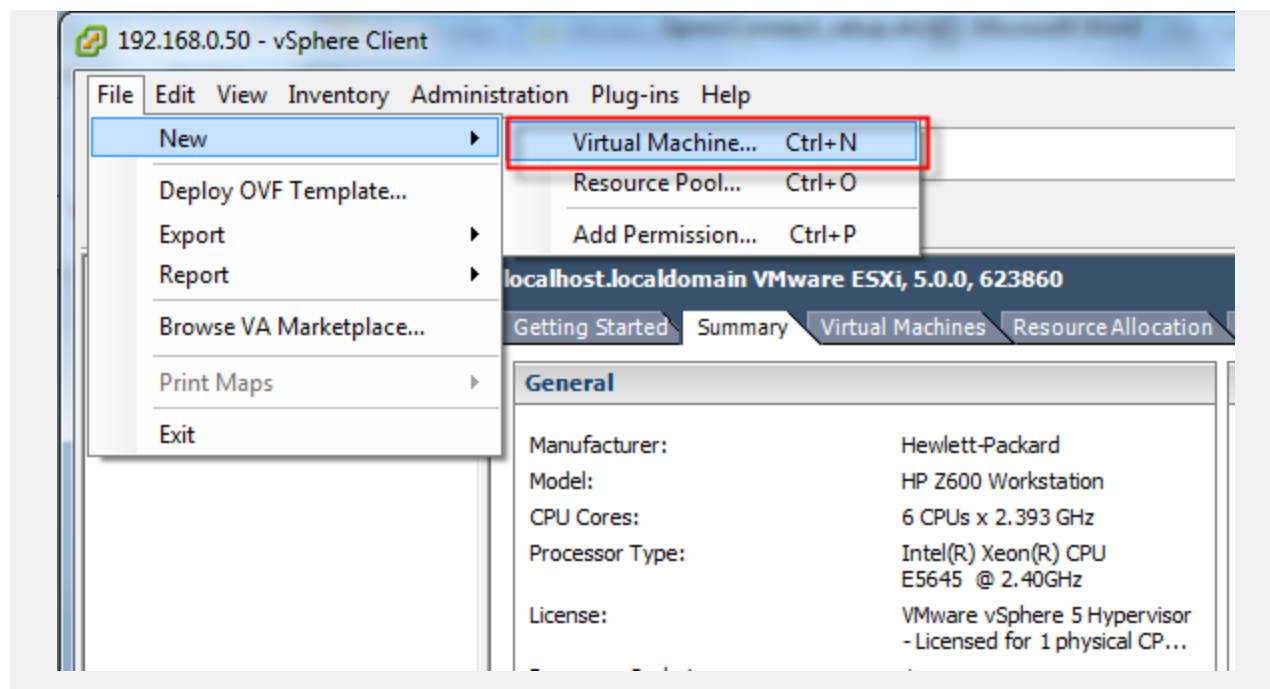


## 2.2 Windows Server Configuration

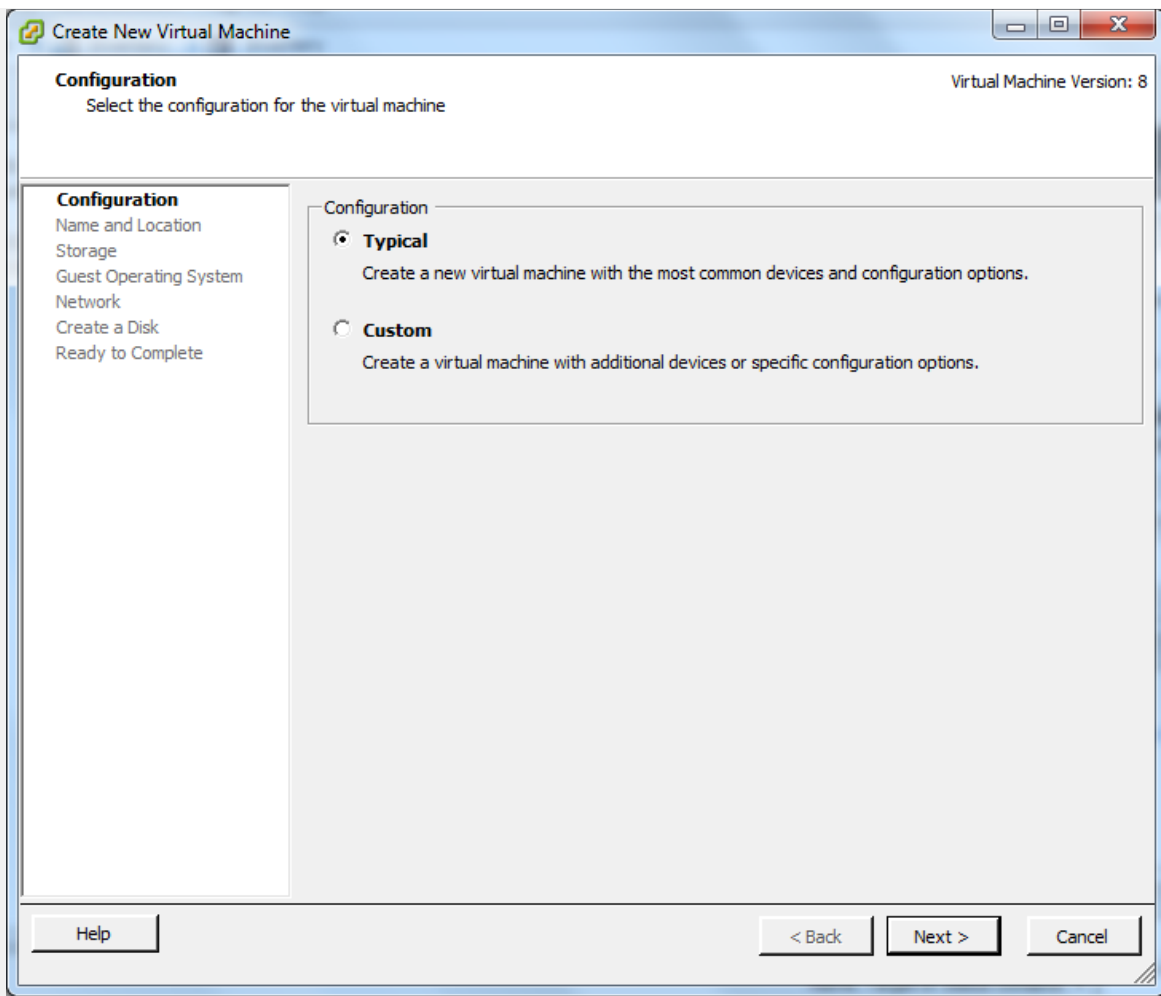
You will need to configure a number of services as supporting infrastructure, such as Active Directory, DNS, Certificate Authority, Network Policy Server, etc. Some of these are optional, or may differ in a more complicated lab configuration.

### 2.2.1 Initial Setup of Windows Server VM

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







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

Create New Virtual Machine

Name and Location

Virtual Machine Version: 8

Specify a name and location for this virtual machine

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.

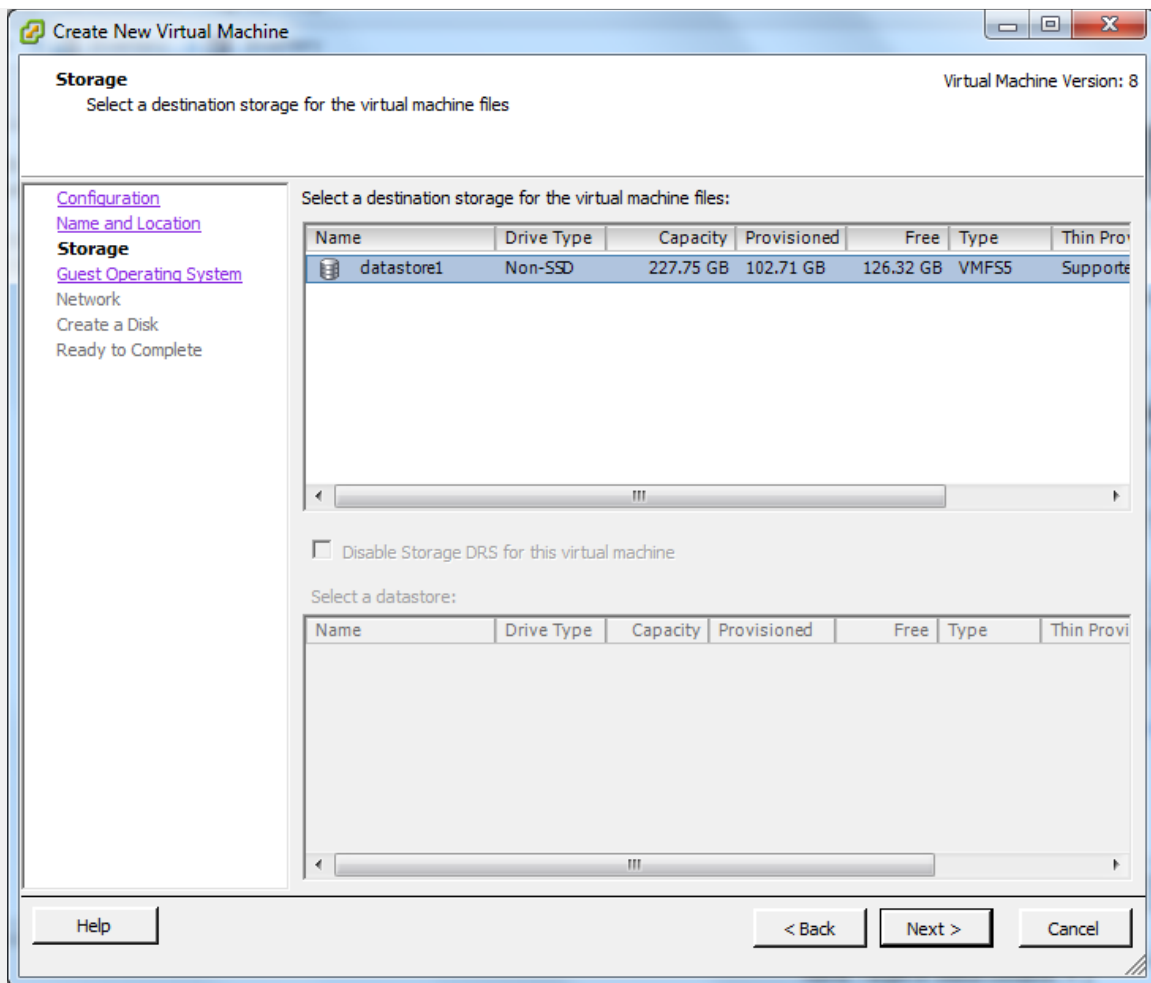
VM folders are not viewable when connected directly to a host. To view VM folders and specify a location for this VM, connect to the vCenter Server.

Help

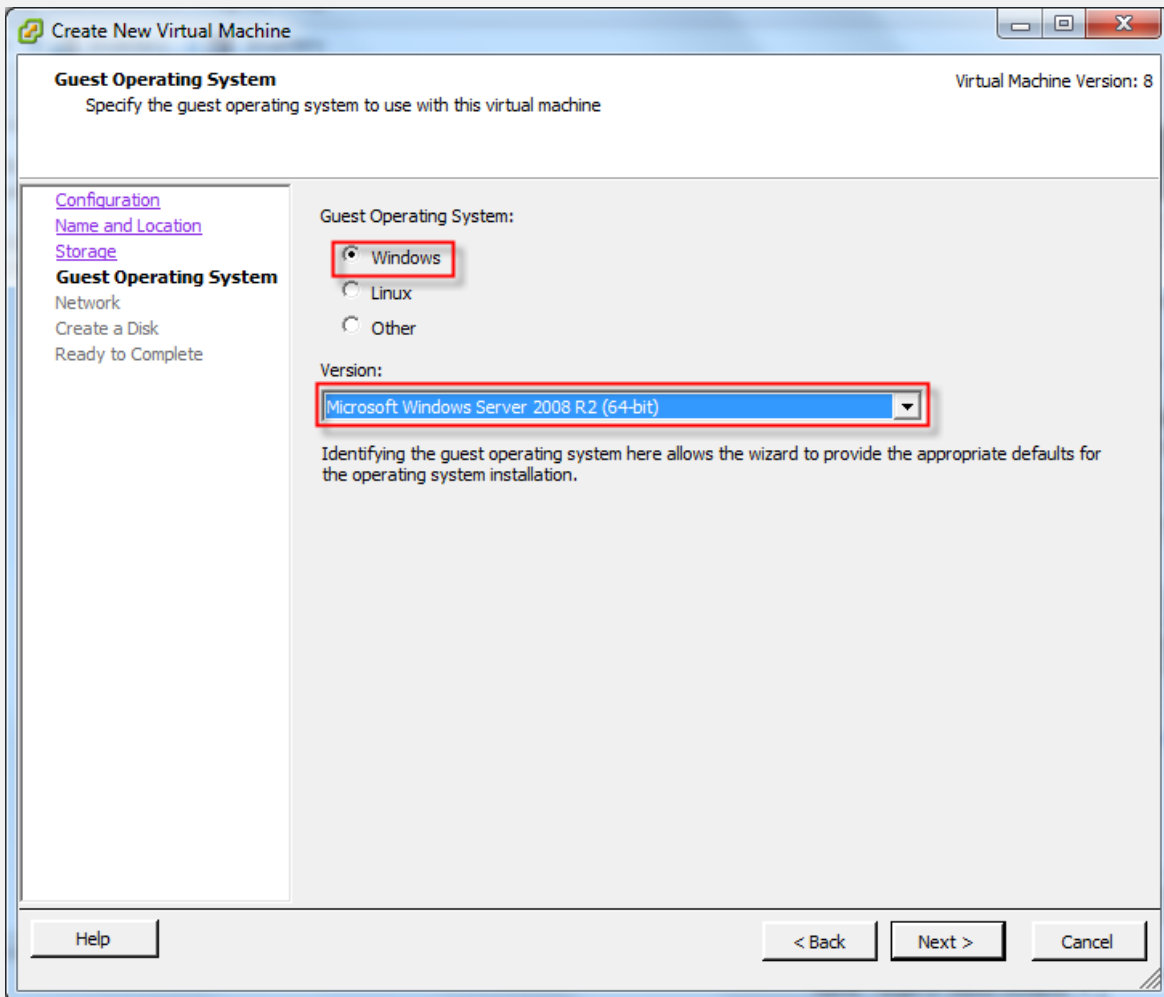
< Back

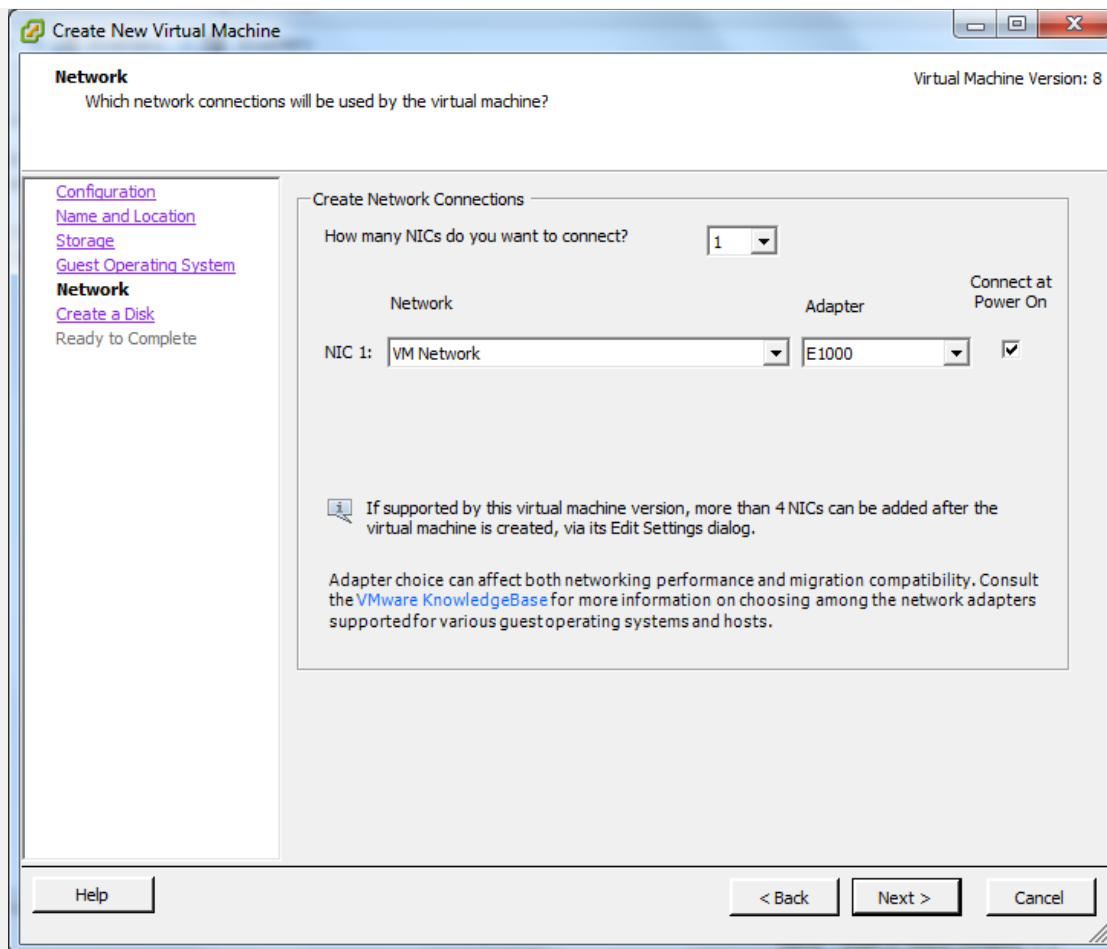
Next >

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.**





- 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** Virtual Machine Version: 8  
Specify the virtual disk size and provisioning policy

[Configuration](#)  
[Name and Location](#)  
[Storage](#)  
[Guest Operating System](#)  
[Network](#)  
**Create a Disk**  
Ready to Complete

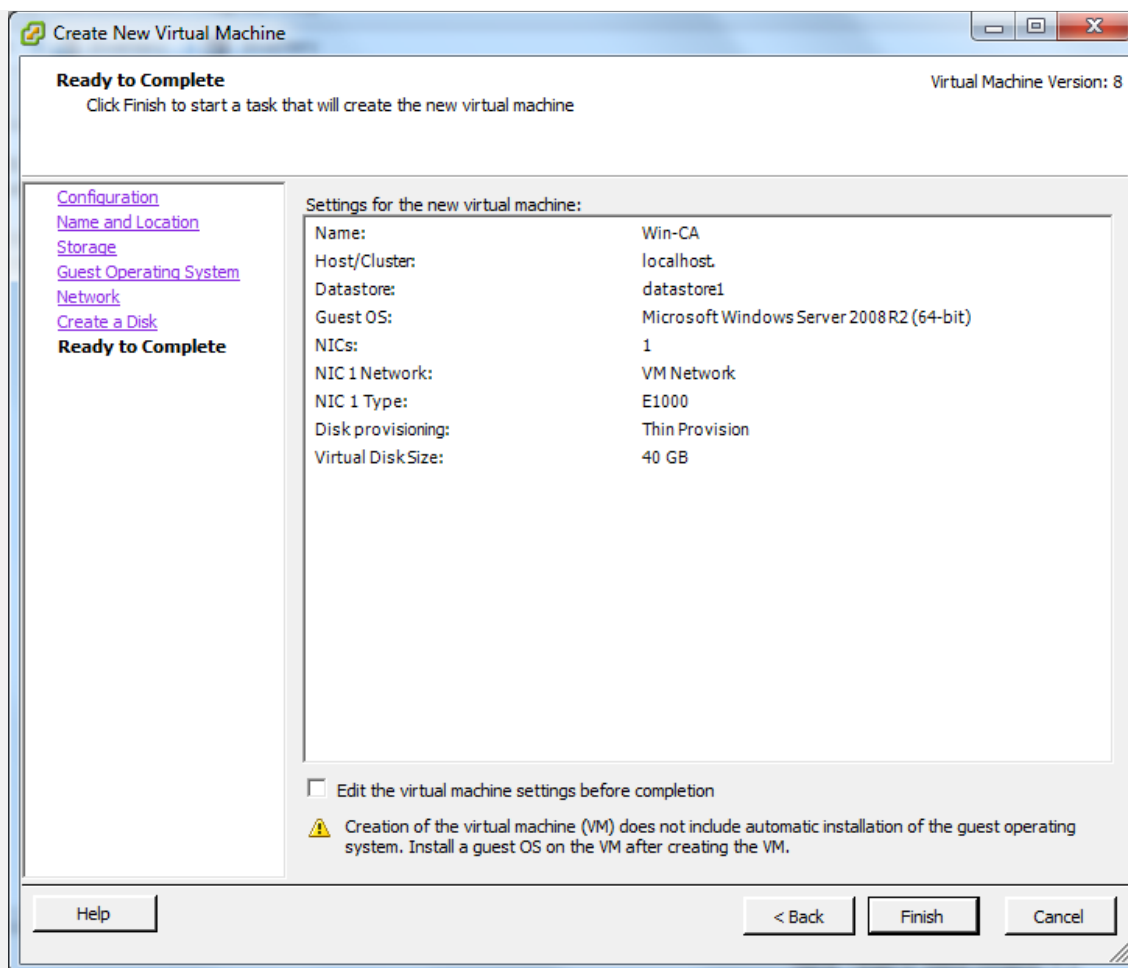
Datastore: datastore 1

Available space (GB): 126.3

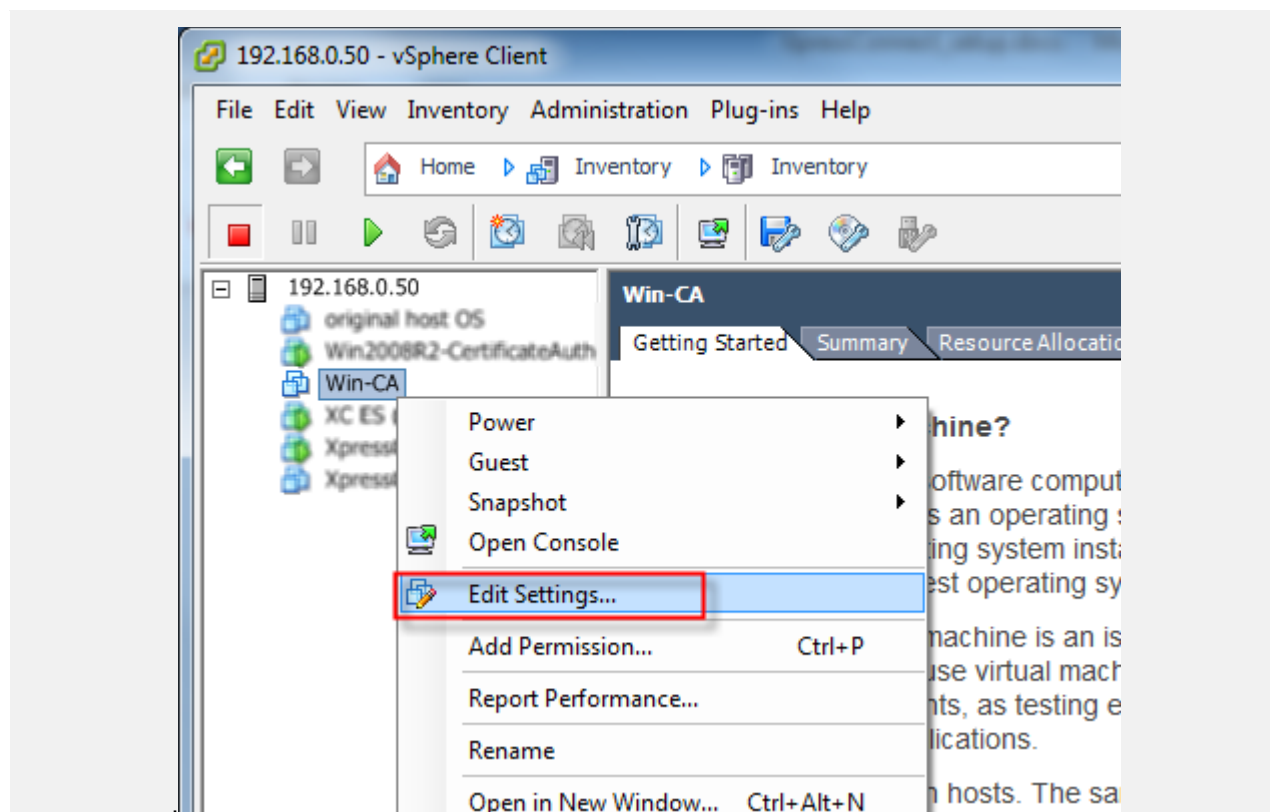
Virtual disk size: 40 GB

☐ Thick Provision Lazy Zeroed  
☐ Thick Provision Eager Zeroed  
☒ Thin Provision

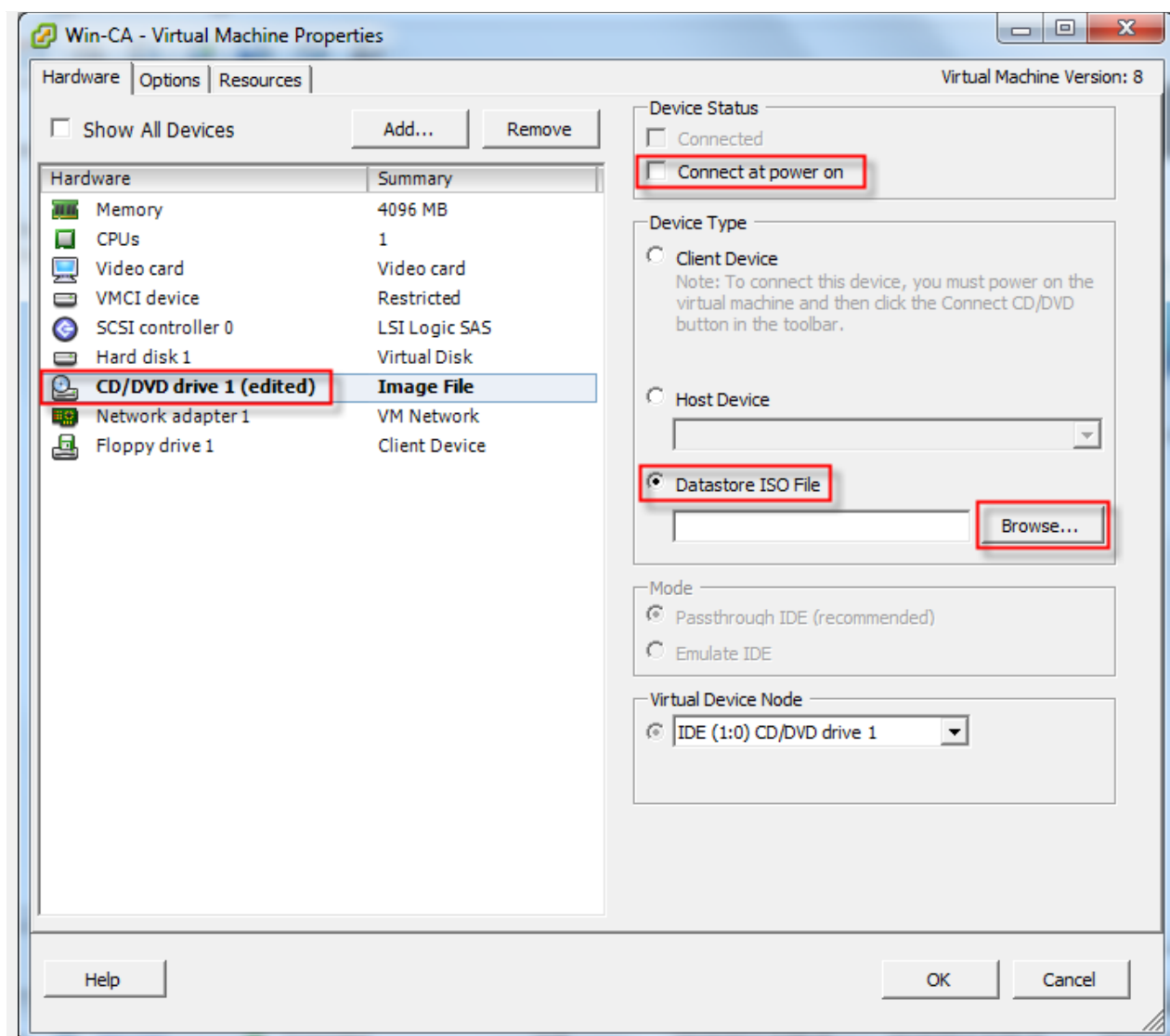
Help < Back Next > Cancel



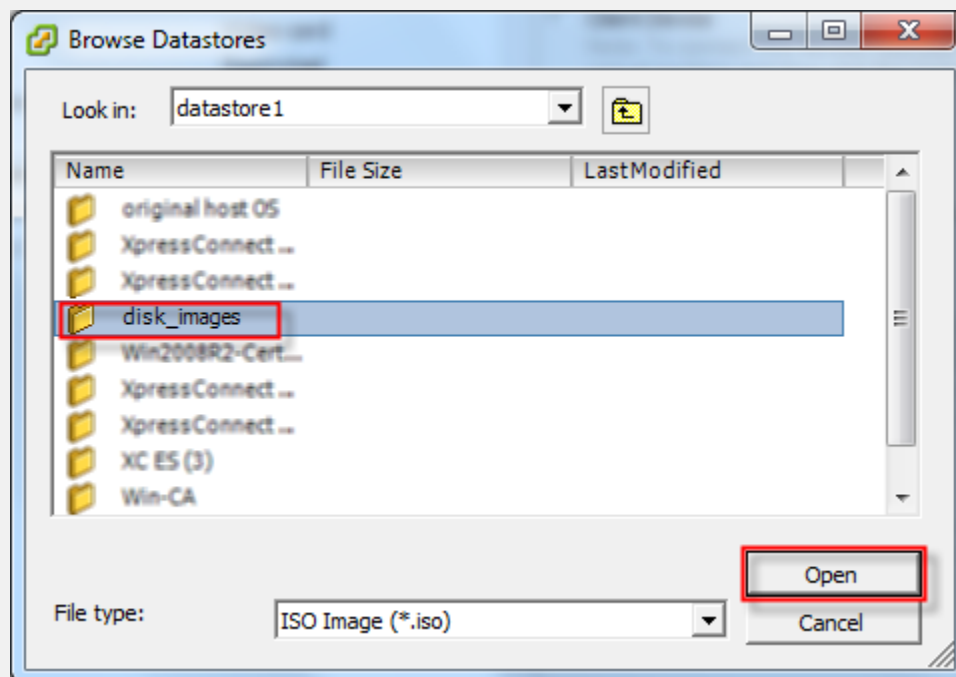
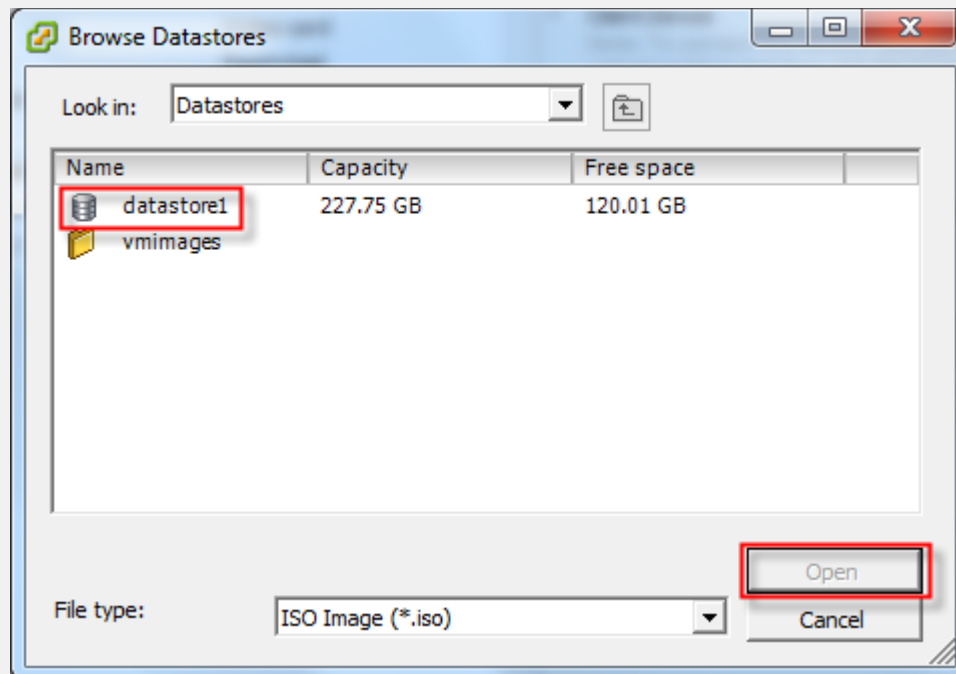
- 5 Right click on the new VM and choose Edit Settings. Click on CD/DVD drive 1. Select Datastore ISO File. Check Connect at power on. Click Browse to choose the ISO image of the Windows Server setup disk.

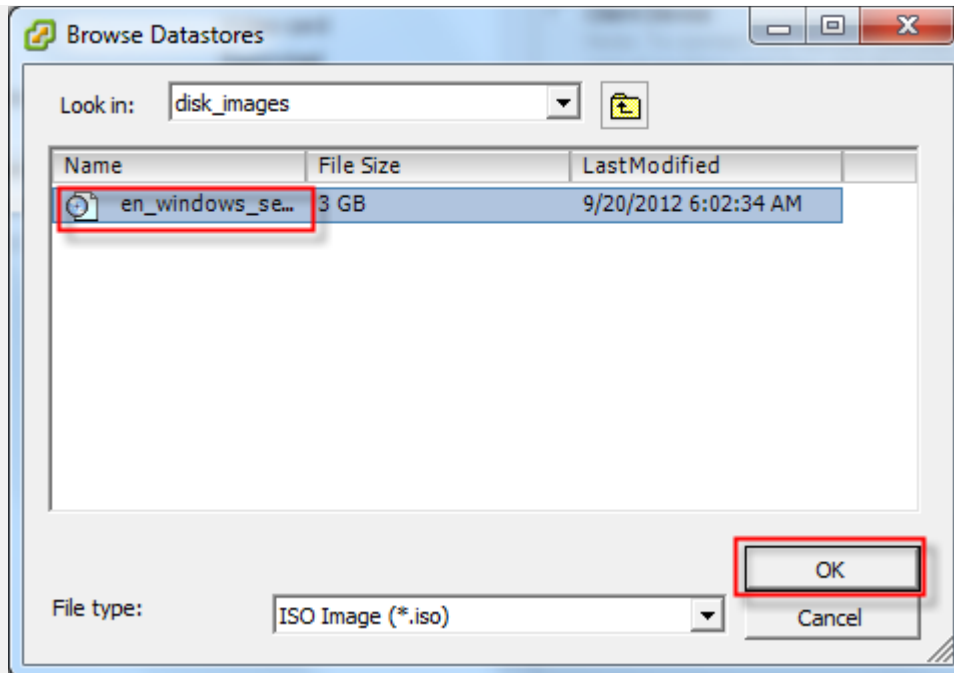




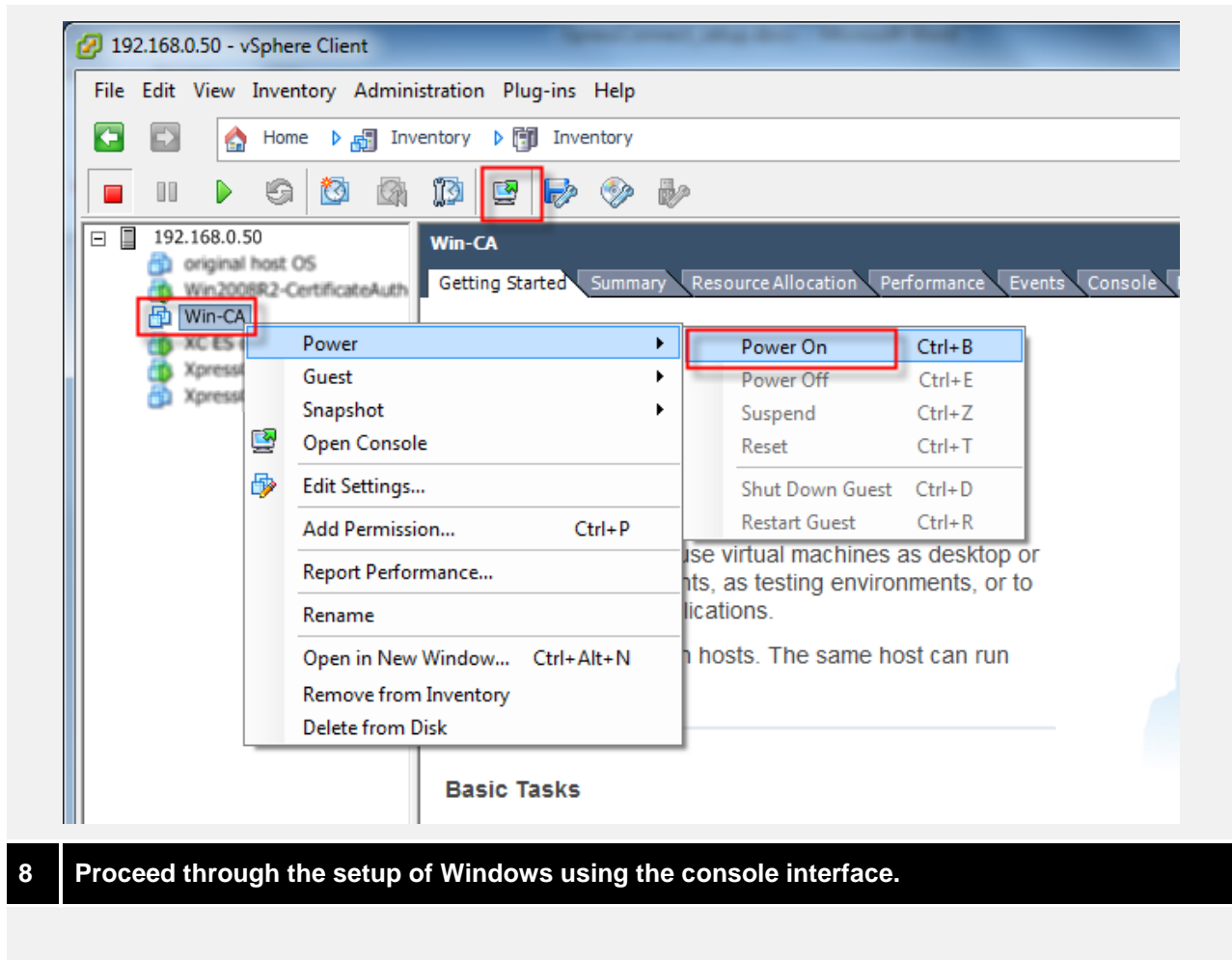


- 6 Click on datastore1, then click Open. Click on your folder where you saved the ISO file and click Open. Click on the Windows Server image file and click OK. Click Ok again.





