Deploying Configuration Manager Current Branch with PKI – Step by Step

Volume 1

Dave Kawula - MVP

Allan Rafuse - MVP

Cristal Kawula - MVP

Émile Cabot - MVP

Foreword by: Ed Aldrich

PUBLISHED BY

MVPDays Publishing
http://www.mvpdays.com

ISBN: 978-1984010261

Warning and Disclaimer

Every effort has been made to make this manual as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Feedback Information

We’d like to hear from you! If you have any comments about how we could improve the quality of this book, please don’t hesitate to contact us by visiting www.checkyourlogs.net or sending an email to feedback@mvpdays.com.

Foreword by: Ed Aldrich

First, I want to thank Dave Kawula for once again asking me to provide a foreword to this latest book on Configuration Manager. From the book's ACKNOWLEDGEMENTS section, I'd like to echo the sentiments of co-author Émile Cabot: "…After all these years I still don't know how you two are able to take on everything that you do in the IT world…". To put it mildly, this team is amazing.

That said, what makes *this* book compelling to you, the reader? Is this yet another in the seemingly endless list of How-to books on installing and configuring Configuration Manager? In my rather lengthy experience, dating back to SMS2.0, RTM, the simple answer is *absolutely not*! Let me give you just a few examples to illustrate.

This book covers the entire end-to-end planning, installing, updating, configuring and deploying a complete system *with a full PKI infrastructure* to boot! That element alone, documented in Chapter 2, cannot be overemphasized and is worth the cost of the book all by itself! When I was looking into the implementation of the then-new and shiny Internet Based Client Management (IBCM) feature many years ago, all I knew of PKI was how to spell it. I would have given anything for this information back then. For you, it's all crystal clear, and found right here in chapter 2.

Beyond that element, you will first see listed out all the prerequisites necessary, the various roles and features to be implemented, the black magic that is SQL Server, your domain configurations clearly explained and necessary (which will keep your Domain Admins away from your desk!), and then walk you through how to install it all. You'll then end up with SSL security, the MDT Toolkit fully integrated, updated to Current Branch 1710, initial configuration settings applied, and clients deployed. In other words, you'll create a completely functional system with all of the latest-and-greatest. If you're naturally lazy like me, and you don't particularly want to go through all of this yourself but just want it DONE so you can get on with it, guess what? *There's a* **SCRIPT** to do it all *FOR* you!!!

Lastly, the authors' then go on to also manage all of that hocus-pocus called networking! I never pretended to be a network engineer. As far as I'm concerned, they all live in a foreign land complete with its own language. NAT? Wasn't that a famous singer back in the day??? What's

that got to do with anything? Well, in a simple-to-follow procedure in the prerequisites section, they make it all clear, and why.

This book is highly recommended as it is loaded with incredibly easy to read procedures, complete with with excellent screen shots, to get your new installation up and running in a hurry, whether in a lab or in your production environment. Having your new system fully loaded with a functional PKI environment and integrated MDT is a hugely important bonus as you likely delve into a Windows 10 migration project as one of your first major undertakings.

Of course, I also suggest you also look at the significant Windows 10 deployment automation tools that fully integrate with and extend your shiny new Configuration Manager system that are available from my employer, 1E (www.1e.com). These are designed to supercharge your Configuration Manager system to help you to #StayCurrent and secure throughout your enterprise!

Acknowledgements

From Dave

Cristal, you are my rock and my source of inspiration. For the past 20 + years you have been there with me every step of the way. Not only are you the "BEST Wife" in the world you are my partner in crime. Christian, Trinity, Keira, Serena, Mickaila and Mackenzie, you kids are so patient with your dear old dad when he locks himself away in the office for yet another book. Taking the time to watch you grow in life, sports, and become little leaders of this new world is incredible to watch.

Thank you, Mom and Dad (Frank and Audry) and my brother Joe. You got me started in this crazy IT world when I was so young. Brother, you mentored me along the way both coaching me in hockey and helping me learn what you knew about PC's and Servers. I'll never forget us as teenage kids working the IT Support contract for the local municipal government. Remember dad had to drive us to site because you weren't old enough to drive ourselves yet. A great career starts with the support of your family and I'm so lucky because I have all the support one could ever want.

A book like this filled with amazing Canadian MVP's would not be possible without the support from the #1 Microsoft Community Program Manager – Simran Chaudry. You have guided us along the path and helped us to get better at what we do every day. Your job is tireless and your passion and commitment make us want to do what we do even more.

Last but not least, the MVPDays volunteers, you have donated your time and expertise and helped us run the event in over 20 cities across North America. Our latest journey has us expanding the conference worldwide as a virtual conference. For those of you that will read this book your potential is limitless just expand your horizons and you never know where life will take you.

From Émile

Before we get to the geeks, I have to deeply thank my wife, Laura, for being so supportive over the past half-dozen years. I've spent countless hours (days even) locked in the office while you

tirelessly kept Tyson and Erick entertained and out of trouble. You're a wonderful wife and an amazing mother. I thank you from the bottom of my heart for being by my side.

Mom and Dad, from my first VIC-20 to my first business, you've always been there to guide and support me. You taught me the value of integrity and ethics early on, and the importance of enjoying life to its fullest.

Cristal and Dave…you're both amazing. After all these years I still don't know how you two are able to take on everything that you do in the IT world while raising six (yes, six!) children, and hockey, cheer, fishing, the cabin, the four things I'm missing, and still manage to generate an income. It's been an absolute pleasure to have had the opportunity to work with you both, and looking forward to many years to come.

To my friends in the MVP Community: The relationships we've developed over the past three years are the thing I was not expecting when I first received my reward. We've had a blast on roadshows, co-presenting, web/podcasting, in Vegas and at Summit. A lot of fun, gig's of memories, and some really great solutions have come out of our endeavours.

Last, but far from least, Simran Chaudry (Sim! Sim! Sim!), you've been a great mentor and continue to help me increase my potential. Your passion shows in everything that you do, and words can't describe how grateful I am to have the opportunity to work with you.

About the Authors

Dave Kawula - MVP

Dave is a Microsoft Most Valuable Professional (MVP) with over 20 years of experience in the IT industry. His background includes data communications networks within multi-server environments, and he has led architecture teams for virtualization, System Center, Exchange, Active Directory, and Internet gateways. Very active within the Microsoft technical and consulting teams, Dave has provided deep-dive technical knowledge and subject matter expertise on various System Center and operating system topics.

Dave is well-known in the community as an evangelist for Microsoft, 1E, and Veeam technologies. Locating Dave is easy as he speaks at several conferences and sessions each year, including TechEd, Ignite, MVP Days Community Roadshow, and VeeamOn.

Recently Dave has been honored to take on the role of Conference Co-Chair of TechMentor with fellow MVP Sami Laiho. The lineup of speakers and attendees that have been to this conference over the past 20 years is really amazing. Come down to Redmond or Orlando in 2018 and you can meet him in person.

As the founder and Managing Principal Consultant at TriCon Elite Consulting, Dave is a leading technology expert for both local customers and large international enterprises, providing optimal guidance and methodologies to achieve and maintain an efficient infrastructure.

BLOG: www.checkyourlogs.net

Twitter: @DaveKawula

Allan Rafuse – MVP

Allan has worked as a senior member of the Windows and VMWare Platform Department at Swedbank. He took part in the architecture and implementation of multiple datacenters in several countries. He is responsible for the roadmap and lifecycle of the Windows Server Environment, including the development of ITIL processes of global server OSD, configuration, and performance.

He is an expert at scripting solutions and has an uncanny ability to reduce complexity and maximize the functionality of PowerShell. Allan has recently rejoined the TriCon Elite Consulting team again as a Principal Consultant.

BLOG: http://www.checkyourlogs.net

Twitter: @allanrafuse

Cristal Kawula – MVP

Cristal Kawula is the co-founder of MVPDays Community Roadshow and #MVPHour live Twitter Chat. She was also a member of the Gridstore Technical Advisory board and is the President of TriCon Elite Consulting. Cristal is also only the 2nd Woman in the world to receive the prestigious Veeam Vanguard award.

Cristal can be found speaking at Microsoft Ignite, MVPDays, and other local user groups. She is extremely active in the community and has recently helped publish a book for other Women MVP's called Voices from the Data Platform.

BLOG: http://www.checkyourlogs.net

Twitter: @supercristal1

Emile Cabot - MVP

Émile is a three-time Microsoft Most Valuable Professional (MVP) who started in the industry during the mid-90s working at an ISP and designing web sites for celebrities. He has a strong background specializing in datacenter and deployment solutions, and has spent many years performing infrastructure analyses and solution implementations for organizations ranging from 20 to over 200,000 employees.

Émile organizes the Calgary Microsoft User Group, blogs on CheckYourLogs.net, and has presented at several conferences, including Ignite, VeeamOn, TechReady, and MVPDays.

He actively volunteers as a member of the Canadian Ski Patrol, providing over 250 hours each year for first aid services and public education at Castle Mountain Resort and in the community.

BLOG: http://www.checkyourlogs.net

Twitter: @ecabot

Technical Editors

Cary Sun – CCIE #4531 (Future Microsoft MVP)

Cary Sun is CISCO CERTIFIED INTERNETWORK EXPERT (CCIE No.4531) and MCSE, MCIPT, Citrix CCA with over twenty years in the planning, design, and implementation of network technologies and Management and system integration. Background includes hands-on experience with multi-platform, all LAN/WAN topologies, network administration, E-mail and Internet systems, security products, PCs and Servers environment. Expertise analyzing user's needs and coordinating system designs from concept through implementation. Exceptional analysis, organization, communication, and interpersonal skills. Demonstrated ability to work independently or as an integral part of team to achieve objectives and goals. Specialties: CCIE /CCNA / MCSE / MCITP / MCTS / MCSA / Solution Expert / CCA

Cary's is a very active blogger at checkyourlogs.net and always available online for questions from the community. He passion about technology is contagious and he makes everyone around him better at what they do.

Blog:http://www.checkyourlogs.net

Twitter:@SifuSun

Contents

Introduction

North American MVPDays Community Roadshow

The purpose of this book is to showcase the amazing expertise of our guest speakers at the North American MVPDays Community Roadshow. They have so much passion, expertise, and expert knowledge that it only seemed fitting to write it down in a book.

MVPDays was founded by Cristal and Dave Kawula back in 2013. It started as a simple idea: "There's got to be a good way for Microsoft MVPs to reach the IT community and share their vast knowledge and experience in a fun and engaging way." I mean, what is the point in recognizing these bright and inspiring individuals, and not leveraging them to inspire the community that they are a part of?

We often get asked the question "Who should attend MVPDays?" Anyone that has an interest in technology, is eager to learn, and wants to meet other like-minded individuals. This Roadshow is not just for Microsoft MVP's, it is for anyone in the IT Community.

Make sure you check out the MVPDays website at: www.mvpdays.com. You never know, maybe the Roadshow will be coming to a city near you.

This book brings you real world step-by-step guidance from our expert MVP Authors on Microsoft System Center Configuration Manager. These are the same experts you come to see in person at the MVPDays Community Roadshow, and is written in the format of a Step-by-Step learning guide. We really hope you find some immense value in what we have written.

Sample Files

All sample files for this book can be downloaded from www.checkyourlogs.net and www.github.com/dkawula

Additional Resources

In addition to all tips and tricks provided in this book, you can find extra resources like articles and video recordings on our blog http://www.checkyourlogs.net.

Chapter 1

Pre-Requisites

Lab Server Names

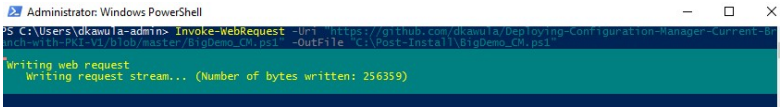
The following table describes the Virtual Machines required to build this lab. This lab is designed to be built on a Hyper-V Host Server with a minimum of 16 GB of RAM. An automation script called **BigDemo_CM.PS1** has been used to provision this lab environment. *A copy of this script can be found in the appendicies.*

Hostname	Role	Operating System
CM01	System Center Configuration Manager 1710 stand alone site server (Running all core Configuration Manager Roles) SQL Server 2016 will be installed locally on the Configruation Manager Server	Windows Server 2016
DC01	Primary Domain Controller running Active Directory Certificate Services as an Enterprise Root	Windows Server 2016
Client01	Configuration Manager Client	Windows Server 2016
Client02	Configuration Manager Client	Windows Server 2016
Router	Windows NAT Router for the lab	Windows Server 2016
DHCP01	DHCP Server for the lab	Windows Server 2016
Management01	Management01	Windows Server 2016

AZHVHost	DS8 Virtual Machine in Azure running Nested Virtualization and Hyper-V. This will be the host that we run the lab on. This could also be a Laptop or physical server in your environment	Windows Server 2016

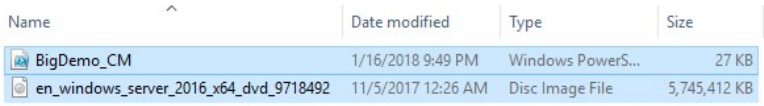
Building the Lab with BigDemo_CM.PS1

For this book, we wanted to help you build a lab that you could easily follow along with. If you have read some of our other books, you would have seen a script that we frequently use, called BigDemo. Basically, BigDemo is a PowerShell script that builds a functional Windows lab environment including: AD, DHCP, Management Servers, Clients, Application Servers, and others. It is highly customizable and we have created a very special edition just for this book. Follow the instructions below to download the script from our Github Repository and start building your very own lab to follow along with.

