

# SSL Certificate Management for XenData Web services

## Table of Contents

XenData Web Services	Error! Bookmark not defined.
1. Creating a Certificate Signing Request (CSR)	
2. Submitting a Re-Key Request for an Existing SSL Cert	
3. Installing the Certificate on the Server	

*Note: Local Administrators* is the minimum group membership required to complete these procedures.

## 1. Creating a Certificate Signing Request (CSR)

If you are ordering your SSL certificate from DigiCert, you can skip steps **1.1** through **1.22** and instead, follow the instructions found here: <u>https://www.digicert.com/kb/util/csr-creation-</u> microsoft-servers-using-digicert-utility.htm

The following instructions will generate a Certificate Signing Request, *they should be followed on the server that the SSL certificate will be installed on*. The CSR can be submitted when requesting an SSL certificate, the Certificate Authority will create an SSL certificate based on the CSR. If an SSL certificate has already been requested and created, the same CSR can be used to request a 're-key', whereupon the Certificate Authority will provide a new SSL certificate based on the CSR.

- 1.1 Right-Click Start, select Run
- 1.2 Type MMC in the Run box and press Enter
- 1.3 Click on the Files menu, then click Add/Remove Snap-in
- 1.4 From the available snap-ins list, click Certificates then click Add

Console1 - [Console]	Add or Remove Snap-ins				×	
Console Root	You can select snap-ins for the snap-ins, you can configure to			le on your computer and configure the selected set of	f snap-ins. For extensible	
	Available snap-ins:			Selected snap-ins:		<b></b>
	Snap-in	Vendor	^	Console Root	Edit Extensions	•
	ActiveX Control	Microsoft Corp Microsoft Corp			Remove	
	Certificates	Microsoft Corp Microsoft Corp			Move Up	
	Computer Managem	Microsoft Corp Microsoft Corp			Move Down	
	Event Viewer	Microsoft and Microsoft Corp Microsoft Corp		dd >		
	Group Policy Object	Microsoft Corp Microsoft Corp				
	IP Security Policy Ma	Microsoft Corp Microsoft Corp				
	Local Backup	Microsoft Corp	~		Advanced	
	Description:					
	The Certificates snap-in allo	ws you to browse t	he cor	s of the certificate stores for yourself, a service, or a c	omputer.	
					OK Cancel	

1.5 Select Computer account, then click Next

Certificates snap-in		×
This snap-in will always manage certificates for: My user account Service account Computer account		
	< Back Next > Cance	əl

1.6 Select Local computer and click Finish

Select Computer	×
Select the computer you want this snap-in to manage. This snap-in will always manage:	
Another computer:	owse
Allow the selected computer to be changed when launching from the command line only applies if you save the console.	e. This
< <u>B</u> ack Finish	Cancel

**1.7** On the Add or Remove Snap-ins dialog, click on OK

ailable <u>s</u> nap-ins:			ſ	Selected snap-ins:	
Snap-in	Vendor	^		Console Root	Edit Extensions
ActiveX Control	Microsoft Corp			🙀 Certificates (Local Computer)	Damage
Authorization Manager	Microsoft Corp				Remove
Certificates	Microsoft Corp				
Component Services	Microsoft Corp				Move Up
Computer Managem	Microsoft Corp				
Device Manager	Microsoft Corp				Move <u>D</u> own
🚏 Disk Management	Microsoft and		<u>A</u> dd >		
🛃 Event Viewer	Microsoft Corp				
🗎 Folder	Microsoft Corp				
Group Policy Object	Microsoft Corp				
IP Security Monitor	Microsoft Corp				
IP Security Policy Ma	Microsoft Corp				
Link to Web Address	Microsoft Corp				
🖢 Local Backup	Microsoft Corp				Advanced
Local Licerc and Gro	Microsoft Corn	1	L		

- **1.8** Under the Console Root folder, expand Certificates (Local computer)
- **1.9** Right-click the Personal folder and select: All Tasks, then Advanced Options, and click Create Custom Request

🚡 Console1 - [Console Root\Certificates (Local Compu	ter)\Personal]		– 🗆 🗙
File Action View Favorites Window Help			_ <i>8</i> ×
🗢 🔿 🙍 🗊 📋 🝳 📾			
Console Root	Object Type		Actions
Certificates (Local Computer)     Personal	Certificates		Personal 🔺
> Trust Find Certificates			More Actions
> 🖆 Enter All Tasks >	Find Certificates		
> 🛄 Trust View >	Request New Certificate		
> C Untru New Window from Here	Import		
> Trust New Taskpad View	Advanced Operations	Create Custom Request	
> Clien Refresh		Manage Enrollment Policies	
> Previ Renesin > Test f Export List			
> Che Help			
Cocal content of the second seco			
Remote Desktop			
Certificate Enrollment Requests			
> 📔 s3archive1.xendata.com			
> Smart Card Trusted Roots			
> 🛄 Trusted Devices			
> indows Live ID Token Issuer			
> WindowsServerUpdateServices	<	>	
&Create Custom Request			