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



## 2.2.2 Configure Networking

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



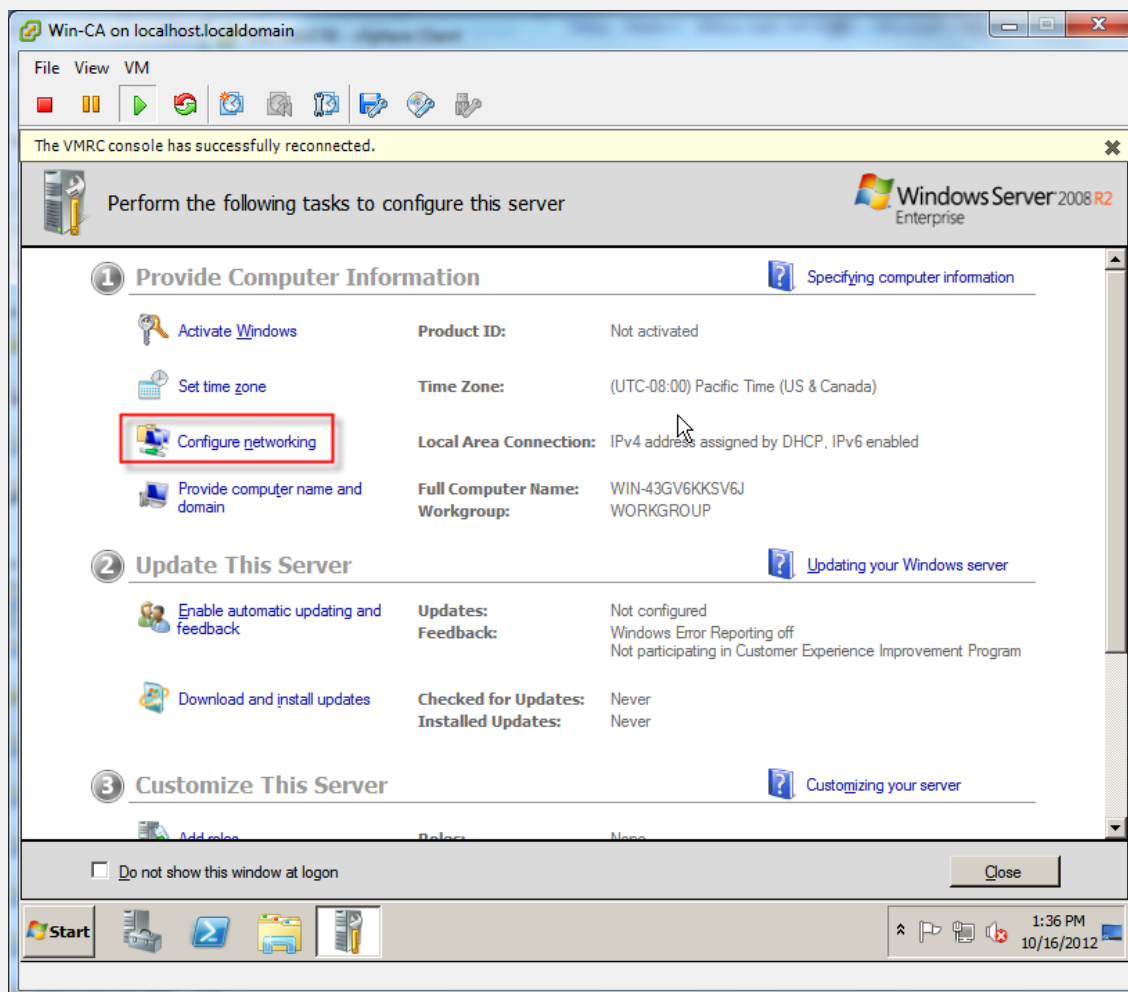
*Note:* Many of the next few sections mention launching tasks from the Initial Configuration Tasks application window. This is a convenient launch point for these next steps. If for some reason you close this window or do not see it, click Start and type "oobe" and press Enter.

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

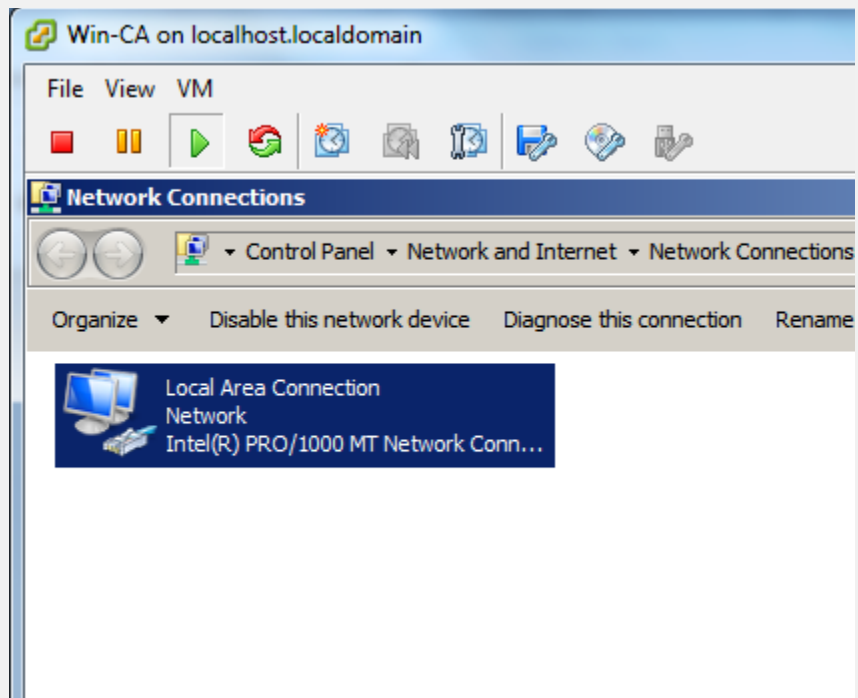


*Note:* The Microsoft Certificate Authority service requires a static IP address assignment for the server. In a lab demo configuration, where multiple services are installed on the same physical or virtual server, these steps are required. In a customer deployment, where services are typically installed 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.

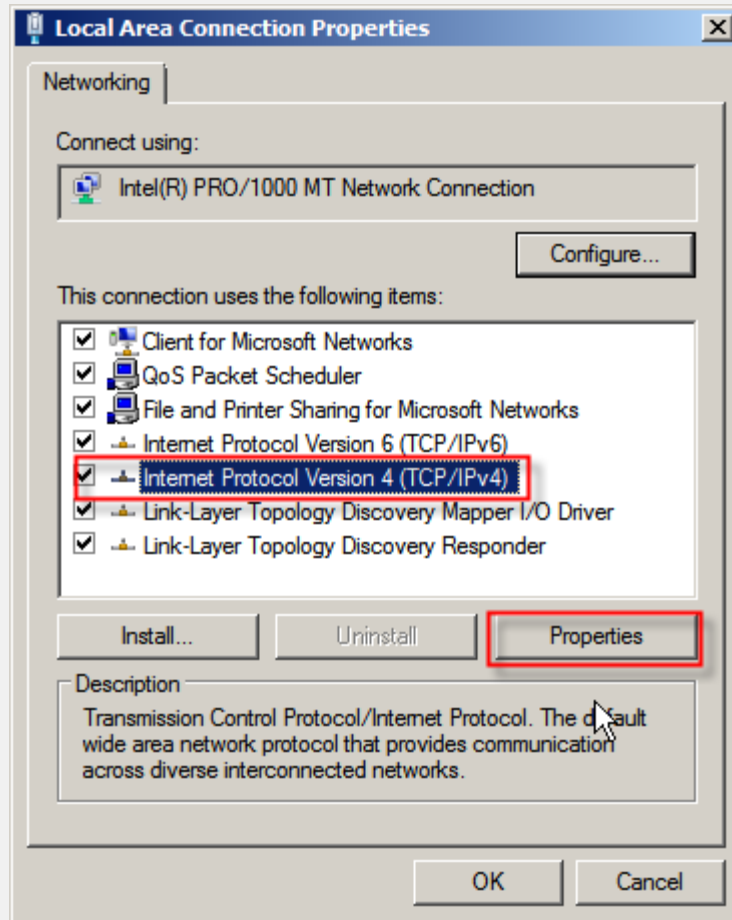
- 1 From the Initial Configuration Tasks application, click **Configure networking** to assign a static IP to the server.



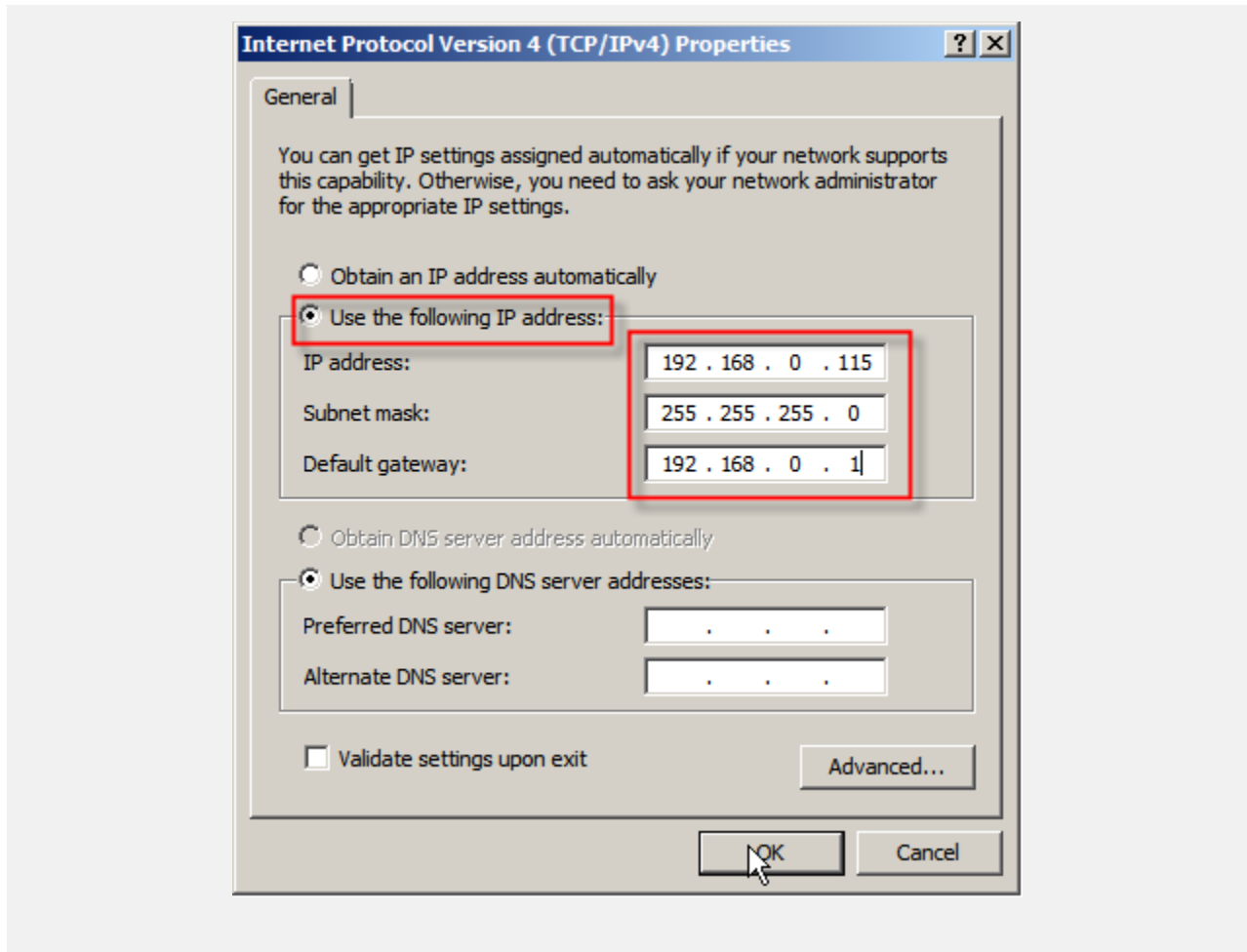
- 2 Right click the network interface and choose **Properties**.



**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.

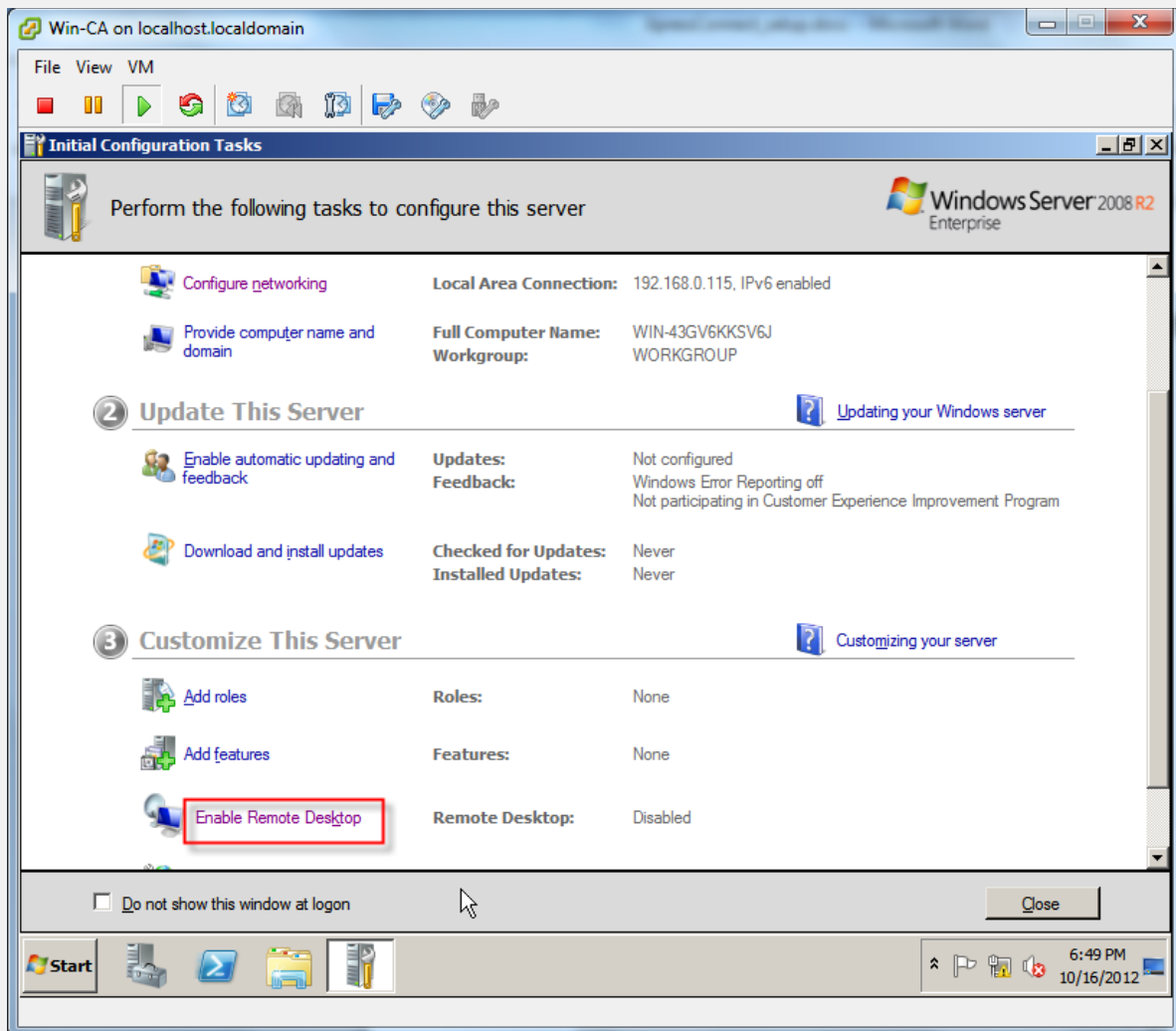


*Note: Remote desktop will generally perform better than the Virtual Machine Console interface of vSphere Client.*

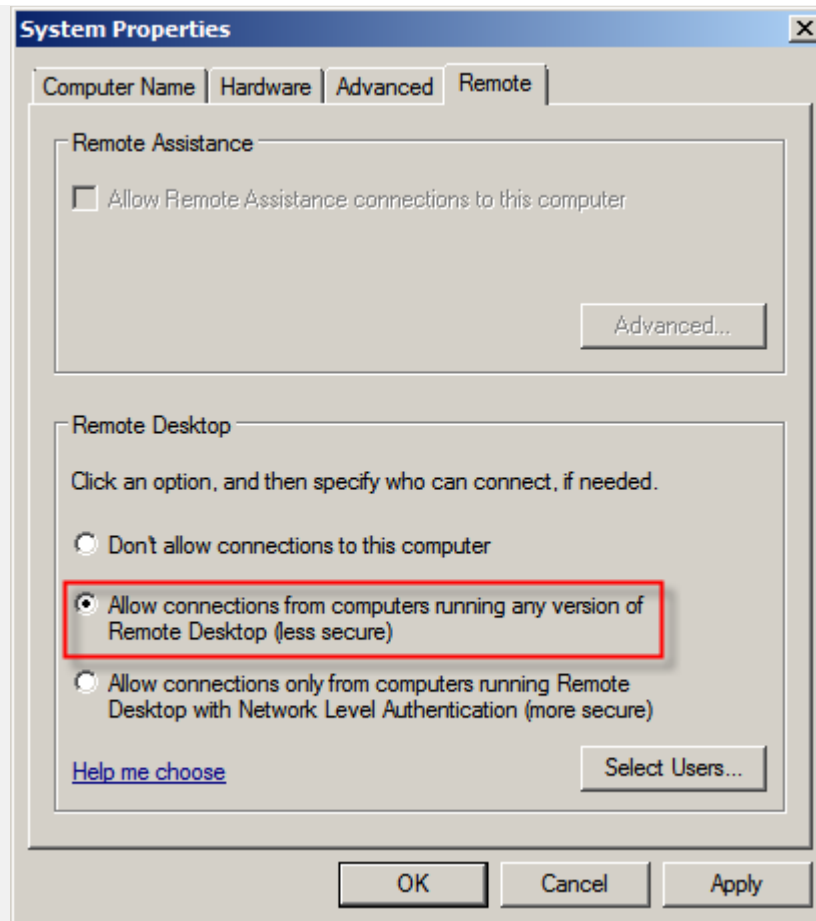
1

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

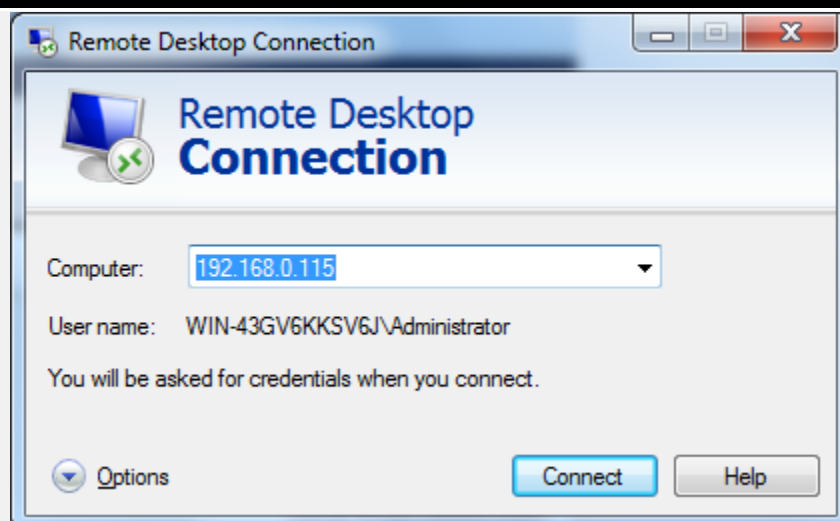




2 Choose to Allow connections. Click OK at the security pop up box. Then click OK again.



- 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

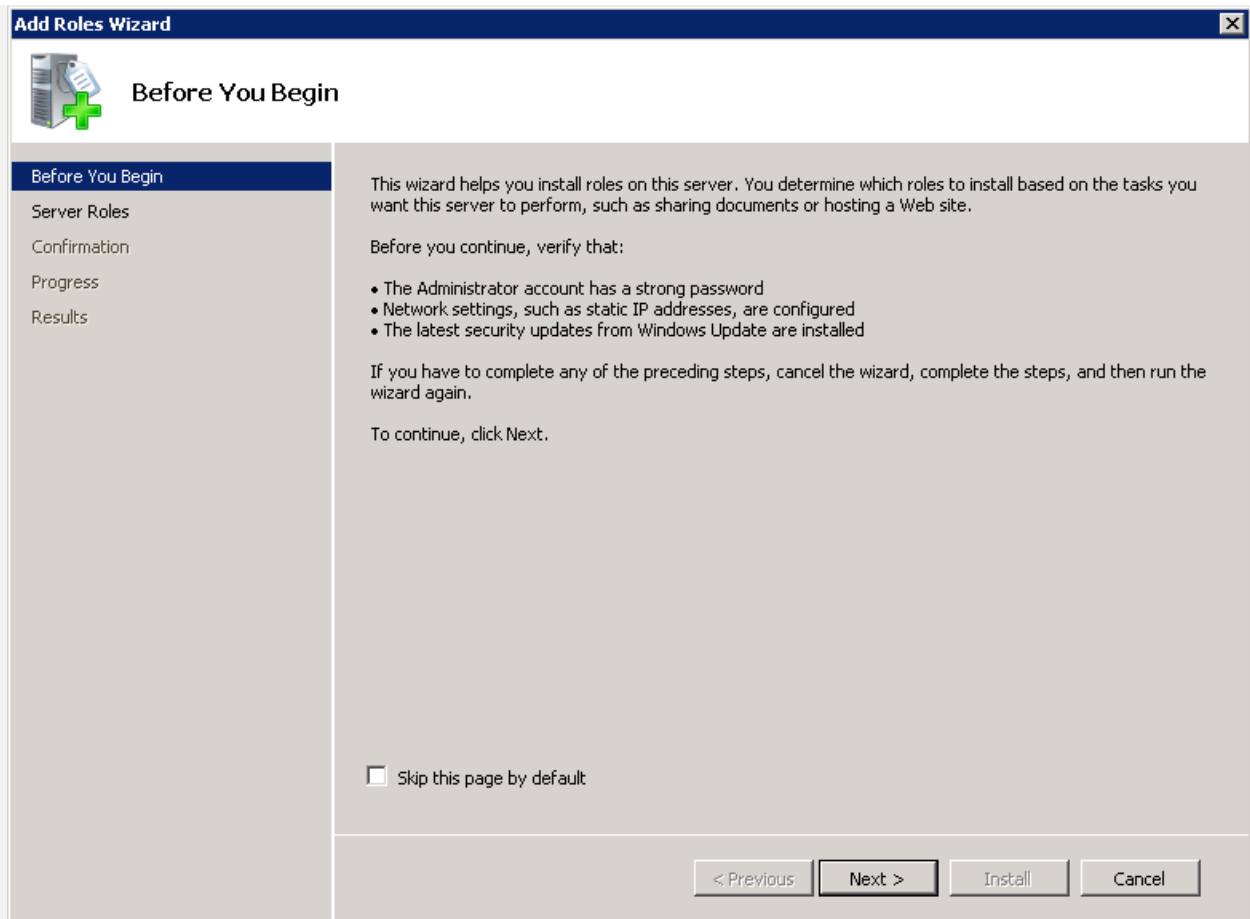
Perform the following tasks to configure this server

- #### 1 Provide Computer Information

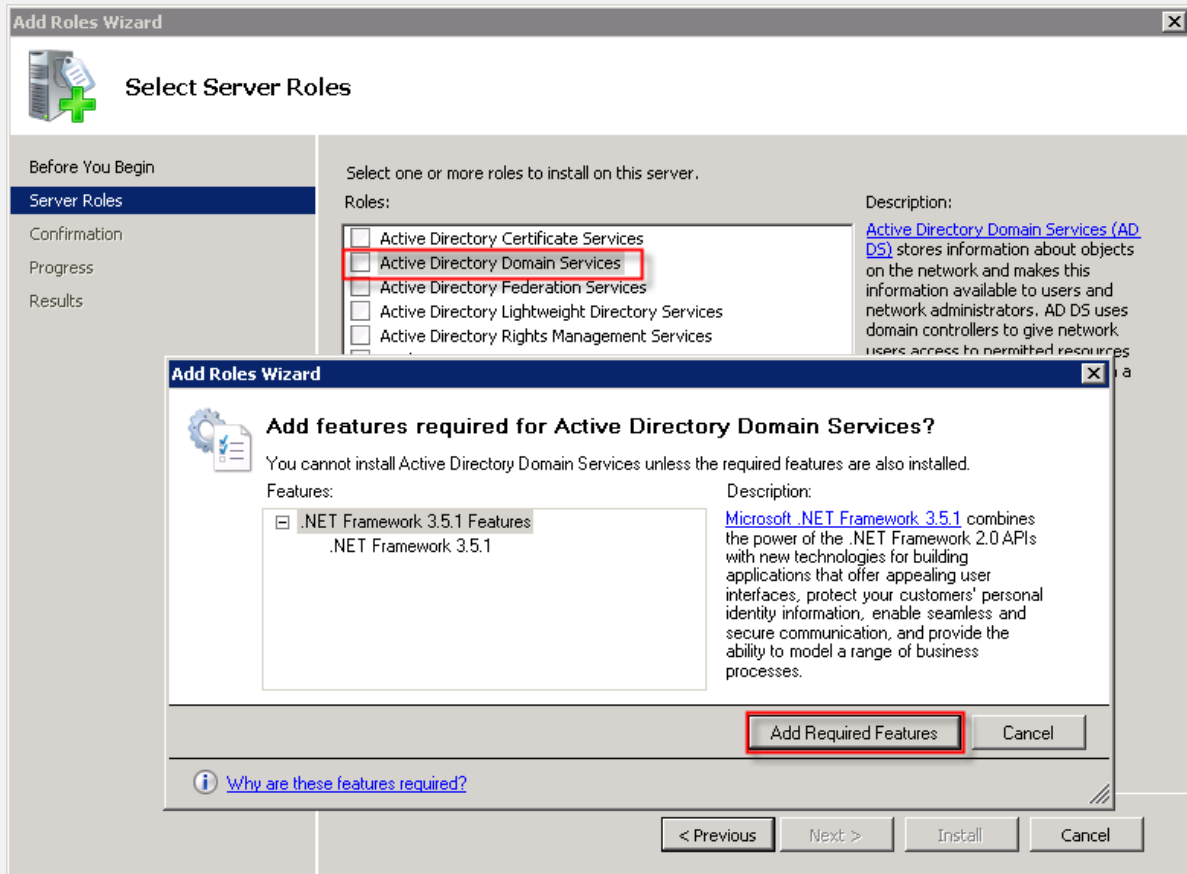
 <a href="#">Activate Windows</a>	<b>Product ID:</b>	M
 <a href="#">Set time zone</a>	<b>Time Zone:</b>	(
 <a href="#">Configure networking</a>	<b>Local Area Connection:</b>	1
 <a href="#">Provide computer name and domain</a>	<b>Full Computer Name:</b>	\
	<b>Workgroup:</b>	\
- #### 2 Update This Server

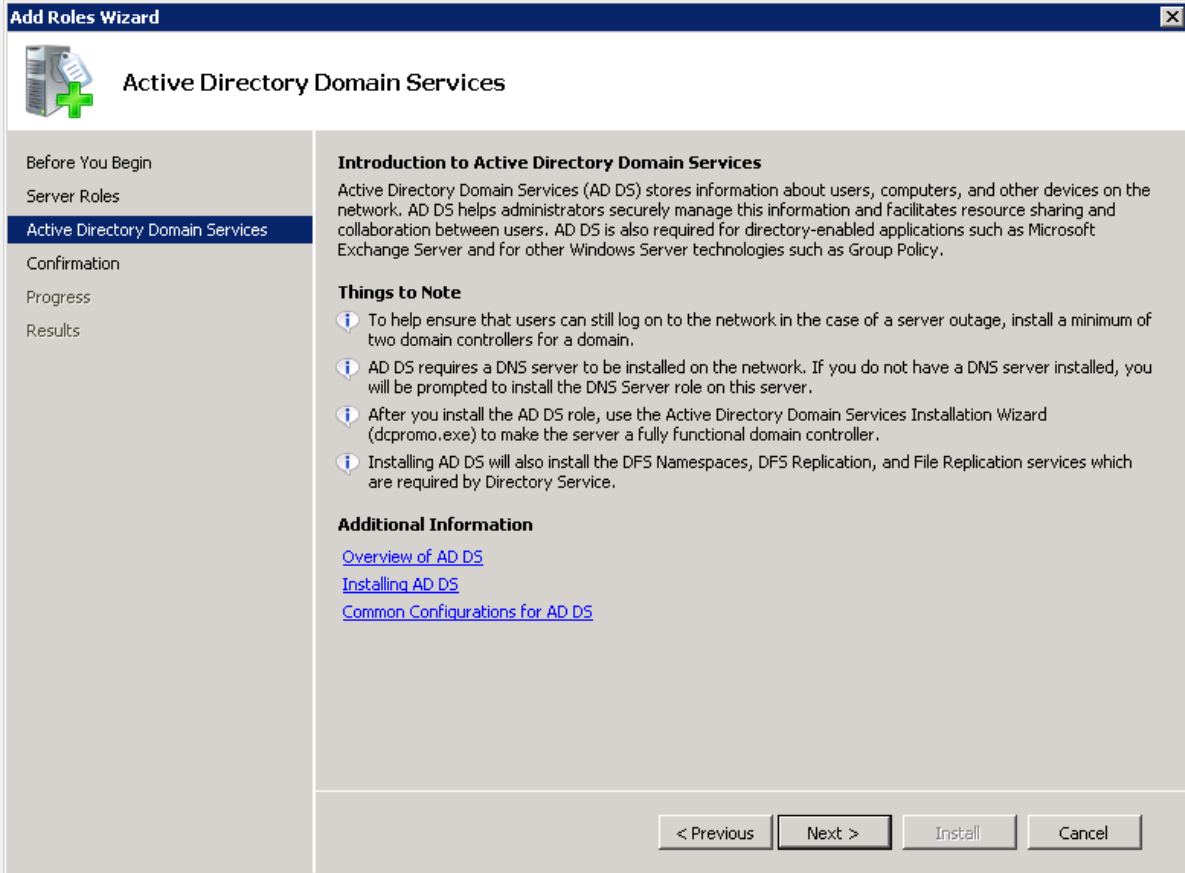
 <a href="#">Enable automatic updating and feedback</a>	<b>Updates:</b>	M
	<b>Feedback:</b>	\
		M
 <a href="#">Download and install updates</a>	<b>Checked for Updates:</b>	M
	<b>Installed Updates:</b>	M
- #### 3 Customize This Server

 <a href="#">Add roles</a>	<b>Roles:</b>	M
 <a href="#">Add features</a>	<b>Features:</b>	M
 <a href="#">Enable Remote Desktop</a>	<b>Remote Desktop:</b>	E
 <a href="#">Configure Windows Firewall</a>	<b>Firewall:</b>	F

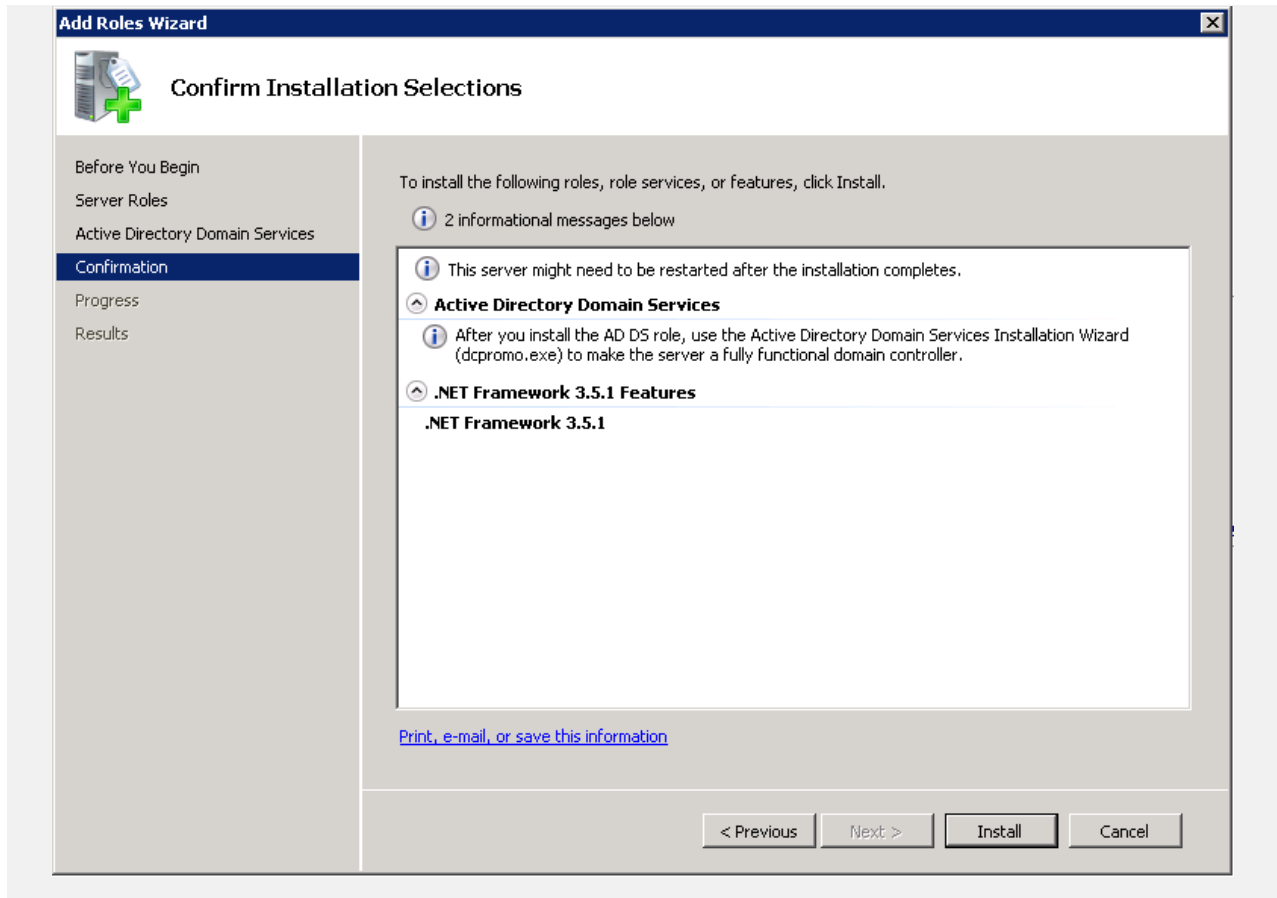


- 2 Check Active Directory Domain Services. When the pop up appears click Add Required Features. Click Next. Then click Next again.