Instructions	Screenshot (if applicable)
1. Logon to the AZHVHost machine in Azure as Administrator	
2. Open an administrative PowerShell prompt and type:	`Invoke-WebRequest -Uri "https://github.com/dkawula/Deploying-Configuration-Manager-Current-Branch-with-PKI-V1/blob/master/BigDemo_CM.ps1" -OutFile "C:\Post-Install\BigDemo_CM.ps1"` 
3. Next Download a copy of Windows Server 2016 RTM from the Microsoft Eval Center. For our lab we have a drive on our Hyper-V Host F:\	https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016/

Save the ISO to
F:\DCBuild_CM

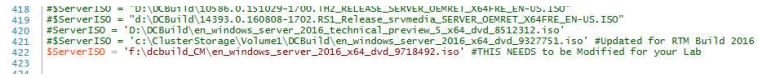
4. Copy **BigDemo_CM.PS1** from **C:\Post-Install** to **F:\BigDemo_CM**



5. Open **BigDemo_CM.PS1** with the **PowerShell ISE** edit lines 425 and 434 putting in **Your Product key received with the EVAL Version of Windows Server 2016** Downloaded above

6. Edit line 422 **$ServerISO** with the actual path and name of your Server ISO Downloaded which should have been downloaded to something like **F:\DCBuild_CM**

   Save **BigDemo_CM.PS1**



7. Open an administrative PowerShell prompt. Run **BigDemo_CM.PS1**

   For this book we have used the following parameters:

   WorkingDir: f:\dcbuild_cm

   Organization: MVPDays Rockstarts

   Owner: Dave Kawula

   TimeZone: Mountain Standard Time

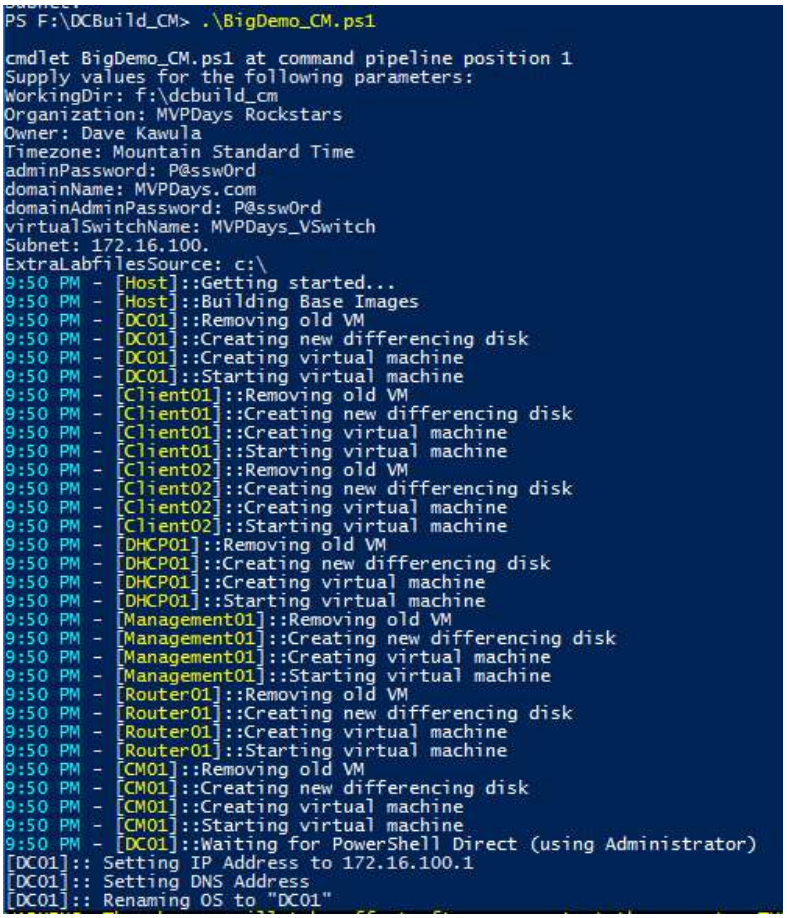
   AdminPassword: P@ssw0rd

   DomainName: MVPDays.com

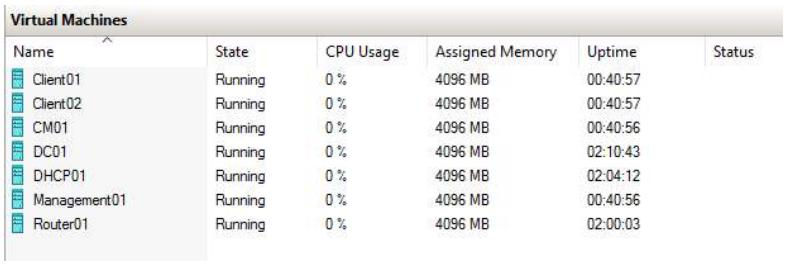
   DomainAdminPassword: P@ssw0rd

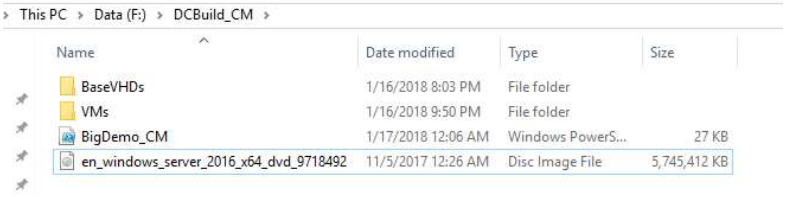
   VirtualSwitchName: MVPDays_VSwitch

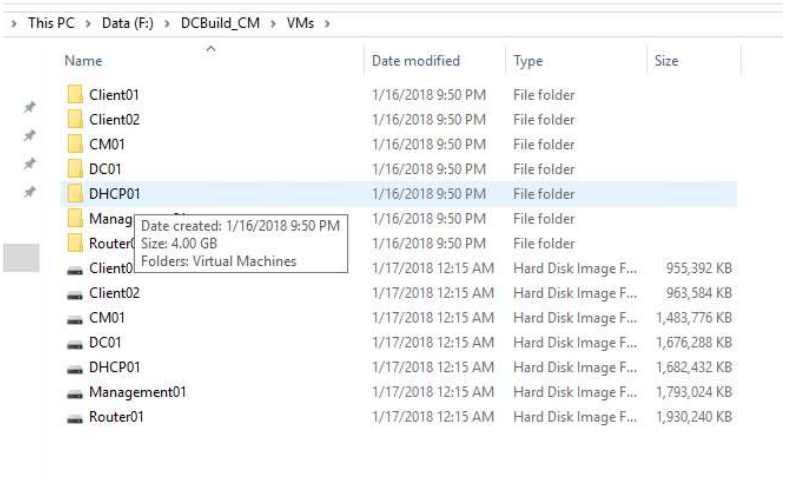
   Subnet: 172.16.100.
   ExtraLabFiles: C:



8. It will take approximately 1 hour to build the Lab Environment





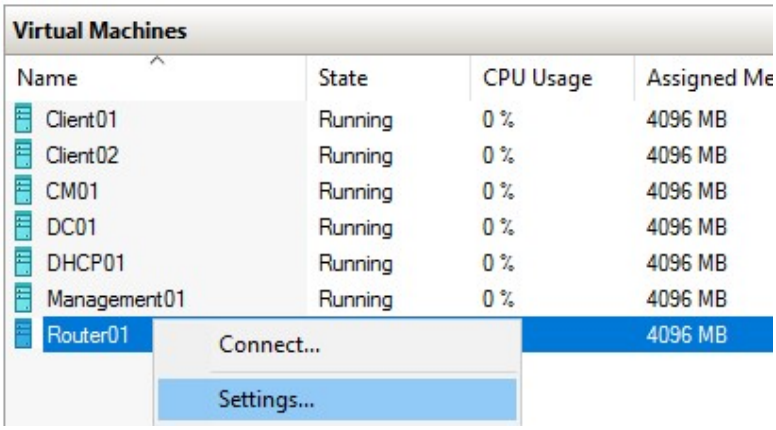


Enable Routing in the Lab

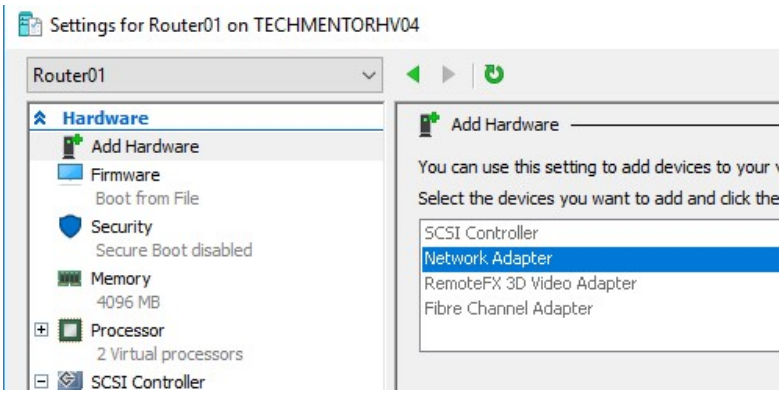
This step-by-step lab guide requires access to the internet for configurations. As the Virtual Machines are on an Internal vSwitch, additional configuration is required on the Hyper-V host in Azure to enable access to the internet. The steps below will create a Gateway IP Address of 192.168.0.1, which will be used by the Router VM to get out to the internet. After the NAT Switch is created, you will modify the DHCP Scope in the lab to point to the IP address of the router, then configure Windows Routing and Remote Access on the router VM.

Instructions	Screenshot (if applicable)
1. Logon to the AZHVHost machine in Azure as Administrator	

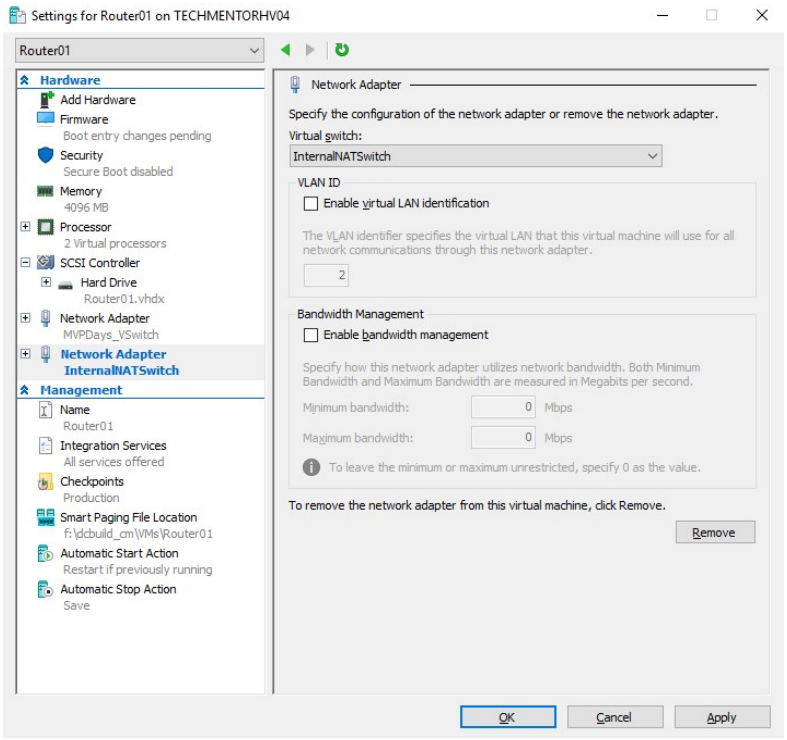
2. Open an administrative PowerShell prompt	`New-VMSwitch -SwitchName "InternalNATSwitch" -SwitchType Internal`
	`Get-NetAdapter`
	`New-NetIPAddress 192.168.0.1 -PrefixLength 24 -InterfaceIndex 23`
	`New-NetNAT -Name "InternalNAT" -InternalIPInterfaceAddressPrefix 192.168.0.0/24`

3. Open the Hyper-V Management Console, Right-Click on **Router01,** and click **Settings**	

4. Click on **Add Hardware**, **Network Adapter,** click **Add**



5. Click the newly added Network Adapter, Click on **Virtual Switch**, and Select **Internal NAT Swtich**, and click **OK**



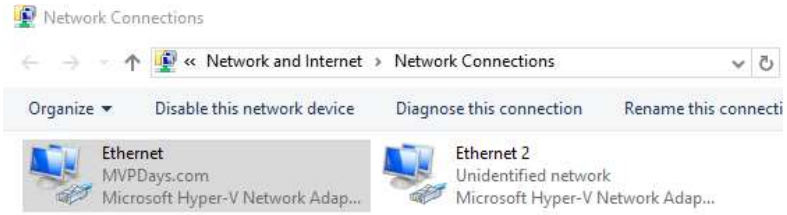
6. Logon to **Router01** with using **Administrator** and a password of **P@ssw0rd**

7. Open an administrative PowerShell prompt and run the command

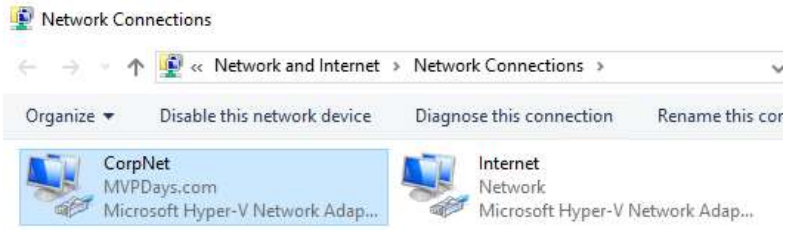
   This will install the Routing and Remote Access Feature

```
Add-WindowsFeature -Name RemoteAccess,Routing,RSAT-RemoteAccess-Mgmt -verbose
```

8. Right-Click **Start**, click **Run,** type **ncpa.cpl**



   Rename the Adapters:
   Ethernet to **Corpnet**
   Ethernet 2 to **Internet**



9. Configure the following IP Address settings:

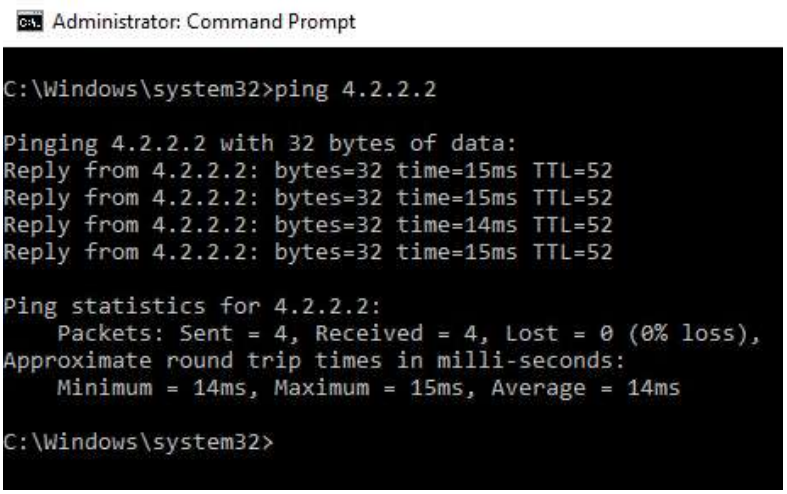
   CorpNet:
   IP = 172.16.100.254
   Subnet = 255.255.255.0
   Gateway = Blank
   DNS = 172.16.100.1

   Internet: 192.168.0.254
   Subnet = 255.255.255.0
   Gateway = 192.168.0.1

10. Open an Administrative Command Prompt, try to ping 4.2.2.2

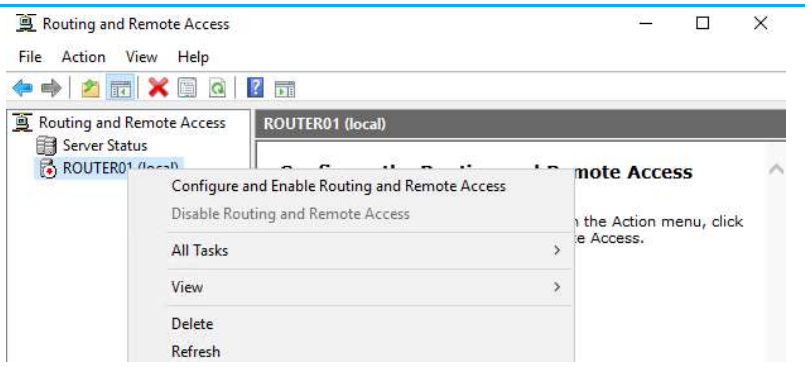
    Ensure that the Router01 VM can ping the internet address by IP prior to continuing

