





ADCS Two Tier PKI Hierarchy Deployment Detailed guide for Basic Configuration





Introduction and overview of the Test Lab:

There are five computers/machines involved in this two-tier PKI hierarchy lab.

- 1. There is one domain controller (DCO1) that is also running Active Directory-integrated Domain Name Service (DNS). This computer will also provide the Lightweight Directory Access Protocol (LDAP) location for the CDP and the AIA point for the PKI configuration.
- 2. One Standalone Offline Root CA (CA01).
- 3. One Enterprise Issuing CA (CA02).
- 4. One Web Server (SRV1) (HTTP CDP/AIA) and
- 5. One Windows 10 (Win10) Client computer.



AD DS forest – encryptionconsulting.com



Virtual Machine	Roles	ОЅ Туре	IP Address	Subnet mask	Preferred DNS server
DC01.encryptioncon- sulting.com	DC & DNS – LDAP CDP/AIA	Windows Server 2019	192.168.1.10	255.255.255.0	192.168.1.10
CA01	Standalone Offline Root CA	Windows Server 2019	NA	NA	NA
CA02.encryptioncon- sulting.com	Enterprise Issuing CA	Windows Server 2019	192.168.1.12	255.255.255.0	192.168.1.10
SRV1.encryptioncon- sulting.com	Web Server - HTTP CDP/AIA	Windows Server 2019	192.168.1.13	255.255.255.0	192.168.1.10
WIN10.encryption- consulting.com	Windows Client Computer	Windows 10	192.168.1.14	255.255.255.0	192.168.1.10

Major Steps:

There are eight major steps in this step-by-step guide as listed below (each includes several sub tasks).

- 1. Install the Active Directory Forest
- 2. Prepare the web server for CDP and AIA publication
- 3. Install the standalone offline root CA
- 4. Perform post installation configuration steps on the standalone offline root CA
- 5. Install Subordinate Issuing CA
- 6. Perform the post installation configuration on the subordinate issuing CA
- 7. Install and configure the online responder
- 8. Verify the PKI hierarchy health



1: Active Directory Forest

Task 1: Configure Server Name and Network Settings

Name server DC01 and create network for this lab:

- 1. Log in as DC01 and the local administrator.
- 2. Select Start, type ncpa.cpl and press ENTER.
- 3. When on Network Connections, right-click the Local Area Connection and then click Properties.
 - 3.1. If there are more than one Local Area Connection icons in the Network Connections, you want to modify the one that is connected to network segment shared by all the computers that you have installed for this lab.
 - 3.2. Click the Internet Protocol Version 4 (TCP/IPv4) and then click Properties.
 - 3.3. Select the **Use the Following IP address**. Configure the **IP address**, **Subnet mask**, and **Default gateway** appropriately for your test network.
 - IP Address: 192.168.1.10
 - Subnet mask: 255.255.255.0
 - Default gateway: <optional>
- 4. Select the Use the following DNS server address. Configure the **Preferred DNS server** for the IP address of your domain controller. Click **OK.** Click **Close**.
 - o Preferred DNS Server: 192.168.1.10
- 5. Click Start, type sysdm.cpl and press ENTER. Click Change.
- 6. In **Computer name**, type **DC01** and then click **OK**.
- 7. When prompted that you need to restart the computer, click **OK**. Click **Close.** Click **Restart Now**.



Task 2: Install a new forest by using Server Manager

To install the EncryptionConsulting.com forest:

- 1. Log onto DC01 as DC01\Administrator.
- 2. Open Server Manager. Select Start, click Administrative Tools, and then click Server Manager.
- 3. In the console tree, right-click Manage and then click Add Roles & Features
- 4. On the Before You Begin page, click Next.
- 5. On the Select Installation type, click Role Based or Feature Based installation
- 6. On Server Selection, select server from server pool and click on DC01. Then click Next
- 7. On the Select Server Roles page, select Active Directory Domain Services. Click Next.
 - O If prompted by the Add Roles Wizard, click Add Required Features and then click Next.
- 8. On the Features page, click next.
- 9. On the Active Directory Domain Services page, click Next.
- 10. On the Confirm Installation Selections page, click Install.
- 11. When completed, Click the hyperlink to Promote this server to a domain controller

	ч -		0	
Installation prog	ress	DESTIN	IATION SER	(VER)C01
Before You Begin	View installation progress			
Installation Type	Feature installation			
Server Selection				
Server Roles	Configuration required. Installation succeeded on DC01.			
Features	Active Directory Domain Services			
AD DS	Additional steps are required to make this machine a domain controller.			
Confirmation	Promote this server to a domain controller			
Results	Group Policy Management			
	Remote Server Administration Tools			
	Role Administration Tools			
	Active Directory module for Windows PowerShell			
	AD DS Tools			
	Active Directory Administrative Center			
	AD DS Snap-Ins and Command-Line Tools			
	You can close this wizard without interrupting running tasks. View task progress again by clicking Notifications in the command bar, and then Task Details.	or open	this page	
	Export configuration settings			
	< Previous Next > C	lose	Cano	vol



- 12. On the Welcome to the Active Directory Domain Services Installation Wizard page, click Next.
- 13. On the **Deployment Configuration** page, select **Add a new forest**, Specify **Forest Root Domain** page, in **FQDN of the forest root domain**, type **EncryptionConsulting.com**, and then click **Next**.



14. On the Set Forest Functional Level page, in the Forest functional level drop down menu, select Windows Server 2016 and then click Next

Domain Control	ler Options		TARGET SERVER DC01
Deployment Configuratio	n Select functional level of the nev	v forest and root domain	
DNS Options	Forest functional level:	Windows Server 2016	~
Additional Options	Domain functional level:	Windows Server 2016	¥.
Paths	Specify domain controller capab	ilities	
Review Options	✓ Domain Name System (DNS)	server	
Prerequisites Check	✓ Global Catalog (GC)		
	Read only domain controller	(RODC)	
Results	Type the Directory Services Rest	ore Mode (DSRM) password	
	Password:	•••••	
	Confirm password:		
	More about domain controller o	ptions	
		< Previous Next >	Install Cancel

On the **Directory Services Restore Mode Administrator Password** page, type and confirm the restore mode password, and then click **Next.** This password must be used to start Restore Mode for tasks that must be performed offline.



DNS server is selected by default so that your forest DNS infrastructure can be created during AD DS installation. In our scenario we are going to use Active Directory—integrated DNS so we have selected to install DNS

15. On the Additional **Options** page, click **Next.**

Additional Option	S		TARGET SERVER DC01
Deployment Configuration Domain Controller Options DNS Options	Verify the NetBIOS name assigned The NetBIOS domain name:	d to the domain and change it if necessary ENCRYPTIONCONSU	
Additional Options			
Paths			
Review Options			
Prerequisites Check			
Installation			
Results			
	More about additional options		
		< Previous Next >	Install Cancel

If no static IP address assigned for network adapter, a warning message appears advising you to set static addresses.

The wizard displays a message indicating that it cannot create a delegation for the DNS server. Click Yes to continue.

16. On the Location for Database, Log Files, and SYSVOL page, click Next.

aths			TARGET SERV
Deployment Configuration	Specify the location of the AD DS dat	abase, log files, and SYSVOL	
DNS Options	Database folder:	C:\Windows\NTDS	
Additional Options	Log files folder:	C:\Windows\NTDS	
Paths	SYSVOL folder:	C:\Windows\SYSVOL	
Prerequisites Check Installation Results			
	More about Active Directory paths		
		< Previous Next >	Install Cancel



17. On the Prerequisites Check page, review your selections and click install Active Directory Domain Services.

rereguisites Che	ck	TAI	RGET S	
 All prerequisite checks pass 	ed successfully. Click 'Install' to begin installation.	Show	more	×
Deployment Configuration Domain Controller Options DNS Options	Prerequisites need to be validated before Active Directory Domain Services is installed of Rerun prerequisites check	on this con	nputer	
Additional Options	Niew results			
Paths Review Options Prerequisites Check Installation Results	 Windows Server 2019 domain controllers have a default for the security setting n cryptography algorithms compatible with Windows NT 4.0" that prevents weaker algorithms when establishing security channel sessions. For more information about this setting, see Knowledge Base article 942564 (http://wink/?Linkld=104751). A delegation for this DNS server cannot be created because the authoritative par found or it does not run Windows DNS server. If you are integrating with an exist infrastructure, you should manually create a delegation to this DNS server in the ensure reliable name resolution from outside the domain "EncryptionConsulting action is required. 	amed "Alla cryptogra o://go.micr ent zone c ing DNS parent zon com". Othe	ow phy osoft.co annot t e to erwise,	om/ be no
	 All prerequisites checks passed successfully. Click 'Install' to begin installation. 			
	A If you click Install, the server automatically reboots at the end of the promotion ope More about prerequisites	eration.		