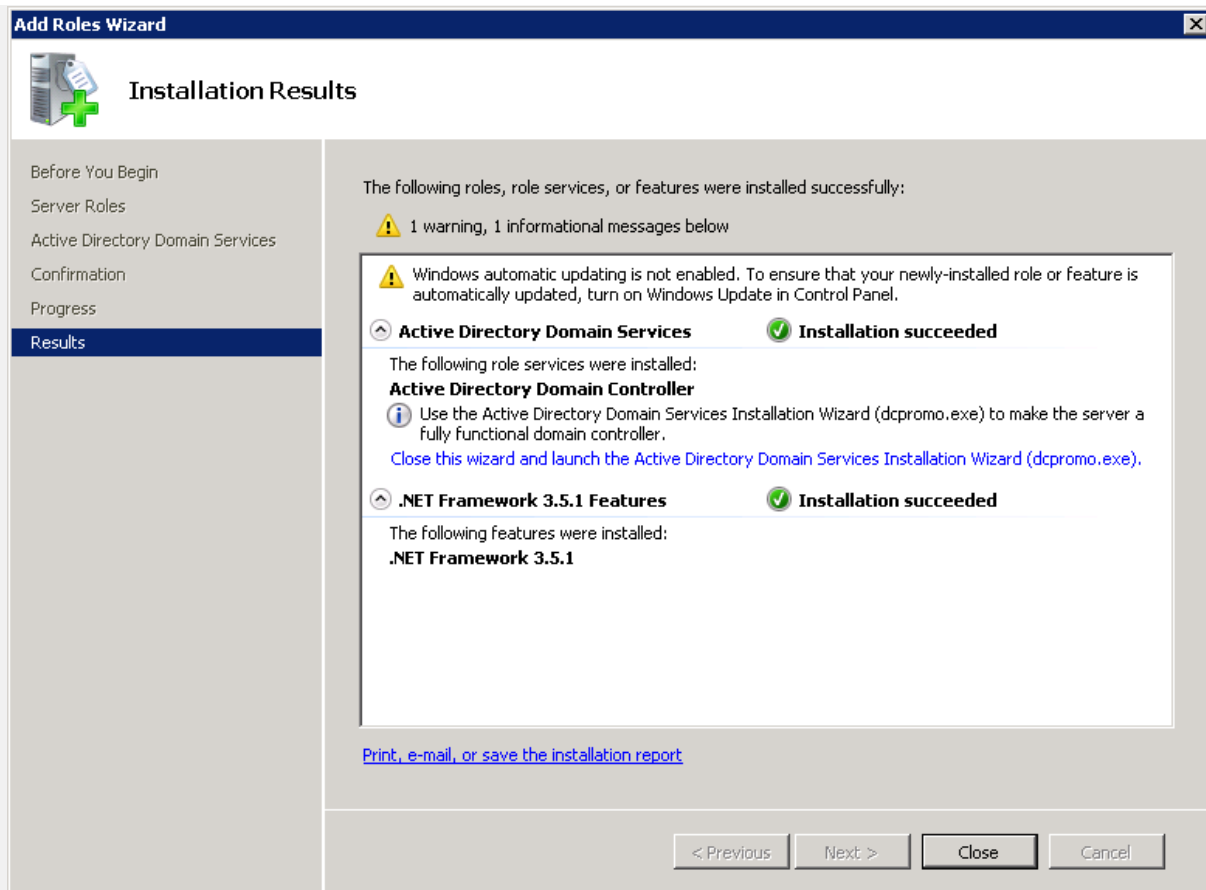




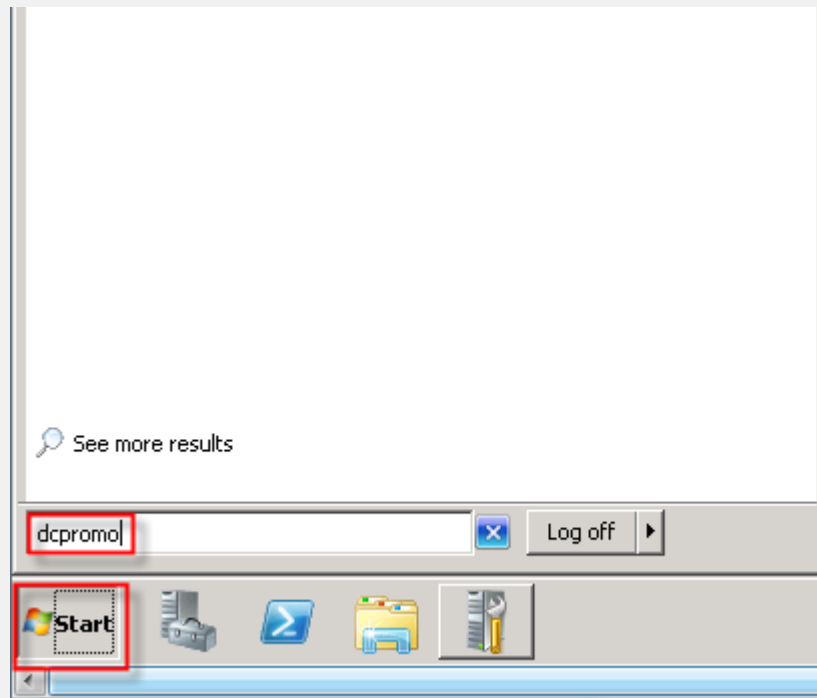
3 Click Install. Click Close after it finishes installing.

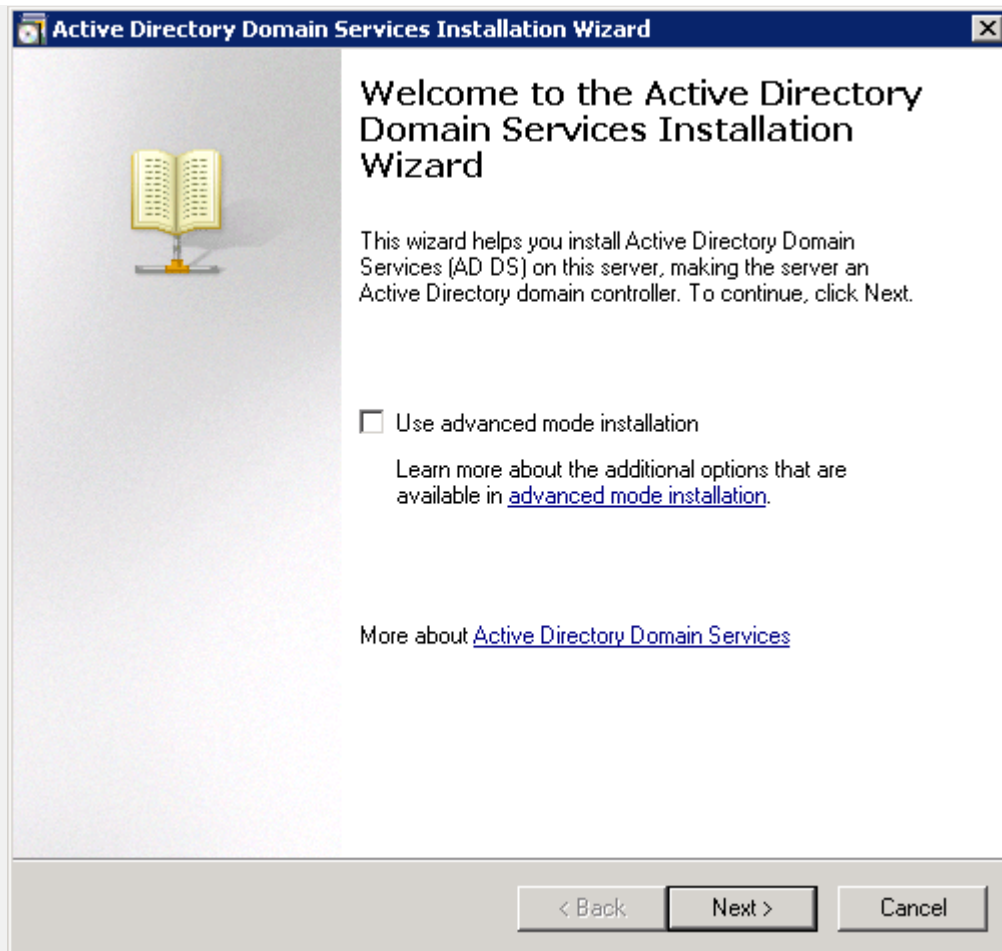


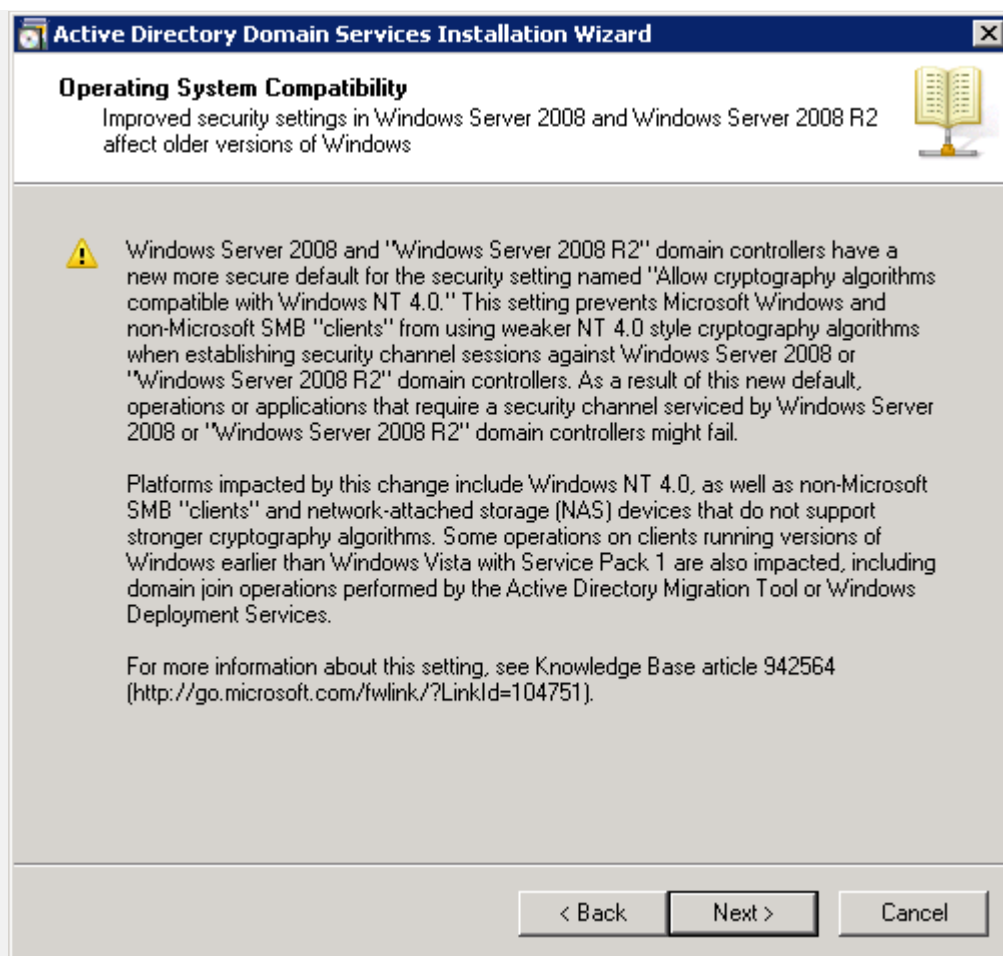




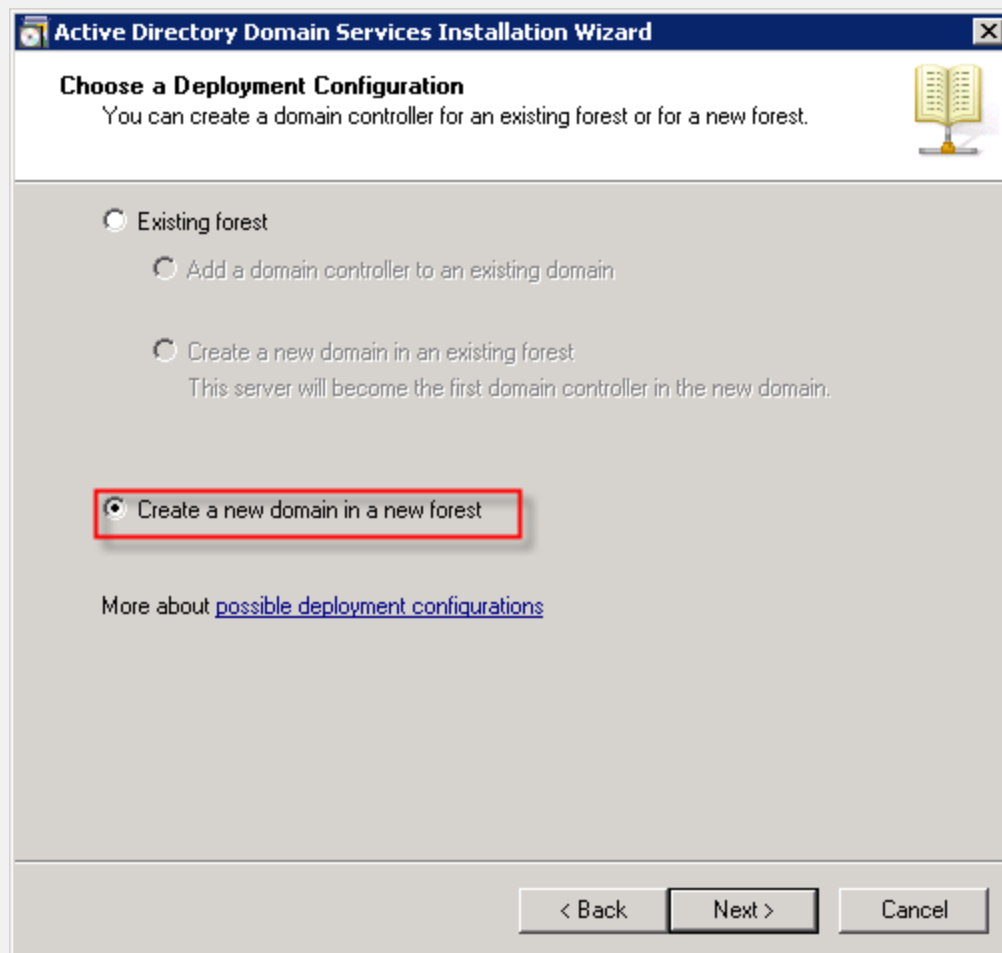
- 4 Click Start. Type dcpromo in the box and press Enter. Click Next to begin the Wizard. Click Next again.







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



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

**Active Directory Domain Services Installation Wizard**

**Name the Forest Root Domain**

The first domain in the forest is the forest root domain. Its name is also the name of the forest.

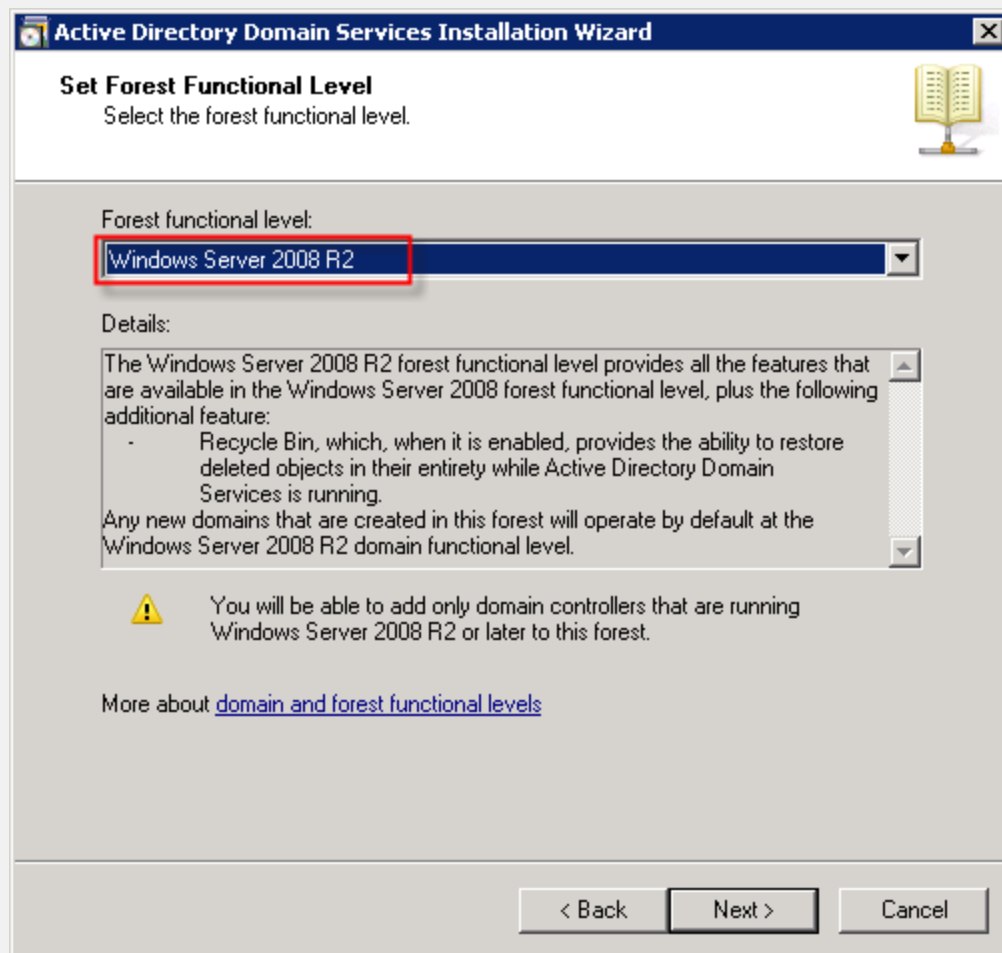
Type the fully qualified domain name (FQDN) of the new forest root domain.

FQDN of the forest root domain:

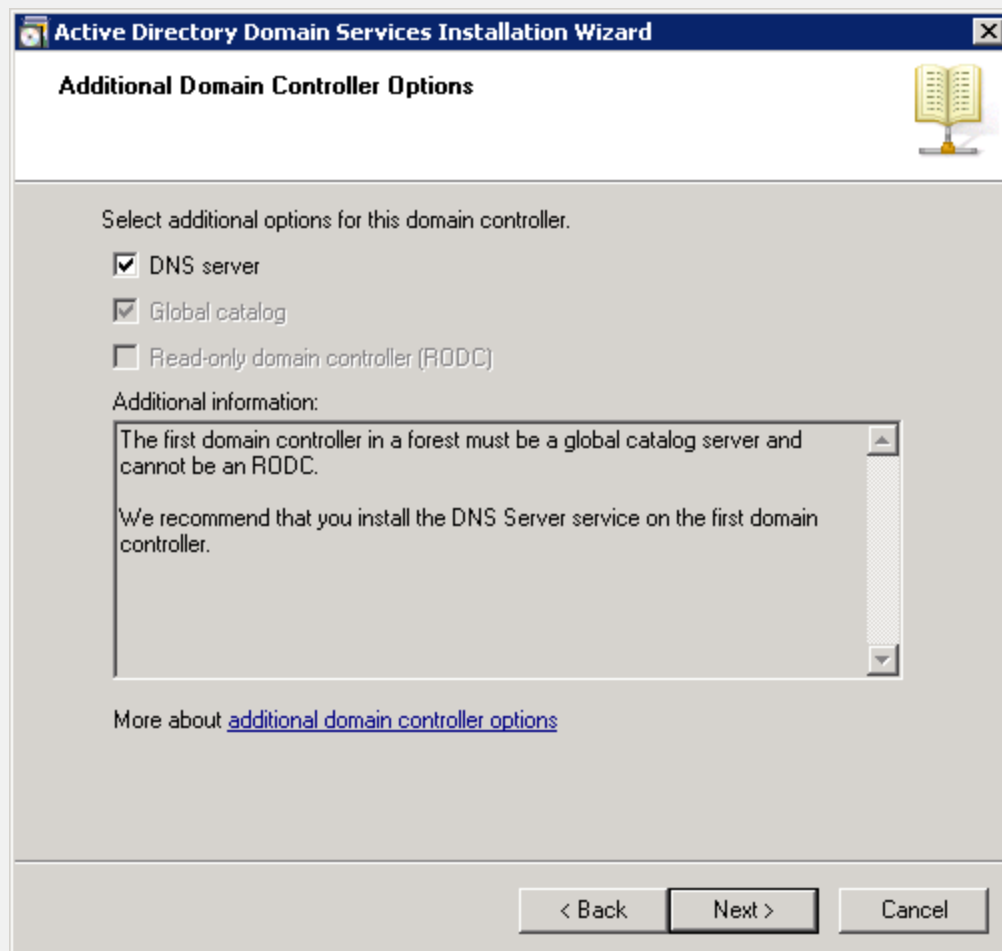
Example: corp.contoso.com

< Back   Next >   Cancel

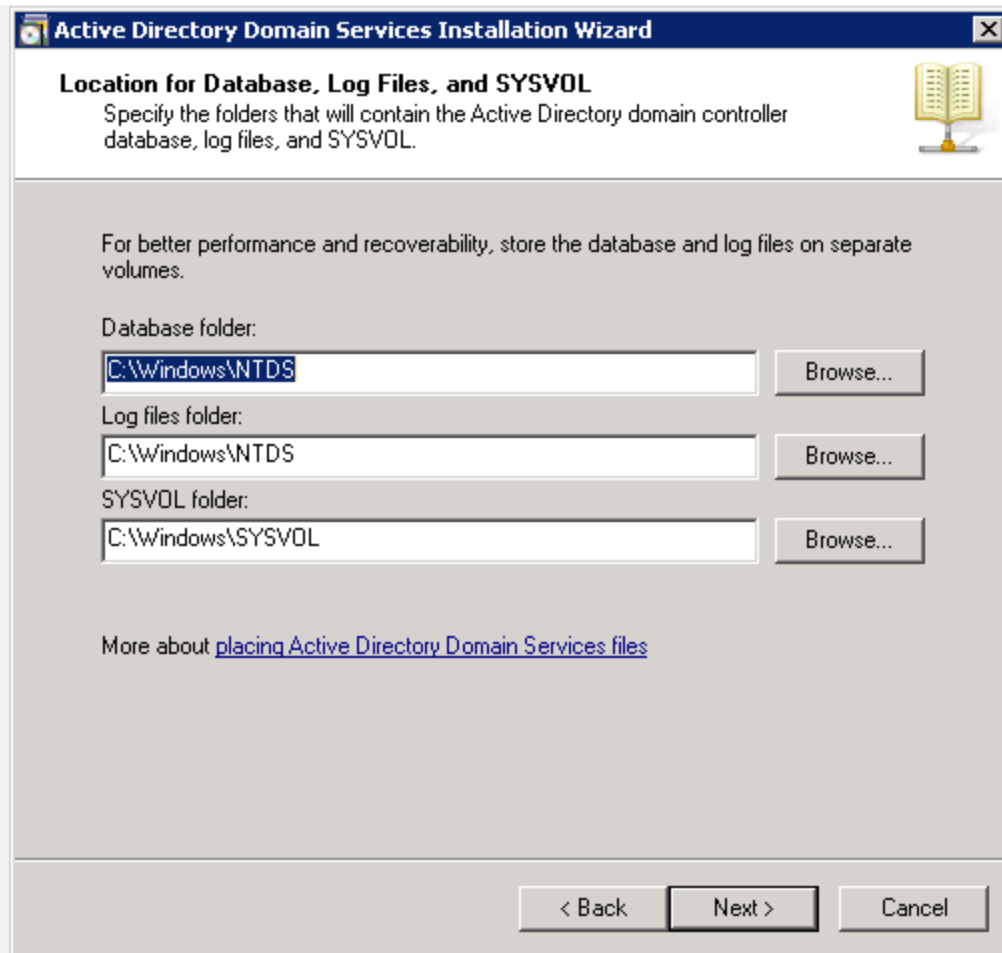
**7** | Select Windows Server 2008 R2. Click Next. At the warning dialog box, click Yes.



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







- 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.

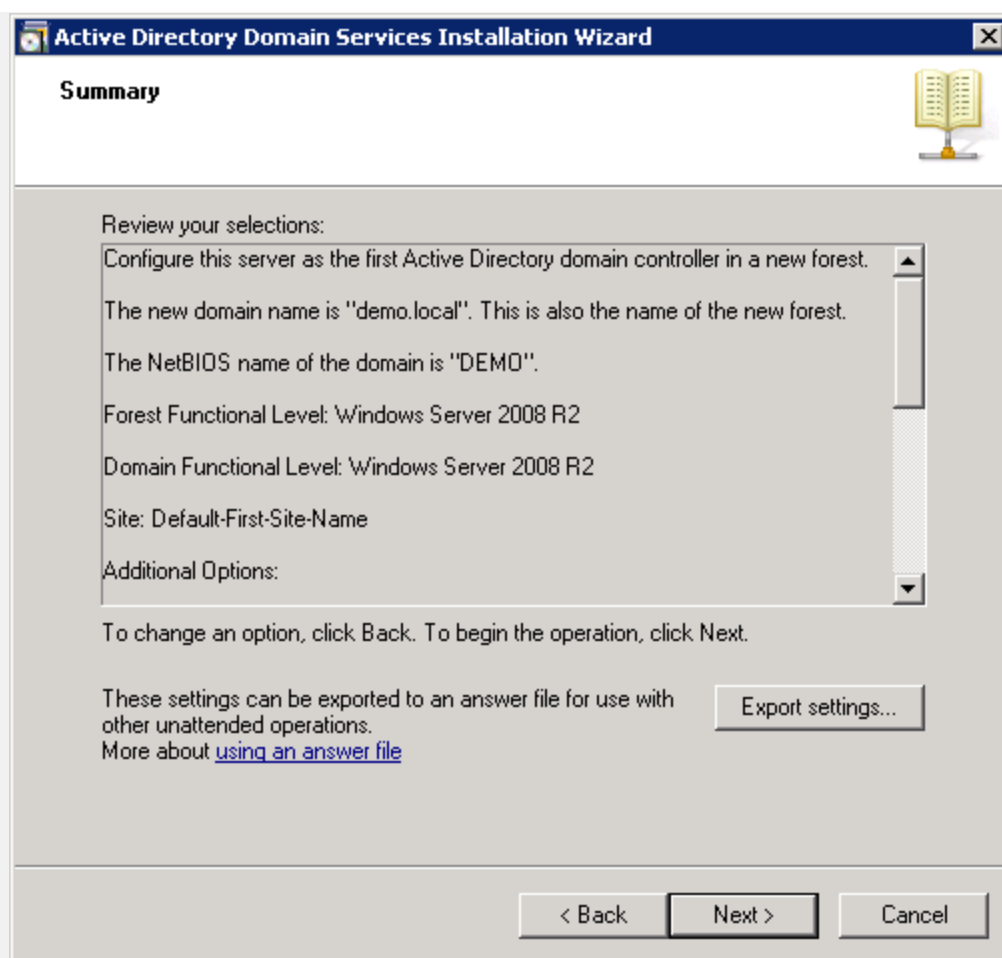
Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

Password:

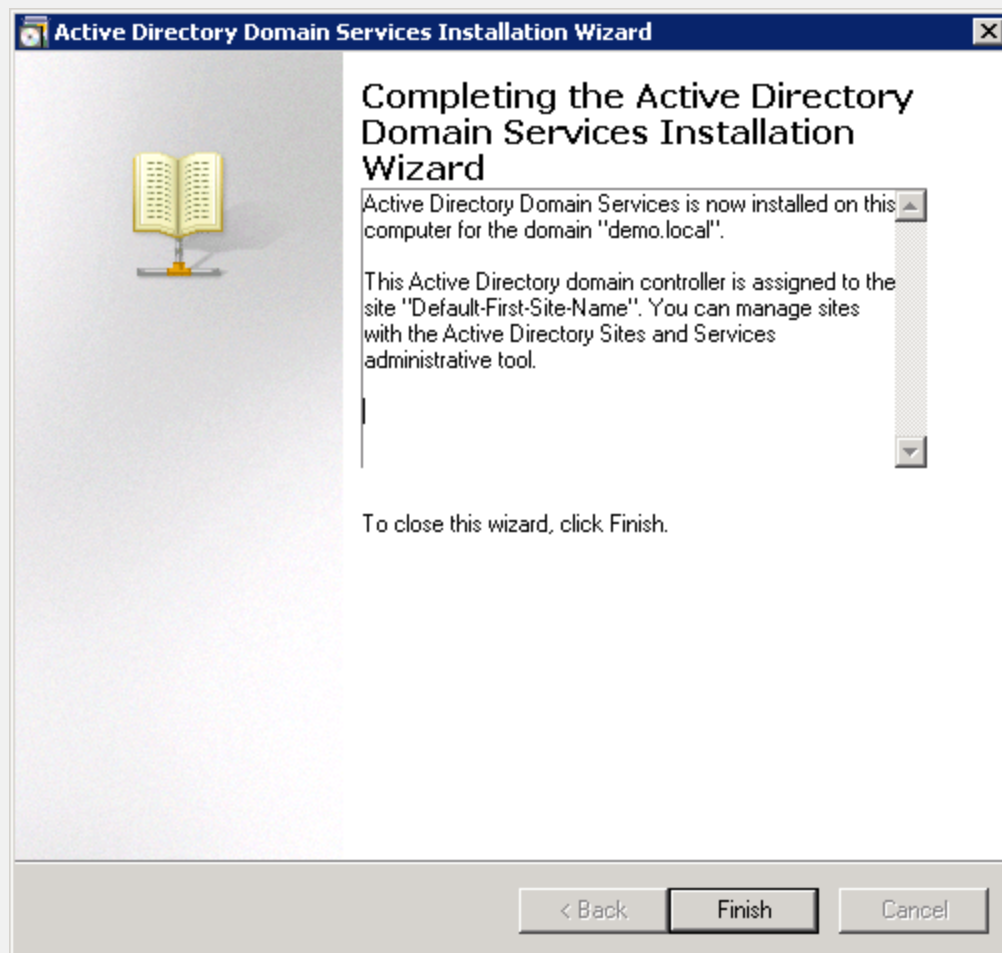
Confirm password:

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.

### 3 Customize This Server



Add roles



Add features



Enable Remote Desktop



Configure Windows Firewall

Roles: DNS Server,

Features: Group Policy

Remote Desktop: Enabled

Firewall: Domain: On

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

### Add Roles Wizard



#### Select Server Roles

Before You Begin

Server Roles

Network Policy and Access Services

Role Services

AD CS

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Web Server (IIS)

Role Services

Confirmation

Progress

Results

Select one or more roles to install on this server.

Roles:

- ☒ Active Directory Certificate Services
- ☒ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☒ DNS Server (Installed)
- ☐ Fax Server
- ☐ File Services
- ☐ Hyper-V
- ☒ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Desktop Services
- ☒ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description:

[Network Policy and Access Services](#) provides Network Policy Server (NPS), Routing and Remote Access, Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.

[More about server roles](#)


< Previous

Next >

Install

Cancel

**Add Roles Wizard**

 **Select Role Services**

Before You Begin  
Server Roles  
Network Policy and Access Services  
**Role Services**  
AD CS  
  Role Services  
  Setup Type  
  CA Type  
  Private Key  
    Cryptography  
    CA Name  
    Validity Period  
  Certificate Database  
Web Server (IIS)  
  Role Services  
Confirmation  
Progress  
Results

Select the role services to install for Network Policy and Access Services:

Role services:


- ☒ **Network Policy Server**
- ☐ Routing and Remote Access Services
  - ☐ Remote Access Service
  - ☐ Routing
- ☐ Health Registration Authority
- ☐ Host Credential Authorization Protocol

Description:  
[Network Policy Server \(NPS\)](#) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization. With NPS, you can also deploy Network Access Protection (NAP), a client health policy creation, enforcement, and remediation technology.

[More about role services](#)

< Previous    Next >    Install    Cancel

**Add Roles Wizard** [X]

 **Select Role Services**

**Before You Begin**

**Server Roles**

**Network Policy and Access Services**

**Role Services**

**AD CS**

**Role Services**

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Web Server (IIS)

Role Services

Confirmation

Progress

Results

Select the role services to install for Active Directory Certificate Services:

Role services:

- ☒ Certification Authority
- ☐ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☐ Certificate Enrollment Policy Web Service

Description:


[Certification Authority \(CA\)](#) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

[More about role services](#)

< Previous   Next >   Install   Cancel

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

**Add Roles Wizard**

 **Specify Setup Type**

Before You Begin  
Server Roles  
Network Policy and Access Services  
    Role Services  
AD CS  
    Role Services  
**Setup Type**  
CA Type  
    Private Key  
        Cryptography  
        CA Name  
        Validity Period  
    Certificate Database  
Web Server (IIS)  
    Role Services  
Confirmation  
Progress  
Results

Certification Authorities can use data in Active Directory to simplify the issuance and management of certificates. Specify whether you want to set up an Enterprise or Standalone CA.

☒ **Enterprise**  
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.

☐ Standalone  
Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.


[More about the differences between enterprise and standalone setup](#)

< Previous   Next >   Install   Cancel

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



**Add Roles Wizard**

 **Specify CA Type**

Before You Begin

Server Roles

Network Policy and Access Services

Role Services

AD CS

Role Services

Setup Type

**CA Type**

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Web Server (IIS)

Role Services

Confirmation

Progress

Results

A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

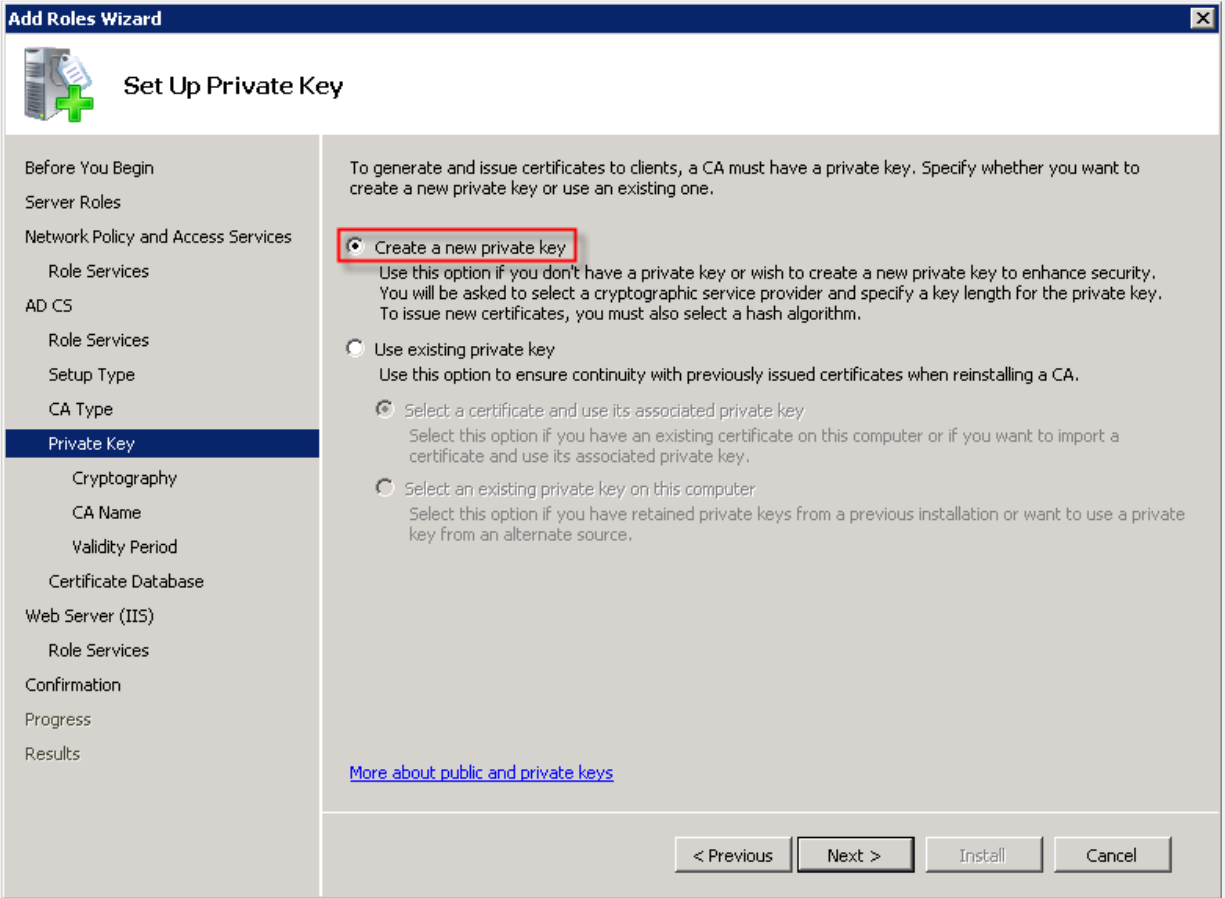
☒ **Root CA**  
Select this option if you are installing the first or only certification authority in a public key infrastructure.