    This validates that the NAT Switch is working properly

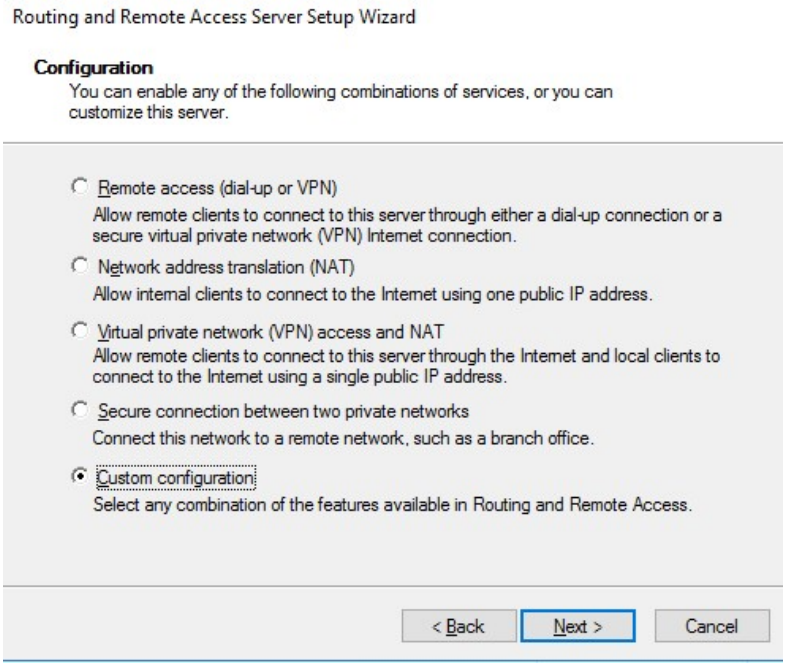


11. Open the **Routing and Remote Access** Management Console

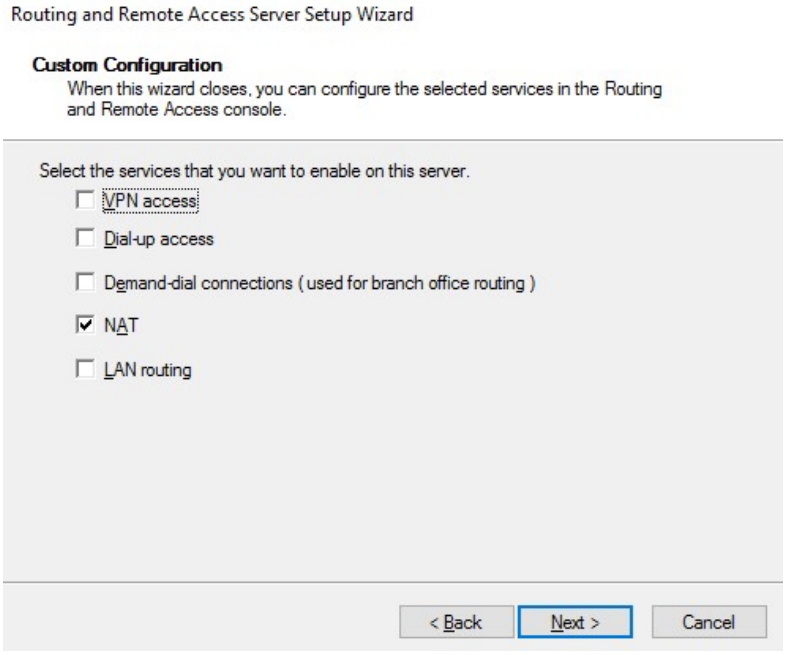
12. Right-Click on **Router01** and click, **Configure and Enable Routing and Remote Access**



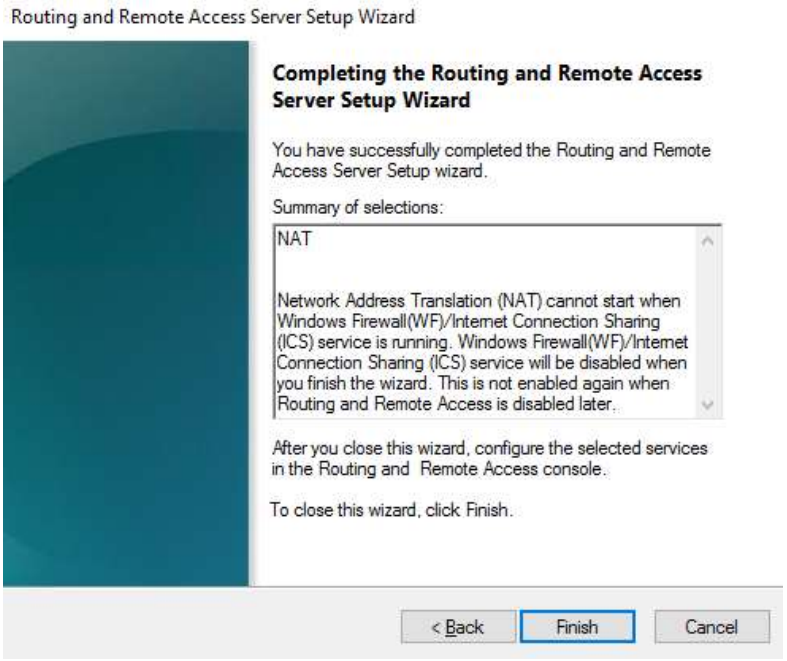
13. On the **Routing and Remote Access Server Setup Wizard** page select **Custom Configuration** and click **Next**



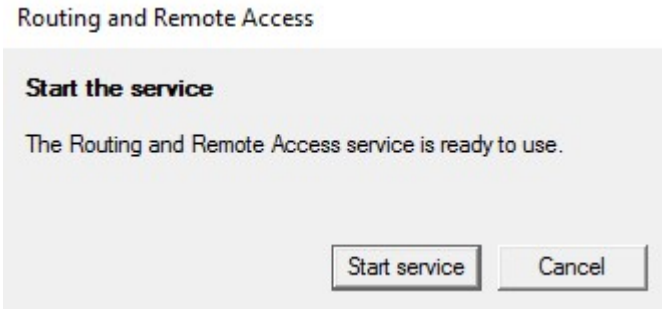
14. On the **Custom Configuraiton** page Select **NAT** and click **Next**



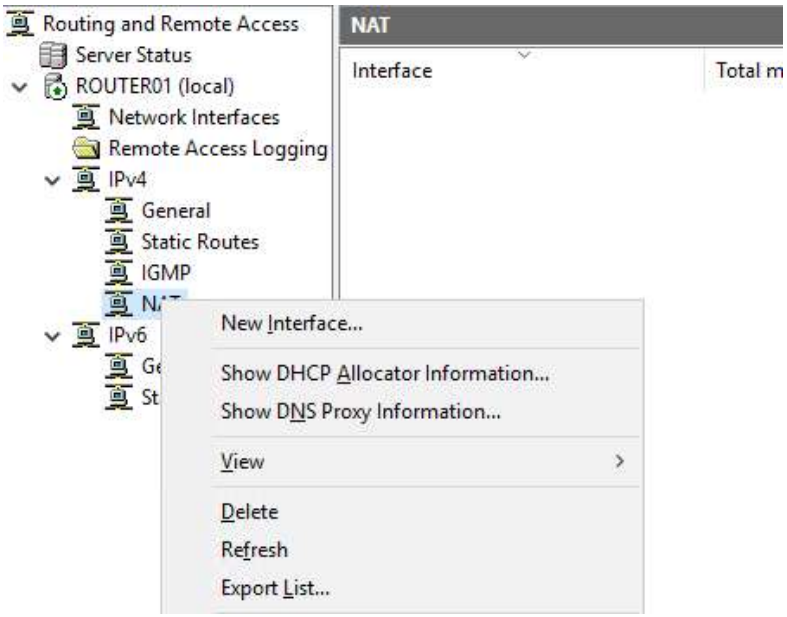
15. On the **Completing the Routing and Remote Access Server Setup Wizard** page click **Finish**



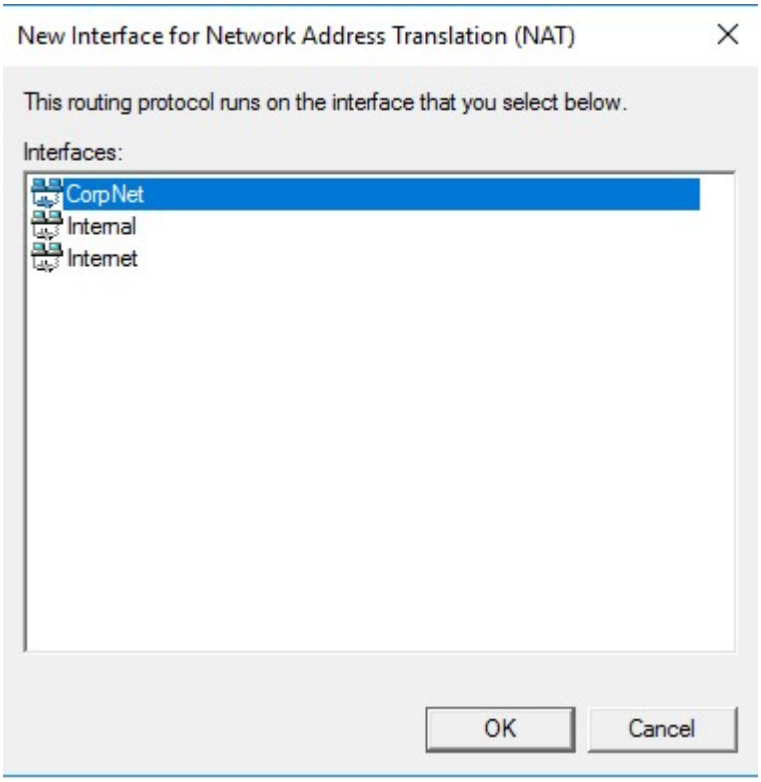
16. When prompted click **Start Service**



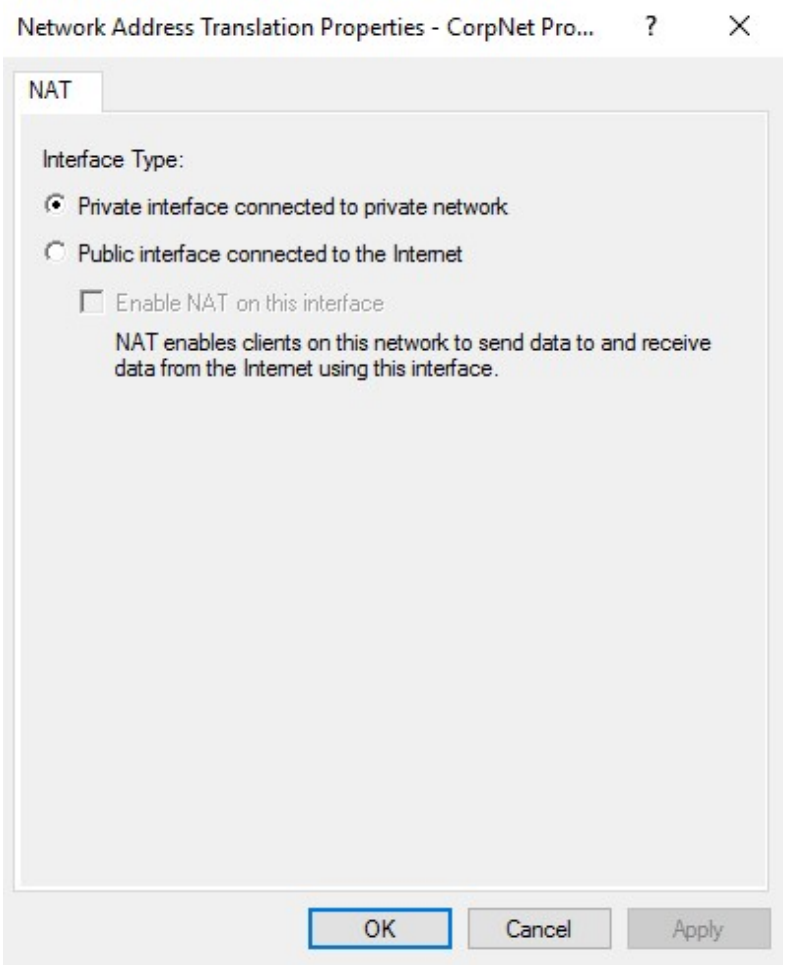
17. In the **Routing and Remote Access** management console, expand **Router01**, **IPv4, NAT**. Then Right-Click **NAT** and click **New Interface…**



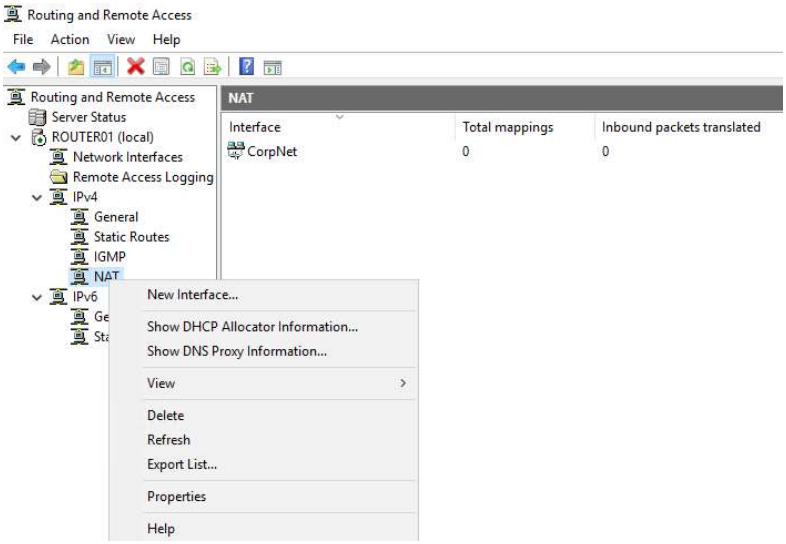
18. Select **CorpNet** and click **OK**



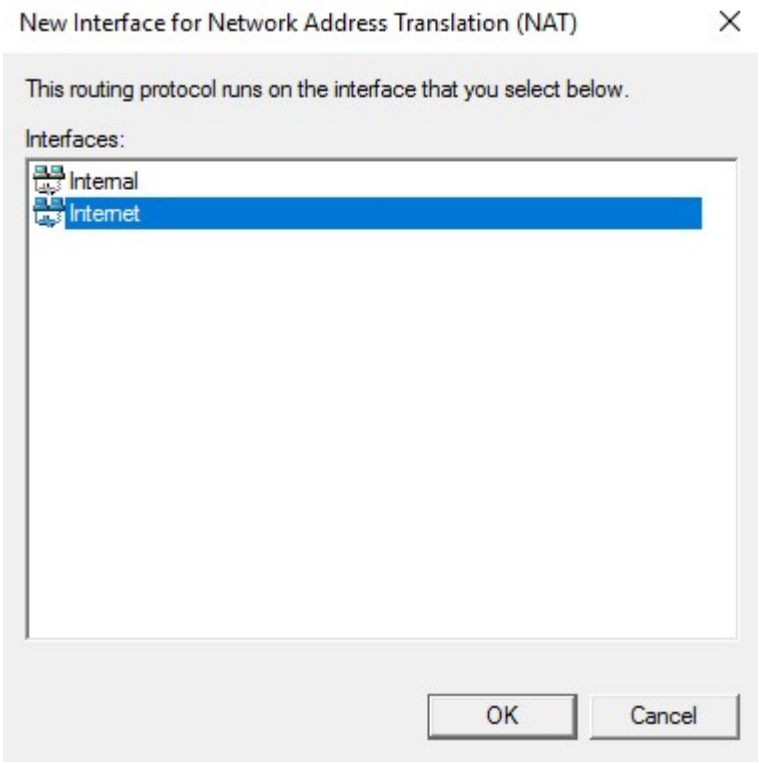
19. On the **NAT** page ensure **Private interface connected to the private network** is selected and click **OK**