18. Wait for some time until installation completes and system restarts.

NOTE: If you are using Active Directory-integrated DNS, the IP address for the **Preferred DNS server** for the first domain controller in the forest is automatically set to the loopback address of 127.0.0.1. This helps assure that the IP address of the first domain controller will be resolved in DNS even if the static IP address of the server is changed. **If you prefer to configure actual IP address of the DNS sever rather than loop-backaddress, then replace it with 192.168.1.10 after the restart.**



Task 3: HTTP Web Server: CDP and AIA Publication

- 1. Log on to SRV1 as the local administrator
- 2. Click Start, type ncpa.cpl and press ENTER.
- 3. In Network Connections, right-click the Local Area Connection and then click Properties.
 - If there are more than one Local Area Connection icons in the Network Connections, you want to modify the one that is connected to network segment shared by all the computers that you have installed for this lab.
- 4. Click the Internet Protocol Version 4 (TCP/IPv4) and then click Properties.
- 5. Select the Use the Following IP address. Configure the IP address, Subnet mask, and Default gateway appropriately for your test network.
 - o IP Address: 192.168.1.13
 - o Subnet mask: 255.255.255.0
 - **O Default gateway:** <optional>
- 6. Select the Use the following DNS server address. Configure the **Preferred DNS server** for the IP address of your domain controller. Click **OK**. Click **Close**.
 - o Preferred DNS Server: 192.168.1.10
- 7. Click Start, type sysdm.cpl and press ENTER. Click Change.
- 8. In **Computer name**, type **SRV1** and then click **OK**.
- 9. When prompted that you need to restart the computer, click OK. Click Close. Click Restart Now.
- 10. After SRV1 restarts, log on as a local administrator.
- 11. Click Start, type sysdm.cpl and press ENTER. Click Change.
- 12. In Member of, select Domain, and then type EncryptionConsulting.com Click OK.
- 13. In Windows Security, enter the User name and password for the domain administrator account. Click OK.
- 14. You should be welcomed to the Encryption Consutling domain. Click OK.
- 15. When prompted that a restart is required, click **OK**. Click **Close**. Click **Restart Now**.

🔢 Dashboard	PROPERTIES For SRV1		TASKS 🔻
Local Server All Servers	Computer name Domain	SRV1 EncryptionConsulting.com	Last installed updat Windows Update Last checked for up
	Windows Defender Firewall Remote management Remote Desktop NIC Teaming Ethernet0	Domain: On Enabled Disabled Disabled 192.168.1.13, IPv6 enabled	Windows Defender Feedback & Diagno IE Enhanced Securit Time zone Product ID
	Operating system version Hardware information	Microsoft Windows Server 2019 Datacenter VMware, Inc. VMware7,1	Processors Installed memory (F Total disk space >



Task 4: Install Web Server (IIS) Role

- 1. Log on to SRV1.EncryptionConsulting.com as Encryptionconsu\Administrator. (Ensure that you switch user to log on as Encryptionconsu\Administrator)
- 2. Open Server Manager.
- 3. Right-click on Roles and then select Add Roles.
- 4. On the Before You Begin page select Next.
- 5. On the Select Installation type page, Select Role-based or feature-based installation

L Add Roles and Features Wizard \times DESTINATION SERVER Select installation type SRV1.EncryptionConsulting.com Select the installation type. You can install roles and features on a running physical computer or virtual Before You Begin machine, or on an offline virtual hard disk (VHD). Installation Type Role-based or feature-based installation Server Selection Configure a single server by adding roles, role services, and features. Server Roles Remote Desktop Services installation Features Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or Web Server Role (IIS) session-based desktop deployment. **Role Services** Confirmation < Previous Next > Install Cancel



6. On Select Destination Server, select server from server pool and click on SRV1.EncryptionConsulting.com, then click Next

Add Roles and Features Wizar	d			1000	٥	>
Select destinatio	on server			DESTI SRV1.Encryption	NATION SEF	RVER .com
Before You Begin Installation Type Server Selection Server Roles Features	Select a server or a virtual hard di Select a server from the serve Select a virtual hard disk Server Pool	sk on which to ins r pool	tall roles and features.			
Web Server Role (IIS) Role Services	Name	IP Address	Operating System		1	
Results	5RV1.EncryptionConsulting.com	192.168.1.13	Microsoft Windows Se	erver 2019 Datacer	iter	
	1 Computer(s) found					
	This page shows servers that are have been added by using the Ac servers from which data collection	running Windows Id Servers comman n is still incomplete	Server 2012 or a newer rel nd in Server Manager, Offl e are not shown.	ease of Windows : ine servers and ne	Server, and wly-addec	d tha
		< Pr	evious Next >	Install	Cano	el

7. On the Select Server Roles page select Web Server (IIS) and then click Next

elect server role	S	DESTINATION SERVE SRV1.EncryptionConsulting.com
Before You Begin Installation Type	Select one or more roles to install on the selected server.	Description
Server Selection Server Roles Features Web Server Role (IIS) Role Services Confirmation Results	Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server Fax Server File and Storage Services (1 of 12 installed) Host Guardian Service Hyper-V Network Controller Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services Volume Activation Services Windows Deployment Services Windows Server Update Services	Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

8. On the **Select features** page, click **next**



9. On Web Server (IIS) page, click Next



10. Leave the defaults on Select Role Services page and then click Next.

Select role servi	ces	DESTINATION SERVER SRV1.EncryptionConsulting.com
Before You Begin	Select the role services to install for Web Server (IIS)	
Installation Type	Role services	Description
Server Selection Server Roles Features	Web Server Common HTTP Features Default Document	 Web Server provides support for HTM Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server
Web Server Role (IIS) Role Services		to host an internal or external Web sit or to provide an environment for developers to create Web-based
Confirmation	WebDAV Publishing	applications.
Results	 Health and Diagnostics HTTP Logging Custom Logging Logging Tools ODBC Logging Request Monitor Tracing Yerformance Static Content Compression Dynamic Content Compression Security Request Filtering Basic Authentication 	*



11. On Confirm Installation Selections page, click Install.

📥 Add Roles and Features Wizard

- 🗆 X

Refere Veu Regin		
beiore rou begin	To install the following roles, role services, or features or	n selected server, click Install.
Installation Type	Restart the destination server automatically if requi	red
Server Selection	Optional features (such as administration tools) might b	e displayed on this page because they have
Server Roles	been selected automatically. If you do not want to instal their check boxes.	II these optional features, click Previous to c
Features		
Web Server Role (IIS)	Web Server (IIS)	
Role Services	Management Tools	
Confirmation	Web Console	
Results	Common HTTP Features	
	Default Document	
	Directory Browsing	
	HTTP Errors	
	Static Content	
	Health and Diagnostics	
	Export configuration settings	
	openit of dictione source pairs	

12. On the Installation Results page, click Close





Task 5: Create CertEnroll Folder and grant Share & NTFS Permissions to Cert Publishers group

- 1. Log onto SRV1.EncryptionConsulting.com as Encryptionconsu\Administrator.
- 2. Click Start and select Computer to open Windows Explorer and then go to C: drive.
- 3. Create folder called **CertEnroll** at the root of **C**: drive.
- 4. Right-click on CertEnroll folder and select Properties.



- 5. On CertEnroll Properties page select Sharing tab to configure share permissions.
- 6. Click on Advanced Sharing option and then select Share this folder.
- 7. Click on Permissions and then click Add.
- 8. On Select Users or Groups page, in the Enter the object names to select, type Encryptionconsu\Cert Publishers and then click OK.
- 9. On **Permissions for CertEnroll** dialog box, select **Cert Publishers** group and then in the **Allow** column select **Change** permission. Click **OK** twice to go back to **CertEnroll Properties** page.



- 10. Select **Security** tab and click **Edit** to configure NTFS permissions.
- 11. On **Permissions for CertEnroll** page click **Add.**
- 12. On Select Users or Groups page, under the Enter the object names to select, enter EncryptionConsulting\Cert Publishers and then click OK.
- 13. On **Permissions for CertEnroll** page highlight **Cert Publishers** group and then under the **Allow** column select **Modify** permission. Click **OK**.

57 - F		folder		· •				- Invert
Organize r		New			Open			Se
	📜 CertEn	roll Properties					×	
			-					• • • •
	General	Sharing Security	Previous V	ersions	Customize			
	Object na	ame: C:\CertEnroll						
	Group or	user names:						
	SYS SYS	TEM				~		
	Cert	Publishers (ENCRY	PTIONCON	ISU\Cert	Publishers))		
	Adm State	inistrators (SRV1\Ad	Iministrators	s)		~		
	<	re (SR\/1\Tleare)				>		
	To chang	e permissions, click	Edit.	[Eda			
					Eult			
	Permissio	ns for Cert Publisher	s	Allow	Der	ny		
	Full co	ntrol				^		
	Modify			~				
	Read 8	execute		~				
	List fold	der contents		~				
	Read			~				
	Write			~		~		
	For speci click Adv	al permissions or adv anced.	anced sett	ings,	Advanc	ed		
		Oł	(Cancel	1	Apply		

14. On CertEnroll Properties page, click OK.



Task 6: Create CertEnroll Virtual Directory in IIS

- 1. Ensure you are logged on to SRV1.EncryptionConsulting.com as Encryptionconsu\Administrator.
- 2. Click Start, Administrative Tools and then select Internet Information Services (IIS) Manager.
- 3. On the Connections, expand SRV1 and then expand Sites.
- 4. Right-click on Default Web Site and select Add Virtual Directory.
- 5. On Add Virtual Directory page, in Alias, type CertEnroll. In Physical path, type C:\Certenroll, and then click OK.



- 6. In the Connections pane, under the Default Web Site, ensure the CertEnroll virtual directory is selected.
- 7. In the CertEnroll Home pane, double-click on Directory Browsing.
- 8. In Actions pane click Enable.





Task 7: Enable Double Escaping on IIS Server

Allowing double escaping makes it possible for the web server to host Delta CRLs.

- 1. Ensure you are logged on to SRV1.EncryptionConsulting.com as Encryptionconsu\Administrator.
- 2. Open a Command Prompt. To do so, click **Start**, click **Run**, and then type **cmd**. Click **OK**.
- 3. Then type cd %windir%\system32\inetsrv\ and press ENTER.
- 4. Type following command and press Enter. Appcmd set config "Default Web Site" /section:system.webServer/Security/re questFiltering -allowDoubleEscaping:True
- 5. Restart IIS service. To do so, type **iisreset** and press ENTER.