☐ Subordinate CA  
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

[More about public key infrastructure \(PKI\)](#)


< Previous   Next >   Install   Cancel

**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.

Add Roles Wizard



Configure CA Name

Before You Begin

Server Roles

Network Policy and Access Services

Role Services

AD CS

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Web Server (IIS)

Role Services

Confirmation

Progress

Results

Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:  
demo-CA

Distinguished name suffix:  
DC=demo,DC=local

Preview of distinguished name:  
CN=demo-CA,DC=demo,DC=local

[More about configuring a CA name](#)

< Previous

Next >

Install

Cancel

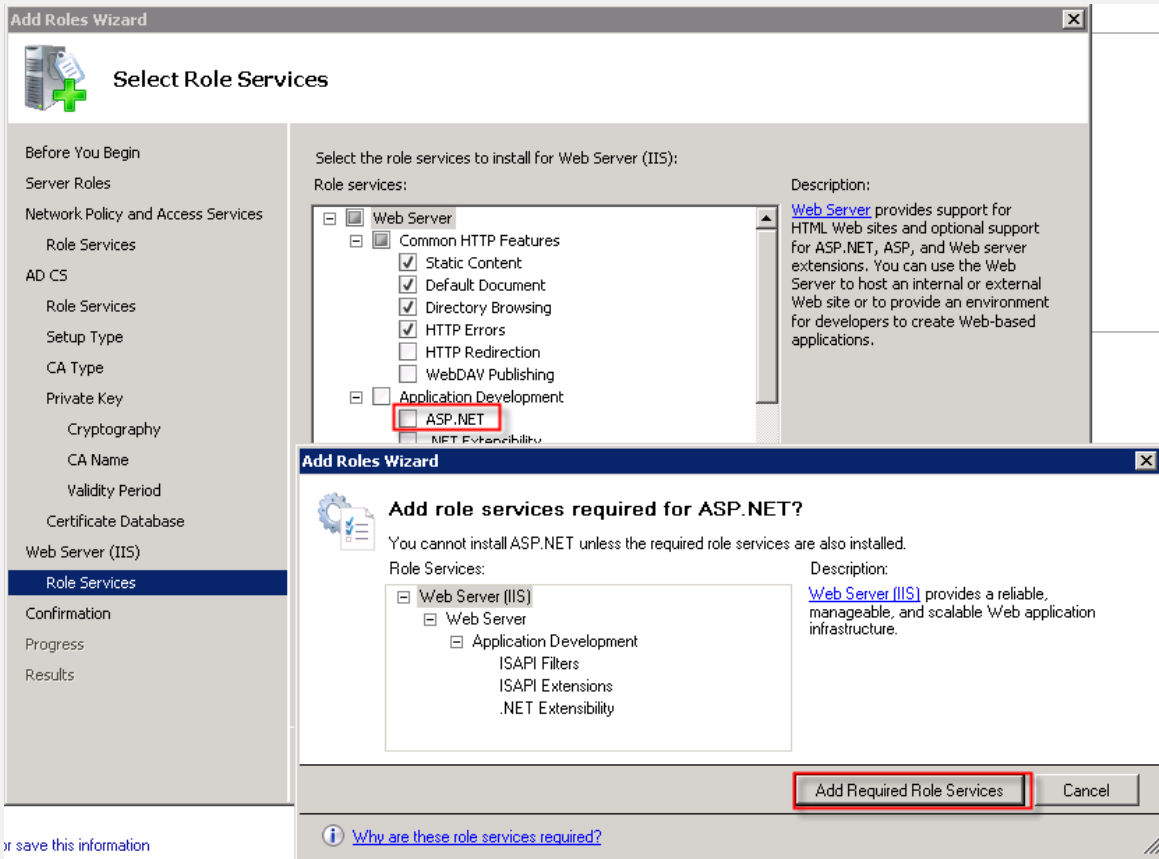
8

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

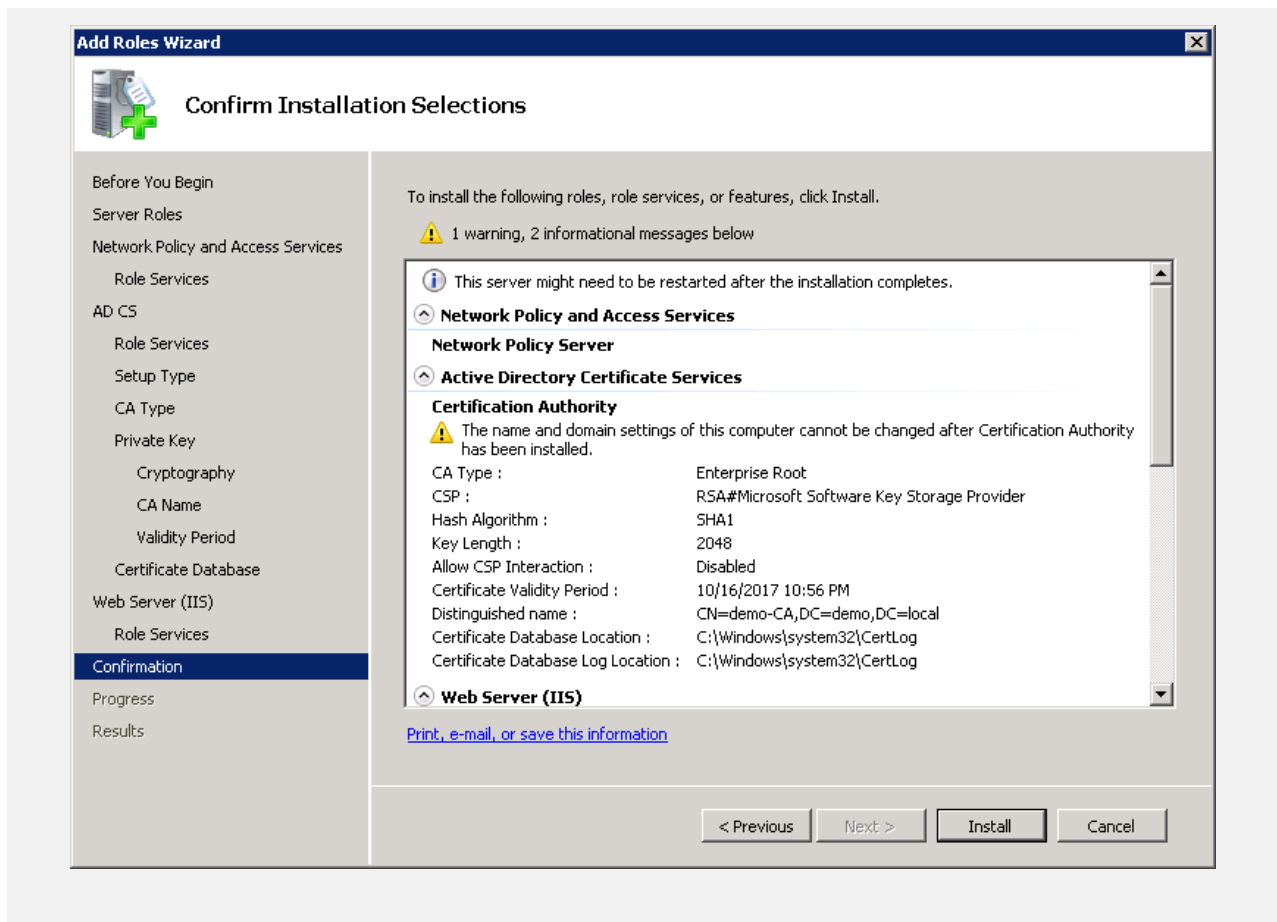
ZEBRA CONFIDENTIAL: INTERNAL USE ONLY

ZEBRA TECHNOLOGIES

51



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

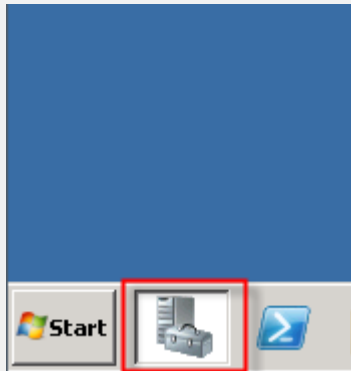


## 2.2.6 Configure DNS

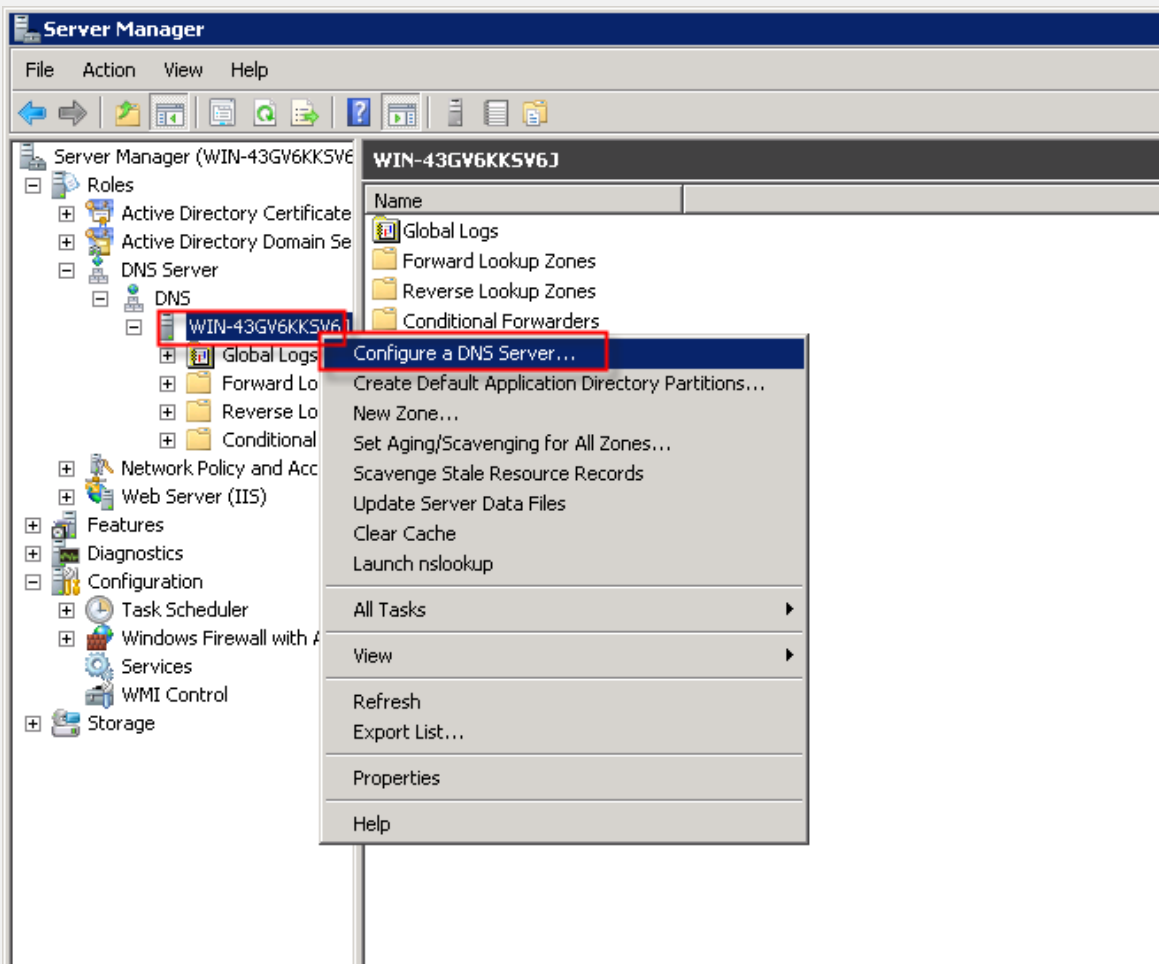
This will setup the DNS service to resolve any names in the “.local” hierarchy and forward any unknown queries to other public DNS servers. This will allow use of DNS names within the lab configuration and allow the certificate hierarchy to function with minimal extra configuration, while still allowing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

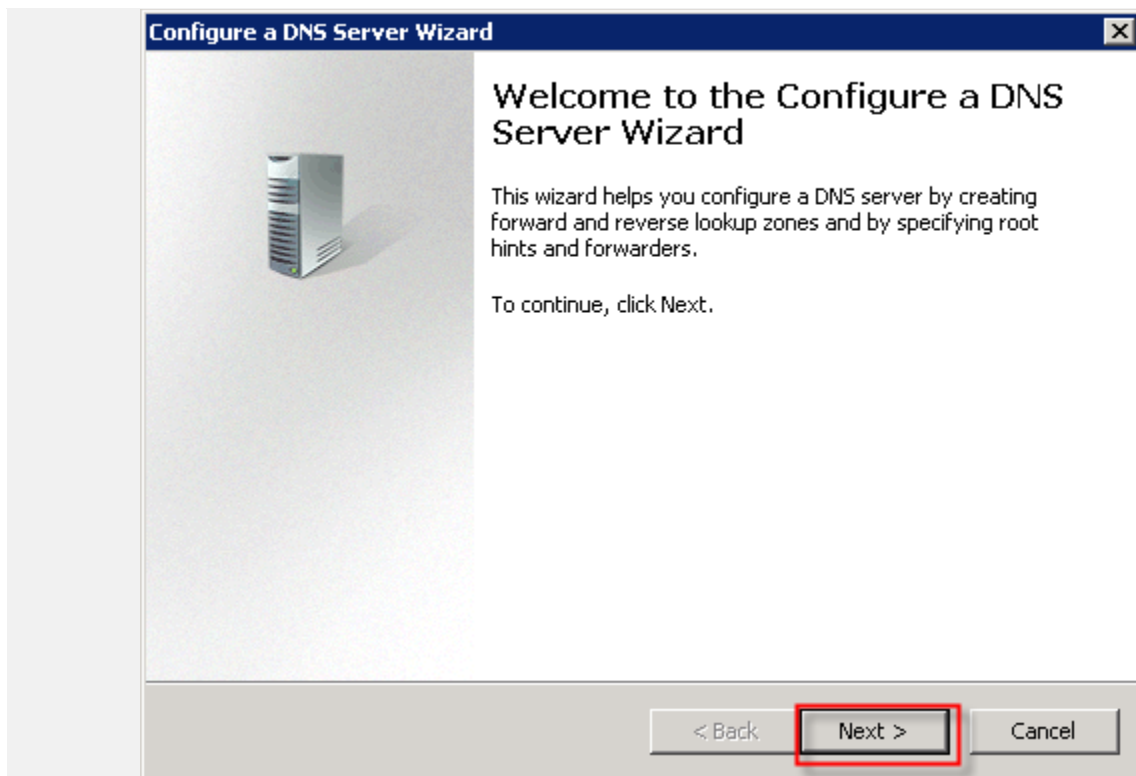
For the demo environment to work properly and clients or servers in the lab that are part of the demo, should be assigned to use this Windows Server as the DNS server. For example, if this server has an IP address of 192.168.0.115, then a DHCP server would need to be configured with the option for DNS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

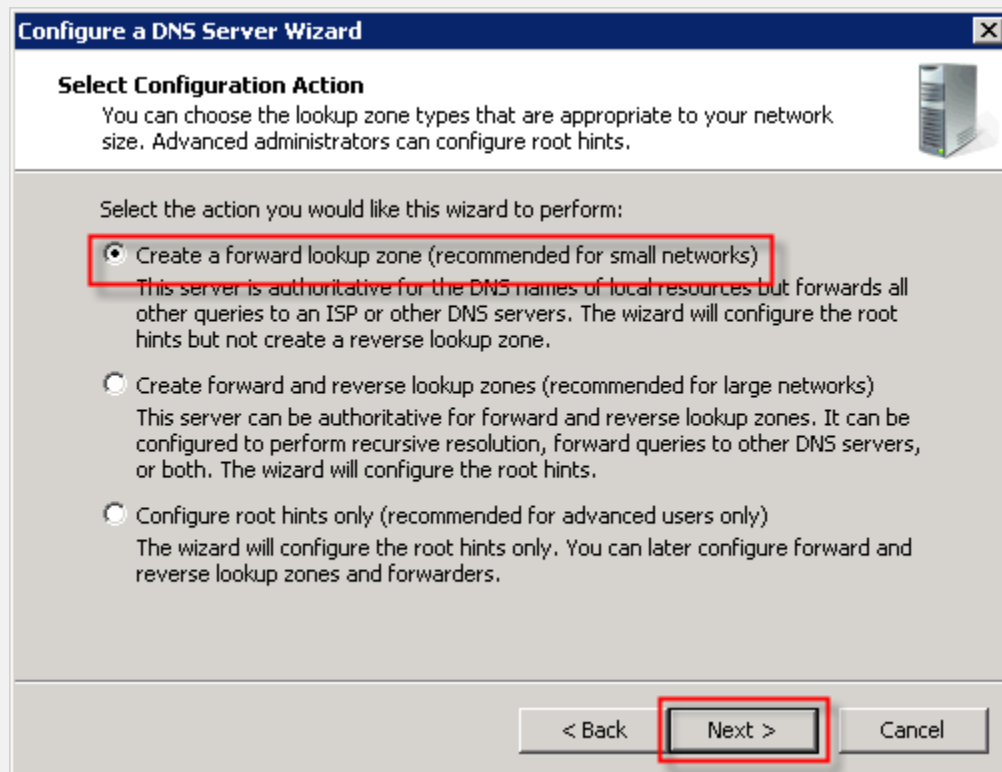


- 2 Expand Roles → DNS Server → DNS. Right click on the name of the server and choose Configure a DNS Server. Click Next.



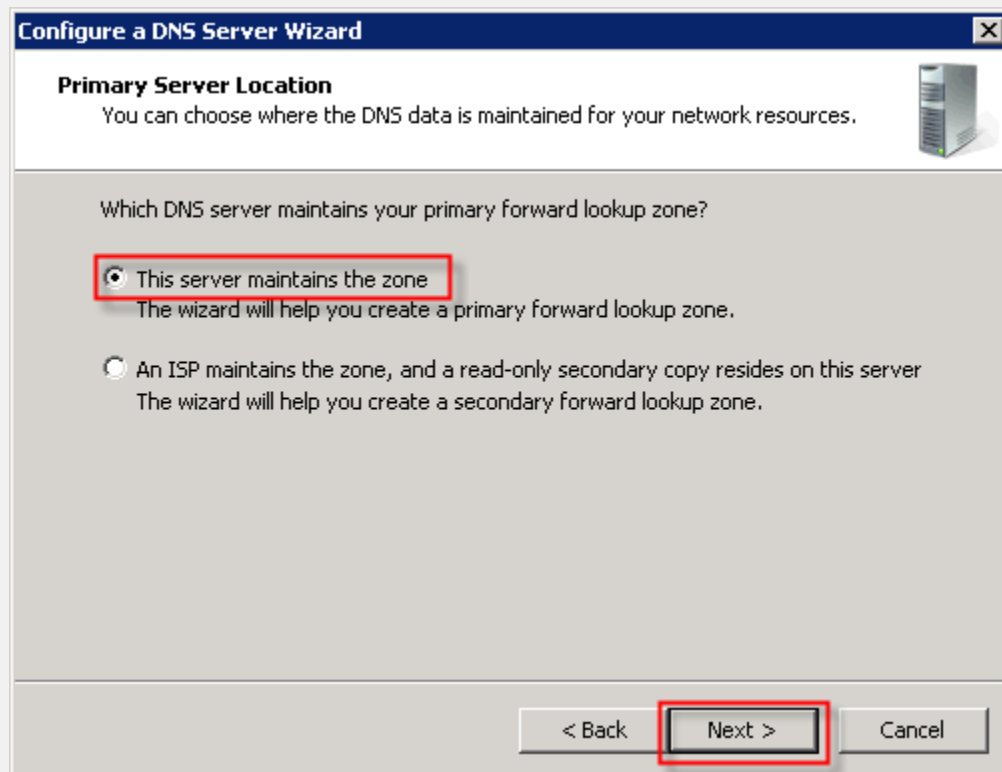


**3** Choose Create a forward lookup zone and click Next.



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** [X]

**Zone Name**  
What is the name of the new zone?

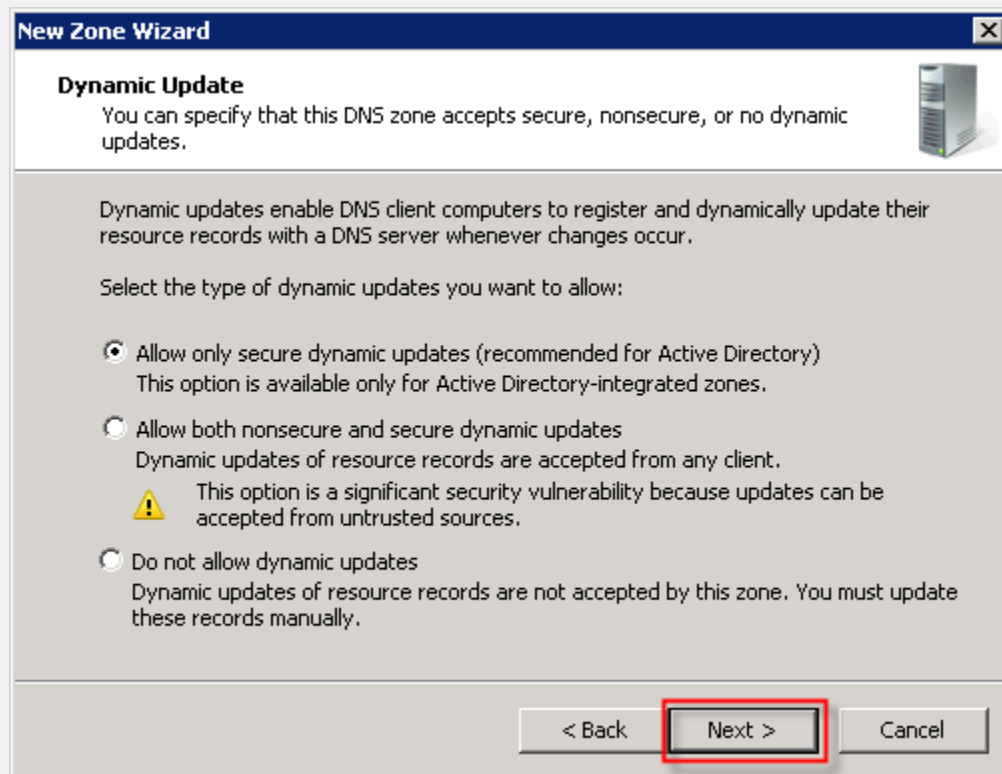


The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name:

< 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

☐ 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:  
 208.67.222.222 208.67.220.220

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

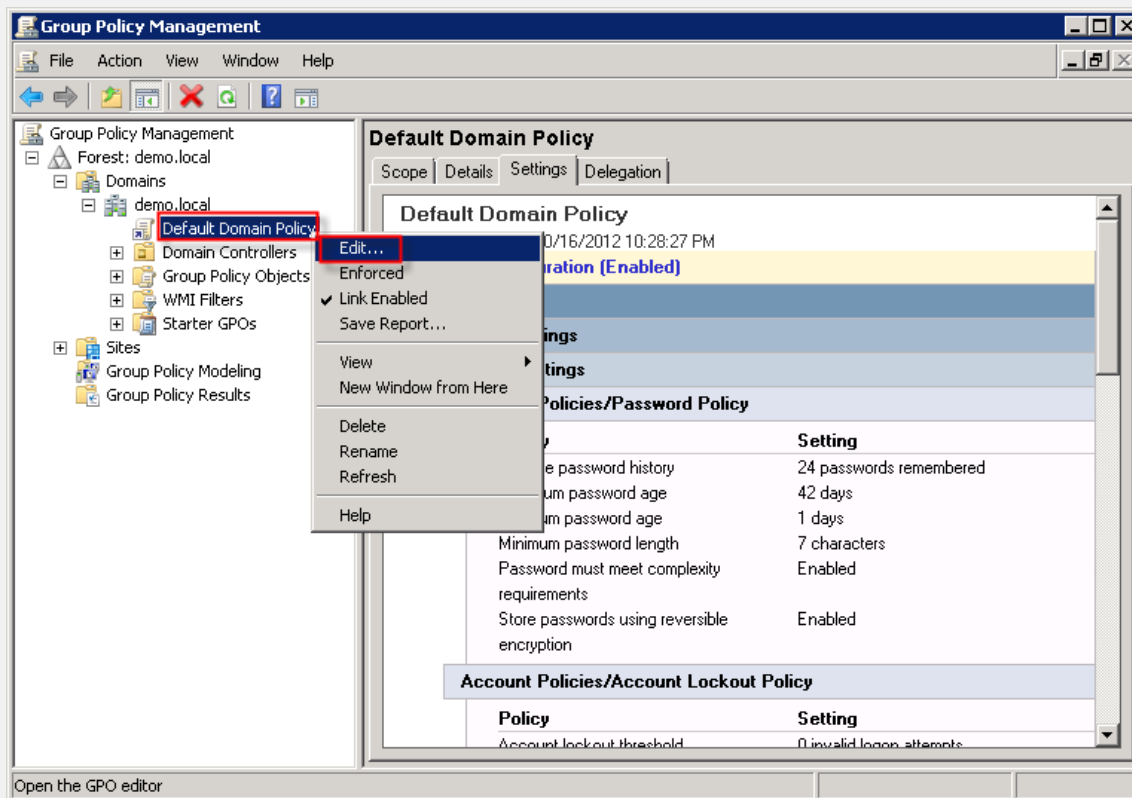
## 2.2.7 Configure Windows Server Password Policy

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.

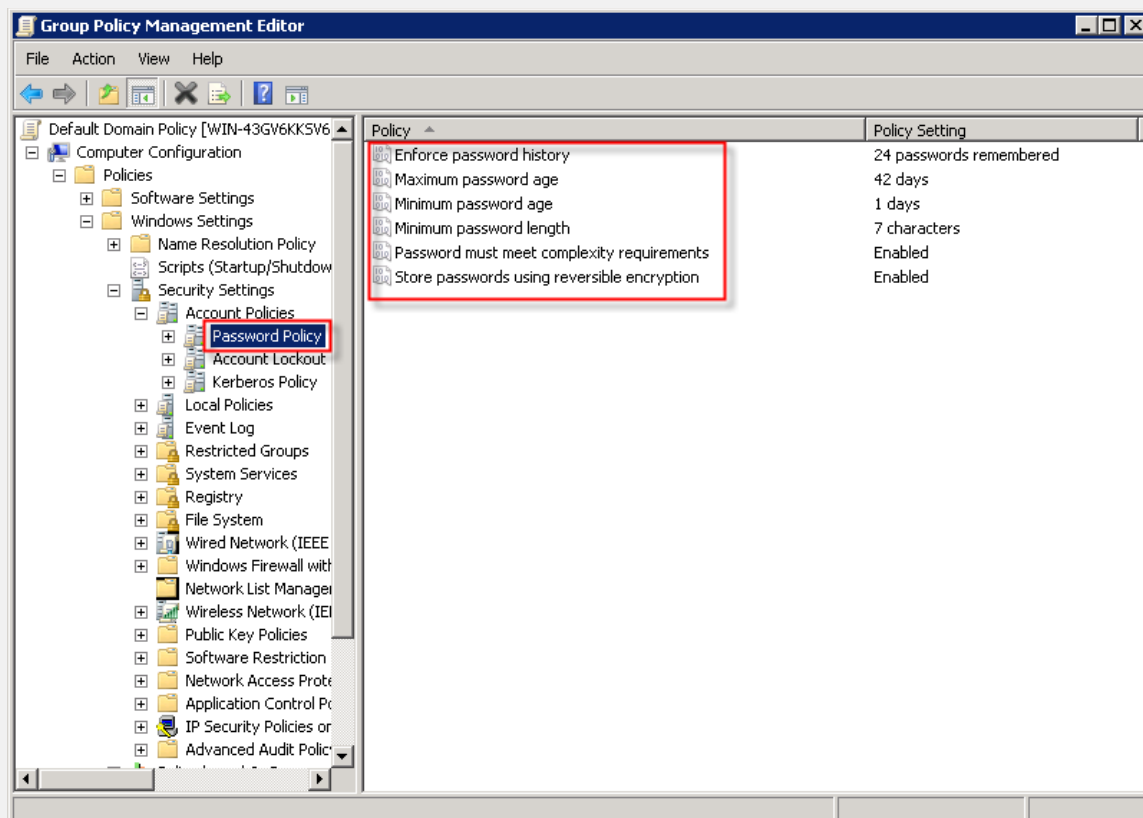


*Note: Making changes to the group policy may take a few minutes to take effect because of Active Directory synchronization. If the password policy does not appear to have taken effect after steps 1-2 are performed, then follow step 3.*

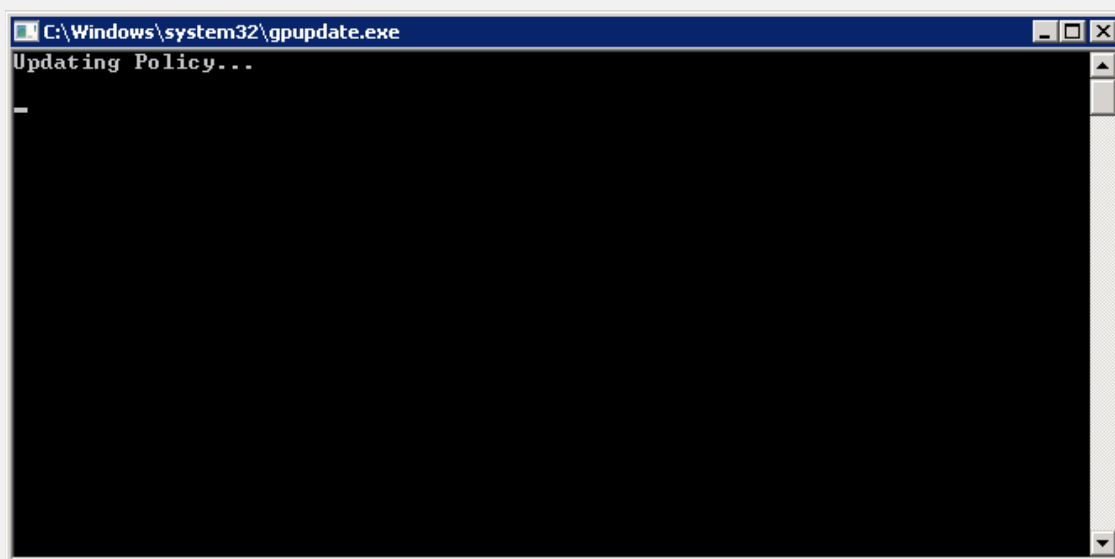
- 1 Click Start, type `gpmmc.msc` and press Enter. Expand the Forest: <domain name> → Domains → <domain name>, then right-click on Default Domain Policy and select Edit.



- 2 Expand Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies, 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

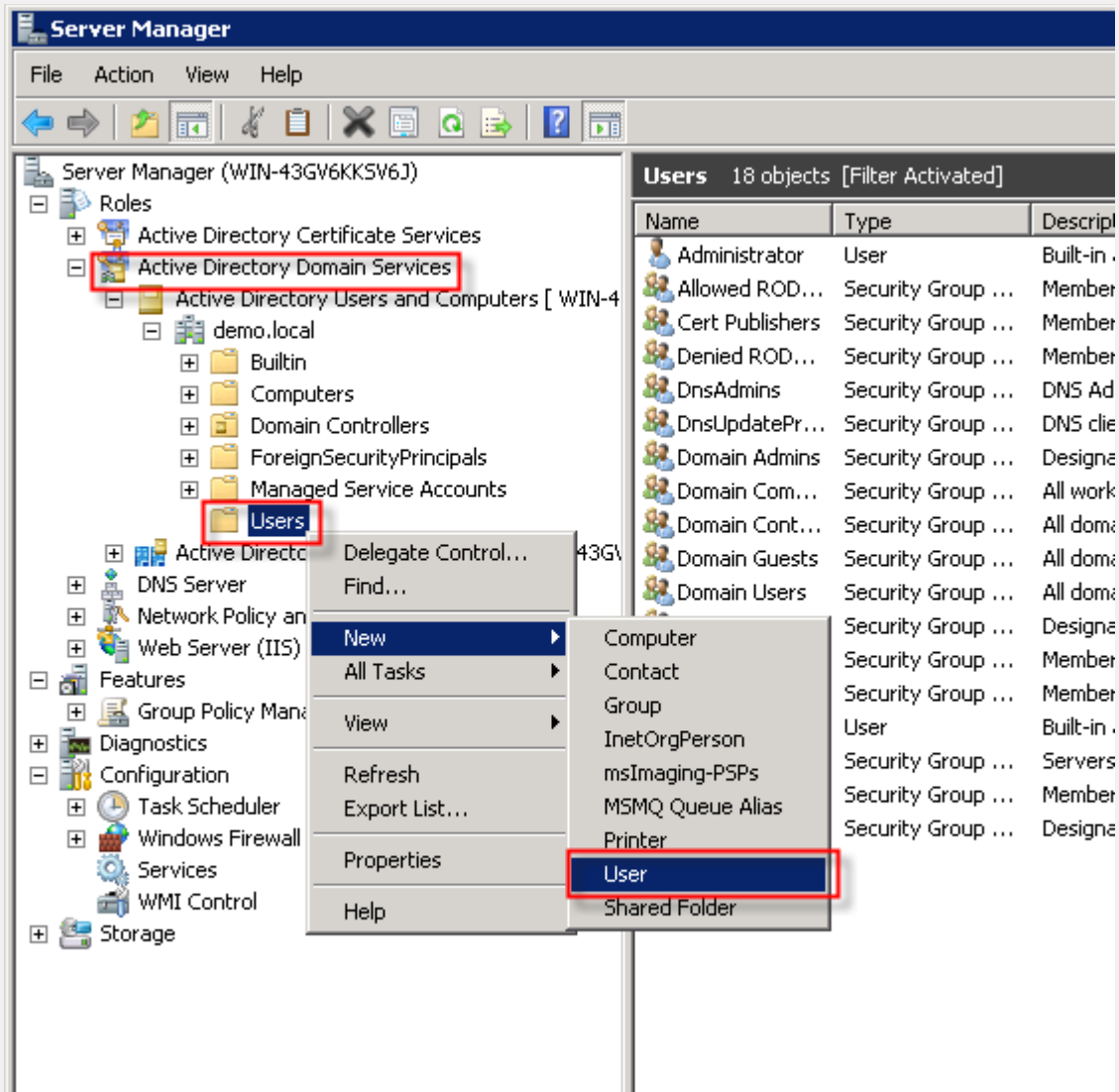
You will need to add a few user accounts and groups for testing onboarding and certificate generation. The group will be used for checking permission to onboard. In a future step, you will configure the enrollment server which has a default regex that matches the group string "BYOD APP\*". The group 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.



**New Object - User** [X]

 Create in: demo.local/Users

---

First name:  Initials:

Last name:

Full name:


User logon name:

User logon name (pre-Windows 2000):

---

- 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** [X]

 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** [X]

 Create in: demo.local/Users

---

When you click Finish, the following object will be created:

Full name: employee

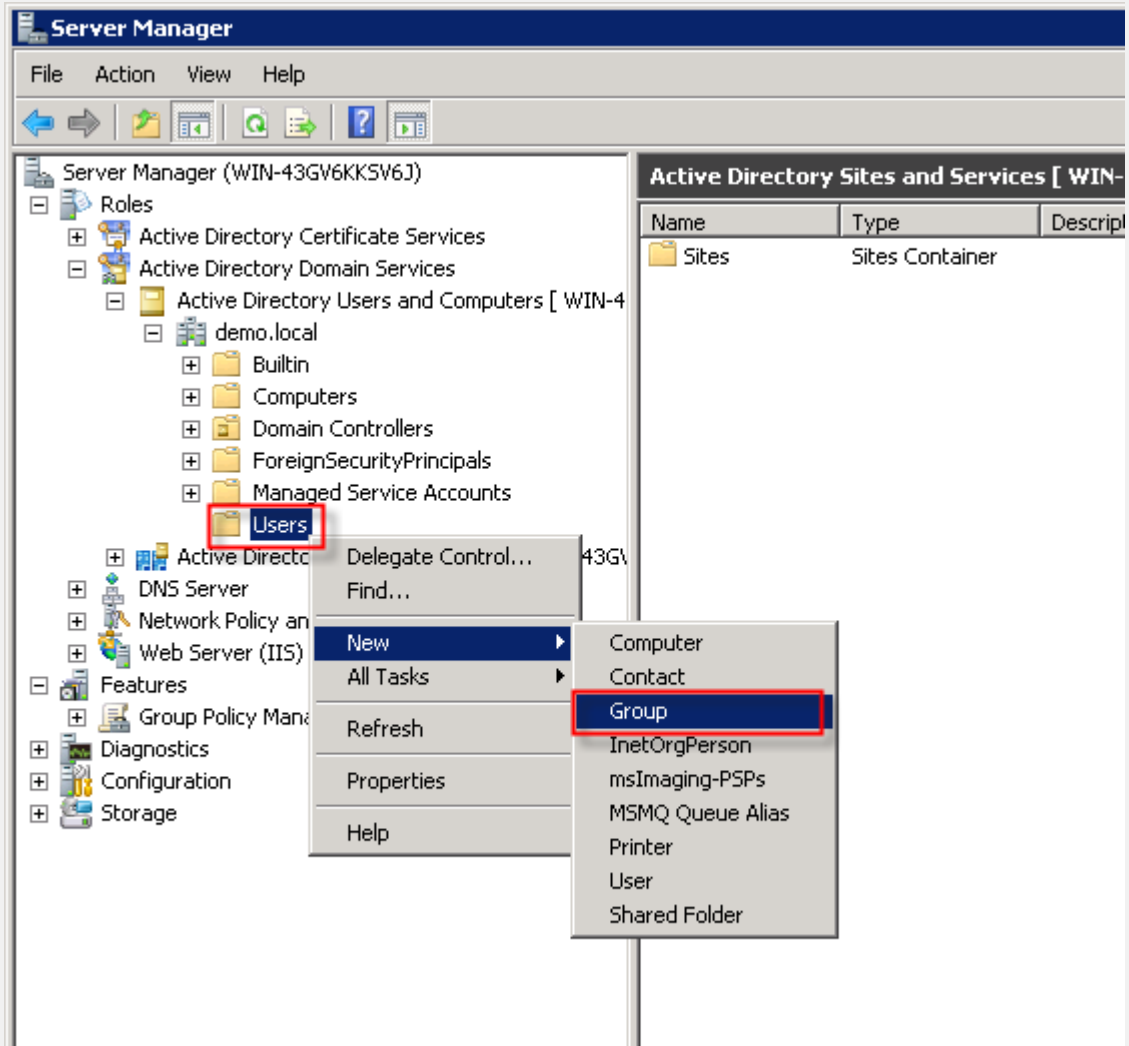
User logon name: employee@demo.local

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.