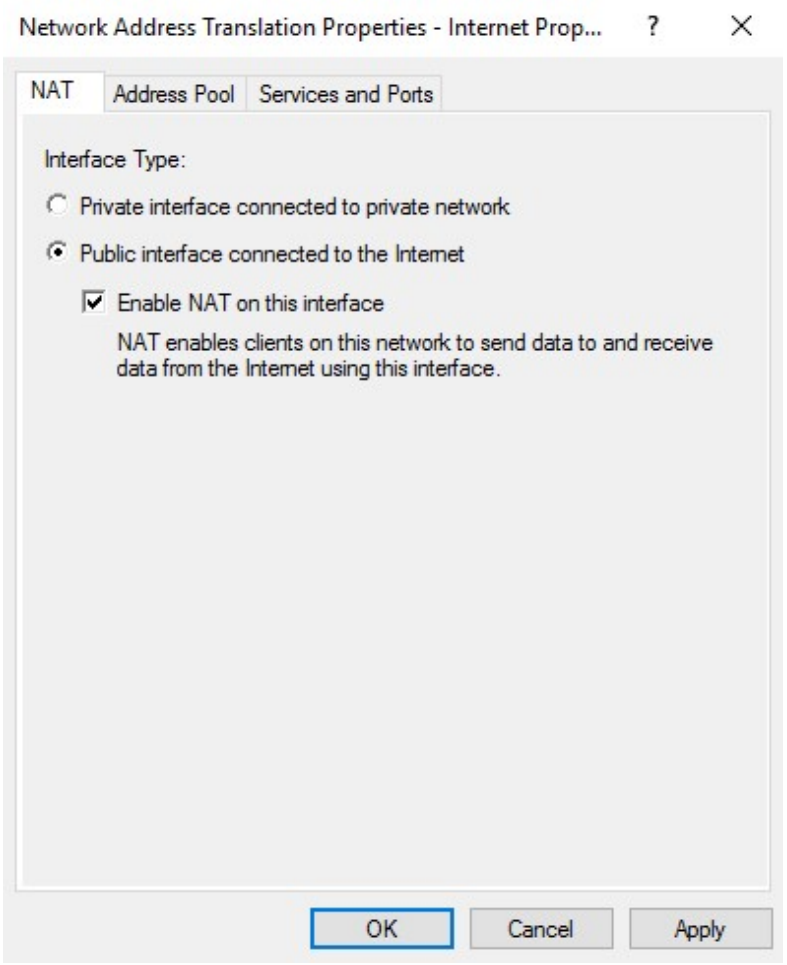
20. In the **Routing and Remote Access** management console, expand **Router01**, **IPv4, NAT**. Then Right-Click **NAT** and click **New Interface…**



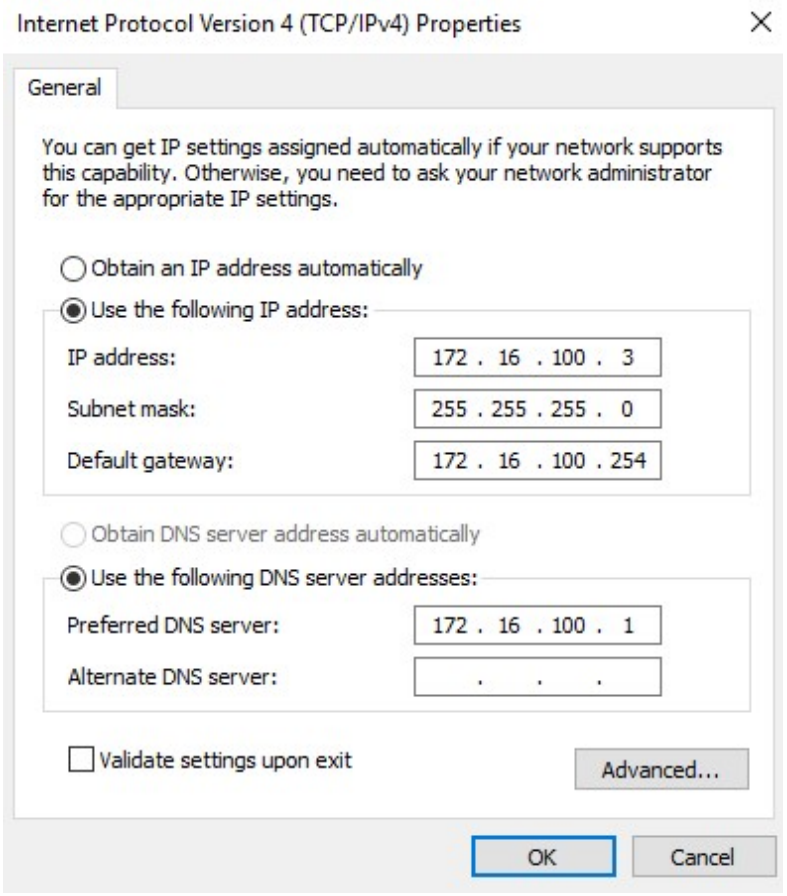
21. Select **Internet** and click **OK**



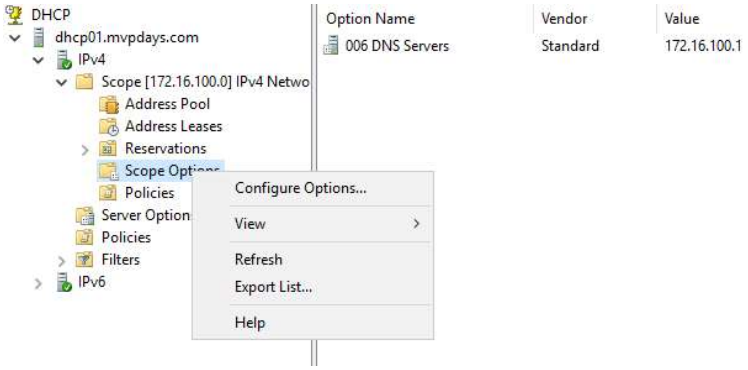
22. On the **NAT** page select **Public Interface connected to the Internet** and select **Enable NAT on this Interface** and click **OK**



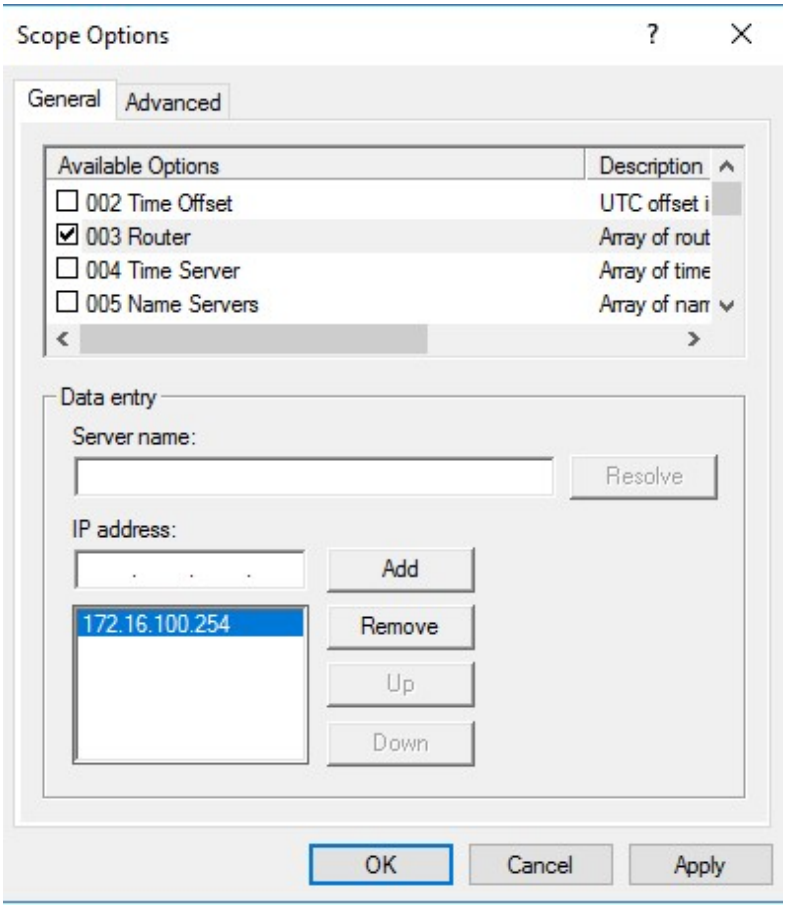
23. Logon to **DHCP01** as **MVPDays\Administrator**
24. Open the Network Control Panel (**NCPA.CPL**) and add a default gateway on the **Ethernet** adapter of 172.16.100.254



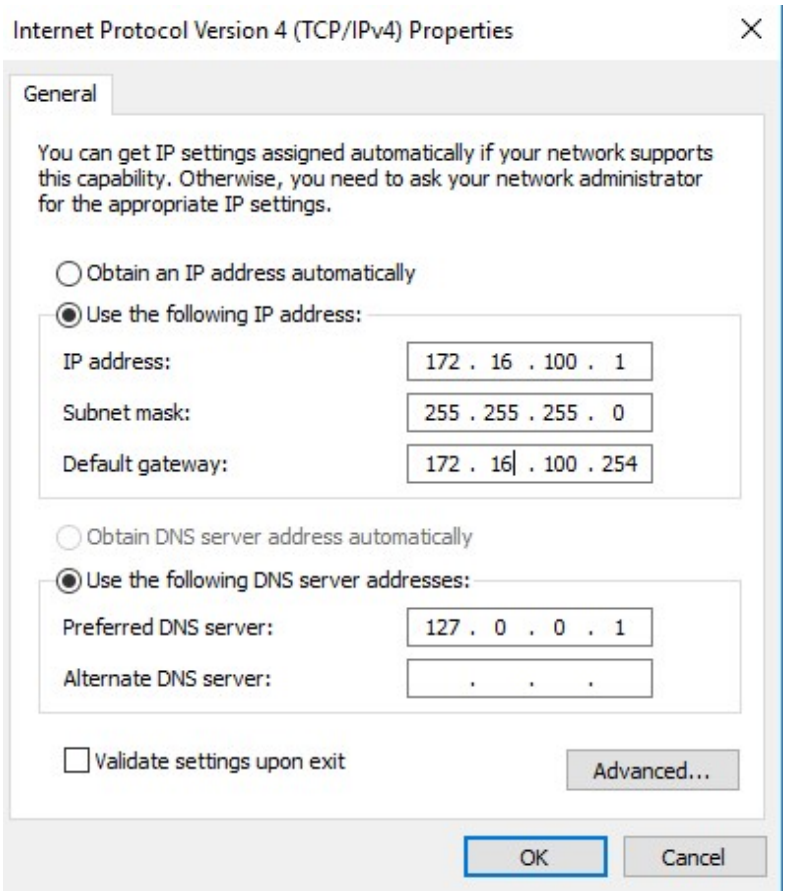
25. Open the **DHCP Management Console (DHCPMGMT.MSC)**
26. Expand **DHCP01, IPv4, Scope (172.16.100.0), Scope Options**
27. Right-Click on **Scope Options** and click **Configure Options**



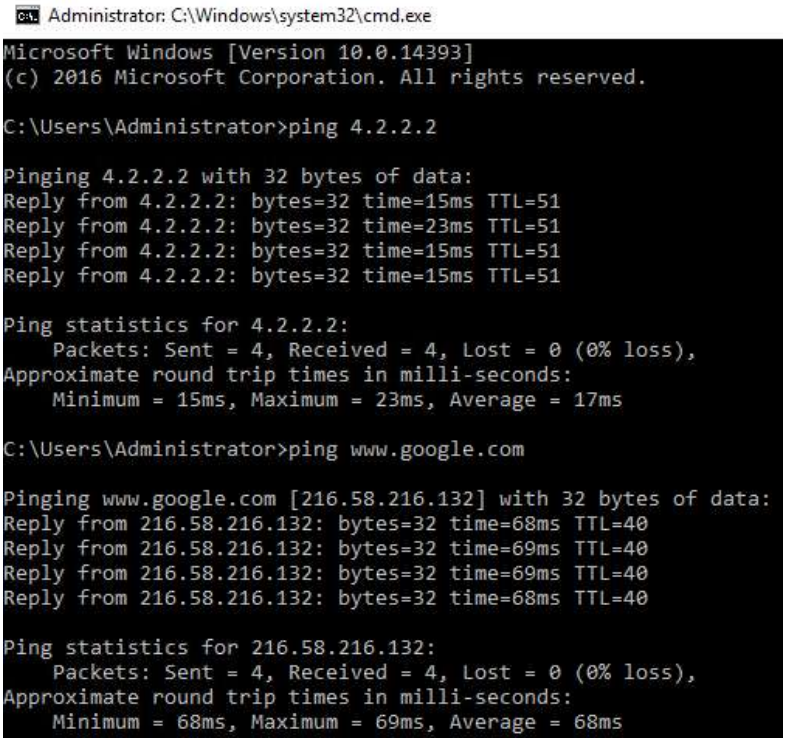
28. Select **003 Router** and in **IP Address** type **172.16.100.254** and click **Add** then click **OK**



29. Logon to **DC01** as **MVPDays\Administrator** and add a **Gateway of** 172.16.100.254 to the **Ethernet Adapter**



30. Open an Administrative command prompt and try pinging: **4.2.2.2** and **www.google.com**



31. Restart the following VM's:
Client01
Client02
Management01
CM01

This will ensure that they all get updated IP addresses from the **DHCP01** Server

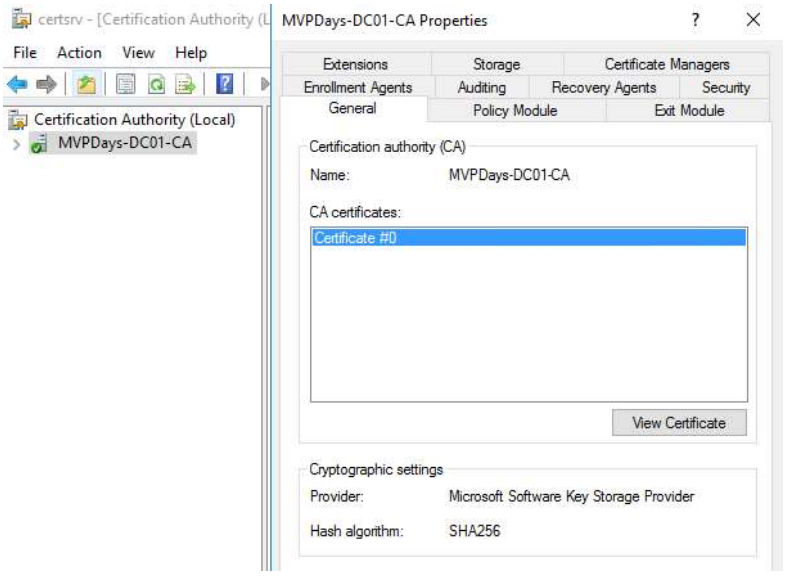
Software Requirements

The following table provides a summary of the Microsoft software that is used in this guide.