Task 8: Create CNAME (pki.EncryptionConsulting.com) in DNS

- 1. Ensure that you are logged on to DC01.EncryptionConsulting.com as Encryptionconsu\Administrator.
- 2. Open the DNS Console. You can do so by clicking **Start**, click **Run**, and then type **dnsmgmt.msc**. Click **OK**.
- 3. Expand Forward Lookup Zones, select and then right-click EncryptionConsulting.com zone. Click New Alias (CNAME).
- 4. In Alias name (uses parent domain if left blank), type PKI. In the Fully qualified domain name (FQDN) for target host field, type SRV1.EncryptionConsulting.com. and then click OK.

Note - Include the terminating "." in the FQDN in the previous step. In a production environment this alias can resolve to a lad balancer which distributes requests to any number of web servers that contain the CA certificates and CRLs.





Activity 2: Install the Standalone Offline Root CA

The standalone offline root CA should not be installed in the domain. As a matter of fact, it should not even be connected to a network at all.

Task 1: Create a CAPolicy.inf for the standalone offline root CA

To create a CAPolicy.inf for the standalone offline root CA:

- 1. Log onto CA01 as CA01\Administrator.
- 2. Click Start, click Run and then type notepad C:\Windows\CAPolicy.inf and press ENTER.
- 3. When prompted to create new file, click **Yes.**
- 4. Type in following as contents of the file.
 - [Version]

Signature="\$Windows NT\$"

- [Certsrv_Server]
- RenewalKeyLength=2048; recommended 4096
- RenewalValidityPeriod=Years
- RenewalValidityPeriodUnits=20
- AlternateSignatureAlgorithm=0
- 0

Click File and Save to save the CAPolicy.inf file under C:\Windows directory.

Warning CAPolicy.inf with the .inf extension. Type .inf at the end of the file name and select the options as described, the file will be saved as a text file and will not be used during CA installation.

5. Close Notepad.

NOTE: Make sure you change the computer name as "CA01". Windows > Run > sysdm.cpl > Change the computer name and restart the machine.



Task 2: Installing the Standalone Offline Root CA

To install the standalone offline root CA:

- 1. Log onto CA01 as CA01\Administrator.
- 2. Click Start, click Administrative Tools, and then click Server Manager.
- 3. Right-click on Roles and then click Add Roles.
- 4. On the **Before You Begin** page click **Next.**
- 5. On the Installation Type page, choose Role based or Featured based installation and then click Next.
- 6. On the server selection page, click next.
- 7. On the Select Server Roles page select Active Directory Certificate Services, and then click Next.



8. On the select features page, click next.

9. On the Introduction to Active Directory Certificate Services page, click Next.



10. On the Select Role Services page, ensure that Certification Authority is selected, and then Next.



11. On the confirmation page, click install

📥 Add Roles and Features Wizard		(11 1)	٥	×
Installation progre	SS	DESTIN	IATION SER	IVER CA01
Before You Begin Installation Type Server Selection Server Roles	View installation progress Feature installation Configuration required. Installation succeeded on CA01.			
Features AD CS Role Services Confirmation Results	Active Directory Certificate Services Additional steps are required to configure Active Directory Certificate Services on the Configure Active Directory Certificate Services on the destination server Certification Authority Remote Server Administration Tools Role Administration Tools Active Directory Certificate Services Tools Certification Authority Management Tools	e destina	ition serv	er
	You can close this wizard without interrupting running tasks. View task progress of again by clicking Notifications in the command bar, and then Task Details. Export configuration settings	r open	this page	
	< Previous Next > Clo	se	Canc	el



- 12. Click on configure "Active Directory Certificate Services on the destination server".
- 13. On the **Specify Credential to configure roles and services** page, credential should be **CA01\Administrator**, then click **Next**.
- 14. On the Select Role services to configure page, choose Certificate Authority and then click Next.
- 15. On the **Specify Setup Type** page, ensure that **Standalone** is selected, and then click **Next.**
 - Note: Enterprise option is greyed out as CA01 server is not joined to Active Directory domain.

Lange AD CS Configuration	- 0 X
Setup Type	DESTINATION SERVER CA01
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	 Specify the setup type of the CA Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates. Enterprise CA Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies. Standalone CA Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).
	More about Setup Type
	< Previous Next > Configure Cancel



16. On the Specify CA Type page, ensure that Root CA is selected, and then click Next.



17. On the Set Up Private Key page, ensure that Create a new private key is selected, and then click Next.





- 18. Leave the defaults on the **Configure Cryptography for CA** page, and then click **Next**.
 - Important: In a production environment, you would set the CSP, Hash Algorithm, and Key length to meet application compatibility requirements.

AD CS Configuration			- 🗆 X
Cryptography fo	or CA		DESTINATION SERVER CA01
Credentials Role Services Setup Type CA Type	Specify the cryptographic options Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider	*	Key length: 2048 ×
Private Key	Select the hash algorithm for signing certificates issued by	this CA:	
CA Name Validity Period Certificate Database Confirmation Progress Results	SHA256 SHA384 SHA512 SHA1 MD5	accessed	by the CA.
	More about Cryptography		Configure

19. On **Configure CA Name** page, under Common name for this CA, clear the existing entry and type **EncryptionConsulting Root CA.** Click **Next.**

Note: A **Distinguished Name Suffix** is optional for a root CA. This will be configured in a later step.

AD CS Configuration	×
CA Name	DESTINATION SERVER CA01
Credentials Role Services	Specify the name of the CA
Setup Type CA Type Private Key	Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.
Cryptography	EncryptionConsulting Root CA
Validity Period Certificate Database	Distinguished name suffix:
Confirmation	Preview of distinguished name:
Progress Results	CN=EncryptionConsulting Root CA
	More about CA Name



20. On **Set Validity Period** page, under **Select validity period for the certificate generated for this CA**, clear the existing entry and then type **20**. Leave the selection box set to **Years**. Click **Next**.

AD CS Configuration						<u>—</u> 73		×
Validity Period						DESTINA	ATION SE	RVER CA01
Credentials Role Services Setup Type	Speci Select ti	ify the validit	y period or the certificat	e generated fo	r this certifica	tion authority (CA):	
CA Type	20	Years	Ŷ					
Private Key Cryptography CA Name	CA expiration Date: 12/15/2039 12:13:00 PM The validity period configured for this CA certificate shoul certificates it will issue.					e validity perio	d for the	
Validity Period								
Certificate Database								
Confirmation								
Progress Results								
	More al	bout Validity Period	1				P	
			< Pre	vious Ne	xt >	Configure	Canc	.el



21. Keep the default settings on the **Configure Certificate Database** page, and then click **Next.**



22. On the **Confirm Installation Selections** page, review the settings, and then click **Configure.**





23. Review the information on the Installation Results page to verify that the installation is successful and then click Close.



Activity 3: Perform Post Installation Configuration for Root CA

- 1. Ensure that you are logged on to CA01 as CA01\Administrator.
- 2. Open a command prompt. To do so, you can click **Start**, click **Run**, type **cmd** and then click **OK**.
- 3. To define Active Directory Configuration Partition Distinguished Name, run the following command from an administrative command prompt:

Certutil -setreg CA\DSConfigDN "CN=Configuration,DC=EncryptionConsulting,DC=com"

- 4. To define **CRL Period Units** and **CRL Period**, run the following commands from an administrative command prompt:
 - Certutil -setreg CA\CRLPeriodUnits 52
 - Certutil -setreg CA\CRLPeriod "Weeks"
 - O Certutil -setreg CA\CRLDeltaPeriodUnits 0
- 5. To define **CRL Overlap Period Units** and **CRL Overlap Period**, run the following commands from an administrative command prompt:
 - O Certutil -setreg CA\CRLOverlapPeriodUnits 12
 - Certutil -setreg CA\CRLOverlapPeriod "Hours"
- 6. To define **Validity Period Units** for all issued certificates by this CA, type following command and then press Enter. In this lab, the Enterprise Issuing CA should receive a 10 year lifetime for its CA certificate. To configure this, run the following commands from an administrative command prompt:
 - O Certutil -setreg CA\ValidityPeriodUnits 10
 - O Certutil -setreg CA\ValidityPeriod "Years"



Task 1: Enable Auditing on the Root CA

CA auditing depends on system **Audit Object Access** to be enabled. The following instructions describe how to use Local Security Policy to enable object access auditing.

- 1. Click Start, click Administrative Tools, and then select Local Security Policy.
- 2. Expand Local Policies and then select Audit Policy.
- 3. Double click Audit Object Access and then select Success and Failure then click OK.

🚡 Local Security Policy





- 4. Close Local Security Policy editor.
- 5. Enable auditing for the CA by selecting which group of events to audit in the Certificate Authority MMC snap-in or by configuring AuditFilter registry key setting. To configure Auditing for all CA related events, run the following command from an administrative command prompt: **Certutil -setreg CA\AuditFilter 127**



Task 2: Configure the AIA and CDP

There are multiple different methods for configuring the Authority Information Access (AIA) and certificate revocation list distribution point (CDP) locations. You can use the user interface (in the Properties of the CA object), certutil, or directly edit the registry. The AIA is used to point to the public key for the certification authority (CA). The CDP is where the certificate revocation list is maintained, which allows client computers to determine if a certificate has been revoked. In this lab there will be three locations for the AIA and four locations for the CDP.