**New Object - Group**

Create in: demo.local/Users

Group name:  
**BYOD APPROVED**

Group name (pre-Windows 2000):  
BYOD APPROVED

Group scope:

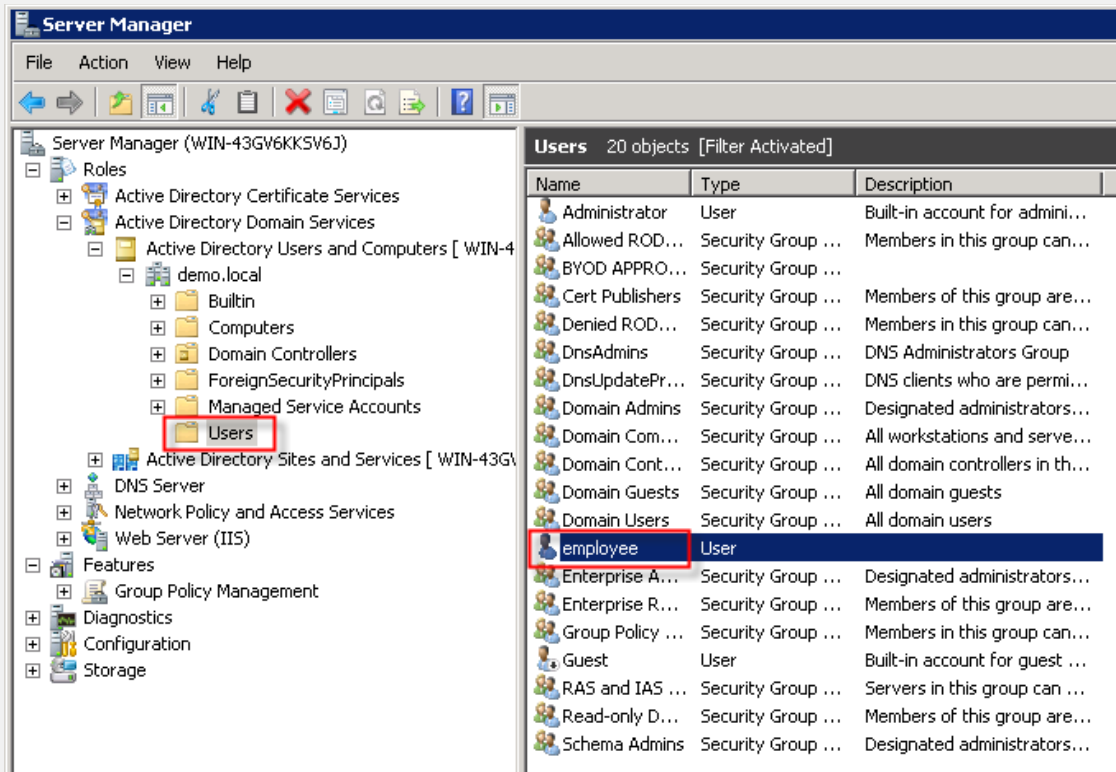
- ☐ Domain local
- ☒ Global
- ☐ Universal

Group type:

- ☒ Security
- ☐ Distribution

**OK** Cancel

- 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** [?] [X]

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	
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

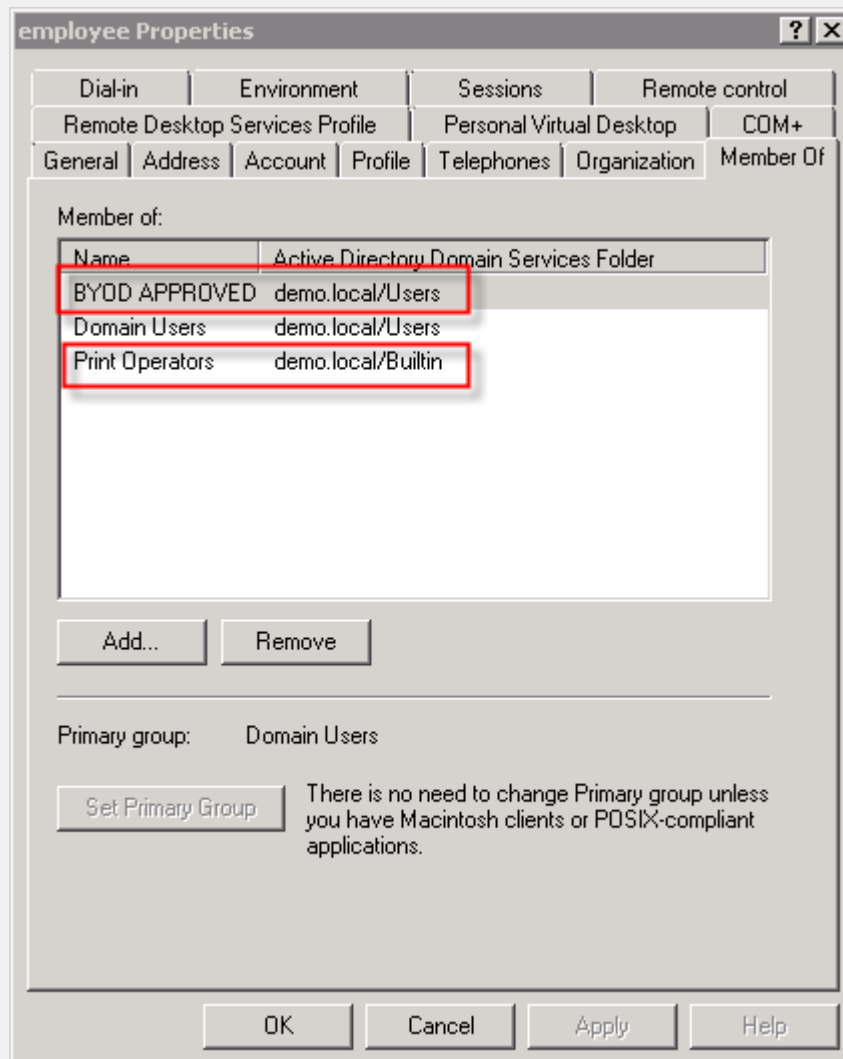
**Select Groups** [?] [X]

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

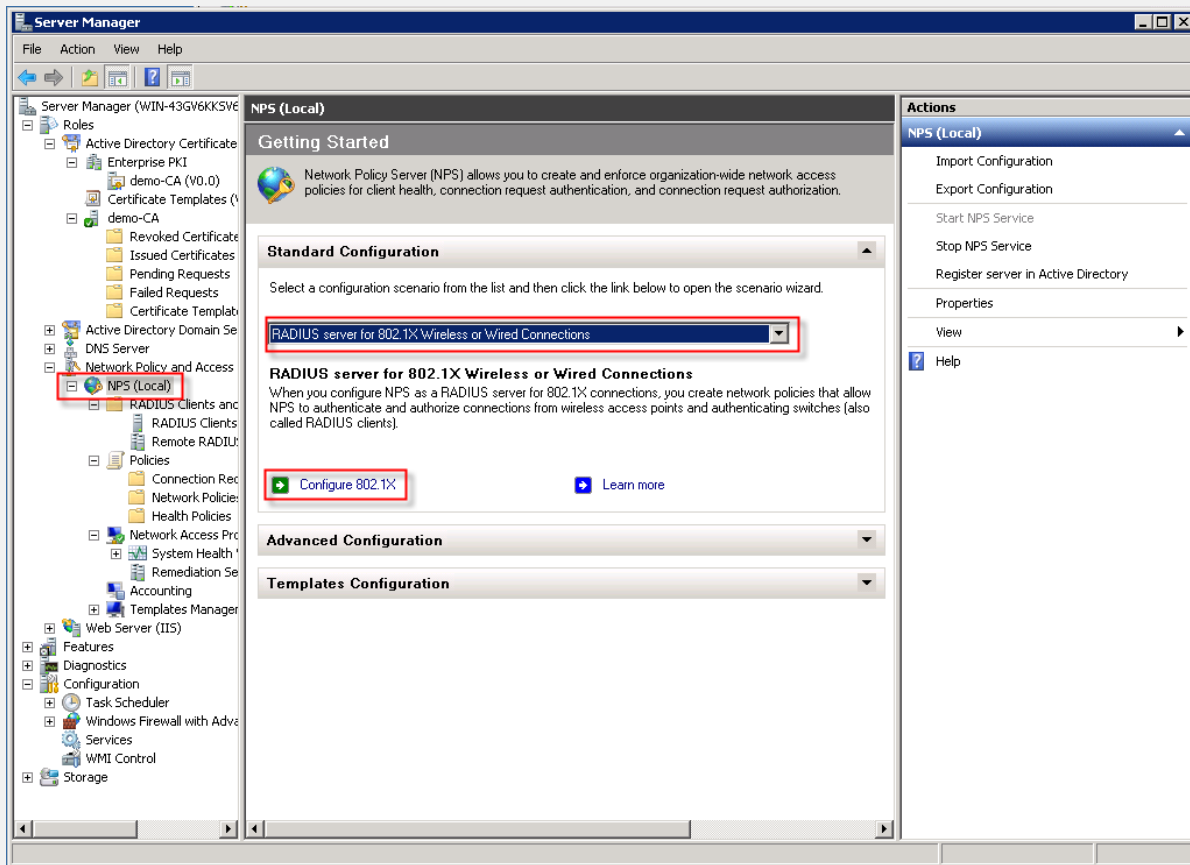
Advanced... **OK** Cancel



- 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.



**Configure 802.1X**

## Select 802.1X Connections Type

**Type of 802.1X connections:**

☒ Secure Wireless Connections  
When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points.

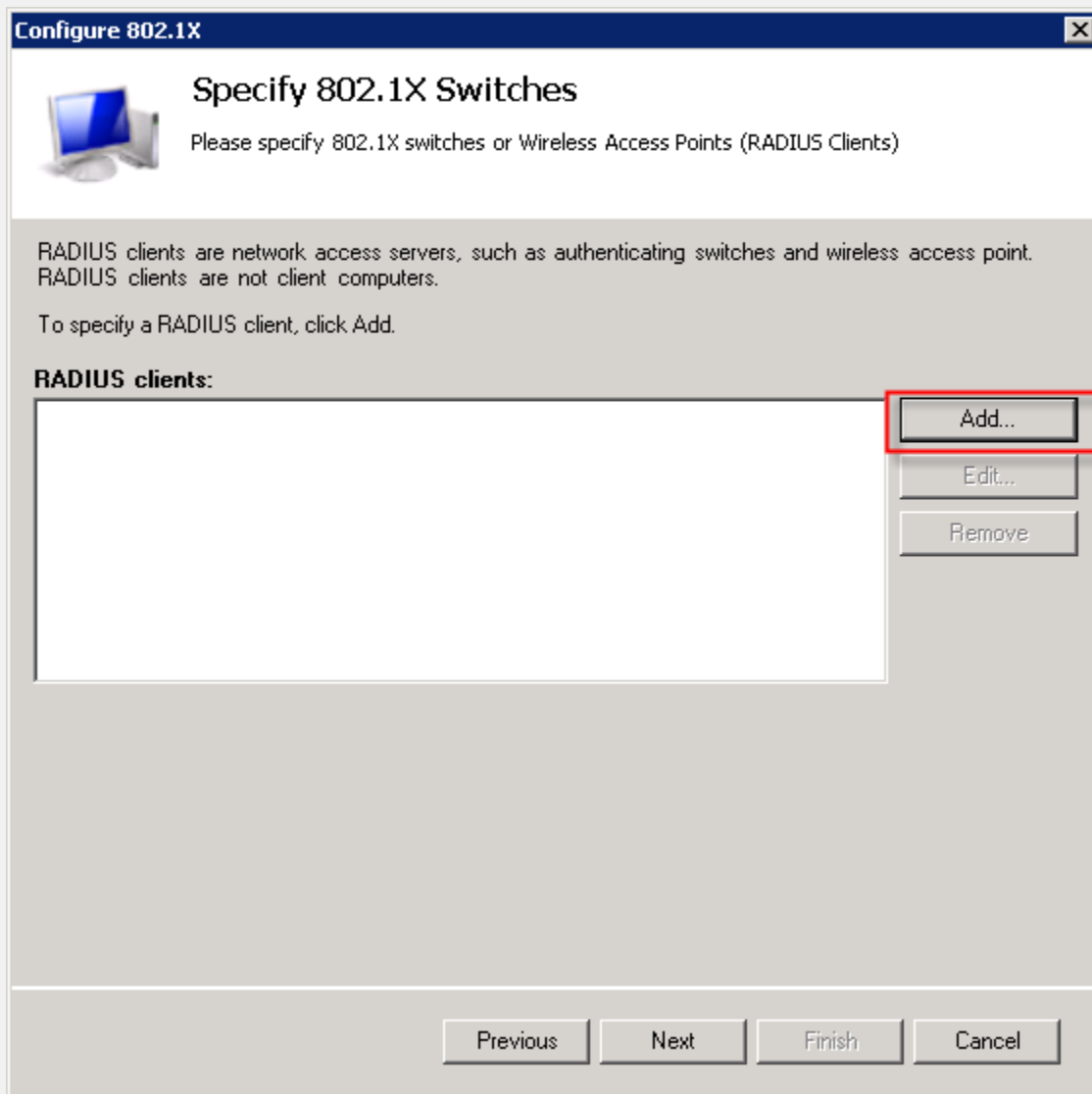
☐ Secure Wired (Ethernet) Connections  
When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethernet clients connecting through the switches.

**Name:**  
This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it .

Secure Wireless Connections

Previous **Next** Finish Cancel

**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.

**New RADIUS Client**

Settings

☐ Select an existing template:

Name and Address

Friendly name:  
RFS4000

Address (IP or DNS):  
192.168.0.105 Verify...

Shared Secret

Select an existing Shared Secrets template:  
None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

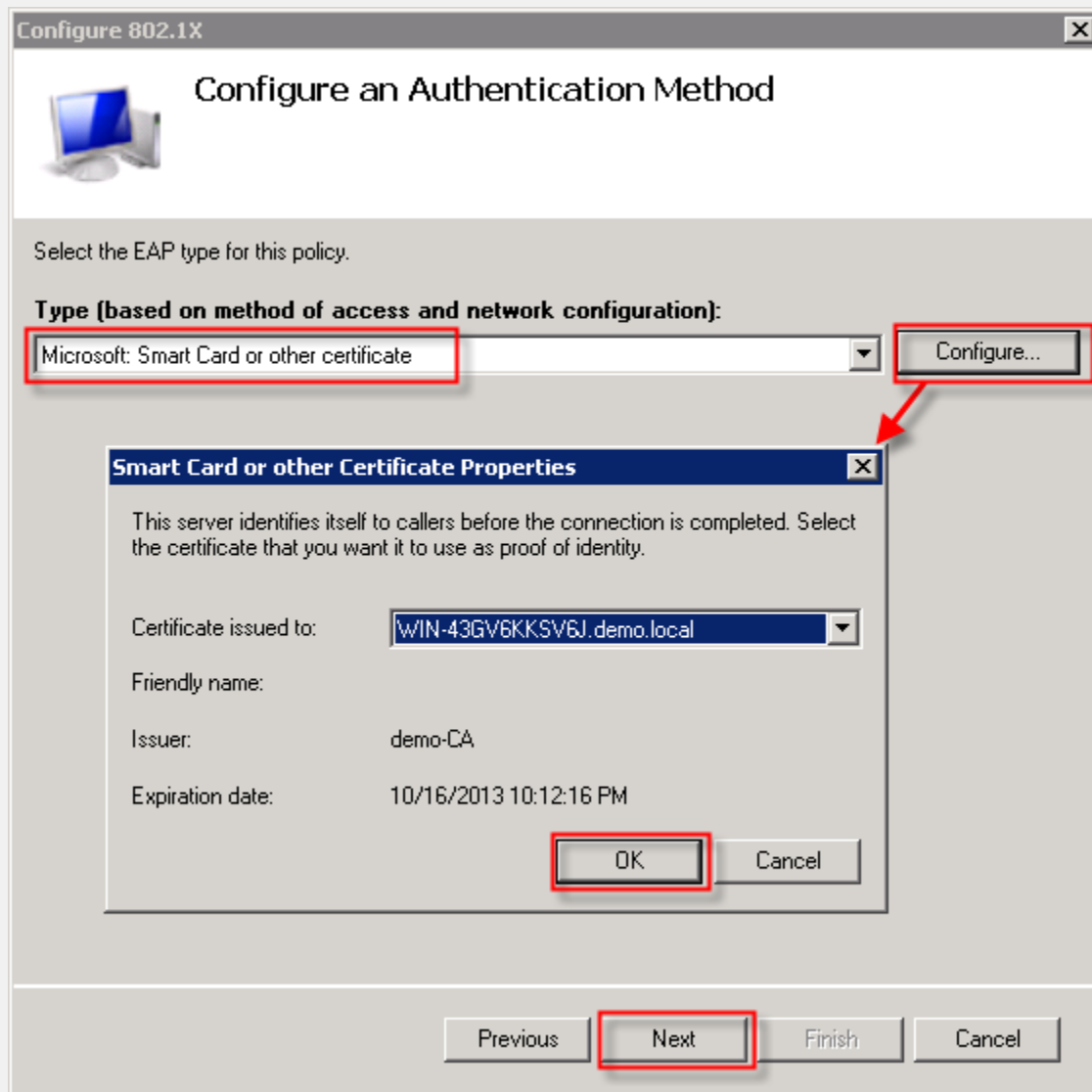
☒ Manual ☐ Generate

Shared secret:  
.....

Confirm shared secret:  
.....

OK Cancel

- 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.



## 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 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.

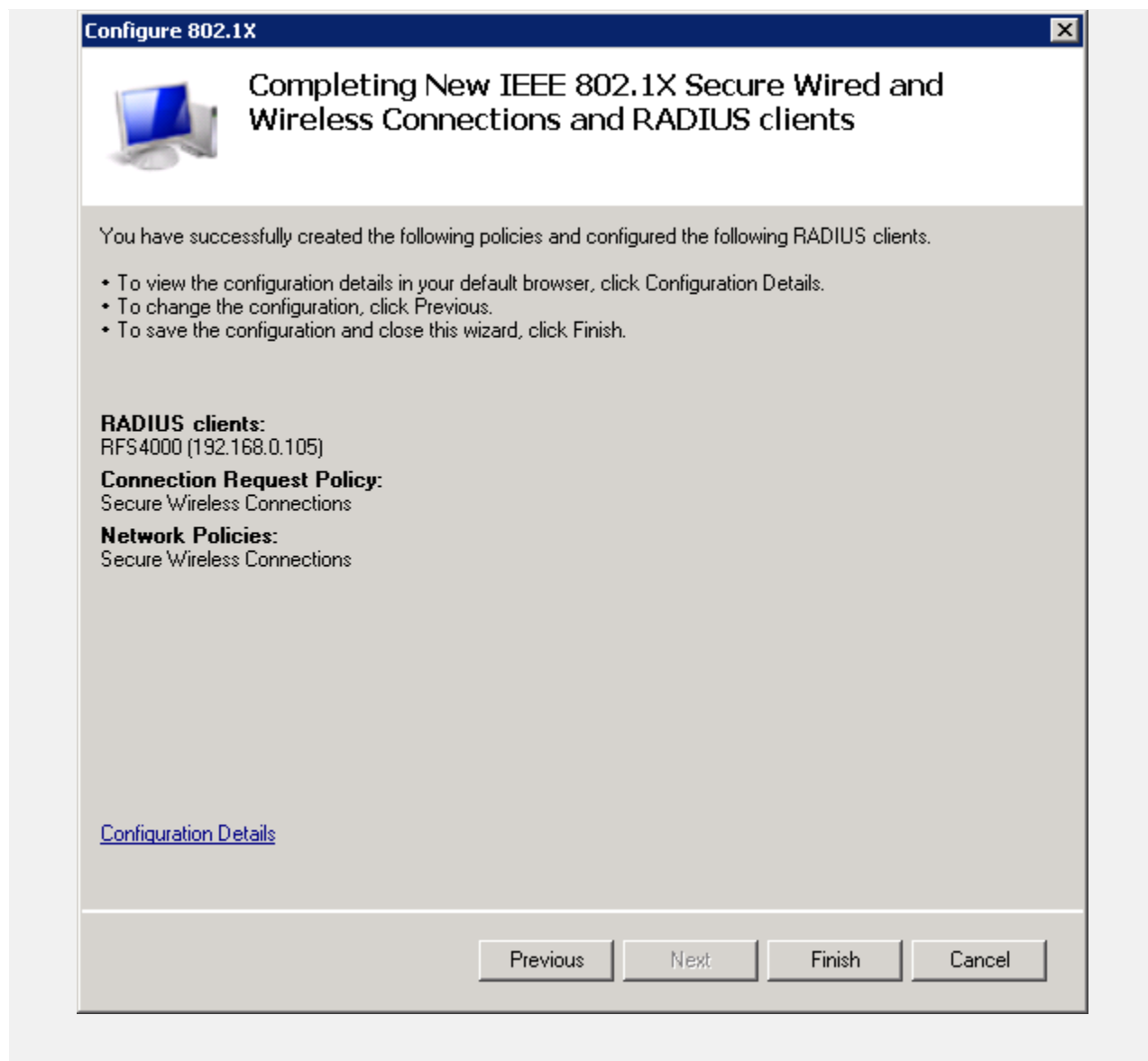
Configure...

Previous

Next

Finish

Cancel



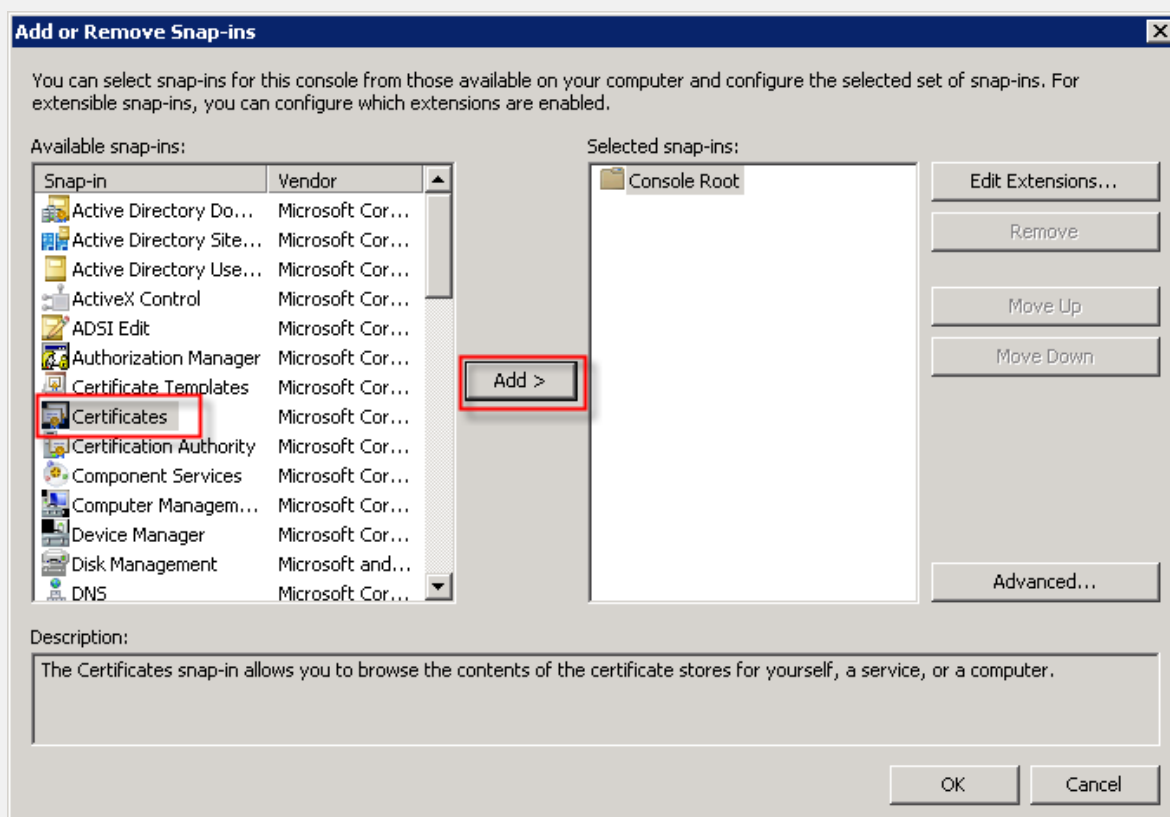
## 2.2.10 Export Root CA Certificates

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.

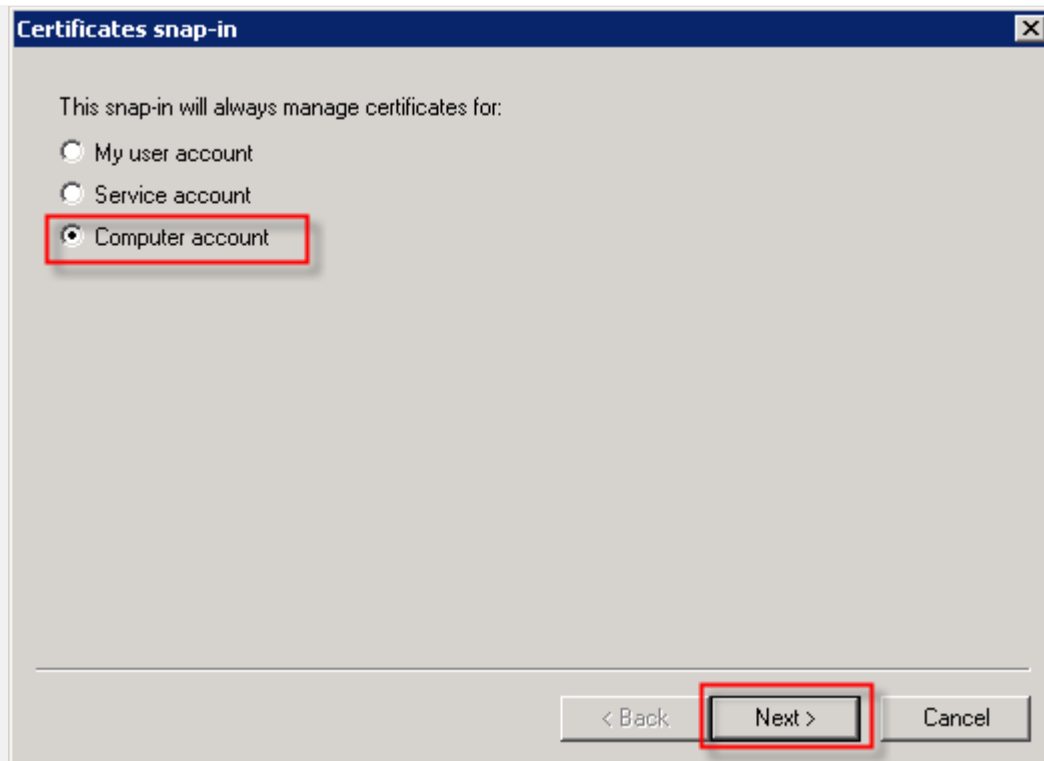


*Note: The root CA certificate will be installed on clients as a trusted root certificate so that they don't generate security warnings about untrusted servers. The NPS (RADIUS) certificate will be installed on clients and selected as the expected RADIUS server certificate, which allows clients to authenticate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

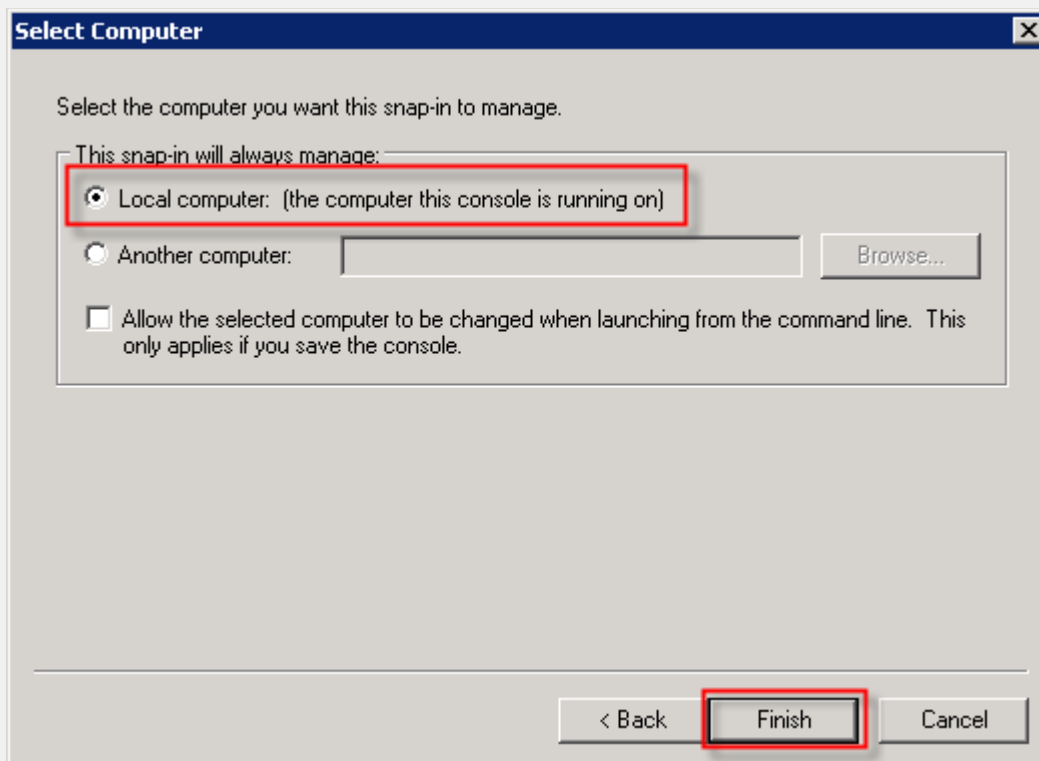
- 1 Click Start, type mmc and press Enter to launch the Microsoft Management Console. Click File → Add/Remove Snap-in. Choose Certificates. Click Add. Choose Computer account. Click Next.



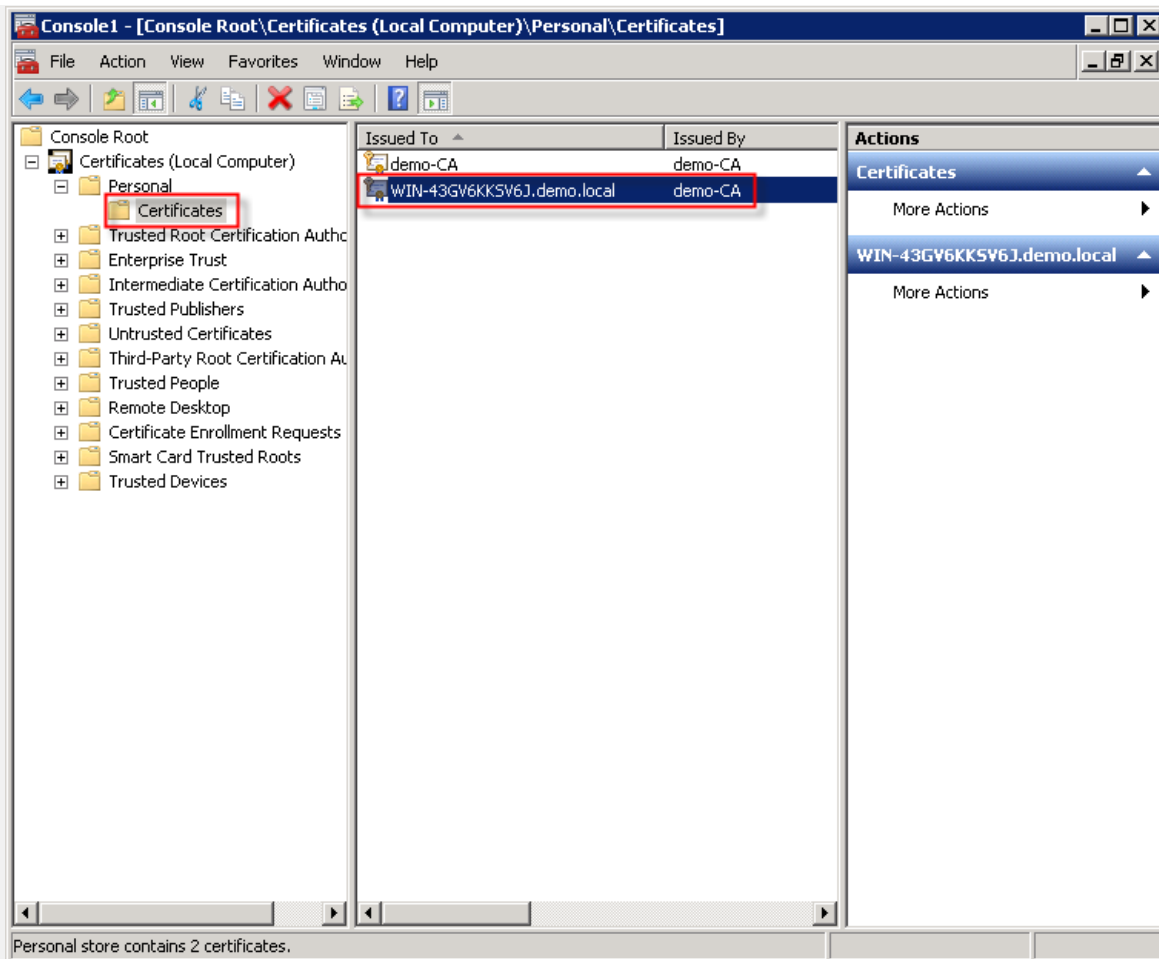




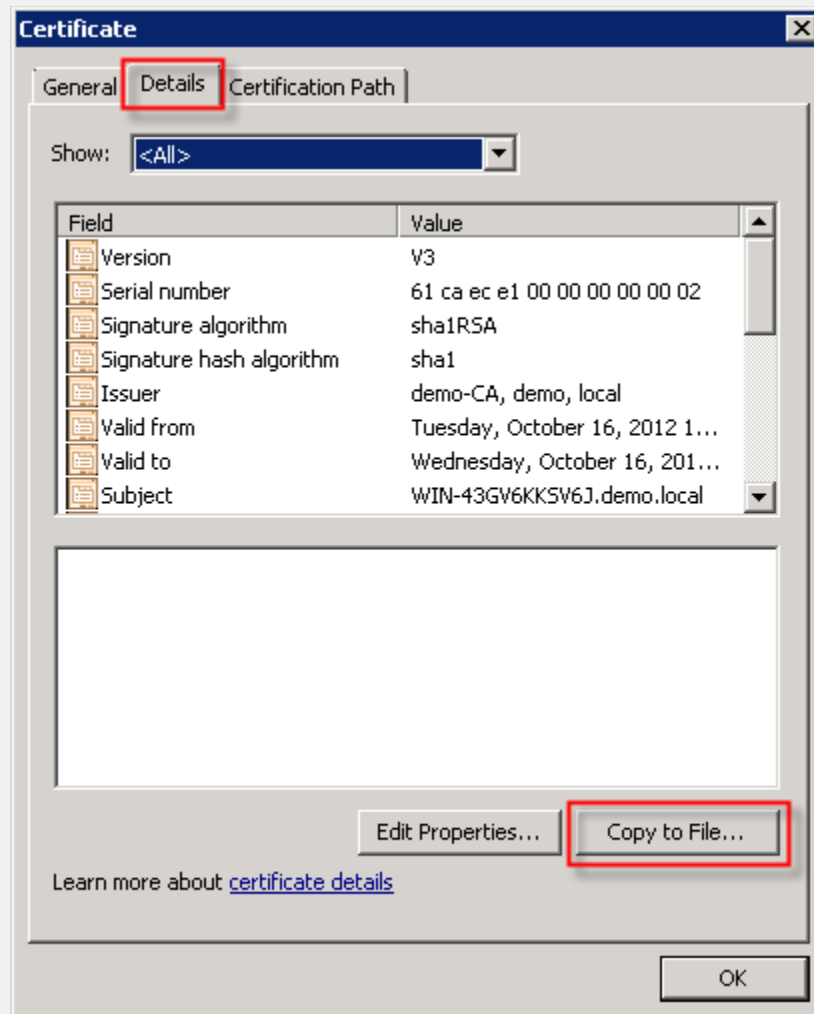
**2** Click Finish and then click OK.