Software	Additional Information
System Center Configuration Manger 1702 Volume License Media (Basline Media)	Live In-Console Update will be used to bring Configuraiton manager to 1710 CB
SQL 2016 SP1 Volume License Media	Standard Edition

Configure Certificate Authority to Support SHA256 certificates

In this lab build, an Enterprise Root CA has already been configured on DC01 as part of the BigDemo_CM.PS1 Script. You can validate that the CA is setup for SHA256 certifciate support using the steps below.

Instructions	Screenshot (if applicable)
1. Logon to **DC01** as **MVPDays\Administrator**	
2. Launch the **Certification Authority** console 3. Right-click the *CA server* and select **Properties** 4. Verify the Cryptographic settings provider shows **SHA256** as the hash algorithm	

Create Configuration Manager Groups and Users

The following Global Security groups need to be created in Active Directory prior to installing Configuration Manager. You can add domain users to groups to administer Configuration Manager rather than applying console permissions directly to specific user(s). At minimum, the ConfigMgr Administrators group should be created as we will grant it permissions rights to SQL.

Group	Scope
ConfigMgr Administrators	Full control over Configuration Manager, the hierarchy, and all classes/instances
ConfigMgr Server Managers	Limited to server management functions (servers outside of the ConfigMgr server itself)
ConfigMgr Client Managers	Limited to client management functions

The following two Active Directory user accounts are required for operation of Configuration Manager. They are not required for the installation of Configuration Manager in this guide. You can create these users now, or after the site server is installed.

The first account is a **Client Push Installation Account**. This account is used to push the Configuration Manager client agent to remote computers for installation. This account must be a member of the local administrators group on any computers or servers that will require the client agent to be installed. It is strongly recommended that the Client Push Installation Account does NOT have any other administrator rights in the domain (e.g. do not make it a member of Domain Admins). The Client Push Installation Account can have any account name you desire, based on your naming standards. The account and its password will be required when you are configuring the Configuration Manager site server. The password for this account should not expire.

The second account is the **Network Access Account**. This is a standard domain user account and does not require elevated privileges on any clients or servers. This account is used during OS deployment to connect to NTFS shares while booted in Windows PE. The Network Access Account can have any account name you desire, based on your naming standards. The account

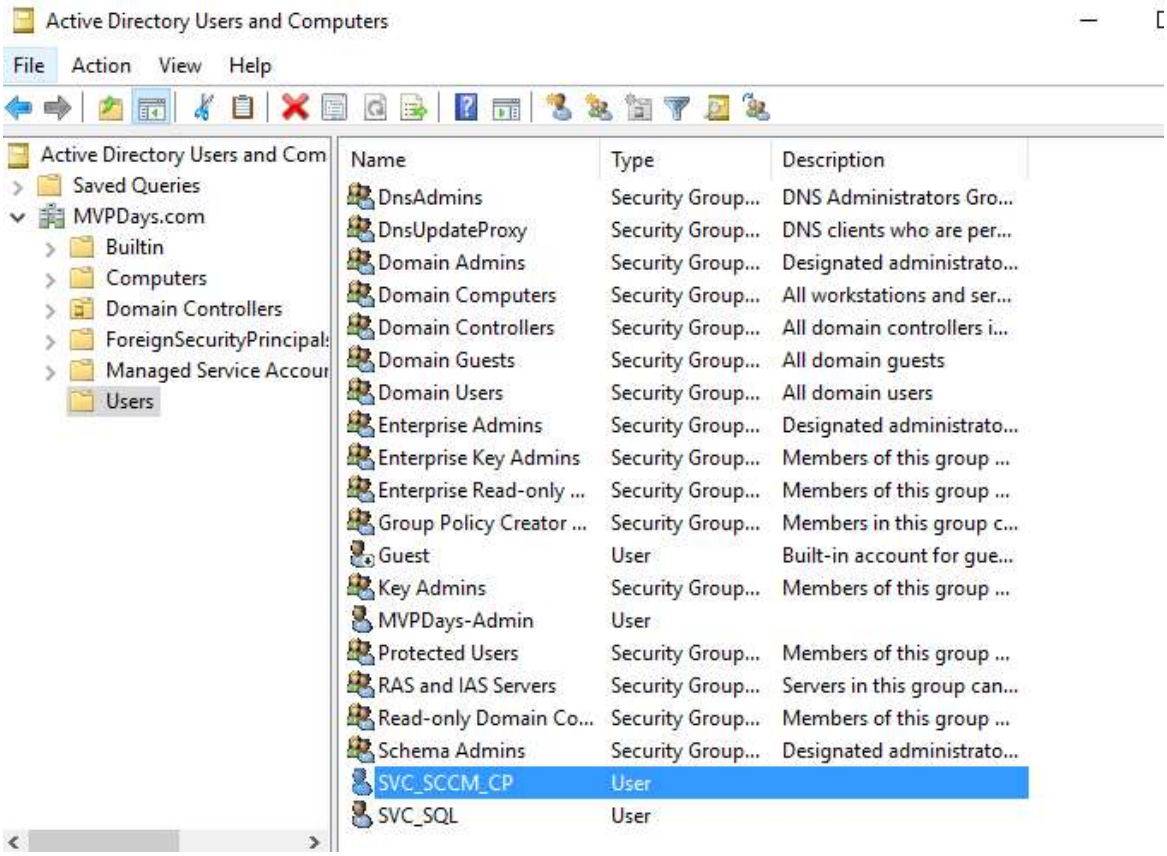
and its password will be required when we are configuring the Configuration Manager site server. The password for this account should not expire.

Configuration Manager Service Accounts Required for Build

The following accounts have automatically been created in Active Directory with the BigDemo.PS1 script. These are the only accounts required for the base installation in our lab for this book.

Service Account / Groups	Scope
svc_SQL	SQL Server Agent / SQL Server Database Engine / SQL Server Reporting Services are running from this account
SVC_SCCM_CP	SCCM Client Push Installation Account. This Account must be made a member of the local administrators group on each machine.

Config Manager Service Accounts for ADDS Domain



Chapter 2

Configuring PKI for Configuration Manager Current Branch

Create and Issue Web Certificates

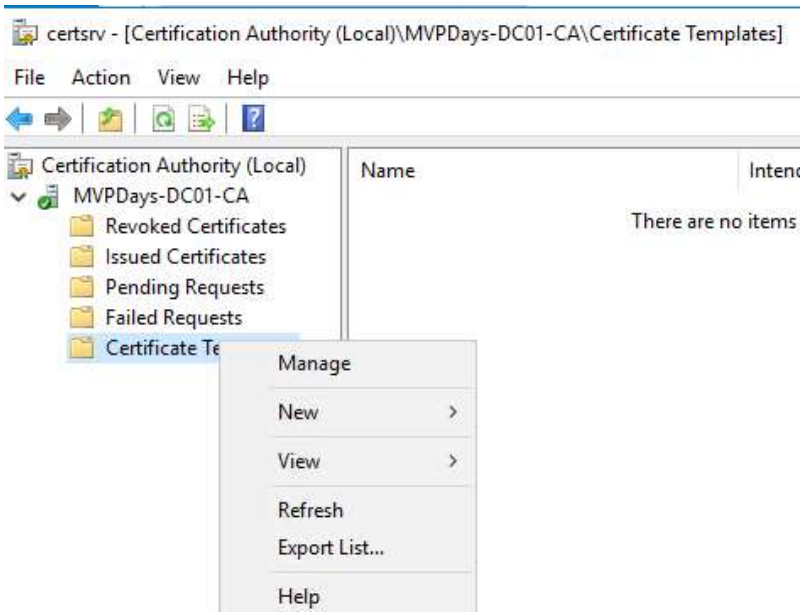
In order to configure Configuration Manager clients to communicate securely with the Configuration Manager servers, certificate based authentication must be used. To configure the required PKI infrastructure, we will use an Enterprise Root CA that has been configured by the BigDemo_CM.PS1 script. It is simply a base install of the Root CA and the single line of PowerShell used to configure it, and can be found inside the build script

Traffic to and from the clients can either run on port 80 (HTTP) or port 443 (SSL). If you do not wish to use secured communication, you can skip all the steps in this chapter and proceed with the installation of Configuraiton Manager.

Instructions	Screen shot (if applicable)
1. Logon to **DC01 and MVPDays\Administrator**	
2. The first certificate is for site systems that run Internet Information Services (IIS) and that are configured for HTTPS client connections. This	

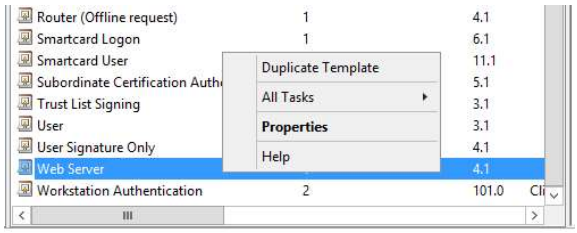
	is the Configuration Manager primary site server
This certificate is a Web Server certificate, with Enhanced Key Usage of Server Authentication. The Subject Name or Subject Alternative Name must contain the intranet FQDN of the server. Use SHA-2 hash algorithm (if the CA has been upgraded to support SHA-2)	
3. Launch the **Certification Authority**	

4. Expand **Certificate Server> → Certificate Templates, right-click Certificate Templates** and select **Manage**

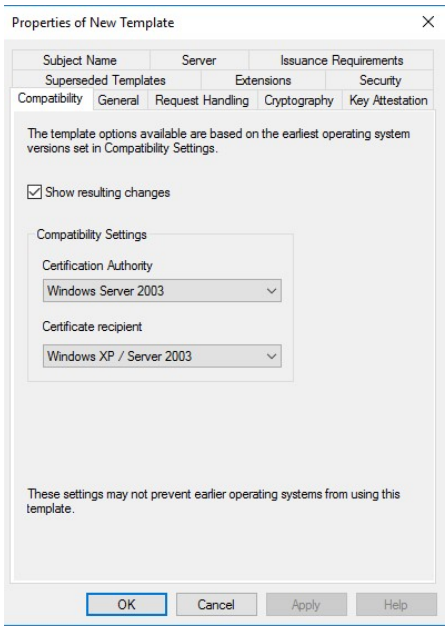


5. Scroll down and locate the **Web Server** certificate

6. Right-click **Web Server** and select **Duplicate Template**

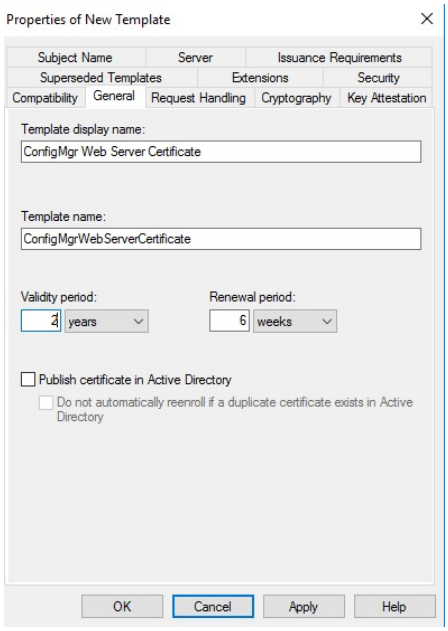


7. On the Compatibility tab verify CA is set to **Windows Server 2003** and Certificate recipient is **Windows XP / Server 2003**



8. Select the **General** Tab

9. Change the *Template Display Name* to **ConfigMgr Web Server Certificate**

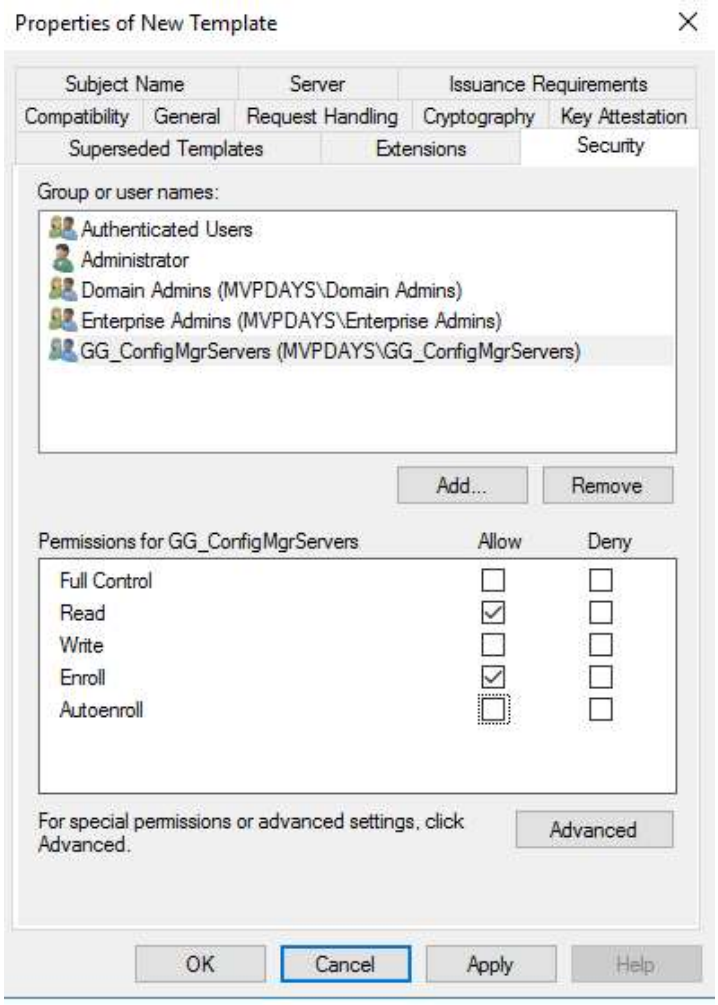


10. Select the **Security** tab

11. Remove the **Enroll** permissions from the security groups **Domain Admins** and **Enterprise Admins**

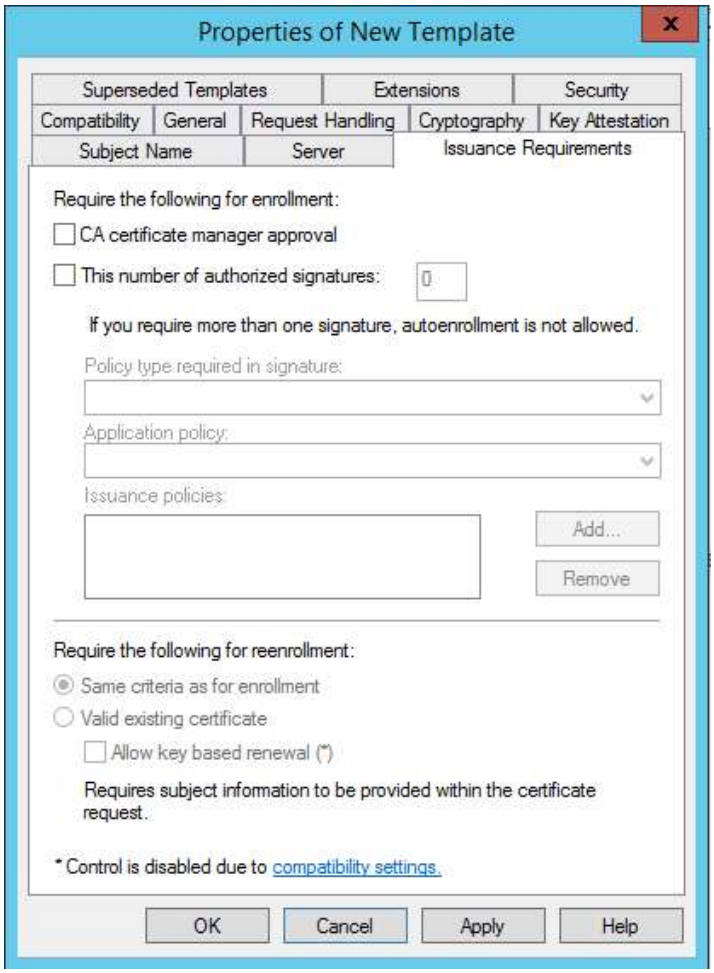
12. Add the computer account for the Configuration Manager site server and grant the **Read** and **Enroll** permission