Task 3: Configure the AIA

Using a certutil command is a quick and common method for configuring the AIA. When you run the following certutil command, you will be configuring a static file system location, a lightweight directory access path (LDAP) location, and http location for the AIA. The certutil command to set the AIA modifies the registry, so ensure that you run the command from an command prompt run as Administrator. Run the following command:

certutil -setreg CA\CACertPublicationURLs "1:C:\Windows\system32\CertSrv\CertEnroll\ %1_%3%4.crt\n2:ldap:///CN=%7,CN=AIA, CN=Public Key Services,CN=Services,%6%11\n2:http://pki.EncryptionConsulting.com/CertEnroll/%1_%3%4.crt"

After you have run that command, run the following command to confirm your settings:

certutil -getreg CA\CACertPublicationURLs

If you look in the registry, under the followingpath:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CertSvc\Configuration\EncryptionConsulting Root CA, you can confirm the CACertPublicationURLs by opening that REG_MULTI_SZ value. You should see the following:

1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt

2:Idap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11

2:http://pki.EncryptionConsulting.com/CertEnroll/%1_%3%4.crt

You can also see this in the the CA (certsrv) console. To open the console, click **Start**, click **Administrative Tools**, and then click **Certification Authority**. In the navigation pane, expand the **Certificate Authority(Local)**. Right-click **EncryptionConsulting Root CA** and then click **Properties**. On the **Extensions** tab, under **Select extension**, click **Authority Information Access (AIA)** and you will see the graphical representation of the AIA settings.

Task 4: Configure the CDP

The certutil command to set the CDP modifies the registry, so ensure that you run the command from an command

certutil -setreg CA\CRLPublicationURLs "1:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl\n10:ldap:///CN=%7%8,CN=%2, CN=CDP,CN=Public Key Services,CN=Services,%6%10\n2:http://pki.EncryptionConsulting.com/CertEnroll/%3%8%9.crl"

After you run that command, run the following certutil command to verify your settings:

certutil -getreg CA\CRLPublicationURLs

In the registry

location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\EncryptionConsulting Root CA you can open the REG_MULTI_SZ valueand see the configuration of these values:

1:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl

10:Idap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10

2:http://pki.EncryptionConsulting.com/CertEnroll/%3%8%9.crl

You can also see this in the the CA (certsrv) console. To open the console, click **Start**, click **Administrative Tools**, and then click **Certification Authority**. In the navigation pane, ensure that **Certificate Authority (Local)** is expanded. Right-click **EncryptionConsultng Root CA** and then click **Properties**. On the **Extensions** tab, under **Select extension**, click **CRL Distribution Point (CDP)** and you will see the graphical representation of the CDP settings.

At an administrative command prompt, run the following commands to restart Active Directory Certificate Services and to publish the CRL.

net stop certsvc

Net start certsvc

certutil -crl



Activity 4: Install Enterprise Issuing CA

Task 1: Join CA02 to the domain

- 1. Log on to CA02 as the local administrator.
- 2. Click **Start**, type **ncpa.cpl** and press ENTER.
- 3. In Network Connections, right-click the Local Area Connection and then click Properties.
- 4. Click the Internet Protocol Version 4 (TCP/IPv4) and then click Properties.
- 5. Select the **Use the Following IP address.** Configure the **IP address, Subnet mask,** and **Default gateway** appropriately for your test network.
 - O IP Address: 192.168.1.12
 - O Subnet mask: 255.255.255.0
 - O **Default gateway**: <optional>
- 6. Select the Use the following DNS server address. Configure the **Preferred DNS server** for the IP address of your domain controller. Click **OK**. Click **Close**.
 - O Preferred DNS Server: 192.168.1.10
- 7. Click Start, type sysdm.cpl and press ENTER. Click Change.
- 8. In **Computer name**, type **CA02** and then click **OK**.
- 9. When prompted that you need to restart the computer, click **OK**. Click **Close**. Click **Restart Now**.
- 10. After CA02 restarts, log on as a local administrator.
- 11. Click Start, type sysdm.cpl and press ENTER. Click Change.
- 12. In Member of, select Domain, and then type EncryptionConsulting.com. Click OK.
- 13. In Windows Security, enter the User name and password for the domain administrator account. Click OK.
- 14. You should be welcomed to the EncryptionConsulting domain. Click **OK**.
- 15. When prompted that a restart is required, click **OK**. Click **Close**. Click **Restart Now**.

Task 2: Create CAPolicy.inf for Enterprise Root CA

- 1. Log onto CA02.EncryptionConsulting.com as EncryptionConsulting\Administrator. (Ensure that you switch user to log on as EncryptionConsulting\Administrator)
- 2. Click Start, select Run and then type notepad C:\Windows\CAPolicy.inf and press ENTER.
- 3. When prompted to create new file, click Yes.
- 4. Type in following as content of the file.

[Version] Signature="\$Windows NT\$" [PolicyStatementExtension] Policies=InternalPolicy [InternalPolicy]



OID= 1.2.3.4.1455.67.89.5 URL=http://pki.EncryptionConsulting.com/cps.txt [Certsrv_Server] RenewalKeyLength=2048 RenewalValidityPeriod=Years RenewalKeyLength=2048 RenewalValidityPeriod=Years AlternateSignatureAlgorithm=0

5. Click File and Save to save the CAPolicy.inf file under C:\Windows directory.

Important: Ensure that the CAPolicy.inf is saved as an .inf file. The file will not be used if it is saved with any other file extension.

6. Close Notepad.

Task 3: Publish the Root CA Certificate and CRL

- 1. Ensure you are logged on to CA02. EncryptionConsulting.com as EncryptionConsulting\Administrator.
- 2. Copy Root CA Certificate (CA01_EncryptionConsulting Root CA.crt) and Root CA CRL(EncryptionConsulting Root CA.crl) files from C:\Windows\System32\CertSrv\CertEnroll directory on CA01 server to removable media (A:).
- 3. On CA02, to publish EncryptionConsulting Root CA Certificate and CRL in Active Directory, run the following commands at an administrative command prompt. Ensure that you substitute the correct drive letter of your removable media (for A:) in the commands that follow:

certutil -f -dspublish "A:\CA01_EncryptionConsulting Root CA.crt" RootCA

certutil -f -dspublish "A:\EncryptionConsulting Root CA.crl" CA01

4. To publish EncryptionConsulting Root CA Certificate and CRL to http://pki. EncryptionConsulting.com/CertEnroll, copy EncryptionConsulting Root CA Certificate and CRL to \\srv1.

EncryptionConsulting.com\C\$\CertEnroll directory. Run the following commands from an administrative command prompt. Ensure that you substitute the correct drive letter of your removable media (for A:)

copy "C:\CA01_EncryptionConsulting Root CA.crt" \\SRV1.EncryptionConsulting.com\C\$\CertEnroll\ copy "C:\EncryptionConsulting Root CA.crl" \\SRV1.EncryptionConsulting.com\C\$\CertEnroll\

- 5. To add EncryptionConsulting Root CA Certificate and CRL in CA02. EncryptionConsulting.com local store, run the following command from an administrative command prompt. Ensure that you substitute the correct drive letter of your removable media (for A:) in the commands that follow:
 - certutil -addstore -f root "CA01_ EncryptionConsulting Root CA.crt"
 - certutil -addstore -f root " EncryptionConsulting CA.crl"



Activity 5: Install Subordinate Issuing CA

Subordinate issuing CA on CA02. EncryptionConsulting com:

- 1. Ensure that you are logged on to CA02. EncryptionConsulting.com as EncryptionConsulting\Administrator.
- 2. Open Server Manager.
- 3. Right-click **Roles** and then select **Add Roles**.
- 4. On the **Before You Begin** page select **Next.**

efore you beg	IN CA02.EncryptionConsulting.com
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	 This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website. To remove roles, role services, or features: Start the Remove Roles and Features Wizard Before you continue, verify that the following tasks have been completed: The Administrator account has a strong password Network settings, such as static IP addresses, are configured The most current security updates from Windows Update are installed If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again. To continue, click Next.
	Skip this page by default



- 5. On the Installation Type page, choose Role based or Featured based installation and then click Next.
- 6. On the **server selection** page, click **next.**
- 7. On the Select Server Roles page select Active Directory Certificate Services, and then click Next.





9. On the Introduction to Active Directory Certificate Services page, click Next.

ᡖ Add Roles and Features Wizar	d		81 <u>—</u> 81		×
Active Directory Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Certificate Services Active Directory Certificate Services (AD CS) provides the of such as secure wireless networks, virtual private networks, Access Protection (NAP), encrypting file system (EFS) and Things to note: • The name and domain settings of this computer cannot (CA) has been installed. If you want to change the comp server to a domain controller, complete these changes information, see certification authority naming.	CAO: Internet Protocol Sec smart card log on. t be changed after a co puter name, join a don before installing the C	DESTINJ 2.EncryptionC re to enable urity (IPSec) ertification nain, or pro :A. For more	ATION SERV onsulting.c : scenaric), Networ authority imote this e	ver om >s k
	< Previous	Next > h	nstall	Cance	2

10. On the Select Role Services page, select Certification Authority and Certification Authority Web Enrollment. If you see the Add Roles Wizard, click Add Required Role Services. Click Next.





11. On the Web Server Role IIS page, click Next.

Ī

- 12. Leave the Role Services as default and click Next.
- 13. On the confirmation page, review the details and click **Install**.