- 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.**

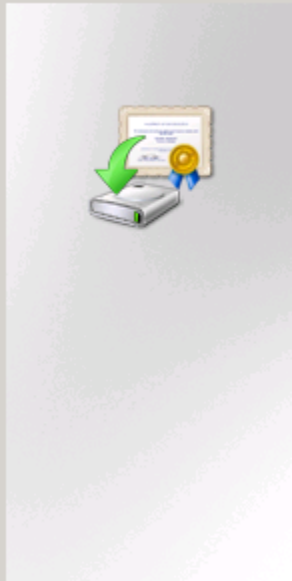


4 Click the Details tab and click Copy to File.



**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.

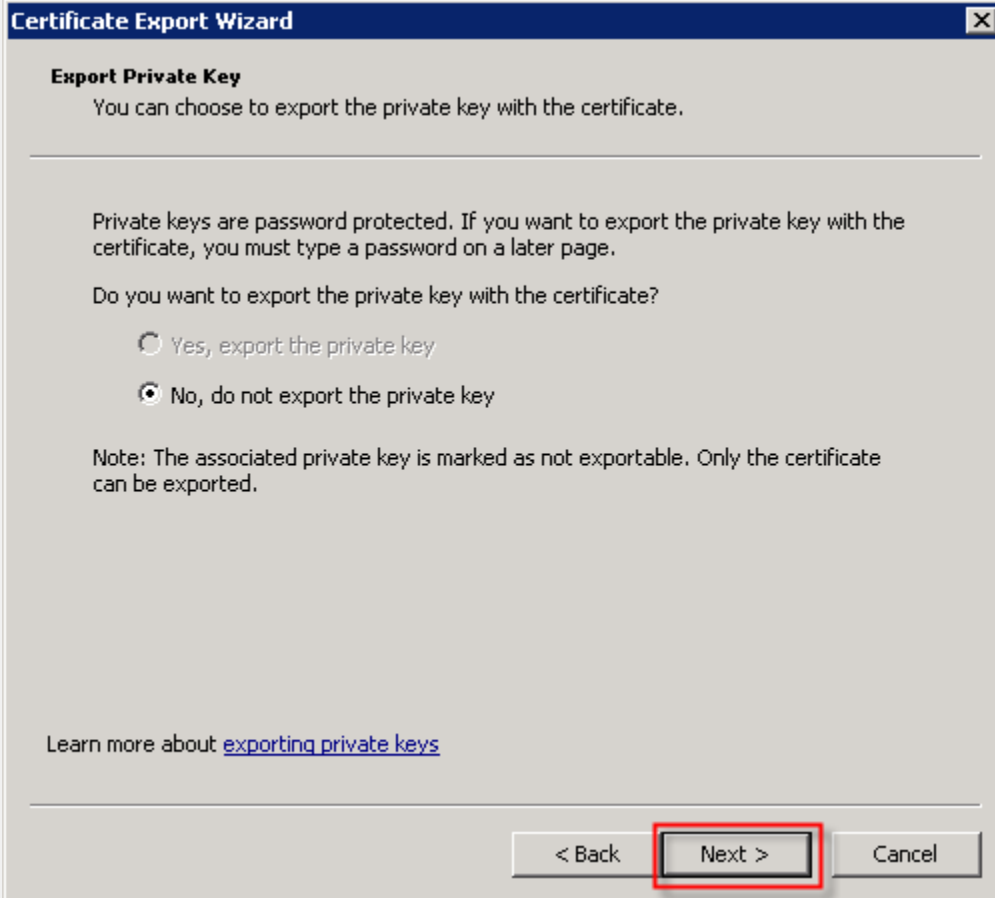
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

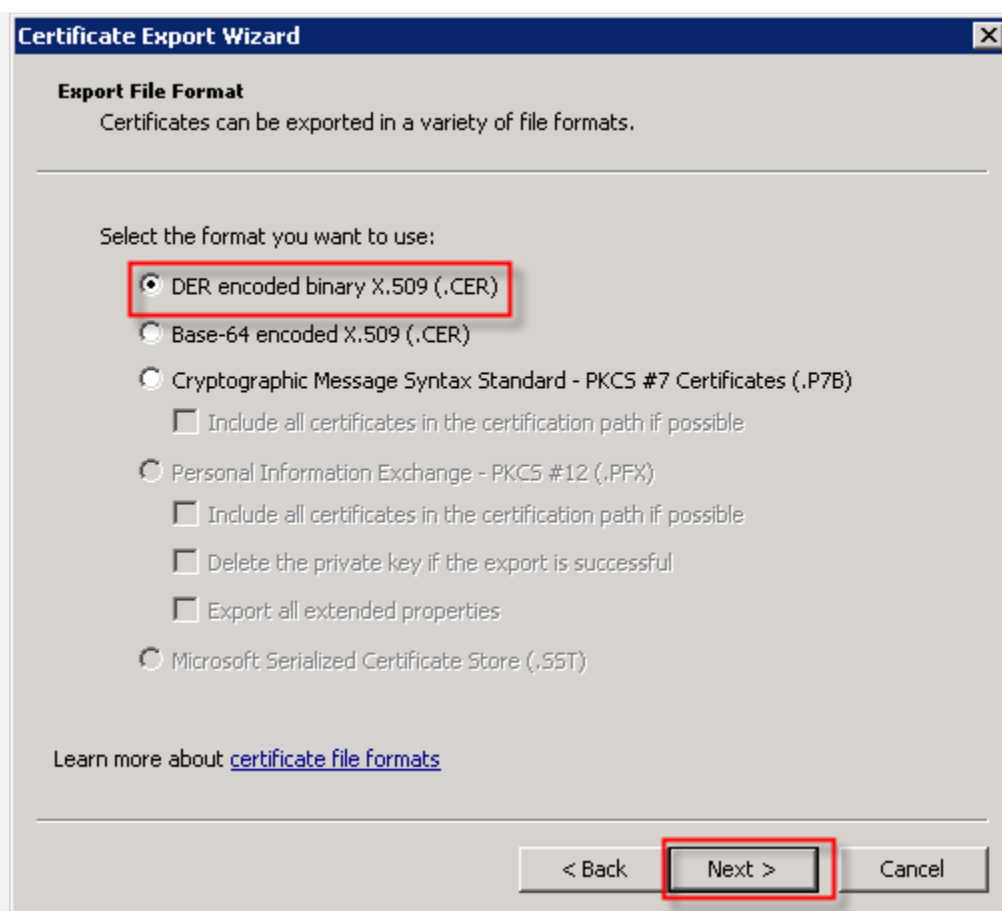
To continue, click Next.

< Back

Next >

Cancel





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

**Certificate Export Wizard** [X]

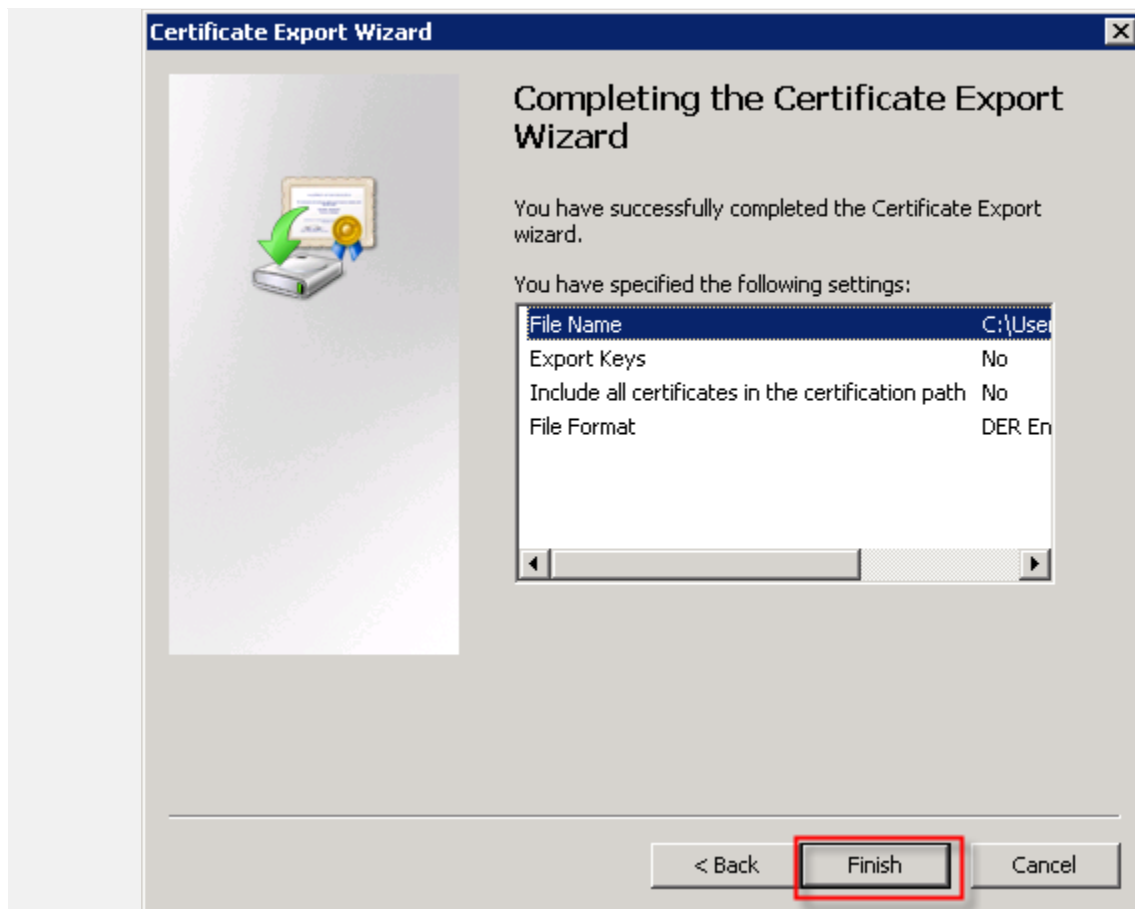
**File to Export**  
Specify the name of the file you want to export

---

File name:

---





- 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.

Introduction

Certificates

Define Networks

Deploy

Advanced

Manage Account

Support

This is a utility page for viewing the certificate chain associate with the RADIUS server certificate.

Certificates and CAs may be **uploaded** as individual files or as ZIP bundles. When using a public certificate authority, we recommend uploading the ZIP bundle received from the CA. When uploading individual files, we recommend beginning with the root CA and progressing toward the server certificate.

RADIUS Server Certificates

WIN-43GV6KKSJ6J.local

This is the server certificate.

Expires: 2013-10-17

Thumbprint: 27 5e 4f 25 5d 75 5d 75 5d 75 5d 75 5d 75 5d 75 5d 75 5d 75 5d 75

Issuer: testCA

testCA

This is a root CA.

Expires: 2017-10-17

Thumbprint: 4b 10 5e bc 3e 82 de de e2 95 4f 4b 57 b9 96 cb 21 d7 db 75

Issuer: testCA

Thumbprint: 4b 10 5e bc 3e 82 de de e2 95 4f 4b 57 b9 96 cb 21 d7 db 75

Upload Certificate

Certificate & CA Upload

Certificates may be uploaded as individual certificate files or as a ZIP bundle. Select the file to be uploaded and click 'Upload'.

File To Upload:

## 2 Repeat for the server certificate.

RADIUS Server Certificates

WIN-43GV6KKSJ6J.local

This is the server certificate.

Expires: 2013-10-17

Thumbprint: 27 5e 4f 25 5d 75 5d 75 5d 75 5d 75 5d 75 5d 75 5d 75 5d 75 5d 75

Issuer: testCA

testCA

This is a root CA.

Expires: 2017-10-17

Thumbprint: 4b 10 5e bc 3e 82 de de e2 95 4f 4b 57 b9 96 cb 21 d7 db 75

Issuer: testCA

Thumbprint: 4b 10 5e bc 3e 82 de de e2 95 4f 4b 57 b9 96 cb 21 d7 db 75

WIN-43GV6KKSJ6J.local

This is the server certificate.

Expires: 2013-10-17

Thumbprint: b7 19 41 83 7e 0f 3d 86 bc 3b 00 c7 90 8f 53 3d 4d 8c ab 4d

Issuer: demo-CA

demo-CA

This is a root CA.

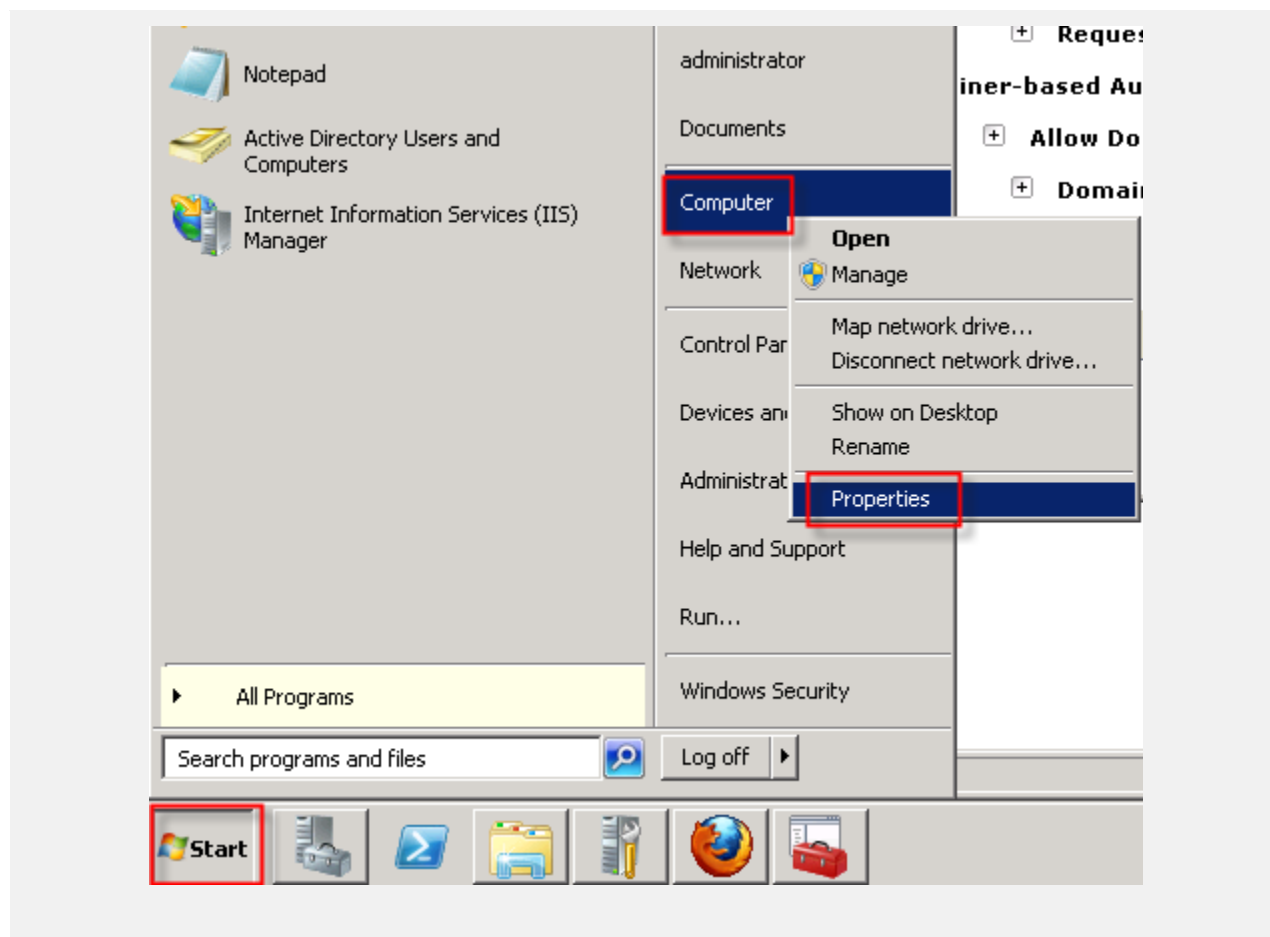
Expires: 2017-10-17

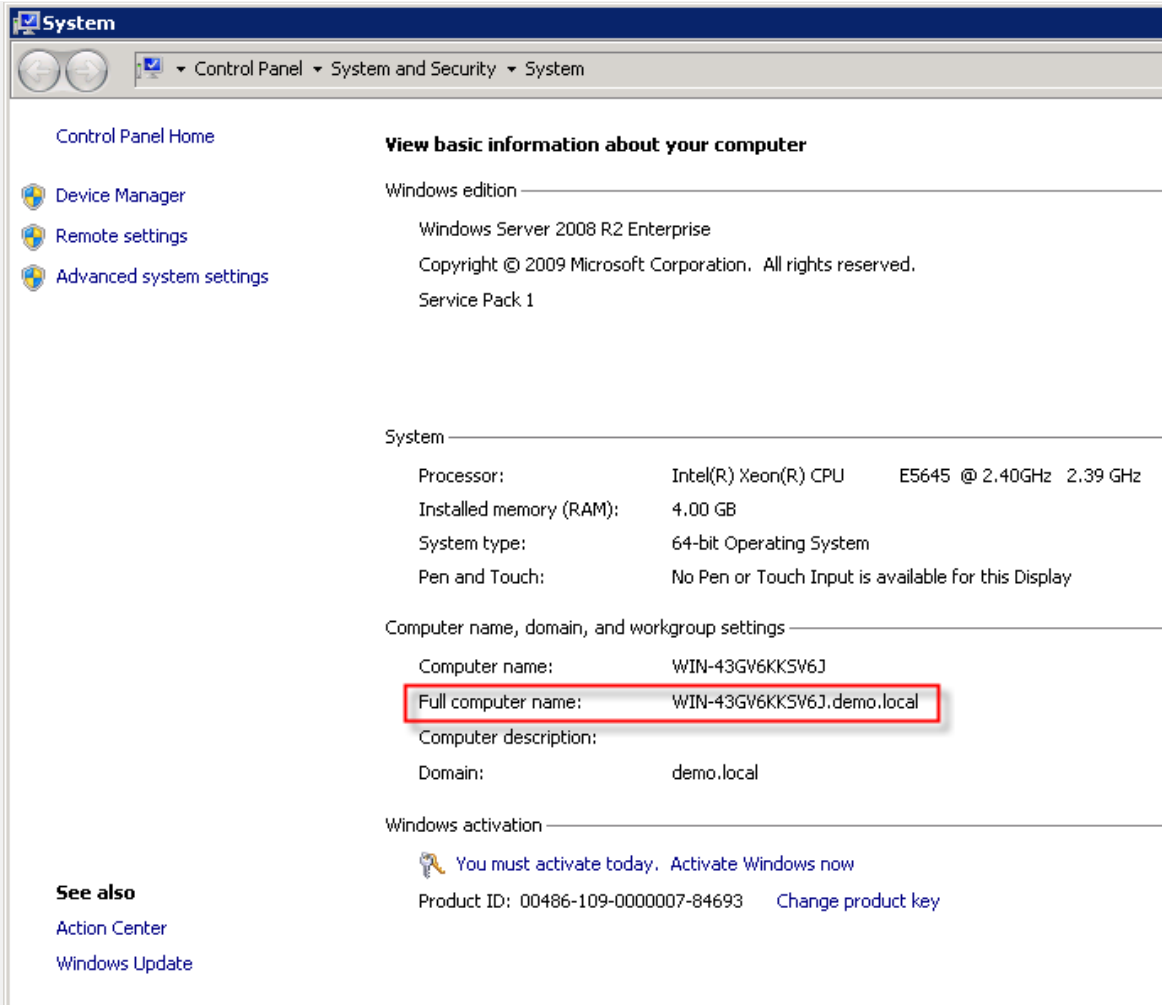
Thumbprint: a6 10 5e bc 3e 82 de de e2 95 4f 4b 57 b9 96 cb 21 d7 db 75

Issuer: demo-CA

Upload 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.





- 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.

Introduction

Certificates

Define Networks

Deploy

Advanced

Manage Account

Support

The Advanced tab allows some of the advanced configuration options of XpressConnect to be specified. These settings are mostly related to user prompts.

Values displayed in light grey are the default values. To reset a value to its default value, simply save it as blank. These settings apply to all servers.

View:

Application Labels

Web Labels

Behavior

Application Look & Feel

Msft CA

Microsoft CA Integration

The following settings affect the XpressConnect Integration Module for Microsoft Certificate Services.

CA Host Name:

Cloudpath.motodcloudpath.com

CA Name:

motodcloudpath-CloudPath-CA

Request Attributes:

CertificateTemplate:User

Use Container-based Authentication:

1

Allow Domain Lookup

1

Domains To Search

motodcloudpath.com

Suppress Password Prompt

1

Edit

Edit: Msft CA

Microsoft CA Integration

The following settings affect the XpressConnect Integration Module for Microsoft Certificate Services.

CA Host Name:

WIN-43GV6KKSJ6J.demo.local

CA Name:

demo-CA

Request Attributes:

CertificateTemplate:User

Use Container-based Authentication:

1

Allow Domain Lookup

1

Domains To Search

demo.local

Suppress Password Prompt

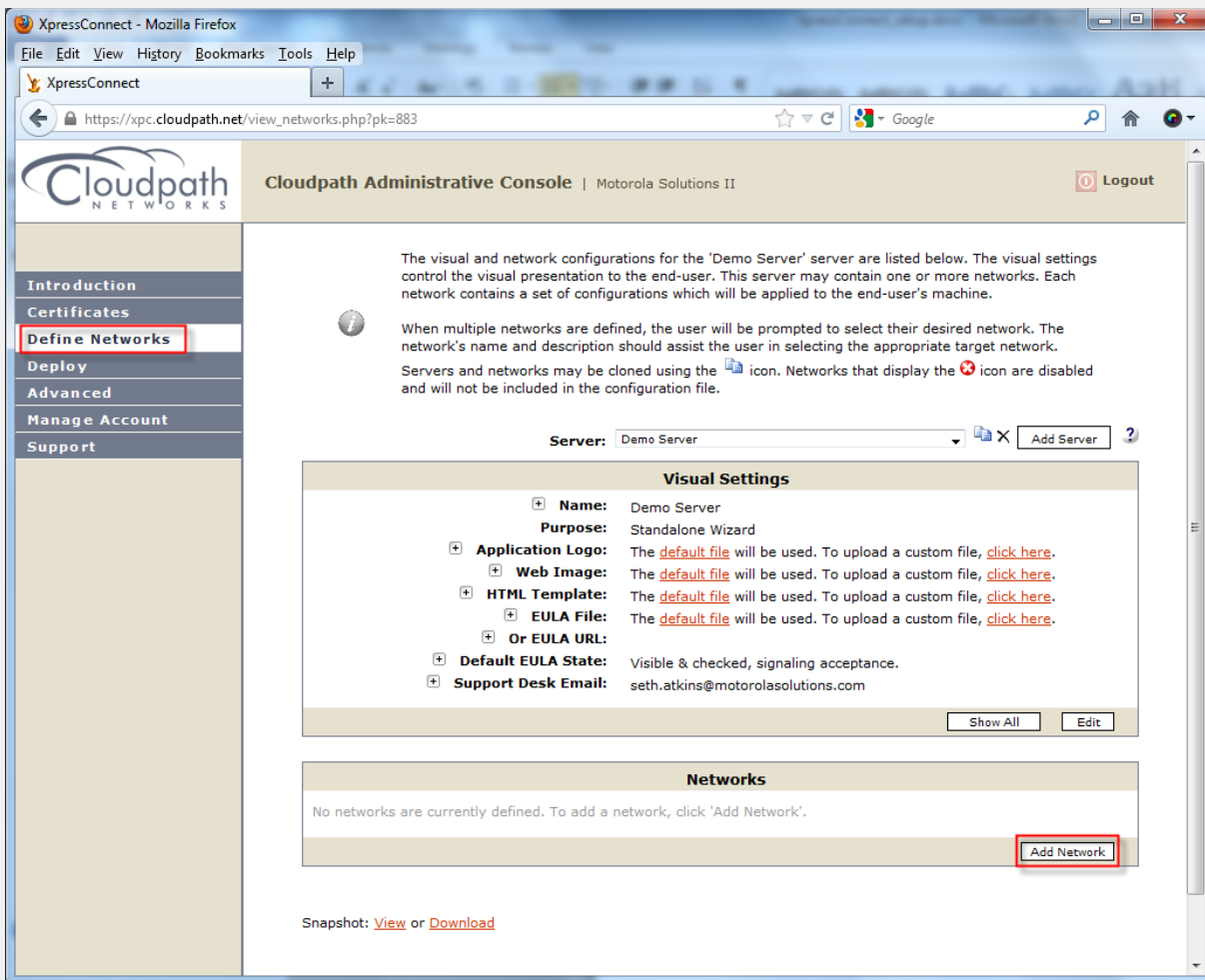
0

Cancel

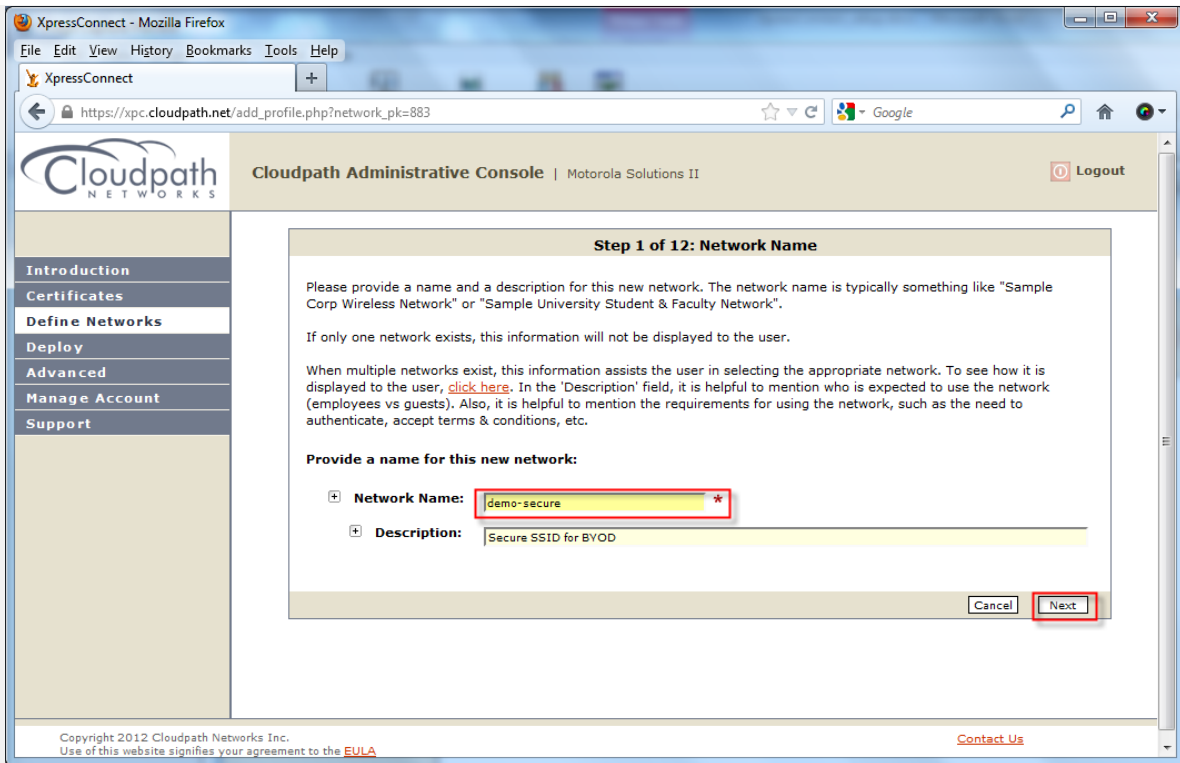
Save

## 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.

XpressConnect - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://xpc.cloudpath.net/add\_profile.php?step=2&display=1

Cloudpath Administrative Console | Motorola Solutions II Logout

**Step 2 of 12: Connection Method**

A single network may support wired and/or wireless network connections. If the network is configured to support both, XpressConnect will configure the machine based on the active network connection.

Select the connection method(s) this network supports:

☐ **Wired Connections**  
If selected, XpressConnect will configure wired connections.

☒ **Wireless Connections**  
If selected, XpressConnect will configure wireless connections.

The following fields are necessary for wireless connections:

**SSID:** demo-secure \*

**Authentication:** WPA2

**Encryption:** AES

**Protocol Preference:** Any (Default) \* Applies to Windows Vista and greater

**Is the SSID broadcast?** Yes, the SSID is broadcast. \* Mac OS X frequently experiences issues with hidden SSIDs.

Back Next

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

**Step 4 of 12: Authentication Method**

Select the type of authentication used on this network:

☒ **This network uses 802.1X.**  
If selected, XpressConnect will configure the user for access based on 802.1X.  
The selection of an EAP type is necessary for 802.1X:

**Supplicant Preference:** Native \*\* Native includes SecureW2.

**EAP Type:** TLS with Enrollment System

☐ **This network uses a web-based login.**  
If selected, XpressConnect will assume that a web-based login mechanism is in place. By specifying the URL of the login page below, XpressConnect will automatically open the browser to the login page once they are migrated to the new network.

**Login URL:** http://

☐ **This network does not use authentication.**

Back Next



### Step 5 of 8: Operating Systems

A network may support one or more operating systems. After the wizard is completed, a profile will be created for each operating system selected below. If an operating system is excluded, support for it may be added later.

Select the operating systems that will be supported:

Wireless	Operating System
<input checked="" type="checkbox"/>	Windows XP
<input checked="" type="checkbox"/>	Windows Vista, 7, & 8
<input checked="" type="checkbox"/>	Mac Tiger
<input checked="" type="checkbox"/>	Mac Leopard, Snow Leopard, Lion, Mountain Lion & iOS
<input checked="" type="checkbox"/>	Ubuntu
<input checked="" type="checkbox"/>	Android

Back

Next

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

### Step 6 of 8: Server Certificate Validation

Within 802.1X, server certificate validation is an important security feature. When enabled, the client will only authenticate to a server that provides a certificate signed by the selected trusted certificate authority. If server certificate validation is disabled, the client will authenticate to any server. Enabling server certificate validation is a security best practice.

Server certificate validation may be changed later using the "Define Networks" tab. If you need to upload multiple CA certificates, upload one here, and upload the additional certificates on the "Define Networks" tab. If you are uncertain about the certificate configuration, contact support@cloudpath.net and we can assist you.

If you choose not to enforce server certificate validation, we recommend adding the server CA certificate to the Mac Leopard & Snow Leopard profile so that XpressConnect can mark the certificate trusted and avoid the user prompt to accept the certificate. This may be done on the Mac Leopard & Snow Leopard tab by clicking *Add Additional Application Settings*.

Select the appropriate setting for server certificate validation:

☐ Disable server certificate validation.

If selected, the user will not validate the certificate provided by the authentication server.

☒ Enable server certificate validation.

If selected, the user will validate the certificate provided by the authentication server. If you have a custom Root CA certificate, you may upload it, and it will be installed for the user. If you use a public Root CA certificate, select it from the list of CAs.

My own CA certificate file:  Browse...

☐ Uploaded Certificate Authorities:

- ☒ demo-CA (a6 10 5e bc 3e 82 de e2 95 4f 4b 57 b9 96 cb 21 d7 db 75)
- ☐ motocloudpath-CLOUDPATH-CA (3c 82 0a e9 3f ee a9 84 b1 11 8c a1 ef 30 62 c8 80 c6 a3 fb)
- ☐ SethLab (84 2f 71 1e 45 8a b1 8d 6c f6 03 7a 38 1d 18 7b 42 47 52 97)
- ☐ lab-LAB-DC-CA (91 06 9c 6d 1c 74 91 eb e4 97 ab 0d fc 9c 21 cc 0c f6 42 1f)

☐ Standard Certificate Authorities:

In addition to verifying the CA, some operating systems can verify the name of the RADIUS server, which is stored in the server certificate. When using a public CA, verifying the server name is a good practice to ensure that computers only authenticate against your RADIUS server.

Step 7 of 8: Additional Options

Based on your answers so far, profiles will be created to handle the configurations you have specified. The options below are settings which are commonly used. You may add, delete, or modify these and other settings at any time on the "Define Networks" tab. If you would like to include any of these settings at this time, select them below.

Do you want to add any of the following settings to the new profiles?

Windows XP

☐ Enable Windows Auto Updates if not enabled.  
☐ Enable Windows Firewall if a firewall is not running.  
☐ Install Impulse SafeConnect NAC Agent ▼.  
☐ Enable Microsoft Network Access Protection (NAP) (XP SP3 Only)  
☐ Install WPA2 Hotfix If Necessary  
☐ Enable 'Automatically Detect' in IE LAN Settings

Windows Vista, 7, & 8

☐ Enable Windows Auto Updates if not enabled.  
☐ Enable Windows Firewall if a firewall is not running.  
☐ Install Impulse SafeConnect NAC Agent ▼.  
☐ Enable Microsoft Network Access Protection (NAP)  
☐ Enable 802.1X Single Sign-on  
☐ Disable Wireless Hosted Network (Win7 Only)  
☐ Enable 'Automatically Detect' in IE LAN Settings

Mac Leopard, Snow Leopard, Lion, Mountain Lion & iOS

☐ Install Impulse SafeConnect NAC Agent ▼.  
☐ Enable Mac OS X Firewall if not running.

Ubuntu

No additional options available.

Android

No additional options available.

Back

Next

6

Click Done.

Step 8 of 8: Summary

XpressConnect will now generate the network based on the information provided. Once generated, you may fine-tune the settings within the network.

Profiles will be created based on the information below:

<b>Operating Systems:</b>	Windows XP, Windows Vista, 7, & 8, Mac Leopard, Snow Leopard, Lion, Mountain Lion & iOS, Ubuntu, Android
<b>Connection Methods:</b>	Only wireless. Wireless uses 'WPA2' using AES and SSID 'demo-secure'.
<b>Authentication Methods:</b>	802.1X using TLS via Enrollment System
<b>Server Cert Validation:</b>	Enabled with 1 predefined CA(s).
<b>Additional Options:</b>	No additional options were selected.

If this information is correct, click 'Done'.