    NOTE: If a group for enrolling in SSL certificates already exists in AD you can use the group for Read/Enroll permissions instead of the site server computer account. Simply add the computer account of the site server to the group before beginning this process

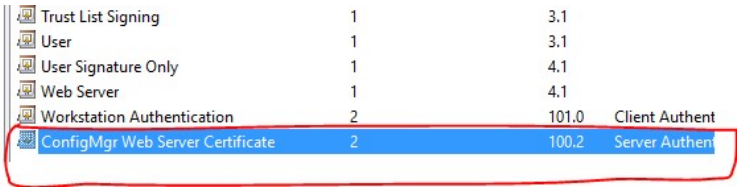


13. Select the **Issuance Requirements** tab

14. If desired, additional controls can be put in place to limit the ability to enroll in this certificate

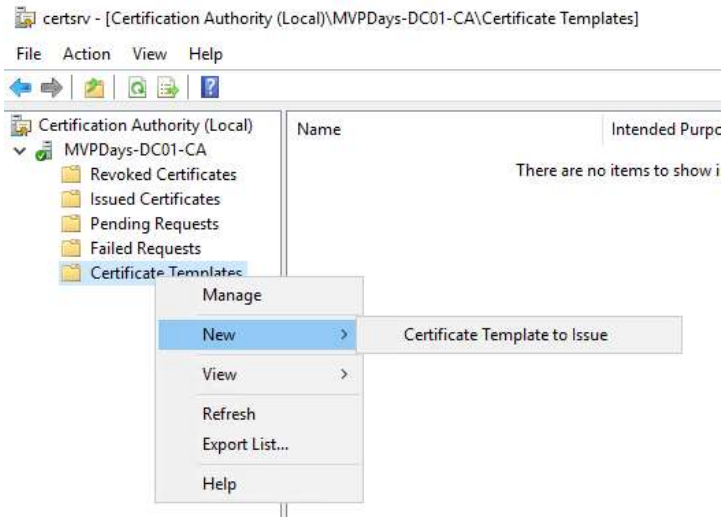


15. Select **OK** to save this new certificate template

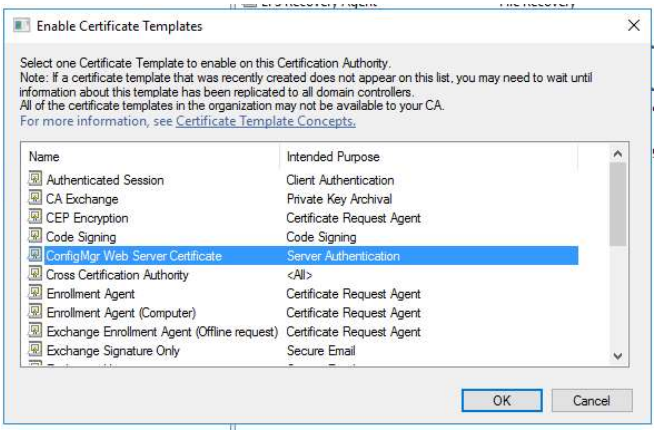


16. Close the Certificate Template Console

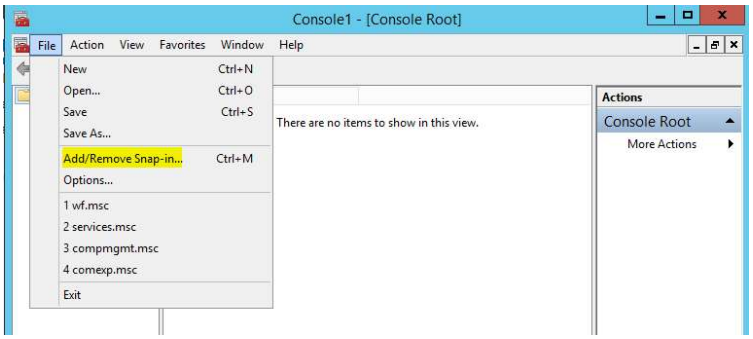
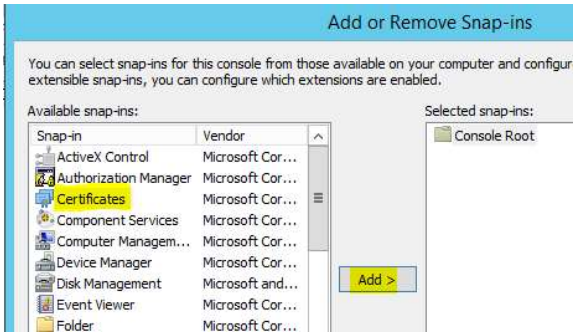
17. **Right-click** the Certificate Templates folder, click **New**, select **Certificate Template to Issue**



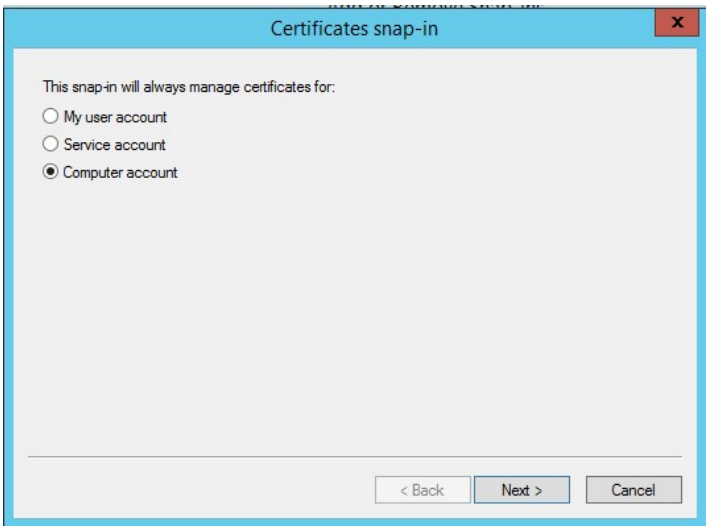
18. Select the template you just created in the **Enable Certificate Templates** wizard screen



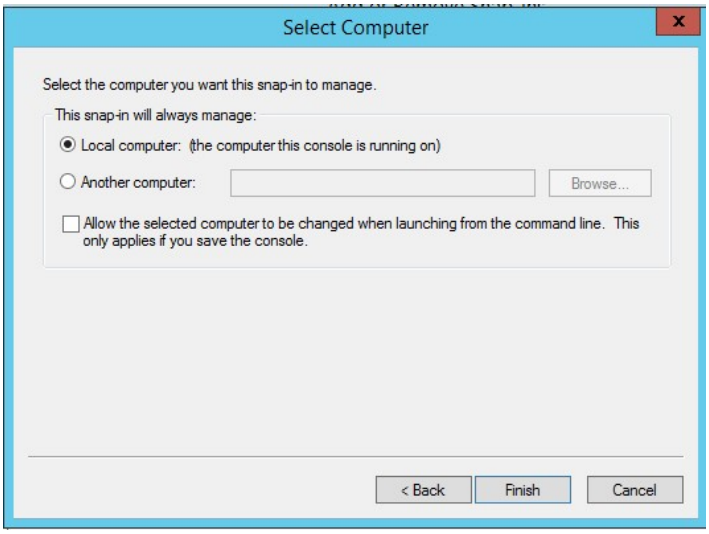
Enroll Web Certificate on the site server

	Instructions	Screen shot (if applicable)
1.	Log onto **CM01** with **MVPDays\Administrator**	
2.	Click **Start**, click **Run**, and type **mmc.exe**. In the empty console, click **File**, and then click **Add/Remove Snap-in**	
3.	In the **Add or Remove Snap-ins** dialog box, select **Certificates**, click **Add**	

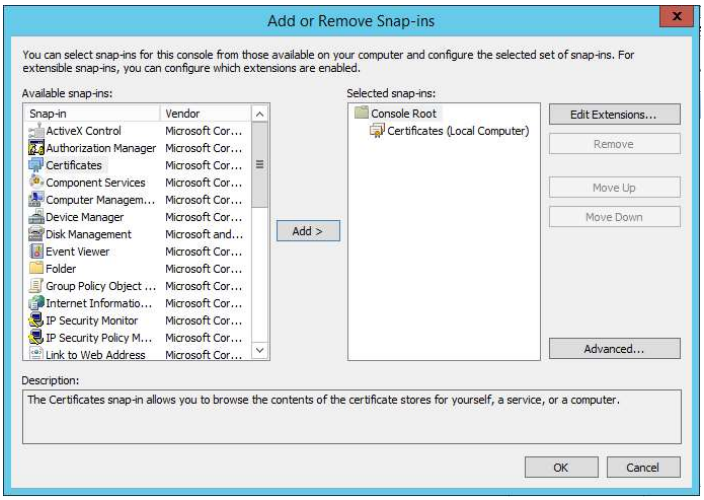
4. In the **Certificate snap-in** dialog box, select **Computer account**, and then click **Next**



5. In the **Select Computer** dialog box, ensure **Local computer: (this computer this console is running on)** is selected, then click **Finish**

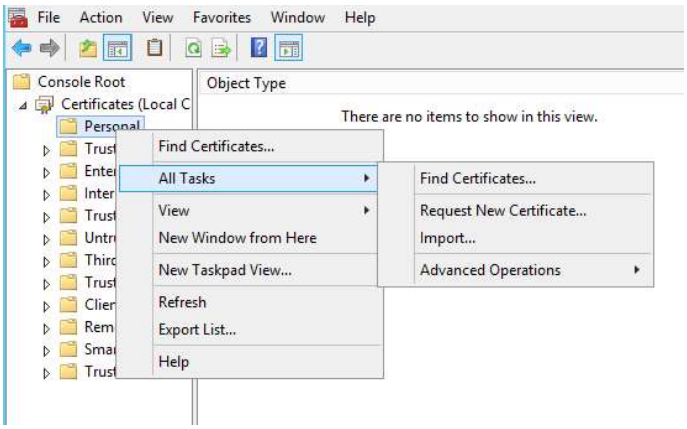


6. In the **Add or Remove Snap-ins** dialog box, click **OK**



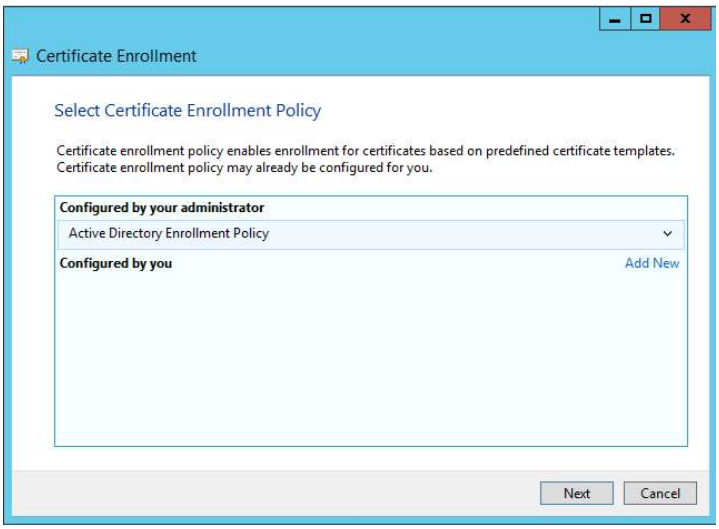
7. In the console, expand **Certificates (Local Computer)**, and then click **Personal**

8. Right-click **Certificates,** click **All Tasks**, and then click **Request New Certificate**

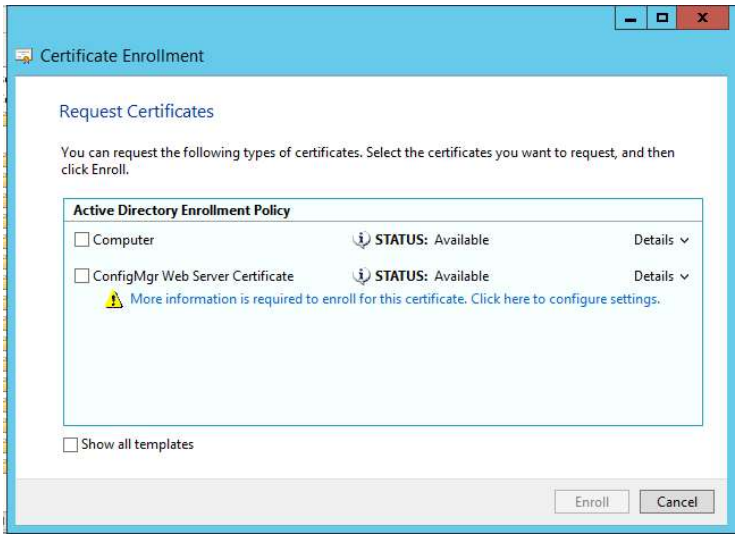


9. On the **Before you Begin** page, click **Next**

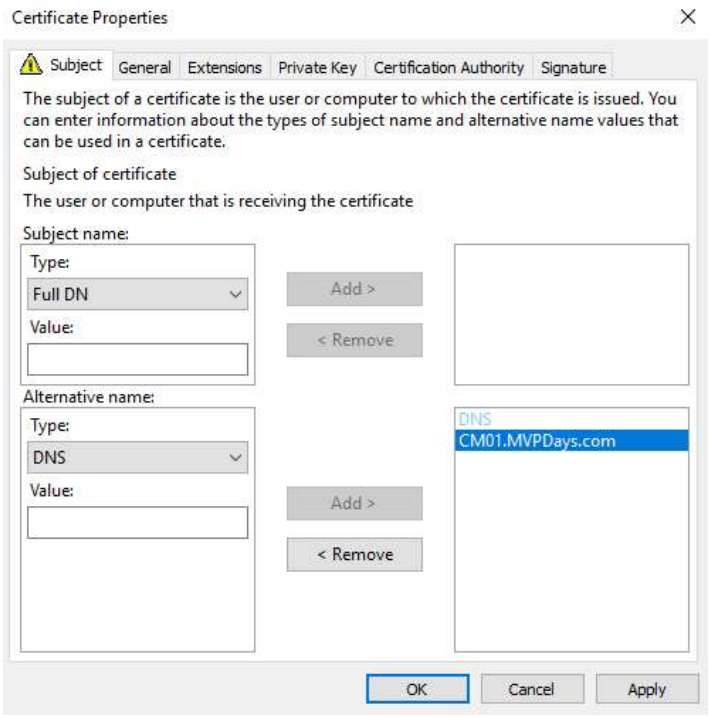
10. If you see the **Select Certificate Enrollment Policy** page, click **Next**