Add Roles and Features Wizard					٥	×
Installation progre	SS			DESTIN CA02.EncryptionC	ATION SER Consulting.	COM
Before You Begin	View installation progress					
Installation Type	Feature installation					
Server Selection				_		
Server Roles	Configuration required. Installation succe	eded on CAC	2.EncryptionCon	sulting.com.		
Features	Active Directory Certificate Services					~
AD CS	Additional steps are required to configure A	ctive Directo	ry Certificate Ser	vices on the destina	tion	
	Server	ar an tha da	rtiantion conver			
Web Server Role (IIS)	Certification Authority	es on the de	sunation server			
	Certification Authority Web Enrollment					
Confirmation	Remote Server Administration Tools					
Results	Role Administration Tools					
	Active Directory Certificate Services	Tools				
	Certification Authority Manage	ment loois				
	Web Server (IIS)					
	You can close this wizard without interru again by clicking Notifications in the con	pting runnin nmand bar, a	g tasks. View task Ind then Task Det	cp <mark>r</mark> ogress or open t tails.	his page	
	Export configuration settings					
		Previous	Next >	Close	Canc	el

- 14. Click on "configure Active Directory Certificate Services on the destination server".
- 15. On the Specify Credential to configure roles and services page, credential should be **Encryptionsu\Administrator**, then click **Next**.



 On the Select Role services to configure page, select Certificate Authority and Certificate Authority Web Enrollment then click Next.



17. On the Specify Setup Type page, ensure that Enterprise is selected, and then click Next.





18. On the Specify CA Type page, select Subordinate CA, and then click Next



19. On the Set Up Private Key page, ensure that Create a new private key is selected, and then click Next.





20. Leave the defaults on the **Configure Cryptography for CA** page, then click **Next**. Important: When installing in a production environment, the CSP, Hash Algorithm and Key length selected must support application compatibility requirements.

AD CS Configuration			-		×
Cryptography fo	r CA	CA	DESTINA 02.EncryptionCo	TION SER	VER com
Credentials Role Services Setup Type	Specify the cryptographic options Select a cryptographic provider:		Key length:		
CA Type	RSA#Microsoft Software Key Storage Provider	v	2048		٠
Cryptography CA Name Certificate Request Certificate Database Confirmation Progress Results	Select the hash algorithm for signing certificates issued SHA256 SHA384 SHA512 SHA1 MD5	by this CA:	by the CA.		
	More about Cryptography Previous	xt >	Configure	Cance	el



1

21. On **Configure CA Name** page, clear the existing entry for Common name for this CA box, and enter **EncryptionConsulting Issuing CA**, then select Next.

Note - Distinguished Name Suffix is automatically populated and should not be modified.

AD CS Configuration	- 🗆 X
CA Name	DESTINATION SERVER CA02.EncryptionConsulting.com
Credentials Role Services	Specify the name of the CA
Setup Type CA Type Private Key	Type a common name to identify this certification authority (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:
CA Name	EncryptionConsulting Issuing CA
Certificate Request Certificate Database Confirmation Progress Results	Distinguished name suffix: DC=EncryptionConsulting,DC=com Preview of distinguished name:
	CN=EncryptionConsulting Issuing CA,DC=EncryptionConsulting,DC=
	More about CA Name
	< Previous Next > Configure Cancel



22. On the **Request certificate from a parent CA** page, select **Save a certificate request to file on the target machine** option then click **Next.**



23. Leave the defaults on the **Configure Certificate Database** page, and then click **Next.**

AD CS Configuration	- 0	×
CA Database	DESTINATION SERVE CA02.EncryptionConsulting.co	ER m
Credentials Role Services	Specify the database locations	
Setup Type	C/windows/system32/CertLog	
Private Key	Certificate database log location:	
Cryptography CA Name Certificate Request	C:\windows\system32\CertLog	
Certificate Database		
Confirmation Progress Results		
	More about CA Database	
	< Previous Next > Configure Cancel	



24. On the **Confirm Installation Selections** page, click **configure.**

Confirmation		DESTINATION SERVE
Confirmation		CA02.EncryptionConsulting.com
Credentials	To configure the following roles, rol	e services, or features, click Configure.
Role Services	(A) Active Directory Certificate S	ervices
Setup Type		
СА Туре	Certification Authority	Enternaine Subardinate
Private Key	Civiptographic provider:	RSA#Microsoft Software Key Storage Provider
Cryptography	Hash Algorithm:	SHA256
CA Name	Key Length:	2048
Certificate Request	Allow Administrator Interaction:	Disabled
Certificate Database	Certificate Validity Period:	Determined by the parent CA
Confirmation	Distinguished Name:	CN=EncryptionConsulting Issuing CA,DC=EncryptionConsulting,DC=com
Progress	Offline Request File Location:	C:\CA02.EncryptionConsulting.com_EncryptionConsulting-CA02-CA.req
Results	Certificate Database Location:	C:\Windows\system32\CertLog
	Certificate Database Log Location:	C:\Windows\system32\CertLog
	Certification Authority Web Enro	llment



- 25. Review the information on the **Installation Results** page to verify that the installation is successful and then click **Close**.
 - The following warning message is expected: "The Active Directory Certificate Services installation is incomplete. To complete the installation, use the request file "C:\CA02.EncryptionConsulting.com_EncryptionConsulting-CA02-CA.req" to obtain a certificate from the parent CA. Then, use the Certification Authority snap-in to install the certificate. To complete this procedure, right-click the node with the name of the CA, and then click Install CA Certificate. The operation completed successfully. 0x0 (WIN32: 0)."

AD CS Configuration		- 0 >
Results		DESTINATION SERVER CA02.EncryptionConsulting.com
Credentials Role Services	The following roles, role services, or features wer	e configured:
Secup type CA Type Private Key Cryptography CA Name Certificate Request Certificate Database Confirmation Progress Results	Certification Authority	Configuration succeeded with warnings allation is incomplete. To complete the installation, use the om_EncryptionConsulting-CA02-CA.req" to obtain a Certification Authority snap-in to install the certificate. To the with the name of the CA, and then click Install CA fully. 0x0 (WIN32: 0) Configuration succeeded

- 26. Copy C:\ CA02.EncryptionConsulting.com_EncryptionConsulting-CA02-CA.req to your removable media. For example, if you want to copy to a floppy disk drive using the drive letter A:, you would run the following command from a command prompt:
 - o copy "C:\CA02. EncryptionConsulting.com_ EncryptionConsulting Issuing CA.req" A:\

Task 1: Submit the Request and Issue EncryptionConsulting Issuing CA Certificate

To submit the certificate request and issue the requested certificate:

- 1. Ensure that you are logged on to CA01 as CA01\Administrator. Place the removable media with the certificate request into CA01.
- 2. On CA01, open an administrative command prompt. Then, submit the request using the following command (assuming that A:\ is your removable media drive letter):
 - o certreq -submit "A:\CA02.EncryptionConsulting.com_EncryptionConsulting-CA02-CA.req"
 - Note: Pay attention to the **RequestID** number that is displayed after you submit the request. You will use this number when retrieving the certificate.
- 3. In the Certification Authority List dialog box, ensure that EncryptionConsulting Root CA is selected and then click OK
- 4. Open the Certification Authority console. To do so, click **Start**, click **Administrative Tools**, click **Certification Authority**.
- 5. In the **certsrv** [Certification Authority (Local)] dialog box, in the console tree, expand EncryptionConsulting Root CA.
- 6. Click **Pending Requests.** In the details pane, right-click the request you just submitted, click **All Tasks**, and then click **Issue**.

File Action View Help	, () p					w 192
🗢 🄿 🙍 🙆 🔯						
Certification Authority (Local) EncryptionConsulting Root cA Revoked Certificates Subsequed Certificates Pending Requests Failed Requests	Request ID	Requester Name CA01\Administrator	Binary Certificate	Certificate Template SubCA	Serial Number 160000002eb9	Certificate 9/24/2020

- 7. Return to the administrative command prompt to accept the issued certificate by running the following command. Ensure that you substitute the appropriate drive letter of your removable media for **A**: as well as the correct RequestID for **2**:
 - o certreq -retrieve 2 "A:\ CA02.EncryptionConsulting.com_EncryptionConsulting-CA02-CA.crt"
- 8. In the **Certification Authority List** dialog box, ensure that **EncryptionConsulting Root CA** is selected and then click **OK**.

Task 2: Install the Encryption Consulting Issuing CA Certificate on CA02

To install the certificate and start the Certification Authority service on CA02:

- 1. Ensure that you are logged on to CA02. EncryptionConsulting.com as EncryptionConsu\Administrator. Place the removable media with the issued certificate for CA02. EncryptionConsulting.com into CA02.
- 2. Open the Certification Authority console.
- 3. In the **Certification Authority** console tree, right-click **EncryptionConsulting Issuing CA**, and then click **Install CA Certificate**.
- 4. In the Select file to complete CA installation, navigate to your removable media. Ensure that you are displaying All Files (*.*) and click the CA02.EncryptionConsulting.com_EncryptionConsulting-CA02-CA certificate. Click Open.



- 5. In the console tree, right-click **EncryptionConsulting Issuing CA**, click All Tasks, and then click **Start Service**.
- 6. In the console tree, expand EncryptionConsulting Issuing CA and then click Certificate Templates. Notice there are no certificates shown in the details pane. This is because the CAPolicy.inf specified not to install the default templates in the line LoadDefaultTemplates=0.

a certsrv - [Certification Authority (L	certsrv - [Certification Authority (Local)\EncryptionConsulting Issuing CA\Certificate Templates]		٥	×
File Action View Help				
🗢 🔿 🙇 🙆 👔				
Certification Authority (Local) Certification Consulting Issuing Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates	Name	Intended Purpose There are no items to show in this view.		

Activity 6: Perform Post Installation Configuration Tasks on the Subordinate Issuing CA

There are multiple settings to configure to complete the installation of the issuing CA. These are like the tasks that were needed to complete the configuration of the root CA.