Back

Done

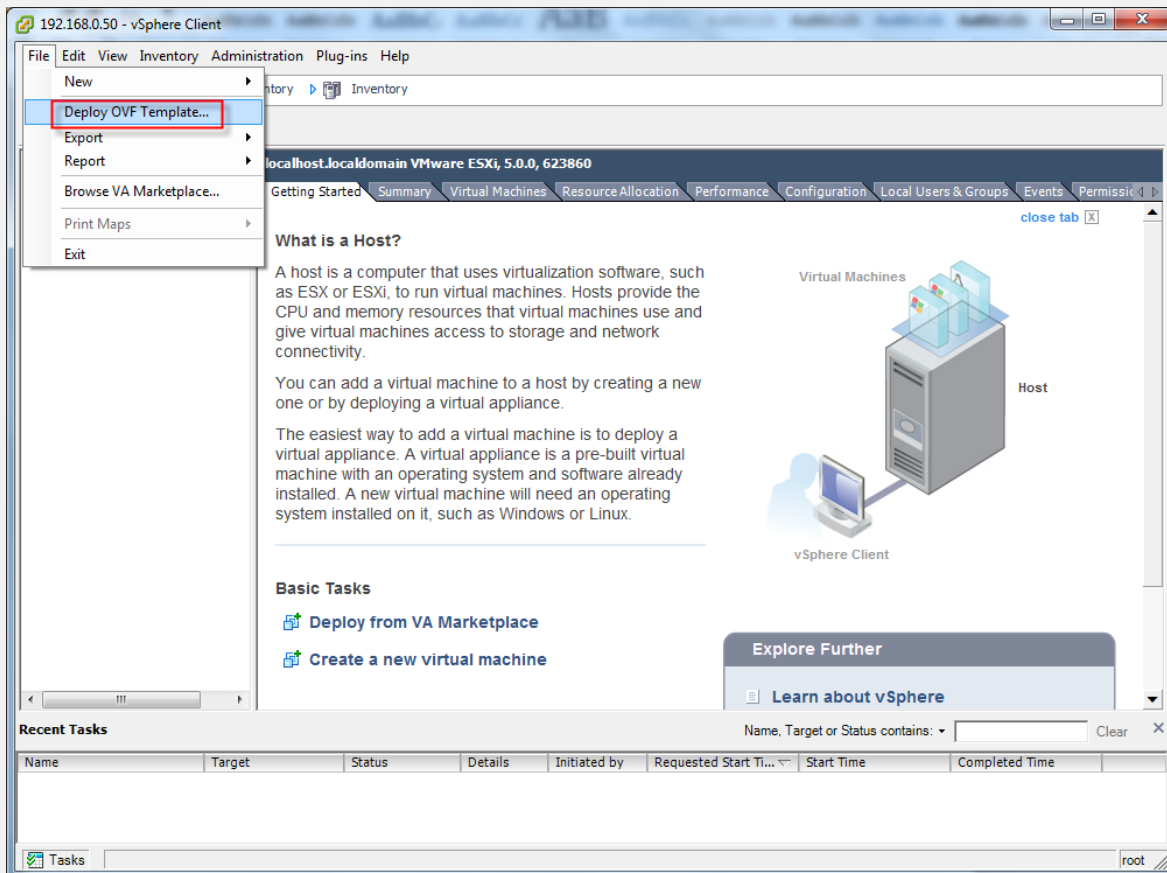
## 2.4 Configure the Enrollment Server Virtual Machine

ZEBRA CONFIDENTIAL: INTERNAL USE ONLY

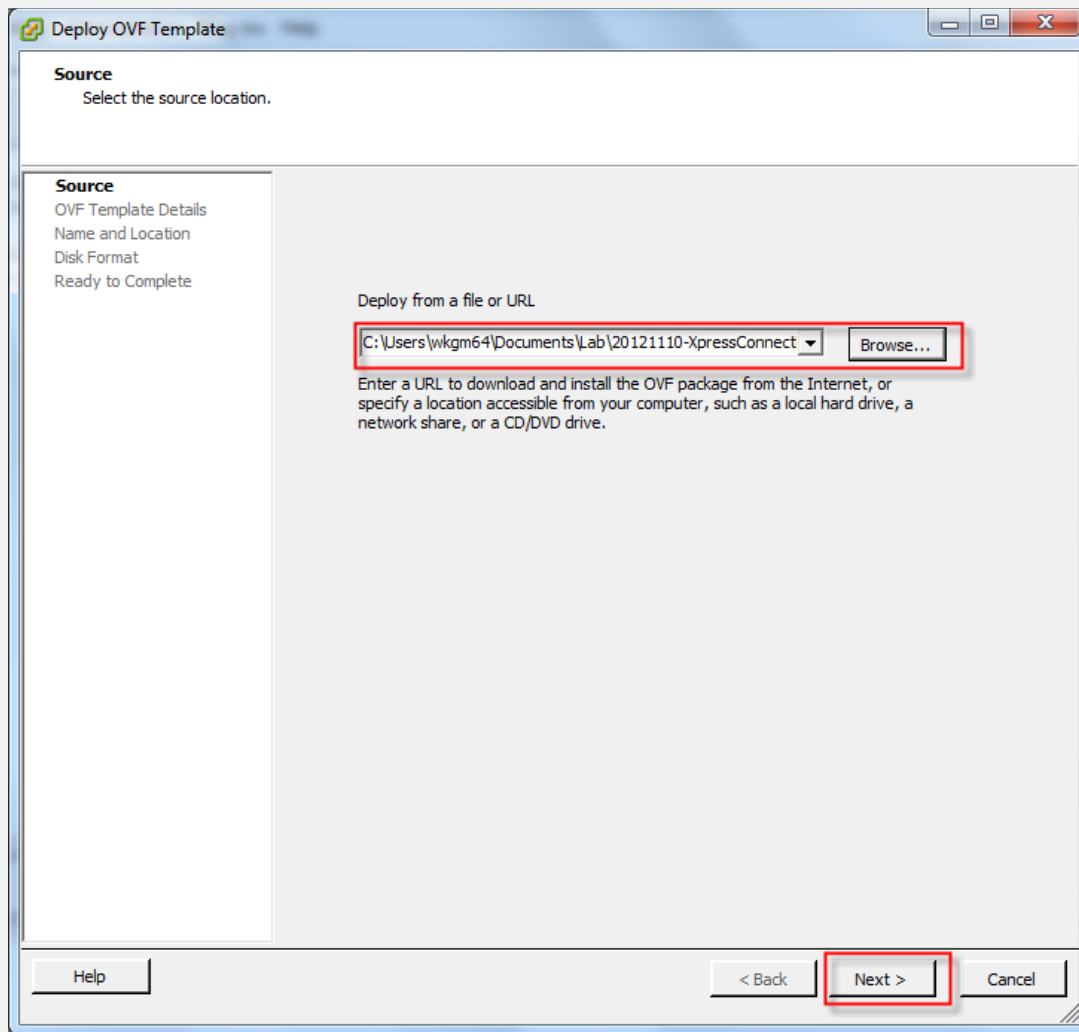
ZEBRA TECHNOLOGIES

98

## 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.

The screenshot shows a Windows-style dialog box titled "Deploy OVF Template". The main heading is "Name and Location" with the instruction "Specify a name and location for the deployed template". On the left, a vertical pane contains links: "Source", "OVF Template Details", "Name and Location" (which is selected), "Disk Format", and "Ready to Complete". The main area has a "Name:" label above a text input field containing "Enrollment\_Server\_VM". A red rectangle highlights this text. Below the input field, a note states: "The name can contain up to 80 characters and it must be unique within the inventory folder." At the bottom, there are three buttons: "Help", "< Back", and "Next >" (highlighted with a red rectangle), and a "Cancel" button.

Deploy OVF Template

**Name and Location**  
Specify a name and location for the deployed template

Source  
OVF Template Details  
**Name and Location**  
Disk Format  
Ready to Complete

Name:  
Enrollment\_Server\_VM

The name can contain up to 80 characters and it must be unique within the inventory folder.

Help < Back Next > Cancel

4 Select Thin Provision, and click Next.

**Deploy OVF Template**

**Disk Format**  
In which format do you want to store the virtual disks?

[Source](#)  
[OVF Template Details](#)  
[Name and Location](#)  
**Disk Format**  
Ready to Complete

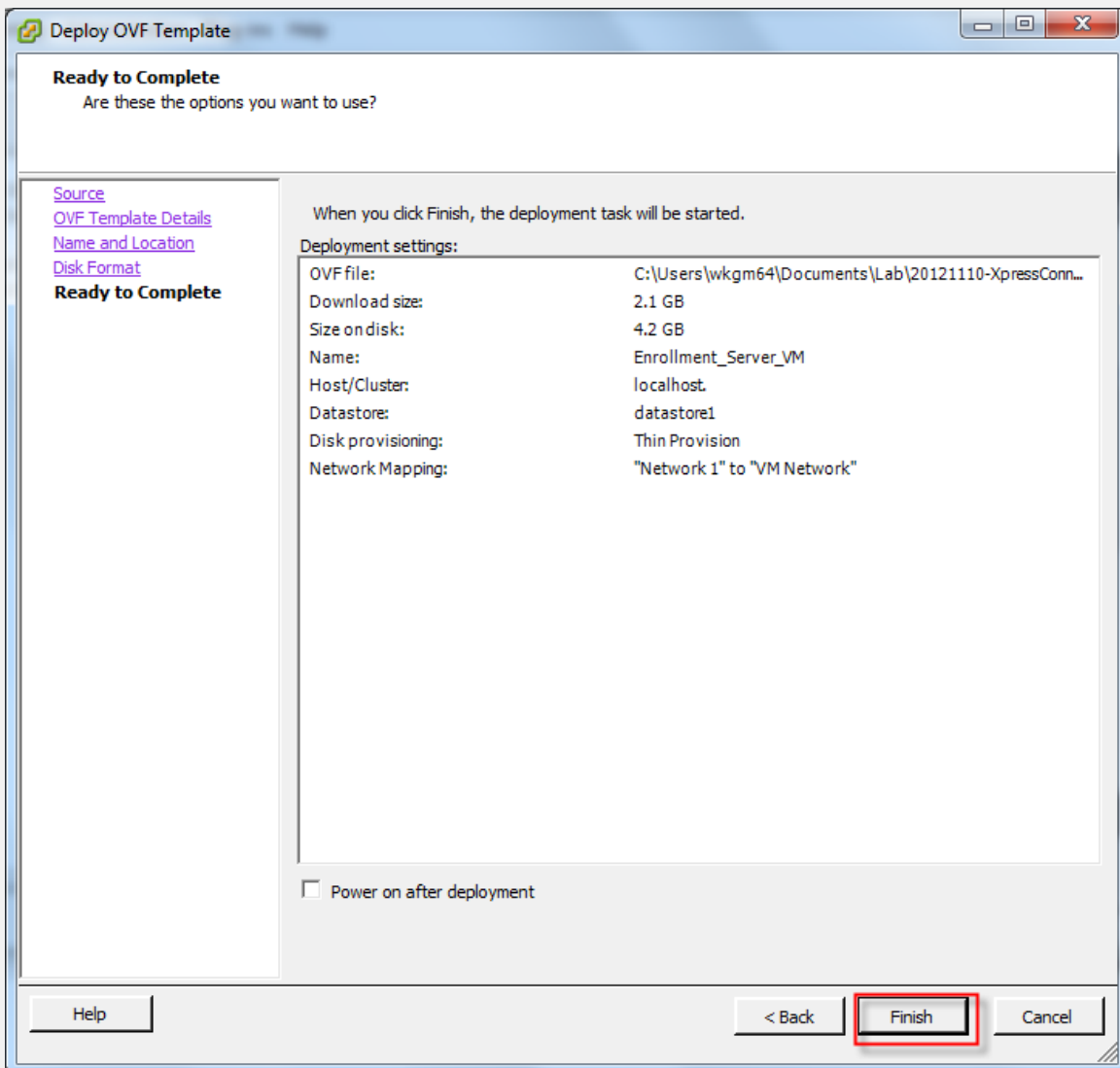
Datastore: datastore1

Available space (GB): 120.0

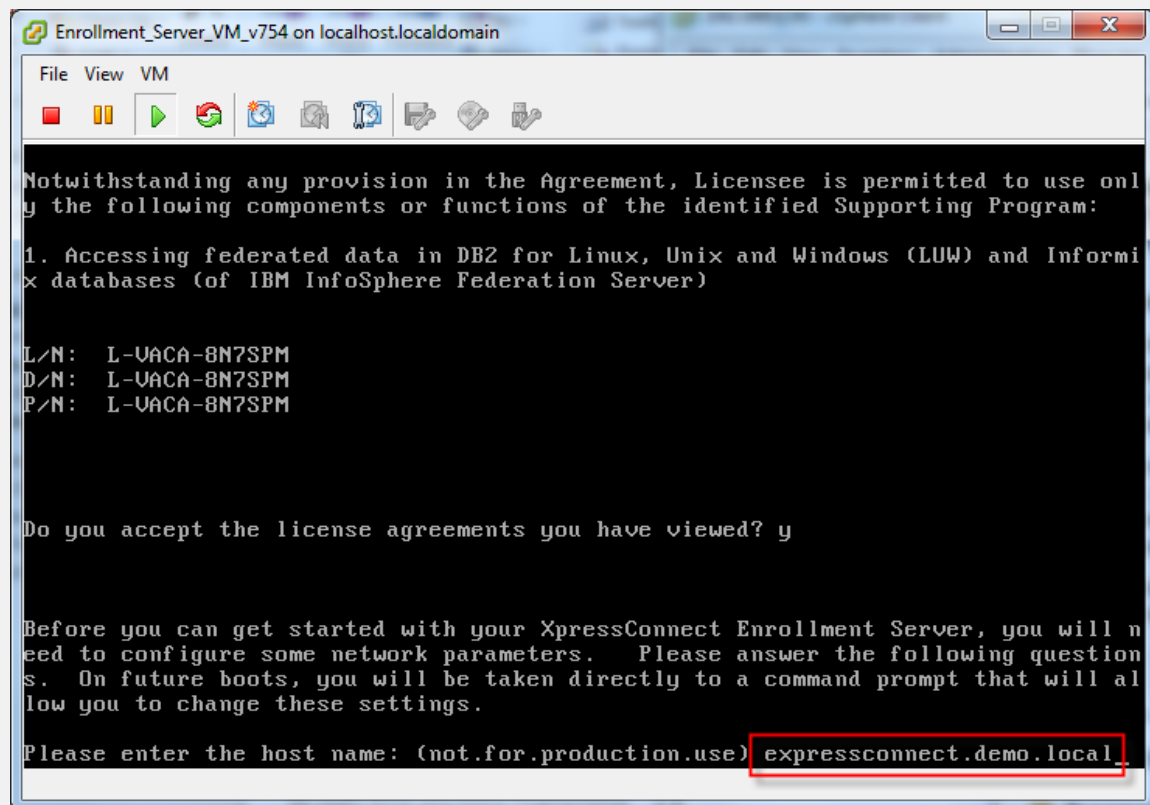
☐ Thick Provision Lazy Zeroed  
☐ Thick Provision Eager Zeroed  
☒ Thin Provision

Help < Back **Next >** Cancel

5 Click Finish.

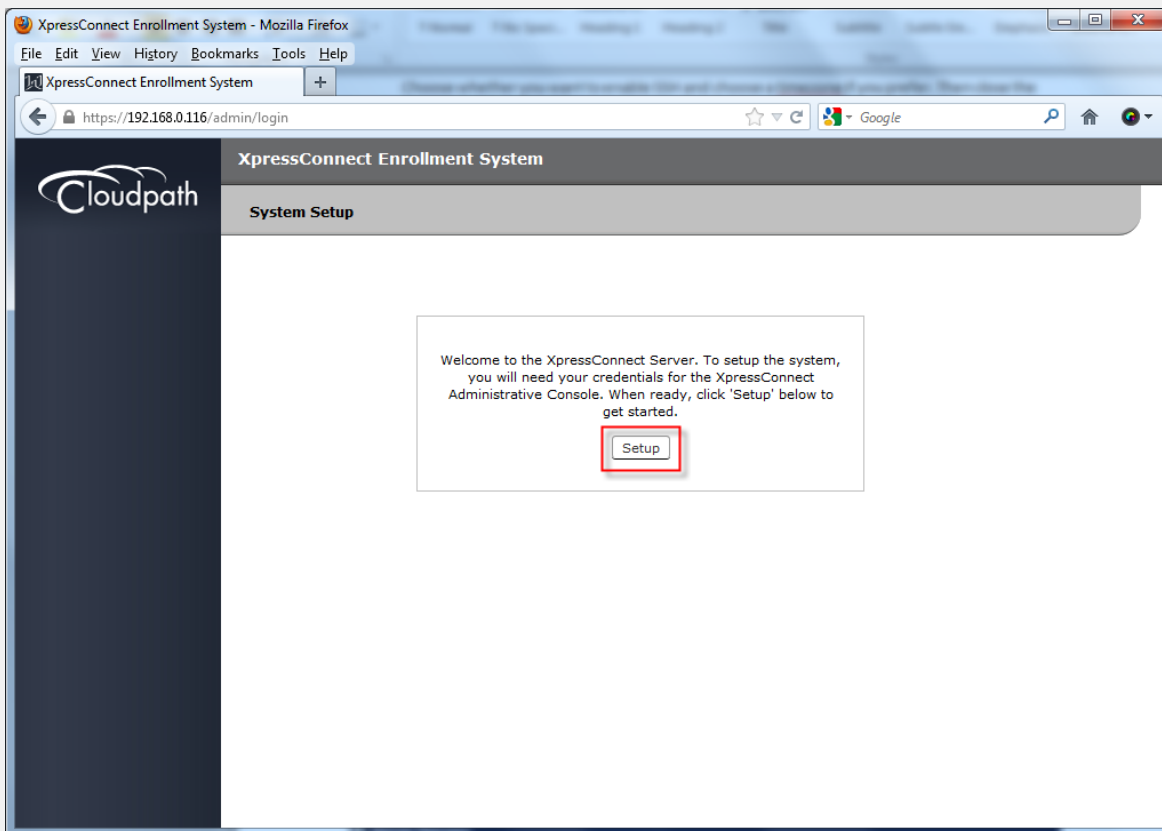


- 6 Start the VM and click Launch Virtual Machine Console. Accept the license agreements. Give the server a hostname such as xpressconnect.demo.local. Note if you want to be able to ping this by DNS name, you will need to configure a record in the DNS server. Configure IP address, mask, gateway, and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





### Login

Email Address:

Password:

☒ Remember email address.

[Forget your password?](#)

9 Type a Name and new password. Click Next.

Change Password

Next >

Enter information below to establish an on-board username and password.

Username:

sriramv-2@motorolasolutions.com

Friendly Name:

Admin

New Password:

••••••

Confirm Password:

••••••

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

Setup

Next >

The URL-Safe Company Name below is the name that will be used within certain URLs. It must not contain spaces or special characters.

URL-Safe Company Name:

MotDemo

**11** Confirm DNS hostname. Click Next.

Setup

Next >

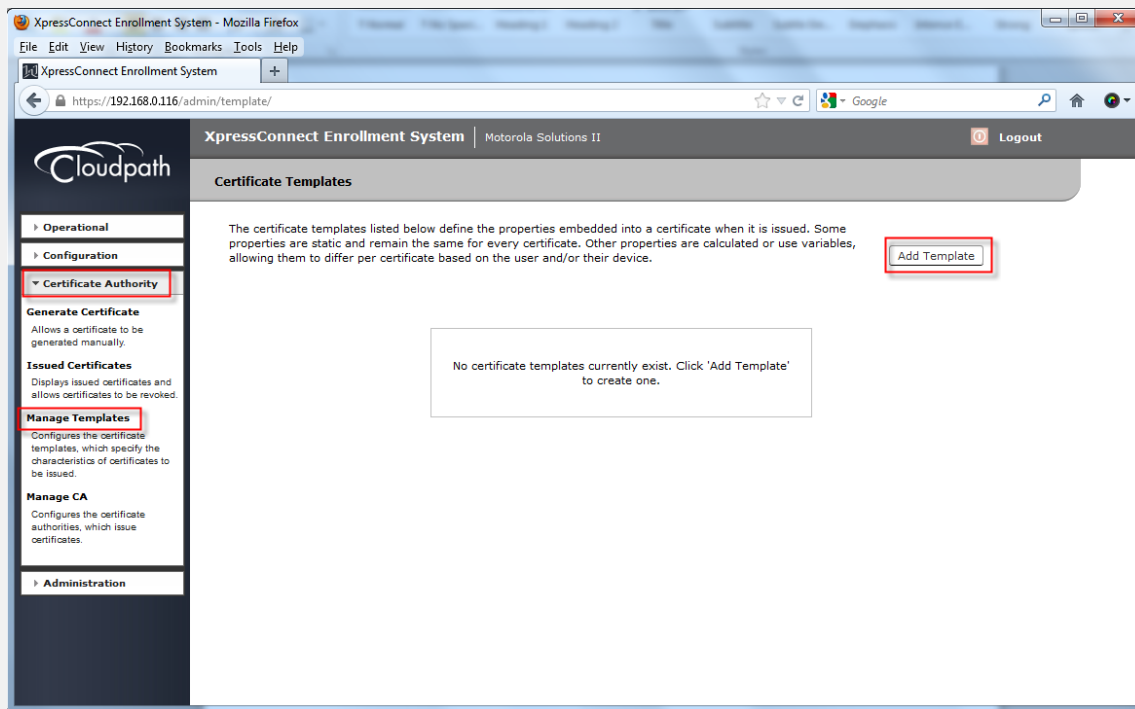
The DNS hostname below is used in multiple locations, including within the URL for OCSP of the root certificate authority. This should be set based on the permanent DNS hostname for this system. It is okay if the DNS entry is not yet setup.

DNS Hostname

expressconnect.demo.local

## 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.

**Certificate Templates**

**Which CA should sign the certificates?** Cancel Next >

- ☐ **Use an on-board certificate authority.**  
This option uses a certificate authority within the XpressConnect Enrollment System to sign certificates.
- ☒ **Use a Microsoft Certificate Authority.**  
This option allows certificates to be pulled from a Microsoft CA. Using a Microsoft CA requires that the Integration Module is installed on a Windows web server on the same domain as the Microsoft CA.
- ☐ **Use a custom external certificate authority.**  
This option allows certificates to be pulled from a remote certificate authority. Using a custom CA requires that the CA expose specific interfaces to enable the necessary interaction.

## 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.

**Microsoft CA Information** Cancel < Back Save

---

**Reference Information**

**Name:** MSFT CA

**Notes:** Integration Module for MSFT CA

**Enabled?** ☒

---

**Integration Module Configuration**

**CA Host Name:** WIN-43GV6KKSJ.demo.local

**CA Name:** demo-CA

**Request Attributes:** CertificateTemplate:User

---

**CA Communication Information**

**Microsoft CA URL:** http://WIN-43GV6KKSJ.demo.local

**CA Chain:**

**Use Static Credentials?** ☐

- 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.

Template 1: MSFT CA

**Notes:** Integration Module for MSFT CA

**Summary:** This template will issue certificates from a Microsoft CA. This requires that the Integration Module is installed on a Microsoft Windows 2008 R2 or greater web server joined to the domain. It may be installed directly on the CA or on a separate server.

**Setup:** To install or update the Integration Module, [download the Integration Module ZIP package](#).

**Status:** Online

**CA Type:** Microsoft CA

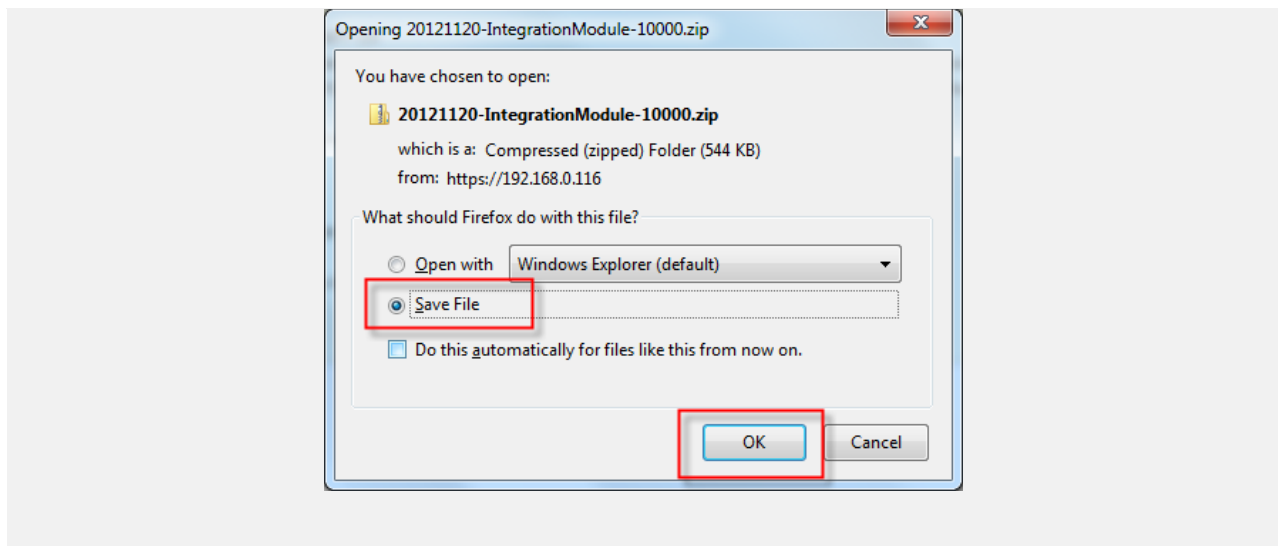
**CA URL:** https://WIN-43GV6KKSJ.demo.local/

**Credentials:** User-Provided

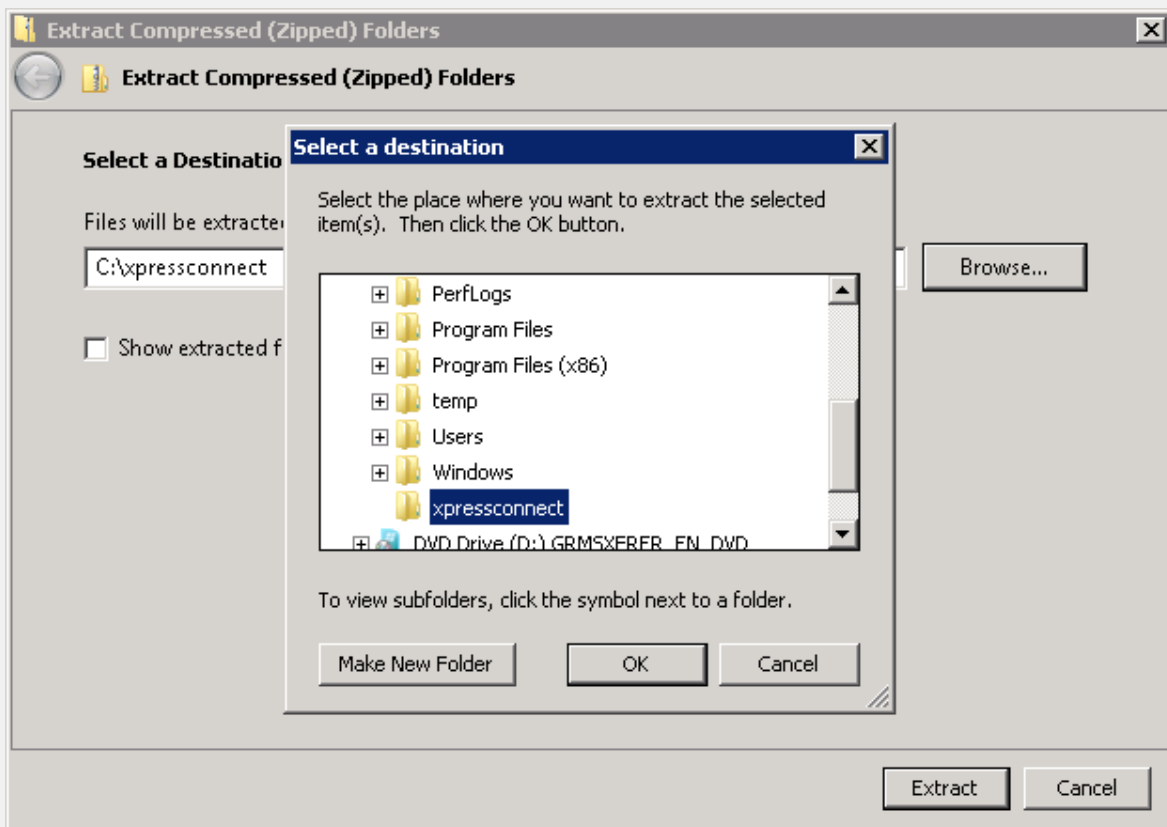
**CA Host Name:** WIN-43GV6KKSJ.demo.local

**CA Name:** demo-CA

**Request Attributes:** CertificateTemplate:User

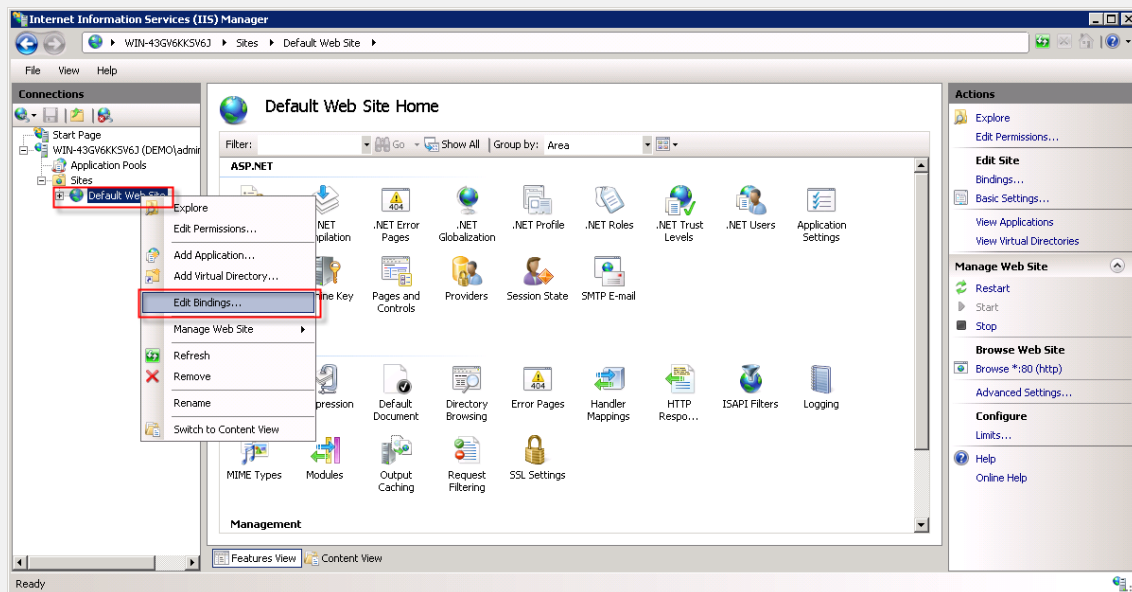


- 5 **Extract the contents of the ZIP file to a local folder. Create a new folder named SecureAccess, and unzip into that folder. Click OK. Click Extract.**

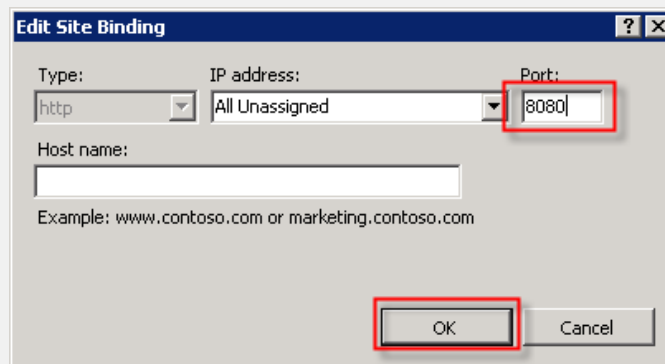
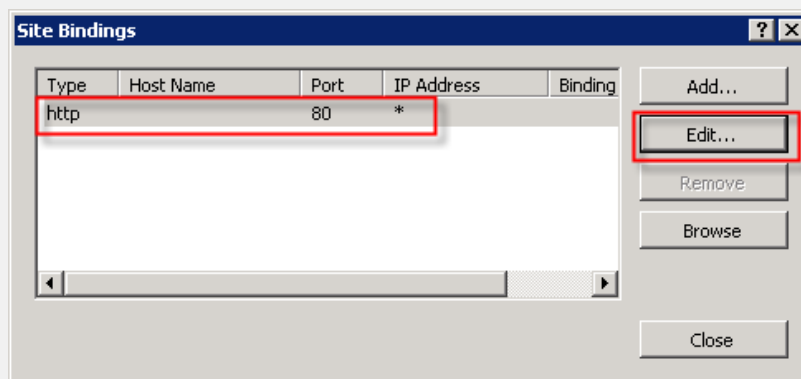


- 6 **Start IIS Manager by clicking Start and typing inetmgr in the search box, and press Enter. In IIS Manager, expand <server\_name> → Sites, and right-click Default Web Site and select Edit**

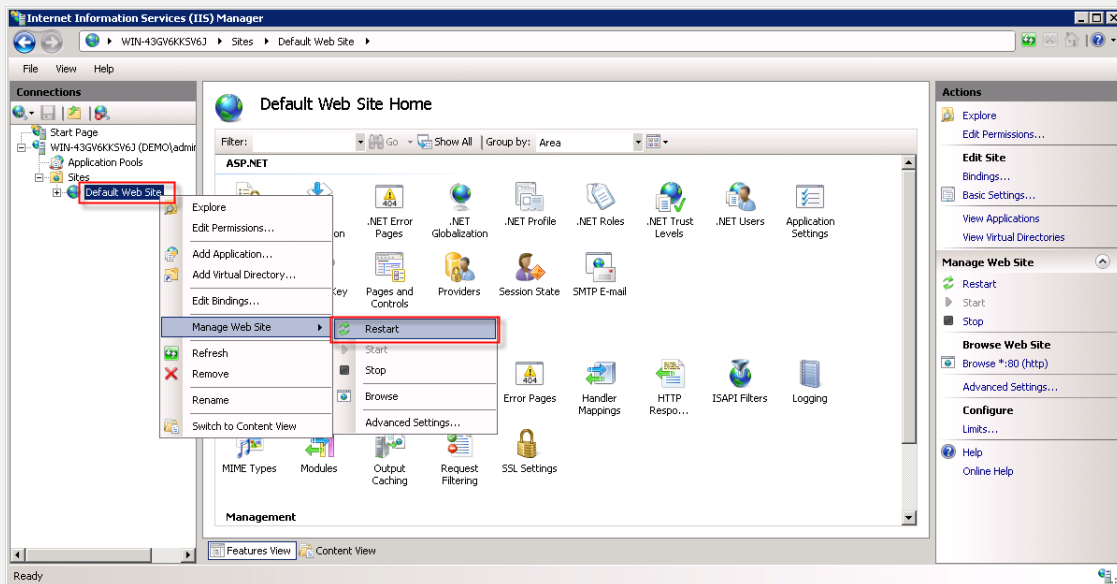
## Bindings.



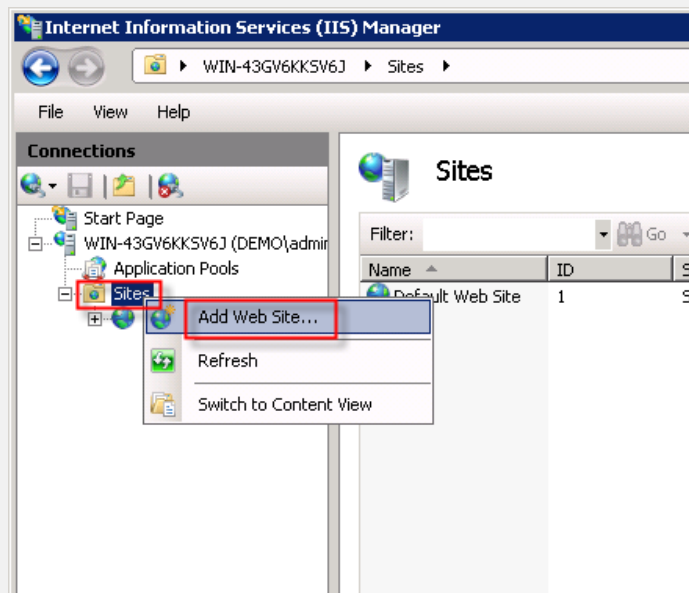
- 7 Click Edit. Change the port number from 80 to something else, such as 8080. Click OK. Click Close.