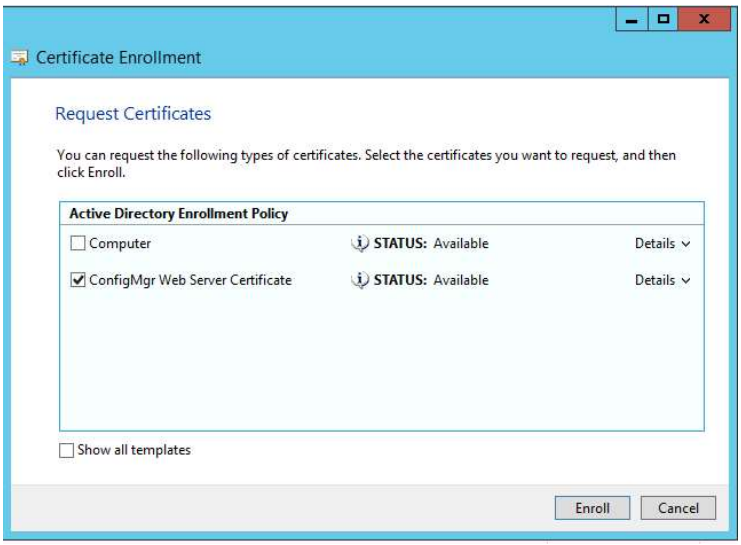
11. On the **Request Certificates** page, identify the **ConfigMgr Web Server Certificate** from the list of displayed certificates, and then click **More information is required…**



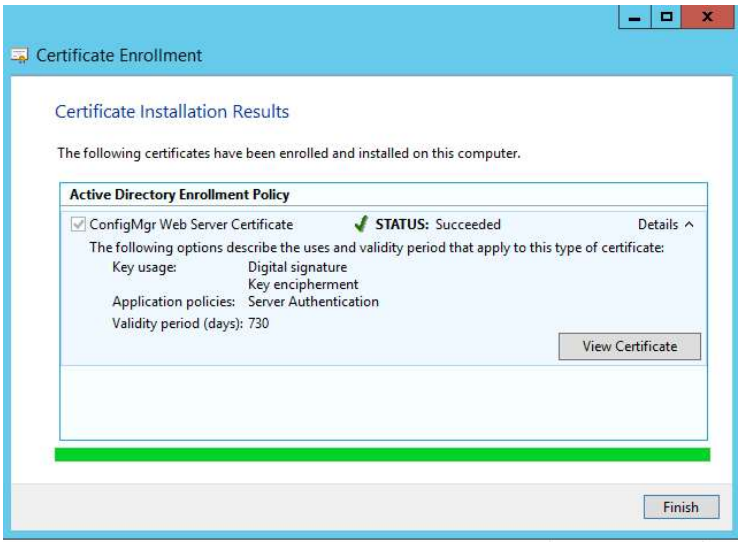
12. On the **Subject** tab under **Alternative name**: Select **DNS** for type and for **Value**: put in the Intranet FQDN of the site server and click **Add**



13. On the **Request Certificates** page, select **ConfigMgr Web Server Certificate** from the list of displayed certificates, and then click **Enroll**



14. On the **Certificates Installation Results** page, wait until the certificate is installed, and then click **Finish**



Create and Issue Windows Client Certificate

This certificate deployment has the following procedures:

- Create and issue the Workstation Authentication certificate template on the Certification Authority
- Configure auto-enrollment of the Workstation Authentication template by using Group Policy
- Automatically enroll the Workstation Authentication certificate and verify its installation on computers

Client communication to site system roles is secured by using either self-signed or PKI certificates. You'll need to use a PKI certificate for computer clients that Configuration Manager detects to be on the internet, and for mobile device clients. The PKI certificate uses HTTPS to secure the client endpoints. The site system roles that clients connect to can be configured for either HTTPS or HTTP client communication. Client computers always communicate by using the most secure method that is available. Client computers only fall back to using the less secure communication method of HTTP on the intranet if you have site systems roles that allow HTTP communication.

When a client is attempting to find servers that host site system roles, it uses service location to find a site system role that supports the client's protocol (HTTP or HTTPS). By default, clients use the most secure method available to them. Consider the following:

To use HTTPS, you must have a public key infrastructure (PKI) and install PKI certificates on clients and servers.

When you deploy a site system role that uses Internet Information Services (IIS) and supports communication from clients, you must specify whether clients connect to the site system by using HTTP or HTTPS. If you use HTTP, you must also consider signing and encryption choices.

Note: When you use PKI certificates for client communication in Configuration Manager, install the fallback status point before you install the clients.

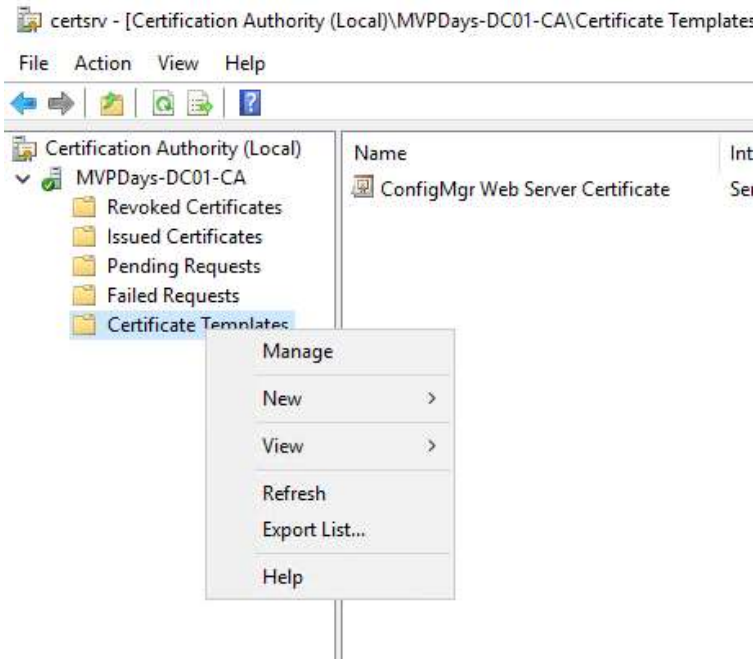
If Configuration Manager site systems do not accept HTTP client communication, you might not know that clients are unmanaged because of PKI-related certificate issues. However, if clients are

assigned to a fallback status point, these certificate issues are reported by the fallback status point.

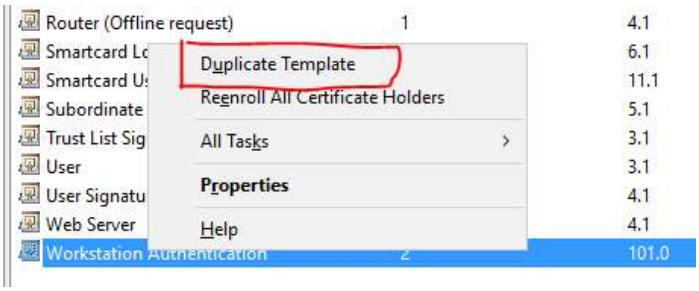
For security reasons, you cannot assign a fallback status point to clients after they are installed. Instead, you can assign this role only during client installation.

Create and issue the Workstation Authentication certificate template on the Certification Authority

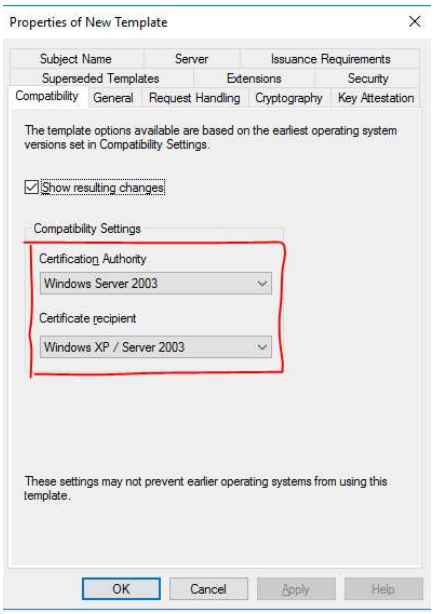
This procedure creates a certificate template for the Configuration Manager client computers and adds it to the Certification Authority. An auto-enrollment Group Policy can be configured to automatically deploy the Certificate to clients in Active Directory.

Instructions	Screenshot (if applicable)
1. On the member server that is running the Certification Authority console, right-click **Certificate Templates**, 2. Then choose **Manage** to load the Certificate Templates management console	 

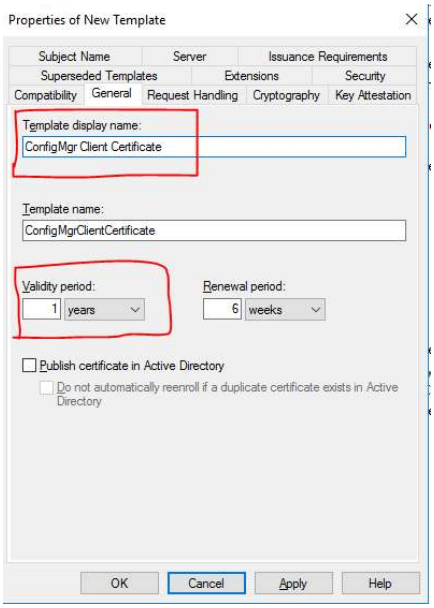
3. In the results pane, right-click the entry that has **Workstation Authentication** in the **Template Display Name** column, and then choose **Duplicate Template**



4. In the **Duplicate Template** dialog box, ensure that **Windows 2003 Server, Enterprise Edition** is selected, and then choose **OK**

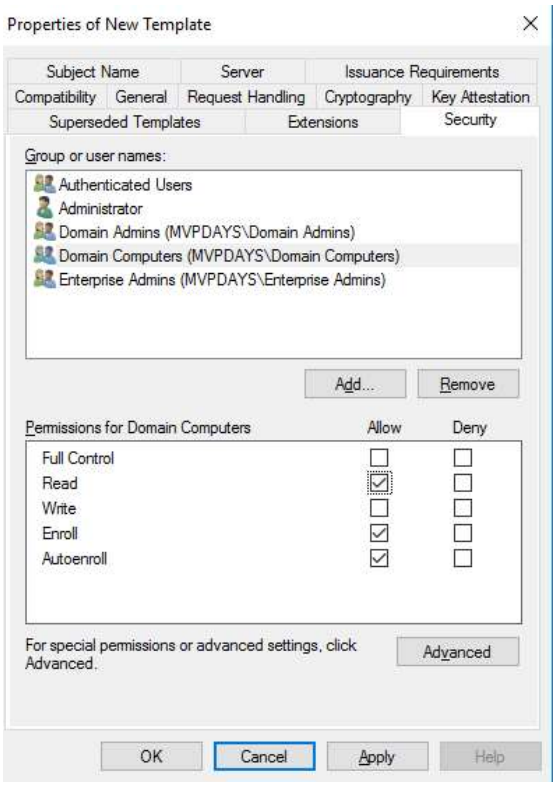


5. In the **Properties of New Template** dialog box, on the **General** tab, enter a template name, like **ConfigMgr Client Certificate**, to generate the client certificates that will be used on Configuration Manager client computers

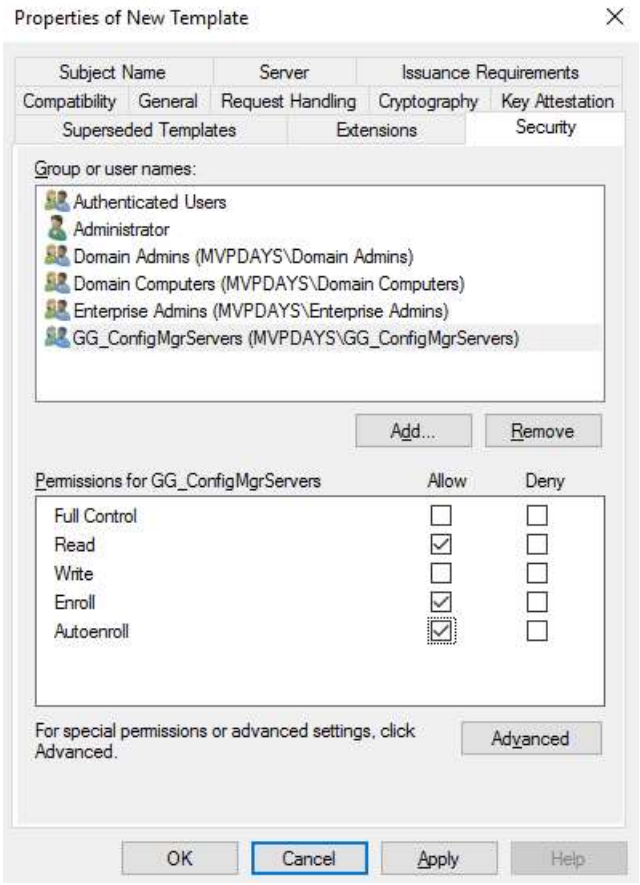


   Review the Validity Period 1 Year is the default. If the machines are set to automatically renew this won't be an issue. If they are not configured for Automatic Renewal you might want to consider extending this time

6. Choose the **Security** tab, select the **Domain Computers** group, and then select the additional permissions of **Read** and **Autoenroll**. Do not clear **Enroll**

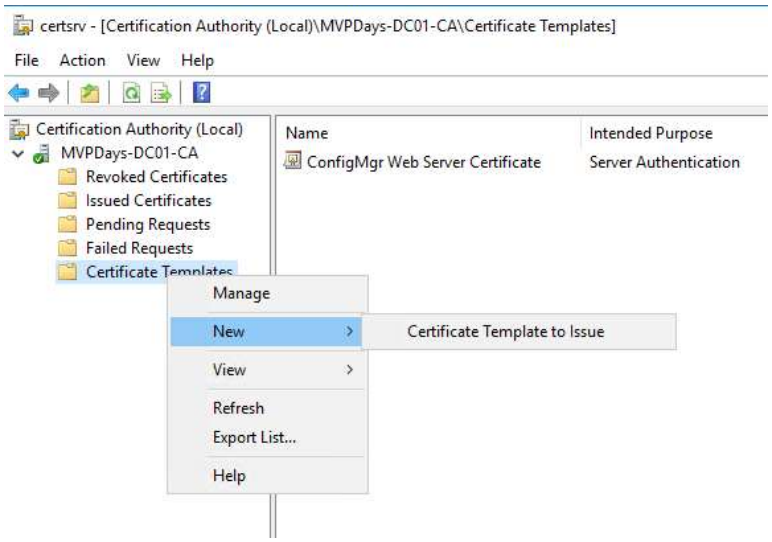


7. Add **GG_ConfigMgrServers** and grant it **Read, Enroll,** and **Autoenroll**

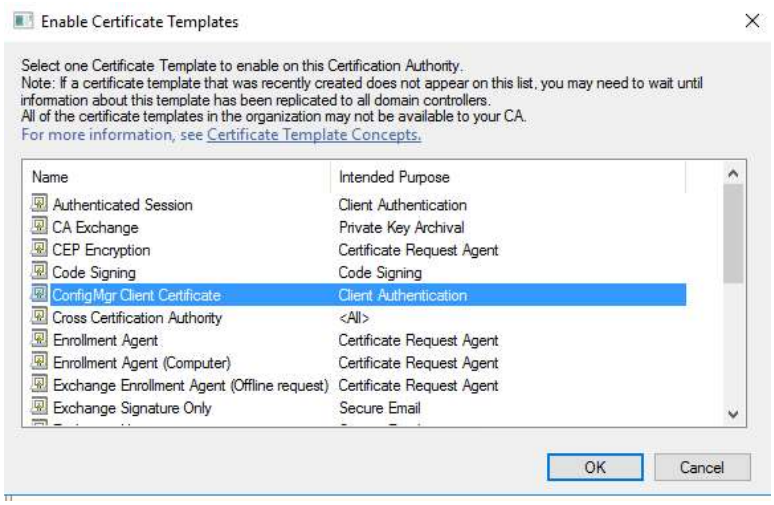


8. Choose **OK**, and then close **Certificate Templates Console**

9. In the **Certification Authority** console, right-click **Certificate Templates**, choose **New**, and then choose **Certificate Template to Issue**