Task 1: Configure Certificate Revocation and CA Certificate Validity Periods

To configure certificate revocation and CA certificate validity periods:

- 1. Ensure that you are logged on to CA02. EncryptionConsulting.com as EncryptionConsu\Administrator.
- 2. Configure the CRL and Delta CRL settings by running the following command from an administrative command prompt:
 - O Certutil -setreg CA\CRLPeriodUnits 1
 - Certutil -setreg CA\CRLPeriod "Weeks"
 - O Certutil -setreg CA\CRLDeltaPeriodUnits 1
 - O Certutil -setreg CA\CRLDeltaPeriod "Days"
- 3. Define CRL overlap settings by running the following command from an administrative command prompt:
 - O Certutil -setreg CA\CRLOverlapPeriodUnits 12
 - Certutil -setreg CA\CRLOverlapPeriod "Hours"
- 4. The default setting for Validity Period is 2 years in registry. Adjust this setting accordingly to meet your needs of entity certificate's lifetime issued from EncryptionConsulting Issuing CA. It is recommended that you do not configure validity periods that are longer than half of total lifetime of EncryptionConsulting Issuing CA certificate, which was issued to be valid for 10 years. To limit issued certificates to 5 years, run the following commands from an administrative command prompt:
 - O Certutil -setreg CA\ValidityPeriodUnits 5
 - O Certutil -setreg CA\ValidityPeriod "Years"

Task 2: Enable Auditing on the Issuing CA

CA auditing depends on system **Audit Object Access** to be enabled. The following instructions describe how to use Local Security Policy to enable object access auditing.

1. Click Start, click Administrative Tools, and then select Local Security Policy.



- 2. Expand Local Policies and then select Audit Policy.
- 3. Double click Audit Object Access and then select Success and Failure then click OK.



- 4. Close Local Security Policy editor.
- 5. Enable auditing for the CA by selecting which group of events to audit in the Certificate Authority MMC snap-in or by configuring AuditFilter registry key setting. To configure Auditing for all CA related events, run the following command from an administrative command prompt:

Certutil -setreg CA\AuditFilter 127



Task 3: Configure the AIA

Using a certutil command is a quick and common method for configuring the AIA. When you run the following certutil command, you will be configuring a static file system location, a lightweight directory access path (LDAP) location, and http location for the AIA. The certutil command to set the AIA modifies the registry, so ensure that you run the command from an command prompt run as Administrator. Run the following command:

certutil -setreg CA\CACertPublicationURLs "1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt\n2:ldap:///CN=%7,CN=AIA, CN=Public Key Services,CN=Services,%6%11\n2:http://pki.EncryptionConsulting.com/CertEnroll/%1_%3%4.crt"



After you have run that command, run the following command to confirm your settings: certutil -getreg CA\CACertPublicationURLs

If you look in the registry, under the following

path: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CertSvc\Configuration\EncryptionConsulting Issuing CA, you can confirm the CACertPublicationURLs by opening that REG_MULTI_SZ value. You should see the following:

1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt

2:Idap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11

2:http://pki.EncryptionConsulting.com/CertEnroll/%1_%3%4.crt

You can also see this in the the CA (certsrv) console. To open the console, click **Start**, click **Administrative Tools**, and then click **Certification Authority**. In the navigation pane, expand the **Certificate Authority (Local)**. Right-click **EncryptionConsulting Root CA** and then click **Properties**. On the **Extensions tab**, under **Select extension**, click **Authority Information Access (AIA)** and you will see the graphical representation of the AIA settings.

From an administrative command prompt, run the following command to copy the EncryptionConsulting Issuing CA certificate to the http AIA location:

copy "c:\Windows\System32\certsrv\certenroll\CA02 EncryptionConsulting.com_ EncryptionConsulting Issuing CA.crt"\\srv1.EncryptionConsulting.com\c\$\certenroll\

Task 4: Configure the CDP

The certutil command to set the CDP modifies the registry, so ensure that you run the command from an command prompt run as Administrator. Run the following command:

certutil -setreg CA\CRLPublicationURLs "65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl\n79:ldap:///CN=%7%8,CN=%2, CN=CDP,CN=Public Key Services,CN=Services,%6%10\n6:http://pki. EncryptionConsulting.com/CertEnroll/%3%8%9.crl\n65:\\srv1. EncryptionConsulting.com\CertEnroll\%3%8%9.crl\%3%8%9.crl

After you run that command, run the following certutil command to verify your settings:

certutil -getreg CA\CRLPublicationURLs

In the registry

location:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\EncryptionConsulting Issuing CA you can open the REG_MULTI_SZ value and see the configuration of these values:

65:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl

79:Idap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10

6:http://pki.EncryptionConsulting.com/CertEnroll/%3%8%9.crl

65:\\srv1.EncryptionConsulting.com\CertEnroll\%3%8%9.crl

You can also see this in the the CA (certsrv) console. To open the console, click **Start**, click **Administrative Tools**, and then click **Certification Authority.** In the navigation pane, ensure that **Certificate Authority(Local**) is expanded. Right-click **EncryptionConsulting Root CA** and then click **Properties.** On the **Extensions** tab, under **Select extension**, click **CRL Distribution Point (CDP)** and you will see the graphical representation of the CDP settings.

At an administrative command prompt, run the following commands to restart Active Directory Certificate Services and to publish the CRL.

net stop certsvc && net start certsvc

certutil -crl



Activity 7: Install and Configure the Online Responder Role Service

Task 1: Install the Online Responder Role Service on SRV1

- 1. Ensure that you are logged on to SRV1. EncryptionConsulting.com as EncryptionConsu\Administrator.
- 2. Open Server Manager.
- 3. Right click on **Roles**, and then click **Add Roles**.
- 4. On the **Before You Begin** page, then select **Next.**
- 5. On the **Select Installation type** page, select **Role-based or feature-based installation** and then click **Next**.
- 6. On the Server Selection page, click Next.
- 7. On the Select Server Roles page, select Active Directory Certificate Services and then click Next.

elect server rol	es	DESTINATION SERVE SRV1.EncryptionConsulting.co
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Select one or more roles to install on the selected server. Roles Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server Fax Server Fax Server File and Storage Services (2 of 12 installed) Host Guardian Service Hyper-V Network Policy and Access Services Frint and Document Services Femote Access Remote Desktop Services Volume Activation Services	Description Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
	Windows Deployment Services	

- 8. On the **Features** page, click **Next.**
- 9. On Introduction to Active Directory Certificate Services page, click Next.



- 10. On the Select Role Services page, clear the Certification Authority, and then select Online Responder. Click Next.
 - Note: You do not want to install a Certification Authority on SRV1.EncryptionConsulting.com, so you are clearing that checkbox.
 - If the Add role services and features required for Online Responder page appears, click Add Required Role Services and then click Next. Then, on the Web Server (IIS), click Next.

Land Roles and Features Wizard	4	- 6 ×
Select role service	ces	DESTINATION SERVER SRV1.EncryptionConsulting.com
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Select the role services to install for Active Directory Certi Role services Certification Authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder	ificate Services
	< Previou	s Next > Install Cancel

11. On the Confirm Installation Selections page, click Install. Click Close when the installation is complete.





12. Click on **"Configure Active Directory Certificate Services on the destination server"**, on the Credential Page, make sure **Encryptionconsu\Administrator** is mentioned, then click **Next**.

📥 AD CS Configuration	
Credentials	DESTINATION SERVER SRV1.EncryptionConsulting.com
Credentials Role Services Confirmation Progress Results	Specify credentials to configure role services To install the following role services you must belong to the local Administrators group: • Standalone certification authority • Certification Authority Web Enrollment • Online Responder To install the following role services you must belong to the Enterprise Admins group: • Enterprise certification authority • Certificate Enrollment Policy Web Service • Certificate Enrollment Web Service • Network Device Enrollment Service Credentials: ENCRYPTIONCONSU\Administrator Change
	More about AD CS Server Roles
	< Previous Next > Configure Cancel





14. On the **confirmation** page, verify the details and click **Next**.



Task 2: Add the OCSP URL to the Encryption Consulting Issuing CA

To add the OCSP URL to the EncryptionConsulting Issuing CA:

- 1. Ensure that you are logged on to CA02. EncryptionConsulting.com as EncryptionConsu\Administrator
- 2. In the Certification Authority console, in the console tree, right-click EncryptionConsulting Issuing CA, and then click Properties.
- 3. On the Extensions tab, under Select extension, select Authority Information Access (AIA), and then click Add.
- 4. In Location, type http://srv1.EncryptionConsulting.com/ocsp and then click OK.
- 5. Select Include in the online certificate status protocol (OCSP) extension.
 - Note: A common misconfiguration is to select both checkboxes in the Extensions tab, which is incorrect.
 Ensure that Include in the online certificate status protocol (OCSP) extension checkbox is the only one selected.