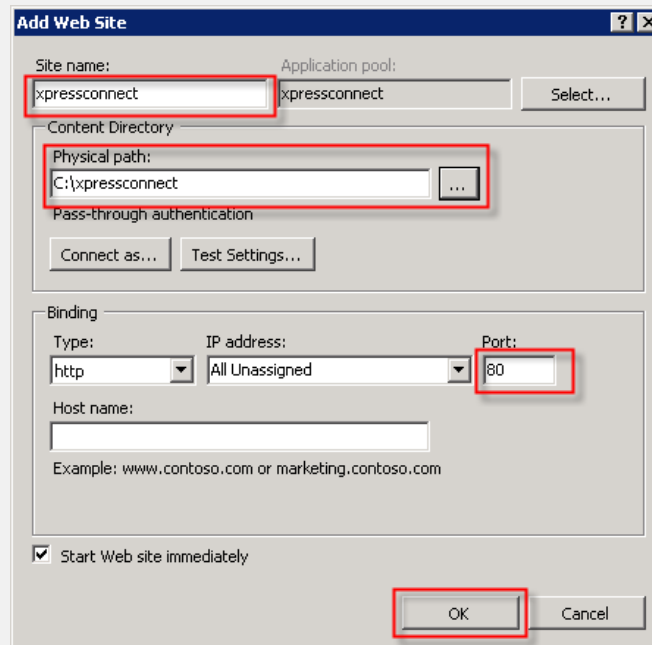
**8 Right-click Default Web Site, select Manage Web Site → Restart to restart the site.**



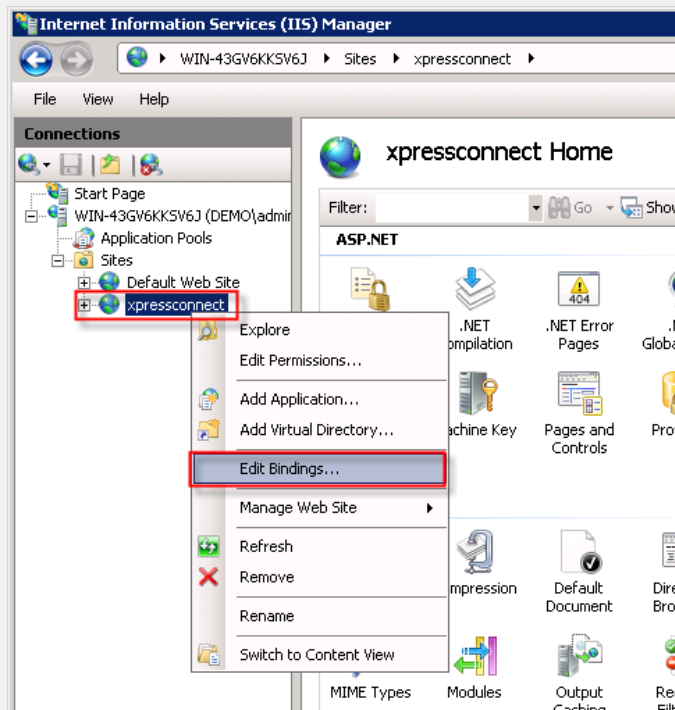
**9 Right-click Sites and select Add Web Site.**



**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.**



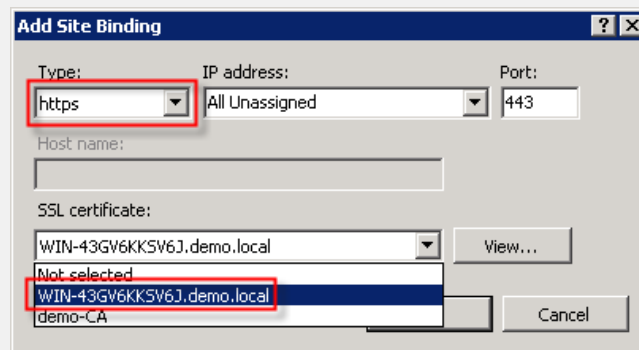
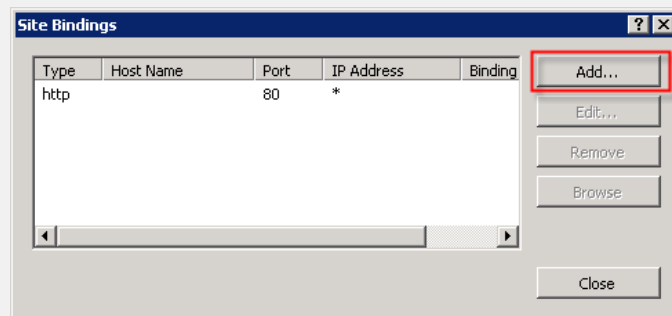
**11** Right-click the new SecureAccess site, and select Edit Bindings.



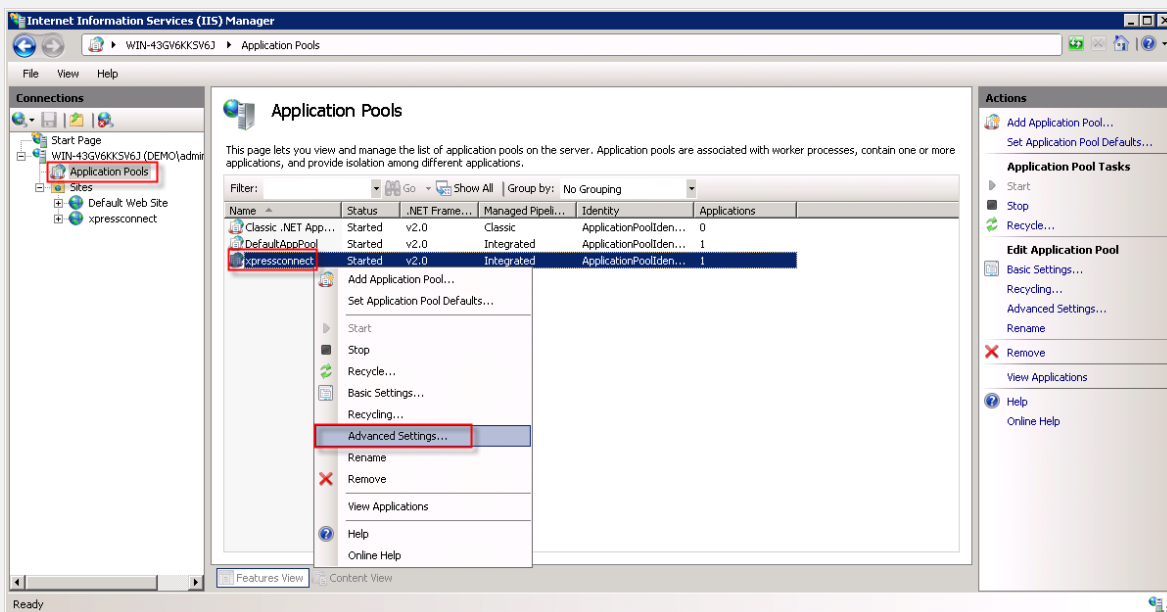
**12** Click Add. Select https. Select the SSL server certificate to be the same certificate used by



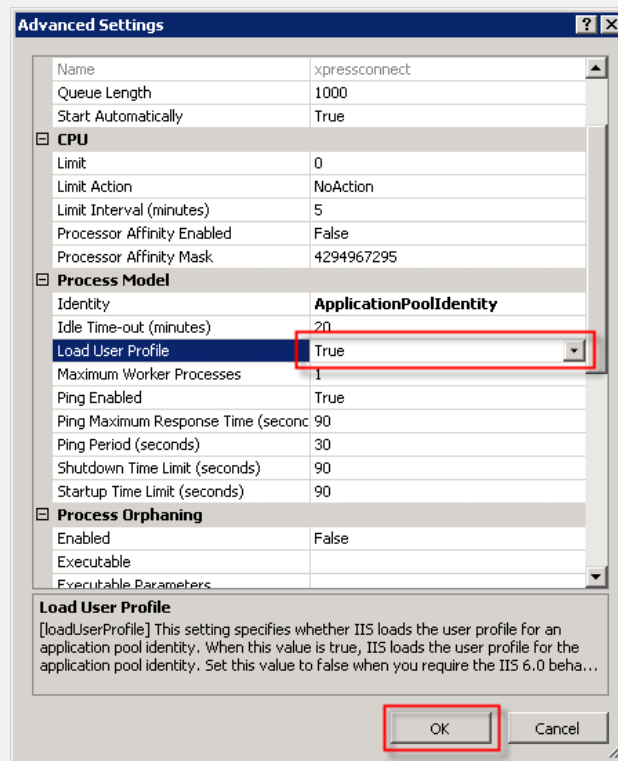
NPS previously (not the root CA certificate). Click OK. Click Close.



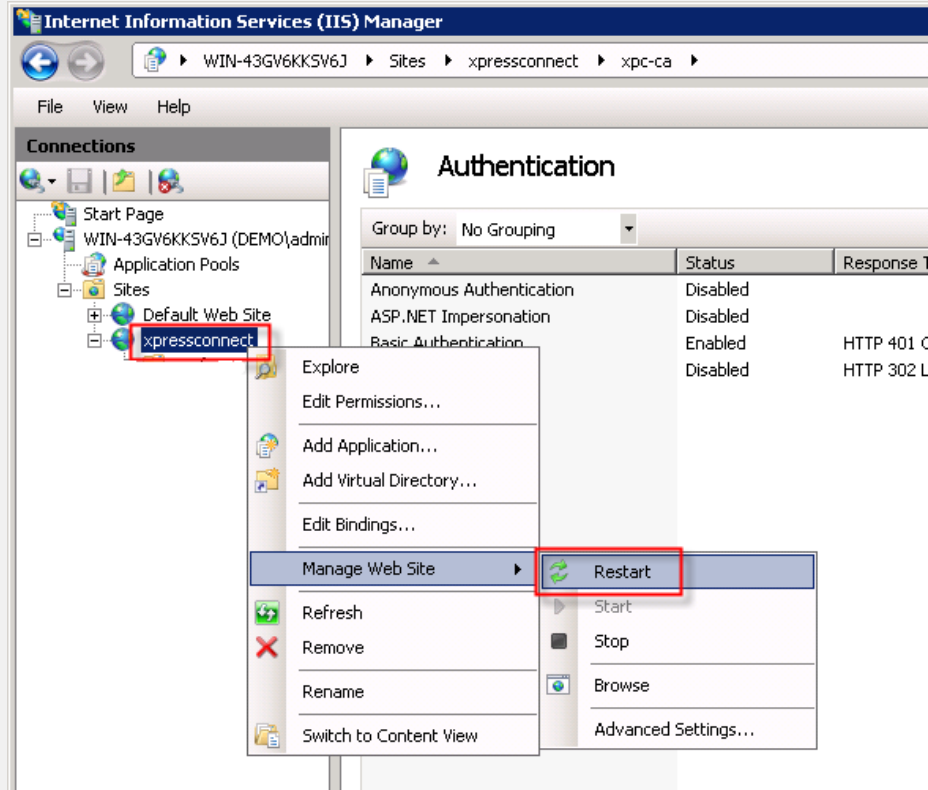
13 Click Application Pools. In the right-hand window pane, right click SecureAccess and select Advanced Settings.



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

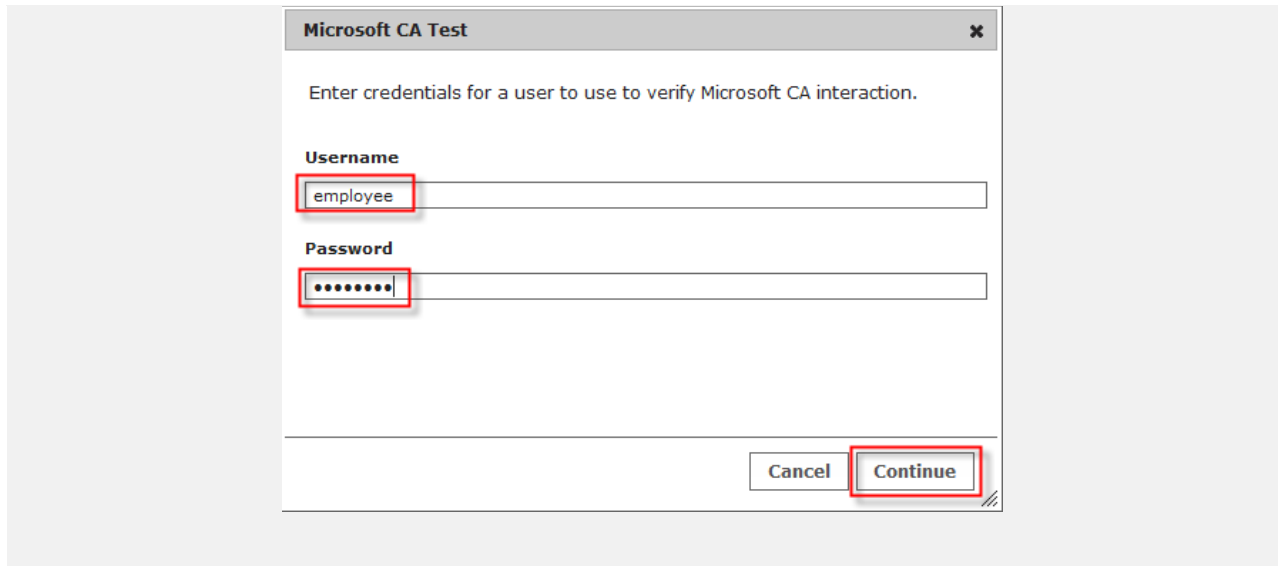


**15** Right-click the SecureAccess site and select Manage Web Site → Restart.



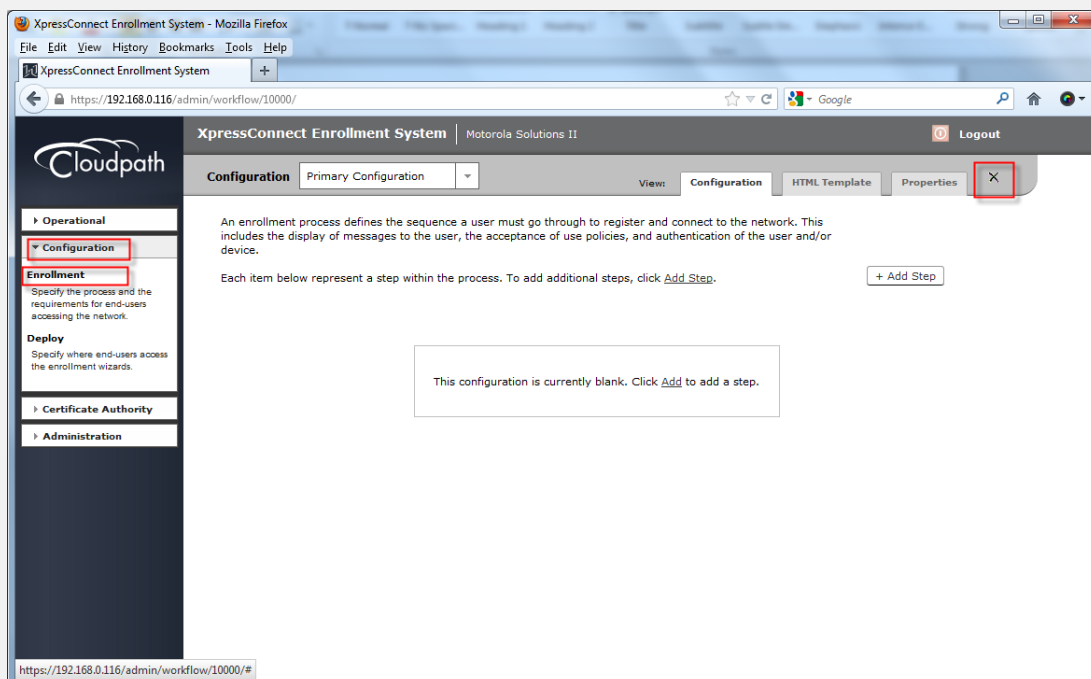
- 16** On the Enrollment Server, click the play button on the template to test the configuration. Provide user credentials and click Continue. You should see success information as well as a certificate in the results screen.





## 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.



**Delete Configuration?** ✕

⚠ Are you sure that you want to delete "Primary Configuration"?

Cancel Delete

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

No configurations exist. [Click here](#) to create a new configuration.

**Create Configuration** Save

**Name:**

**Description:**

**Enabled:** ☒

**Sample Data**

**Include Demo Data:** ☒

- 3 In the new workflow, click Employees → Corporate AD

**Configuration** Demo Workflow View: Configuration HTML Template Properties

An enrollment process defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.

Each item below represent a step within the process. To add additional steps, click [Add Step](#).

+ Add Step

Step 1:	Require the user to accept the AUP <b>Welcome Message and AUP</b>	✎ ✕ 🔍
Step 2:	Select an option: Visitors <b>Employees</b> Partners	✎ ☰ ✕ 🔍
Step 3:	<b>Prompt the user</b> for credentials from <b>Corporate AD</b>	✎ ✕ 🔍 ▶
Step 4:	Select an option: <b>Your Device</b> Company Device	✎ ☰ ✕ 🔍
Step 5:	Require the user to accept the AUP <b>BYOD Use Policy</b>	✎ ✕ 🔍
Result:	End of process. No network or certificate assigned.	✎

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

**Modify Authentication Server** Cancel **Save**

**Reference Information**

+ Name: Corporate AD

+ Description:

**Active Directory Information:**

+ AD Domain: demo.local

+ AD Host: ldap://192.168.0.115

+ AD DN: dc=demo,dc=local

+ Use For Sponsorship? ☒

**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.

**Configuration** Demo Workflow View: Configuration HTML Template Properties

An enrollment process defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.

Each item below represent a step within the process. To add additional steps, click [Add Step](#).

+ Add Step

Step 1:	Require the user to accept the AUP <b>Welcome Message and AUP</b>	
Step 2:	Select an option: Visitors <b>Employees</b> Partners	
Step 3:	<b>Prompt the user</b> for credentials from <b>Corporate AD</b>	
Step 4:	Select an option: <b>Your Device</b> Company Device	
Step 5:	Require the user to accept the AUP <b>BYOD Use Policy</b>	
Result:	End of process. No network or certificate assigned.	

**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.

**Configuration** Demo Workflow View: Configuration HTML Template Properties

An enrollment process defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.

Each item below represent a step within the process. To add additional steps, click [Add Step](#).

+ Add Step

Step 1:	Require the user to accept the AUP <b>Welcome Message and AUP</b>	
Step 2:	Select an option: Visitors <b>Employees</b> Partners	
Step 3:	<b>Prompt the user</b> for credentials from <b>Corporate AD</b>	
Step 4:	Select an option: <b>Your Device</b> Company Device	
Step 5:	Require the user to accept the AUP <b>BYOD Use Policy</b>	
Result:	End of process. No network or certificate assigned.	

**Selection Options** Preview Add Done

Option 1:	Your Device	
Option 2:	Company Device	

**Modify Option**

Cancel
Save

**Webpage Display Information**

+
Name:
Your Device

+
Display Label:
Personal Device

+
Description:
Select this option if the device belongs to you.

+
Icon File:
Browse...

**Restrictions**

+
Group Name Regex:
BYOD APP.\*

+
Allowed IPs:

+
Blocked IPs:

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

Configuration
Demo Workflow

View:
Configuration
HTML Template
Properties

An enrollment process defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.

Each item below represent a step within the process. To add additional steps, click [Add Step](#).

+ Add Step

Step 1:
Require the user to accept the AUP **Welcome Message and AUP**

Step 2:
Select an option:
Visitors
**Employees**
Partners

Step 3:
**Prompt the user** for credentials from **Corporate AD**

Step 4:
Select an option:
**Your Device**
Company Device

Step 5:
Require the user to accept the AUP **BYOD Use Policy**

Result:
End of process. No network or certificate assigned.

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



For which network should users be configured?

Cancel

Next >

☐ None.

Do not configure the user for any network.

☒ An existing network.

Configure the user for an existing network.

Select the Network: 

Demo Server - demo-secu

Motorola Solutions II - test3

Motorola Solutions II - secureSSID

Motorola Solutions II - M-Secure

Motorola Solutions II - Corp-Secure

Enrollment System-test - Seth-secure

Enrollment System-test - Seth-Demo

Enrollment System-test - secure-byod

Enrollment System-test - cert-secure2

Enrollment System-test - cert-secure

Demo Server - demo-secure

9

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

What certificate template should issue the certificate?

Cancel

< Back

Next >

☐ Do not issue a certificate to the user.

☒ An existing certificate template.

Issue the certificate using an existing certificate template.

Select the Certificate Template: 

MSFT CA

**Configuration** Demo Workflow

View: Configuration HTML Template Properties

An enrollment process defines the sequence a user must go through to register and connect to the network. This includes the display of messages to the user, the acceptance of use policies, and authentication of the user and/or device.

Each item below represent a step within the process. To add additional steps, click [Add Step](#).

+ Add Step

Step 1:	Require the user to accept the AUP <b>Welcome Message and AUP</b>	✎ ✕ 🔍
Step 2:	Select an option: Visitors <b>Employees</b> Partners	✎ ☰ ✕ 🔍
Step 3:	<b>Prompt the user</b> for credentials from <b>Corporate AD</b>	✎ ✕ 🔍 ▶
Step 4:	Select an option: <b>Your Device</b> Company Device	✎ ☰ ✕ 🔍
Step 5:	Require the user to accept the AUP <b>BYOD Use Policy</b>	✎ ✕ 🔍
Result:	Move user to <b>demo-secure</b> and assign certificate using <b>MSFT CA</b> .	✎

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

XpressConnect Enrollment System - Mozilla Firefox

File Edit View History Bookmarks Tools Help

XpressConnect Enrollment System

https://192.168.0.116/admin/locations/

XpressConnect Enrollment System | Motorola Solutions II Logout

**Cloudpath**

Operational

**Configuration**

Enrollment  
Specify the process and the requirements for end-users accessing the network.

**Deploy**  
Specify where end-users access the enrollment wizards.

Certificate Authority

Administration

**Deployment Locations**

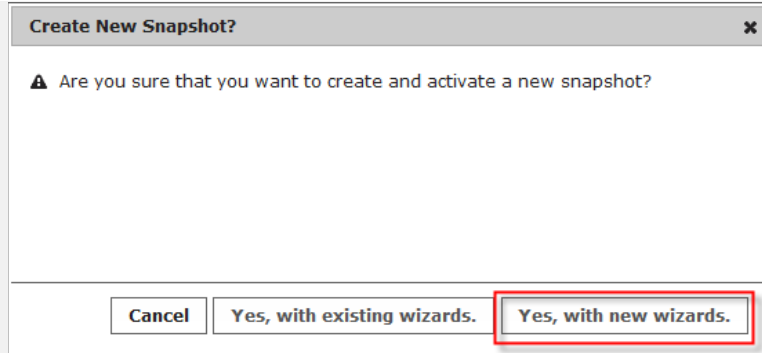
A deployment location represents a URL to where a configuration is deployed. Multiple locations may be used for a variety of reasons. For example, a production configuration may be deployed to /production, and a test configuration may be deployed to /test.

Add Location

Location 1: Production

✎ ✕ 📷

Enrollment URL: /enroll/ or /enroll/MotDemo/ or /enroll/MotDemo/Production/  
Sponsorship Login: /portal/sponsor/  
New Snapshot: Create and deploy a new snapshot using the configuration 'Demo Workflow'. ▶

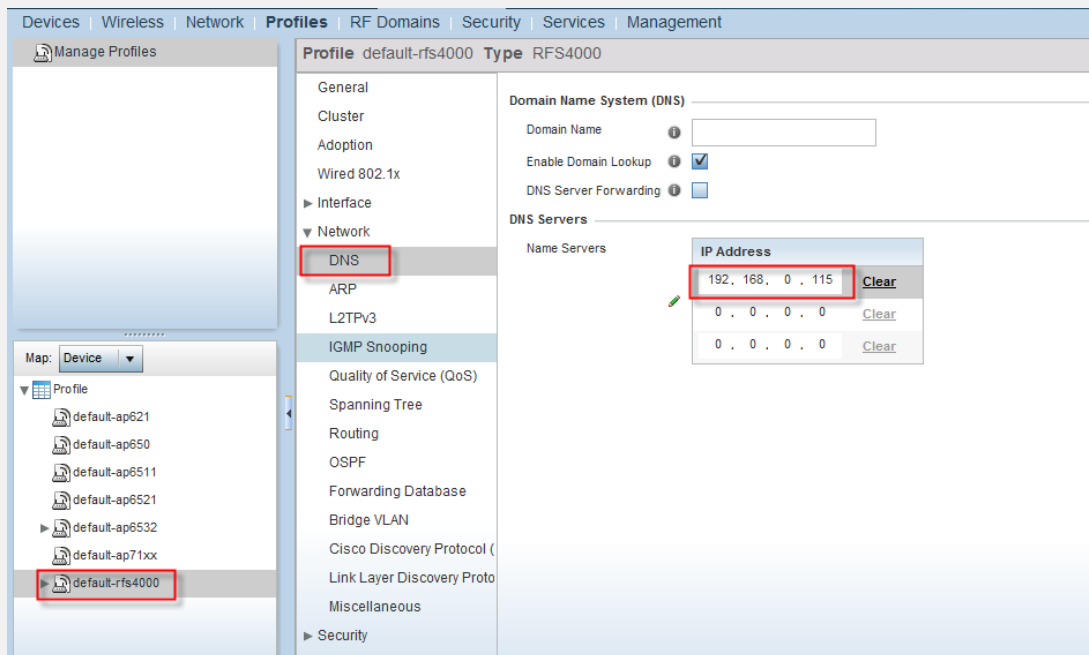


- 11 Point your browser to [http://<server\\_name>/enroll](http://<server_name>/enroll) (or alternatively use the IP address of the server instead of name) to see the onboard webpage. Verify it is working.

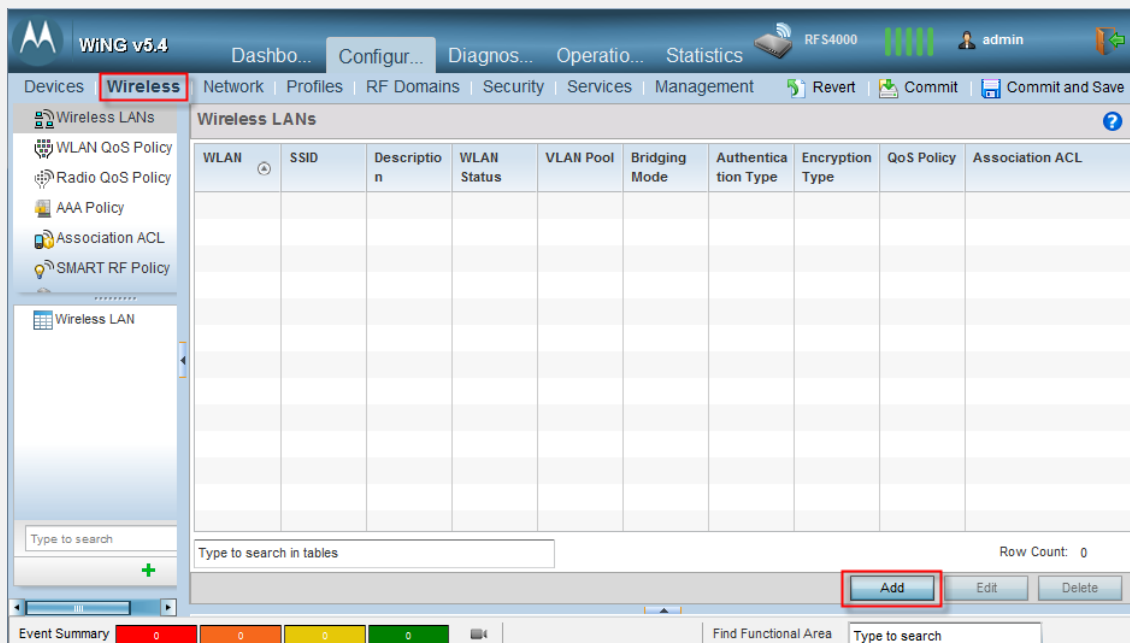
## 2.7 Configure RFS and Access Point

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.

**WLAN** demo-onboard

Basic Configuration

Security

Firewall

Client Settings

Accounting

Client Load Balancing

Advanced

Auto Shutdown

**WLAN Configuration**

SSID: demo-onboard

Description: Onboarding SSID

WLAN Status: ☐ Disabled ☒ Enabled

QoS Policy: default

Bridging Mode: Tunnel

**Other Settings**

Broadcast SSID: ☒

Answer Broadcast Probes: ☒

**VLAN Assignment**

☒ Single VLAN ☐ VLAN Pool

VLAN: 1

**RADIUS VLAN Assignment**

Allow RADIUS Override: ☐

OK Reset Exit

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

**WLAN** demo-onboard

Basic Configuration

**Security**

Firewall

Client Settings

Accounting

Client Load Balancing

Advanced

Auto Shutdown

**Select Authentication**

☐ EAP ☐ EAP-PSK ☐ EAP-MAC ☐ MAC ☐ Kerberos ☒ PSK / None

**Kerberos Configuration** Settings

AAA Policy:

Reauthentication: ☐ 30 (30 to 86,400)

**Captive Portal**

Enforcement: ☒ Captive Portal Enable ☐ Captive Portal if Primary Authentication Fails

Captive Portal Policy:

**MAC Registration**

Enable: ☐

Radius Group Name:

OK Reset Exit

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

Captive Portal Policy enrollment-server

Basic Configuration Web Page

Settings

Captive Portal Server Mode ☒ Internal (Self) ☒ Centralized ☐ Centralized Controller

Hosting VLAN Interface 0 (0 to 4,096)

Captive Portal Server 192.168.0.105 IP Address

Connection Mode ☒ HTTP ☐ HTTPS

Simultaneous Users 1 (1 to 8,192)

Security

AAA Policy

Access

Access Type ☐ No authentication required ☒ Generate Logging Record and Allow Access ☐ Custom User Information for RADIUS Authentication ☒ RADIUS Authentication

RADIUS Lookup Information

Terms and Conditions page

Client Settings


Client Access Time 1440 (30 to 10,080 minutes)

Inactivity Timeout 10 Minutes (5 to 1,440)





DNS Whitelist


DNS Whitelist Add OK Reset Exit


- 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.

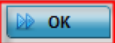


Name 

DNS Entries

DNS Entry	Match Suffix	
192.168.0.116	✗	
facebook.com	✓	
 <input data-bbox="446 472 673 504" type="text" value="linkedin.com"/> <input data-bbox="690 472 771 504" type="button" value="Hostname"/> <input data-bbox="787 472 868 504" type="button" value="Yes"/>	▼	



 Add Row

7

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

Captive Portal Policy enrollment-server

Basic Configuration Web Page

Web Page Source ☐ Internal ☐ Advanced ☒ Externally Hosted

Login URL

Agreement URL

Welcome URL

Fail URL

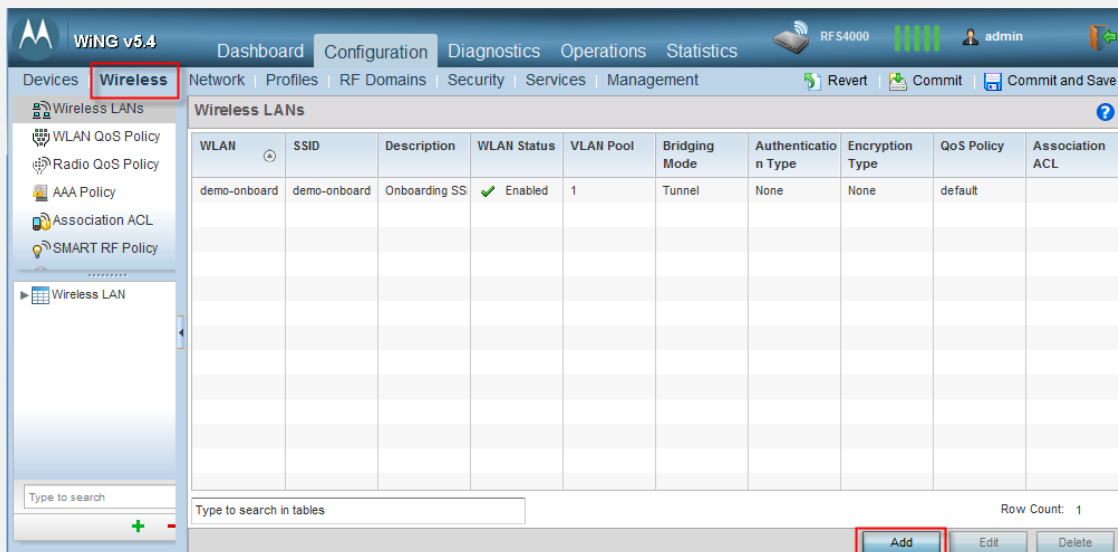
A set of pre-existing web pages outside of the Controller are specified by the provided URLs.  
Four separate URLs point to external web pages for: Logging the user in, Welcoming the user after logging in successfully and Informing the user of a failed login attempt.

OK Reset Exit

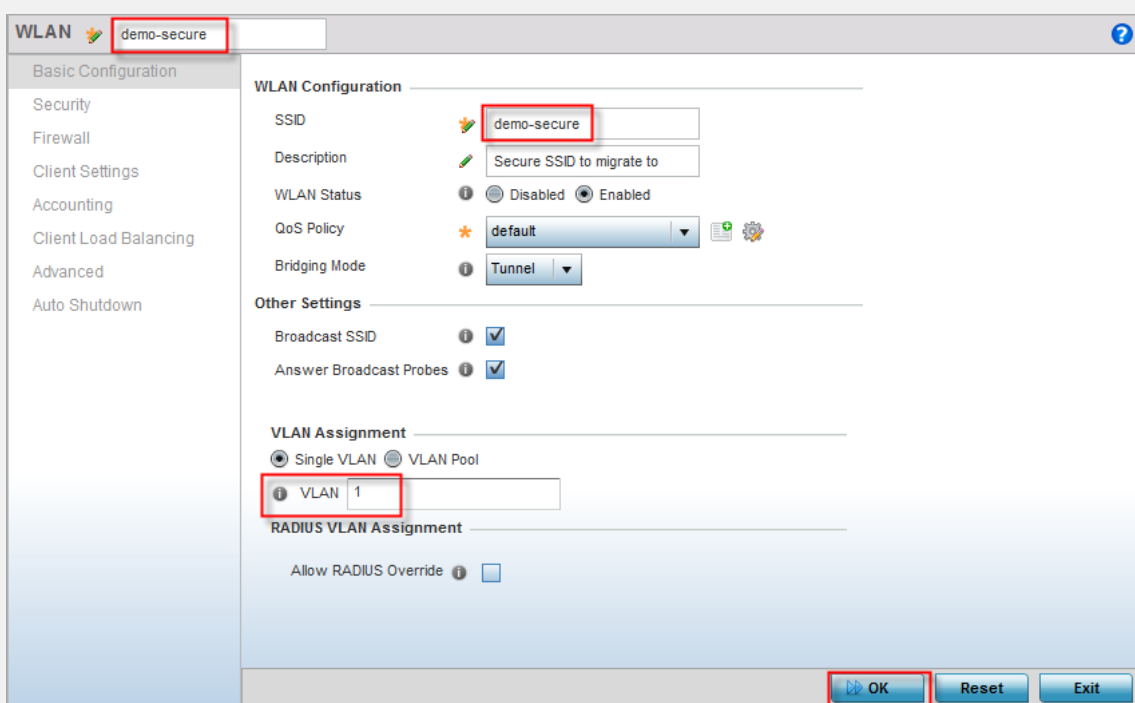
8

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.

**WLAN demo-secure**

Basic Configuration

**Security**

Firewall

Client Settings

Accounting

Client Load Balancing

Advanced

Auto Shutdown

**Select Authentication**

☒ EAP ☐ EAP-PSK ☐ EAP-MAC ☐ MAC ☐ Kerberos ☐ PSK / None

Kerberos Configuration [Settings](#)

AAA Policy \*

Reauthentication i ☐ 30 (30 to 86,400)

**Captive Portal**

Enforcement i ☐ Captive Portal Enable ☐ Captive Portal if Primary Authentication Fails

Captive Portal Policy i

**MAC Registration**

Enable i ☐

Radius Group Name i

OK Reset Exit

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

**AAA Policy** \*

**RADIUS Authentication**

Server Id	Host	Port	Server Type	Request Pro: Mode

**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.

**Authentication Server** [X]

Server Id 1 (1 to 6) [?]

---

**Settings**

Host 192.168.0.115 IP Address

Port 1812 (1 to 65,535)

Server Type Host

Secret secret [Show]

Request Proxy Mode Through Wireless Controller

Request Attempts 3 (1 to 10)

Request Timeout 3 Seconds (1 to 60)

Retry Timeout Factor 100 (50 to 200)

DSCP 46 (0 to 63)

---

**Network Access Identifier Routing**

NAI Routing Enable ☐

Realm

Realm Type ☒ Prefix ☐ Suffix

Strip Realm ☐

OK Reset Exit

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

**WLAN demo-secure**

**Basic Configuration**

**Security**

Firewall

Client Settings

Accounting

Client Load Balancing

Advanced

Auto Shutdown

**Select Encryption**

☐ WPA/WPA2-TKIP ☐ WEP 128 ☐ WEP 64 ☐ Open

☒ **WPA2-CCMP** ☐ KeyGuard

**Key Settings**

Enter 64 HEX or 8-63 ASCII Characters

Pre-Shared Key  ASCII

**Key Rotation**

Unicast Rotation Interval  (30 to 86,400 seconds)

Broadcast Rotation Interval  (30 to 86,400 seconds)

**Fast Roaming**

Pairwise Master Key(PMK) Caching ☒ Pre-Authentication ☐

Opportunistic Key Caching ☒

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

**WiNG v5.4** Dashboard Configuration Diagnostics Operations Statistics

Devices | Wireless | Network | **Profiles** | RF Domains | Security | Services | Management

Revert Commit Commit and Save

Profile default-ap6532 Type AP6532

**Map: Device**

▼ Profile

- default-ap621
- default-ap650
- default-ap6511
- default-ap6521
- default-ap6532**
- default-ap71xx

Type to search

**Radios**

Name	Type	Description	Admin Status	RF Mode	Channel	Transmit Power
radio1	Radio	radio1	✓ Enabled	2.4 GHz WLAN	smart	smart
radio2	Radio	radio2	✓ Enabled	5 GHz WLAN	smart	smart

Type to search in tables

Row Count: 2

**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.**

Radio

WLANs

demo-onboard

demo-secure

MeshPoint

Radio

Advanced Mapping

WLAN/BSS Mappings

WLANs

MeshPoint

Create New WLAN

Create New MeshPoint

OK

Reset

Exit

16

Repeat previous step for the other radio.

17

Commit and Save the changes:

Revert

Commit

Commit and Save

- 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