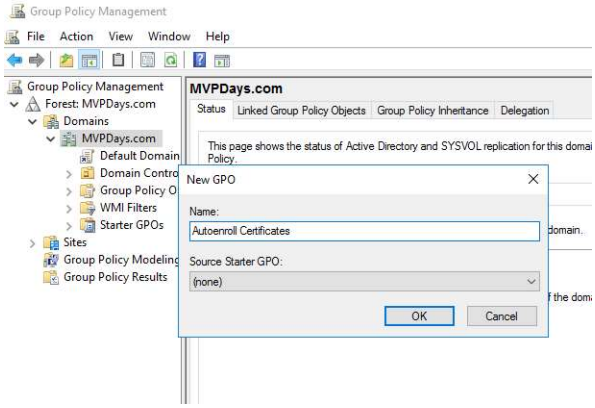


10. In the **Enable Certificate Templates** dialog box, choose the new template that you just created**, ConfigMgr Client Certificate**, and then choose OK

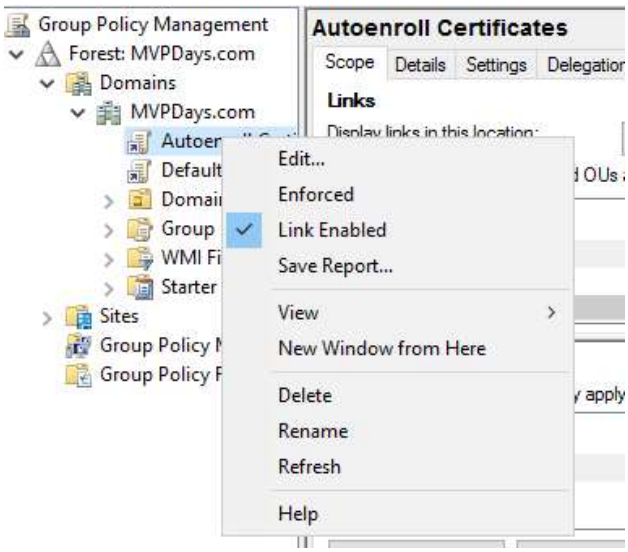


Configure Autoenrollment of the Workstation Authentication Template by using Group Policy

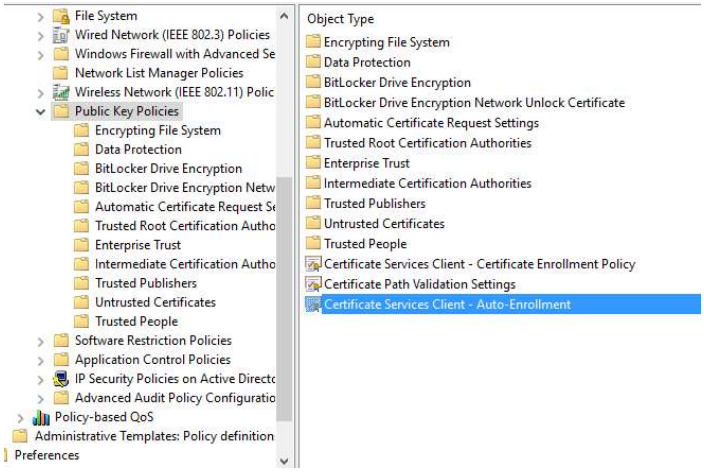
This procedure sets up Group Policy to autoenroll the client certificate on computers.

Instructions	Screenshot (if applicable)
1. On the domain controller, choose **Start**, choose **Administrative Tools**, and then choose **Group Policy Management**	
2. Go to your domain, right-click the domain, and then choose **Create a GPO in this domain, and Link it here**	
3. In the **New GPO** dialog box, enter a name, like **Autoenroll Certificates**, for the new Group Policy, and then choose **OK**	

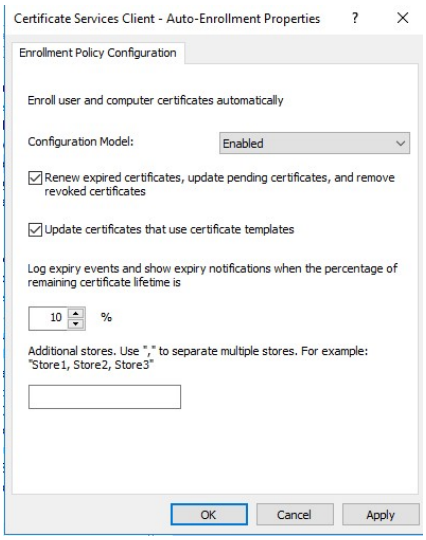
4. In the results pane, on the **Linked Group Policy Objects** tab, right-click the new Group Policy, and then choose **Edit**



5. In the **Group Policy Management Editor**, expand **Policies** under **Computer Configuration**, and then go to **Windows Settings / Security Settings / Public Key Policies**
6. Right-click the object type named **Certificate Services Client - Auto-enrollment**, and then choose **Properties**



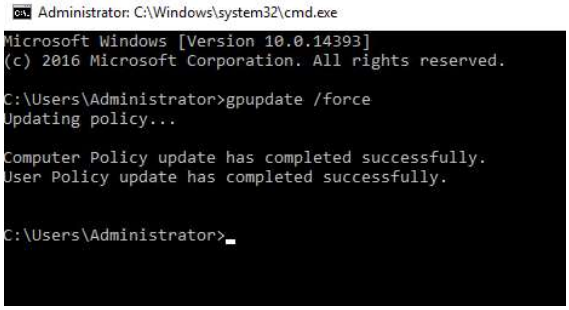
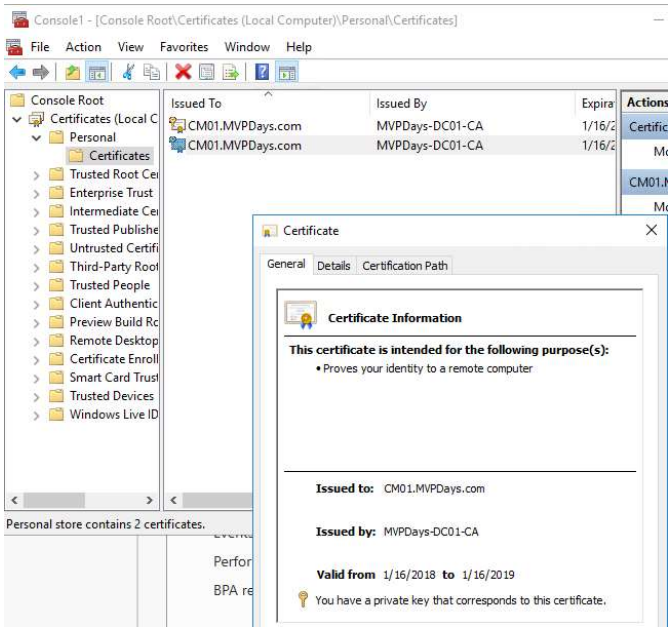
7. From the Configuration Model drop-down list, choose **Enabled**, choose **Renew expired certificates, update pending certificates, remove revoked certificates,** choose **Update certificates that use certificate templates**, and then choose **OK**



8. Close Group Policy Management

Automatically enroll the Workstation Authentication certificate and verity its installation on computers

This procedure installs the client certificate on computers and verifies the installation.

Instructions	Screenshot (if applicable)
1. Logon to a Server that is joined to the **ADS Domain** and run **GPUpdate / Force**	
2. In the search box, enter **mmc.exe**., and then press **Enter** 3. In the empty management console, choose **File**, and then choose **Add/Remove Snap-in** 4. In the console, expand **Certificates (Local Computer),** expand **Personal,** and then choose **Certificates** 5. In the results pane, confirm that a certificate has **Client Authentication** in the **Intended Purpose** column, and that **ConfigMgr Client**	

	Certificate is in the **Certificate Template** column
6.	Close **Certificates (Local Computer)**

Deploy the Client Certificate to Distribution Points

This certificate can also be used for media images that do not use PXE boot, because the certificate requirements are the same.

This certificate deployment has the following procedures:

- **Create and issue a custom Workstation Authentication certificate template on the Certification Authority**
- **Request the custom Workstation Authentication certificate**
- **Export the client certificate for distribution points**

Create and issue a custom Workstation Authentication certificate on the Certificate Authority

This procedure creates a custom certificate template for Configuration Manager Distribution Points, so that the private key can be exported and added to the certificate template in the Certificate Authority.

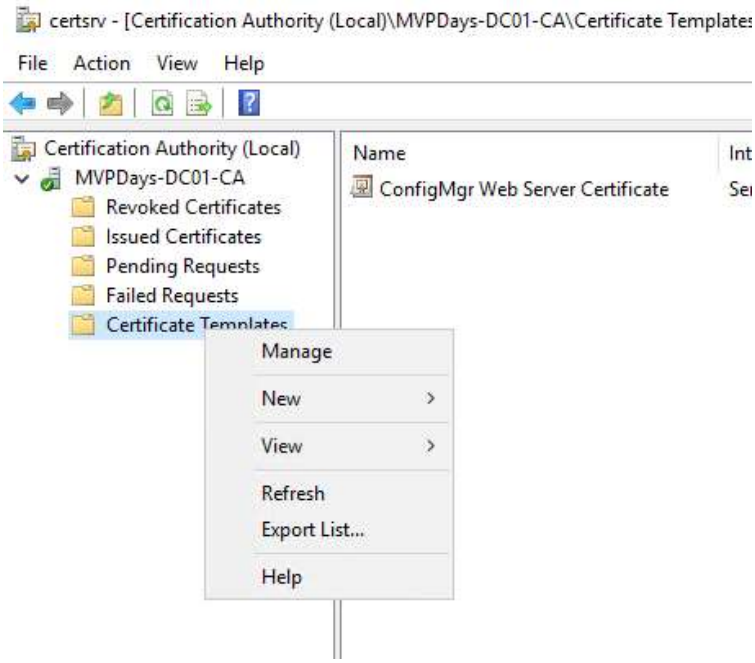
This procedure uses a different certificate template from the certificate template that you created for client computers. Although both certificates require client authentication capability, the certificate for distribution points requires that the private key is exported. As a security best practice, do not set up certificate templates so the private key can be exported unless this configuration is required. The distribution point requires this configuration because you must import the certificate as a file rather than choose it from the certificate store.

When you create a new certificate template for this certificate, you can restrict the computers that can request a certificate whose private key can be exported. In our example deployment, this will be the security group that you previously created for System Center Configuration Manager site system servers that run IIS. On a production network that distributes the IIS site system roles, consider creating a new security group for the servers that run distribution points so that you can restrict the certificate to just these site system servers. You might also consider adding the following modifications for this certificate:

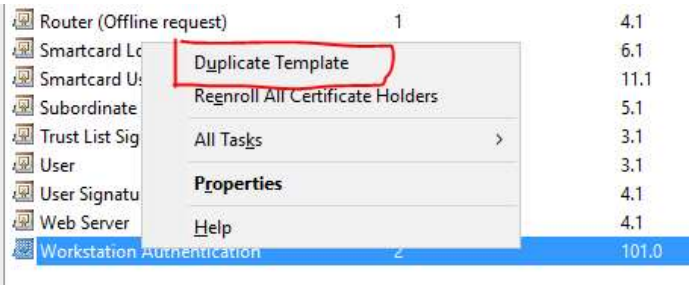
- Require approval to install the certificate for additional security
- Increase the certificate validity period

  - As you must export and import the certificate each time before it expires, an increase of the validity period reduces how often you must repeat this procedure. However, an increase of the validity period also decreases the security of the certificate because it provides more time for an attacker to decrypt the private key and steal the certificate.
- Use a custom value in the certificate Subject field or Subject Alternative Name (SAN) to help identify this certificate from standard client certificates.
  - This can be particularly helpful if you will use the same certificate for multiple distribution points.

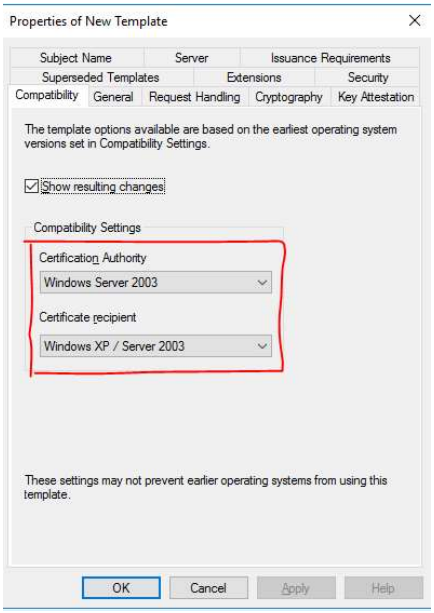
Instructions	Screenshot (if applicable)
1. On the member server that is running the Certification Authority console, right-click **Certificate Templates**, and then choose **Manage** to load the Certificate Templates management console	



2. In the results pane, right-click the entry that has **Workstation Authentication** in the **Template Display Name** column, and then choose **Duplicate Template**

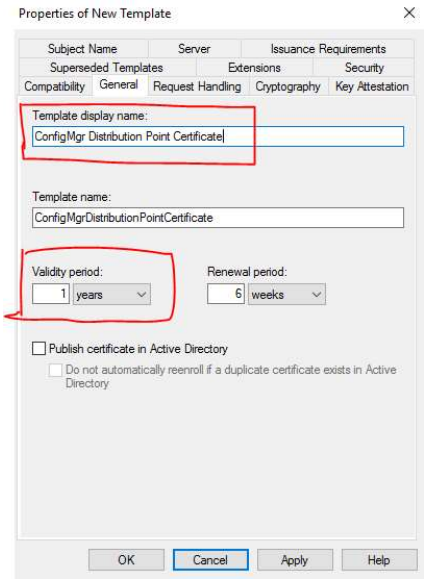


3. In the **Duplicate Template** dialog box, ensure that **Windows 2003 Server, Enterprise Edition** is selected, and then choose **OK**



4. In the **Properties of New Template** dialog box, on the **General** tab, enter a template name, like **ConfigMgr Client Distribution Point Certificate**, to generate the client authentication certificate for distribution points

   Review the Validity Period for this Certificate



5. Choose the **Request Handling** tab, and then choose **Allow private key to be exported**