General Policy Module Exit Module Extensions Storage Certificate Managers Select extension: Authority Information Access (AIA) Specify locations from which users can obtain the certificate for this CA. Specify locations from which users can obtain the certificate for this CA. Select extension: C:\Windows\system32\CertSrv\CertEnroll\ <serverdnsname>_<canarl cn="<CATruncatedName" idap:="">,CN=AIA,CN=Public Key Services,CN http://pki. EncryptionConsulting.com/ocsp Add Add Remove</canarl></serverdnsname>	Enrollment Agents	Auditing	Reco	very Agents	Se	curity
Extensions Storage Certificate Managers Select extension: Authority Information Access (AIA) Specify locations from which users can obtain the certificate for this CA. C:\Windows\system32\CertSrv\CertEnroll\ <serverdnsname>_<canarl cn="<CATruncatedName" idap:="">,CN=AIA,CN=Public Key Services,CN http://pki. EncryptionConsulting.com/CertEnroll/<serverdnsname>_<cher <serverdnsname="" certenroll="">_<cher <serverdnsname="" certenroll="">_<cher <serverdnsname="" certenroll="">_<center certenroll<="" td=""> Include in the AIA extension of issued certificates Include in the online certificate status protocol (OCSP) extension</center></center></center></center></center></center></center></center></center></center></center></center></center></center></center></center></center></center></center></center></cher></cher></cher></serverdnsname></canarl></serverdnsname>	General	Policy M	odule	E	xit Module	э
Select extension: Authority Information Access (AIA) Specify locations from which users can obtain the certificate for this CA. C:\Windows\system32\CertSrv\CertEnroll\ <serverdnsname>_<canar cn="<CATruncatedName" idap:="">,CN=AIA,CN=Public Key Services,CN http://pki.EncryptionConsulting.com/certEnroll/<serverdnsname>_<c <="" http:="" ocsp="" p="" srv1.encryptionconsulting.com=""> Add Remove Include in the AIA extension of issued certificates Include in the online certificate status protocol (OCSP) extension</c></serverdnsname></canar></serverdnsname>	Extensions	Storage		Certificate	Manage	rs
Authority Information Access (AIA) Specify locations from which users can obtain the certificate for this CA. C:\Windows\system32\CertSrv\CertEnroll\ <serverdnsname>_<canar cn="<CATruncatedName" idap:="">,CN=AIA,CN=Public Key Services,CN http://pki. EncryptionConsulting.com/ocsp Add Remove Include in the AIA extension of issued certificates Include in the online certificate status protocol (OCSP) extension</canar></serverdnsname>	Select extension:					
Specify locations from which users can obtain the certificate for this CA. C:\Windows\system32\CertSrv\CertEnroll\ <serverdnsname>_<canar Idap:///CN=<catruncatedname>,CN=AIA,CN=Public Key Services,CN http://pki. EncryptionConsulting.com/CertEnroll/<serverdnsname>_<c http://srv1.EncryptionConsulting.com/ocsp Add Remove Include in the AIA extension of issued certificates Include in the online certificate status protocol (OCSP) extension</c </serverdnsname></catruncatedname></canar </serverdnsname>	Authority Information /	Access (AIA)				- 3
Add Remove	C:\Windows\system3 Idap:///CN= <catrunc http://pki. Encryption http://srv1.Encryption</catrunc 	2\CertSrv\Cert atedName>,C Consulting.con	tEnroll\ <s N=AIA,C n/CertEnro m/ocsp</s 	erverDNSNa N=Public Key bll/ <serverdn< td=""><td>me>_<ca / Services ISName></ca </td><td>aNar s,CN</td></serverdn<>	me>_ <ca / Services ISName></ca 	aNar s,CN
	<				_	>

6. Click **OK**. When prompted by the **Certification Authority** dialog box to restart Active Directory Certificate Services, click **Yes**.

Important: The EncryptionConsulting Issuing CA will now include http://srv1. EncryptionConsulting.com/ocsp URL as part of Authority Information Access (AIA) extension in all newly issued certificates issued or renewed or re-enrolled certificates. However, certificates enrolled from EncryptionConsulting Issuing CA prior to this change will not have this URL.



Task 3: Configure and Publish the OCSP Response Signing Certificate on the Encryption Consulting Issuing CA

To configure the OCSP response signing certificate:

- 1. On CA02. EncryptionConsulting.com, ensure that you are logged on as EncryptionConsu\Administrator.
- 2. In the **Certification Authority** console, ensure that the EncryptionConsulting Issuing CA is expanded in the console tree.
- 3. Right-click on **Certificate Templates** and then click **Manage. Certificate Templates** opens and displays the certificate templates stored in Active Directory.
- 4. In the details pane (middle pane) right-click **OCSP Response Signing** and then click **Properties.**
- 5. On the Security tab click Add. Click Object Types.
- 6. In the **Object Types** dialog box, select **Computers** and then click **OK**.
- 7. In Enter the object names to select, type SRV1 and then click Check Names. Click OK.
- 8. Ensure that SRV1 is selected and in the Allow column, ensure that the Read and Enroll permissions are selected. Click OK.
- 9. Close Certificate Templates MMC console.
- 10. In certsrv console, right-click Certificate Templates, then select New and then select Certificate Template to Issue.
- 11. In the Enable Certificate Templates dialog box, click OCSP Response Signing and the click OK.

🙀 certsrv - [Certification Authority (Lo	ocal)\EncryptionConsulting Issuing CA	\Certificate Templates]	 ٥	×
File Action View Help				
🗢 🄿 🖄 🙆 🖄				
 Certification Authority (Local) EncryptionConsulting Issuing Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates 	Name OCSP Response Signing	Intended Purpose OCSP Signing		

Task 4: Configure Revocation Configuration on the Online Responder

To configure the revocation configuration:

- 1. On SRV1.EncryptionConsulting.com, ensure that you are logged on as EncryptionConsu\Administrator.
- 2. Open Server Manager navigate to **Tools** and click on **"Online Responder Management".**
- 3. Right-click **Revocation Configuration** and then click **Add Revocation Configuration**.



4. On the **Getting Started with Adding a Revocation Configuration** page click **Next.**

Add Revocation Configuration		?	×
Getting star	rted with adding a revocation configuration		
Getting started with addi Name the Revocation Co Select CA Certificate Loca Choose CA Certificate Select Signing Certificate Revocation Provider	 Welcome to the Add Revocation Configuration Wizard. This wizard helps you add revocation configuration to your Online Responder Array. To complete this task, you need to: 1. Specify a name for the new revocation configuration 2. Select a CA certificate to associate with the revocation configuration 3. Select a signing certificate to sign Online Responder responses 4. Configure the revocation provider that will process revocation status requests 	a	
	< Previous Next > Finish Car	ncel	

5. In Name, enter EncryptionConsulting Issuing CA, and then click Next.

Add Revocation Configuration	?	×

ect CA Certificate Loca Name: Second Sec	The CA you would
ect CA Certificate Loca	
Name: Formation Computing Computing Co	
oose CA Certificate	
ect Signing Certificate	
vocation Provider	



6. On the Select CA Certificate Location page ensure that Select a certificate for an Existing enterprise CA is selected, then click Next.

Add Revocation Configuration	?		×
Select CA C	ertificate Location		
Getting started with addi Name the Revocation Co Select CA Certificate Loca Choose CA Certificate Select Signing Certificate Revocation Provider	 Specify the location of the CA certificate that you want to associate with this revocation. Select a certificate for an Existing enterprise CA Select this option if your CA certificate is available in Active Directory or on the CA computer Select a certificate from the Local certificate store Select this option if the CA certificate is available in a certificate store on the local computer Import certificate from a File Select this option if the CA certificate has been saved as a file 	ion	
	< Previous Next > Finish Cance	I.	

- 7. On the **Choose CA Certificates** page, ensure that **Browse CA certificates published in Active Directory** is selected, and then click **Browse.**
- 8. On the Select Certification Authority dialog box, ensure that EncryptionConsulting Issuing CA is selected, and then click OK. Click Next.





9. Leave the defaults on the **Select Signing Certificate** page, and then click **Next.**

Add Revocation Configuration	ing Certificate		?	×
Getting started with addi Name the Revocation Co Select CA Certificate Loca Choose CA Certificate Select Signing Certificate Revocation Provider	Revocation information is sign select a signing certificate auto certificate for each Online Resp Auto-Enroll for an OCSF Certification authority: Certificate Template: Manually select a signing of Note: You will need to speci Online Responder Array. Use the CA certificate for the 	ed before it is sent to a client. T omatically, or you can manually oonder. ng certificate 9 signing certificate CA02.EncryptionConsulting.con OCSPResponseSigning ertificate fy a signing certificate for each the revocation configuration	he Online Responder car select a signing m\EncryptionConsultir Browse wember in the	
10. On the Revocation	Provider page, click Provider.			
Add Revocation Configuration			? ×	

Select CA Certificate Loca	To view and edit the	properties of the	revocation provi	der, click the Pr	ovider button.
Choose CA Certificate					Provider
Select Signing Certificate					
Revocation Provider					

Revocation Provider

0



- 11. Review the choices listed for OCSP Responder to down CRLs in the form of LDAP and HTTP locations.
 - Note: Depending on your needs you could select either the LDAP or HTTP as your primary location for OCSP Responder to download CRLs. You can change order for LDAP and HTTP URLs using Move Up or Move Down button. Leave the defaults as they appear.
- 12. Clear the **Refresh CRLs based on their validity periods**. In the **Update CRLs at this refresh interval (min)** box, type **15**, and then click **OK**. Click **Finish**.
 - Note: Modifying this setting to download CRLs at a faster rate than the CRLs normal expiration makes it possible for the OCSP responder to rapidly download new CRLs rather than use the last downloaded CRLs normal expiration date. Pro duction needs may differ from the value chosen here.
- 13. In the Certification Authority console, expand Array Configuration and then click SRV1.
- 14. Review **Revocation Configuration Status** in the middle pane to ensure there is a signing certificate present and the status reports as OK. The provider is successfully using the current configuration.

Task 5: Configure Group Policy to Provide the OCSP URL for the EncryptionConsulting Issuing CA

This configuration would only be needed to allow existing certificate holders to take advantage of a new OCSP responder without having to re-enroll new certificates with the required OCSP URL added in them.

- 1. Ensure you are logged on to DC01. EncryptionConsulting.com as EncryptionConsu\Administrator.
- 2. Open an administrative command prompt and run the following commands:
 - 0 **cd**\
 - certutil -config "ca02.EncryptionConsulting.com\EncryptionConsulting Issuing CA" -ca.cert EncryptionConsultingissuingca.cer
- 3. Click **Start**, click **Run**, and then type **gpmc.msc**. Press **ENTER**.
- 4. Expand Forest, expand Domains, expand EncryptionConsulting.com, and then expand Group Policy Objects.
- 5. Right click **Default Domain Policy**, then click **Edit**.
- 6. Under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, and then expand **Public Key Policies**.
- 7. Right-click Intermediate Certification Authorities, and then click Import.



8. On the Welcome to Certificate Import Wizard page, click Next.

🛃 Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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.

Store Location	
O Current User	
Local Machine	

To continue, click Next.

Cancel	Next
10	



9. In File name, type C:\EncryptionConsultingissuingca.cer, and then click Next.

Specify the file you want to import.	
ile name:	
C:\EncryptionConsultingissuingca.cer	Browse
Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 Cer Microsoft Serialized Certificate Store (.SST)	tificates (.P7B)



Cancel

Next

- 10. On the **Certificate Store** page, click **Next.**
- 11. On the **Completing the Certificate Import Wizard**, click **Finish**, and then click **OK**.

纋 Certificate Import Wizard

.

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Intermediate Certification Authorities
Content	Certificate
File Name	C:\EncryptionConsultingissuingca.cer

Finish Cancel	Finish
---------------	--------



- 12. In the console tree, select Intermediate Certification Authorities.
- 13. In the details pane, right-click **EncryptionConsulting Issuing CA certificate**, then click **Properties.**
- 14. On the OCSP tab, in Add URL enter http://srv1.EncryptionConsulting.com/ocsp, and then click Add URL. Click OK.

pecify	additional OCSP	download lo	cations.		
Online	e Certificate Stat able Certificate	us Protocol (C Revocation Li	DCSP) Download URL sts (CRL) (not recom	s mended)	
A	dd URL				
http	://srv1.Encrypti	onConsulting.	com/ocsp		
1					
Rei	move URL				
Rei	move URL				

15. Close the Group Policy Management Editor and then close Group Policy Management console.



Activity 8: Verify the PKI Hierarchy Health

Task 1: Win10

- 1. Log on to WIN10 as the local administrator.
- 2. Click Start, type ncpa.cpl and press ENTER.
- 3. In Network Connections, right-click the Local Area Connection and then click Properties.
 - If there are more than one Local Area Connection icons in the Network Connections, you want to modify the one that is connected to network segment shared by all the computers that you have installed for this lab.
- 4. Click the Internet Protocol Version 4 (TCP/IPv4) and then click Properties.
- 5. Select the **Use the Following IP address**. Configure the **IP address**, **Subnet mask**, and **Default gateway** appropriately for your test network.
 - O IP Address: 192.168.1.14
 - O Subnet mask: 255.255.255.0
 - **Default gateway**: <optional>
- 6. Select the Use the following DNS server address. Configure the Preferred DNS server as the IP address of your domain controller. Click OK. Click Close.
 - O Preferred DNS Server: 192.168.1.10.
- 7. Click **Start**, type **sysdm.cpl** and press **ENTER**. Click **Change**. (Ensure the computer name is already set to **WIN10** otherwise change it)
- 8. In **Member of**, select **Domain**, and then type **EncryptionConsulting.com**. Click **OK**.
- 9. In Windows Security, enter the Username and password for the domain administrator account. Click OK.
- 10. You should be welcomed to the EncryptionConsulting domain. Click **OK**.
- 11. When prompted that a restart is required, click **OK**. Click **Close**. Click **Restart Now**.

Task 2: Check PKI Health with Enterprise PKI

To use the Enterprise PKI console to check PKI health:

- 1. On CA02. EncryptionConsulting.com, ensure that you are logged on as EncryptionConsu\Administrator.
- 2. Open Server Manager.
- 3. In the console tree, under Roles and Active Directory Certificate Services, click Enterprise PKI.
 - O Alternatively, you can run Enterprise PKI by running **PKIView.msc** from an administrative command prompt.
- 4. Right click Enterprise PKI and then click Manage AD Containers.



Manage AD Containers

Certification Author	rities Container	Enrollment S	ervices (Container
NTAuthCertificates	AIA Container	CDP Container	KR	A Containe
Name			Status	
EncryptionConsult	ng Issuing CA	(ок	
Add	Remove	lew		

- 5. On the **NTAuthCertificates** tab, verify the EncryptionConsulting Issuing CA certificate appears with a status of **OK**.
- 6. On the AIA Container tab, verify both the EncryptionConsulting Root CA and the EncryptionConsulting Issuing CA certificates are present with a status of OK.
- 7. On **CDP Container** tab, verify **EncryptionConsulting Root CA base CRL, EncryptionConsulting Issuing CA base**, and the **Delta CRLs** are present with a status of **OK**.
- 8. On **Certification Authorities Container**, verify **EncryptionConsulting Root CA** certificate is present with a status of **OK**.
- 9. On Enrollment Services Container, verify EncryptionConsulting Issuing CA certificate is present with a status of OK.

Task 3: Configure Certificate Distribution on the Encryption Consulting Issuing CA

To publish a certificate for computers in the enterprise:

- 1. On CA02. EncryptionConsulting.com, ensure that you are logged on as EncryptionConsu\Administrator.
- 2. In the **Certification Authority** console, ensure that **EncryptionConsulting Issuing CA** is expanded.
- 3. Right-click Certificate Templates select New and select Certificate Template to Issue.
- 4. On the **Enable Certificate Templates** dialog box, click **Workstation Authentication**, page and then click **OK**.

ulting Issuing CA\Certificate Templates]	—	٥	\times
Intended Purpose hentication Client Authentication Signing OCSP Signing			
H S	Iting Issuing CA\Certificate Templates] Intended Purpose Tentication Igning OCSP Signing	Iting Issuing CA\Certificate Templates] — Intended Purpose Tentication Client Authentication Igning OCSP Signing	Iting Issuing CA\Certificate Templates] — 🗍

Task 4: Obtain a Certificate Using WIN10 and Verify PKI Health

To obtain a certificate for WIN10 and verify PKI health:

- 1. Log into Win10. EncryptionConsulting.com as EncryptionConsu\Administrator. (Ensure that you switch user to log on as EncryptionConsu\Administrator)
- 2. Click **Start**, type **mmc** and then press ENTER.
- 3. Click File, and then click Add/Remove Snap-in.



4. Click **Certificates**, then click **Add**. Select **Computer Account**, and then click **Finish**. Click **OK**.

You can select snap-ins for this console extensible snap-ins, you can configure Available snap-ins:	le from those e which exte	available on your computer and configure the selected set of snap-ins. F nines are enabled Certificates snap-in	or		×
Snap-in Vendor ActiveX Control Microsoft Certificates Microsoft Computer Manager Microsoft Computer Manager. Microsoft Device Manager Microsoft Disk Management Microsoft Event Viewer Microsoft Folder Microsoft Disk Management Microsoft Description: The Certificates snap-in allows you to	t Cor t Cor	This snap-in will always manage certificates for: My user account Service account Computer account			
		< Back	Next >	Cano	el

- 5. Expand **Certificates**, right click **Personal**, click **All Tasks**, and then click **Request New Certificate**.
- 6. On the **Before you begin** page, click **Next.**
- 7. On the Select Certificate Enrollment Policy page, click Next.
- 8. Select **Workstation Authentication**, click **Enroll**. When the certificate is enrolled, click **Enroll**.

Console1 -	- [Console Root\Certificates (Local Compute	r)\Personal]		00		×
🚡 File 🥠			5555	\Box >	< <u> </u>	e ×
🗢 🔿 🛛 🖕	Certificate Enrollment					
Consol						
Cer	Request Certificates					-
> 🖆 >	You can request the following types of co click Enroll.	ertificates, Select the certificates you wa	int to request,	and then	ns	
>	Active Directory Enrollment Policy					
	Workstation Authentication	i STATUS: Available		Details 💙		
> 11 > 11 > 11 > 11						
	Show all templates					
٢	10		Enroll	Cancel		



- 9. In the console tree, expand **Personal**, click **Certificates**. In the details pane, right click the **win10**. **EncryptionConsulting.com** certificate, click **All Tasks**, and then click **Export**.
- 10. On the the Welcome to Certificate Export Wizard page, click Next.

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, dick Next.

Next	Cancel
------	--------

 \times



11. On the Export Private Key, click Next. (No, do not export the private key is selected by default).

Export Private Key You can choose to export the private key with the certificate.		
Private keys are certificate, you	password protected. If you want to export the pr ust type a password on a later page.	ivate key with the
Do you want to	xport the private key with the certificate?	
🔿 Yes, exp	ort the private key	
🖲 No, do n	t export the private key	
Note: The assoc can be exported	ated private key is marked as not exportable. Onl	y the certificate

- 12. On the **Export File Format** page, click Next. [DER encoded binary X.509 (.CER) is the default selection].
- 13. On the File to Export page, type C:\win10, and then click Next.
- 14. On the **Completing the Certificate Export Wizard** page, click then **Finish**, and then click **OK**.
- 15. Open a command prompt and run the following commands: (To open a command prompt, click **Start**, type **cmd**, and then press ENTER)
 - o **cd**\
 - o certutil -URL C:\win10.cer
- 16. In the URL Retrieval Tool, perform the following steps, in the **Retrieve** section:
 - o Select OCSP (from AIA) option and then click Retrieve. Confirm that it shows status as Verified.
 - o Select CRLs (from CDP) option and then click Retrieve. Confirm that it shows status as Verified.
 - o Select Certs (from AIA) option and then click Retrieve. Confirm that it shows status as Verified.
- 17. Click **Exit** to close URL Retrieval Tool.
- 18. From command prompt run following command to thoroughly verify certificate chain retrieval and revocation status.
 - o certutil -verify -urlfetch c:\win10.cer
- 19. Review the output and make sure all the chain retrieval and revocation status successfully verified.