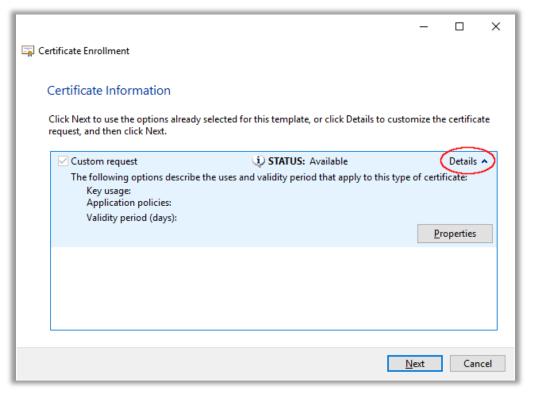
- **1.10** On the Certificate Enrollment dialog, read Before you begin, click on Next
- **1.11** On the Select Certificate Enrollment Policy dialog, select Proceed without enrollment policy, click on Next

		_		×
🔄 C	ertificate Enrollment			
	Select Certificate Enrollment Policy			
	Certificate enrollment policy enables enrollment for certificates based on predefined Certificate enrollment policy may already be configured for you.	certificate	templates	
	Configured by you		Add Ne	w
	Custom Request			
	Proceed without enrollment policy			
		<u>N</u> ext	Cance	el

1.12 On the Custom Request dialog, leave the default values, then click Next

		-		×
🔄 Certificate Enrollment				
Custom request				
Chose an option from	the list below and configure the certificate options as required.			
Template:	(No template) CNG key		~	
	Suppress default extensions			
Request format:	<u>PKCS #10         </u> <u> </u> <u> </u>			
	<u>○ c</u> mc			
	not available for certificates based on a custom certificate reques the certificate template.	t, even v	vhen this	
		<u>N</u> ext	Can	cel

1.13 Expand the details pane and select Properties



**1.14** Add a Friendly name and description for the certificate, then select the Subject tab

General Subject Ex A friendly name and Friendly <u>n</u> ame: s3archive1.xendata. <u>D</u> escription: XenData Archive Se	d descript	Private Key ion will make i	t easier to ide	entify and	d use a cer	tificate.
Friendly <u>n</u> ame: s3archive1.xendata. <u>D</u> escription:	.com	ion will make i	t easier to ide	entify and	d use a cer	tificate.
s3archive1.xendata. Description:						
Description:						
	erver					
XenData Archive Se	erver					
			OK		Cancel	Apply

1.15 Move to the Subject tab, and add certificate details, the ones we used were Common Name, Organization, Organization Unit, Location, County

Certificate Pr	operti	es		)
General Su	bject	Extensions	Private Key	
	forma	tion about	the user or computer to which the certificate is issued. You the types of subject name and alternative name values tha	t
Subject of c	ertific	ate		
The user or	comp	uter that is i	receiving the certificate	
Subject nar	ne:			
Туре:			CN=s3archive1.xendata.com	n
Country		~	Add > O=XenData Inc OU=Engineering	
Value:			L=Walnut Creek	
			< Remove S=California	
Alternative			C=USA	
Type:	name	•	DNS	
DNS			s3archive1.xendata.com	
Value:				
value:			Add >	
			< Remove	
			OK Cancel Apply	

**1.16** Move to the Extensions tab, expand 'Extended Key Usage' and add Server Authentication, and Client Authentication

General	Subject	Extensions	Private Key						
The foll	owing are	the certifica	te extension	s for this cer	tifica	ate type.			^
Key us	age							*	
			_						
Extop	lod Kov II	sage (applica	ation policio	c)				•	
		5			<i>c</i> 1	2000)   (			
				, <u> </u>		ows 2000) def			
		e usea. Select d by this ten		tion policy re	qui	red for valid si	gnatures	01	
certific	ates issue	u by this ten	ipiate.						
	le optior	is:	-			Selected optic			
	Signing	^				Server Authen			
Secure						Client Authen	tication		
	tamping			4.4					
		List Signii	A	.dd >					
		Stamping							
	rity end		< R	emove					
		el termina							
	rity user	~ · · · ·							
Encryp	tina File	Svstem				<		>	
-									
🗌 Mak	e the Exte	nded Key Us	age critical						
Basic o	onstraint	S						•	
									~
				O	K	Cance		Apph	1

**1.17** Move to the Private Key tab and expand 'Cryptographic Service Provider'. Ensure that only RSA Microsoft Software Key Storage Provider is checked

Certificate Properties		×
General Subject Extensions Private Key		
<u>Cryptographic Service Provider</u> A CSP is a program that generates a public and private key pair used in many certificate-related processes. Select cryptographic service provider (CSP):		^
RSA, Microsoft Software Key Storage Provider     DH, Microsoft Software Key Storage Provider     DSA, Microsoft Software Key Storage Provider     ECDH, Microsoft Software Key Storage Provider     ECDH_brainpoolP160r1, Microsoft Software Key Storage Provider     ECDH_brainpoolP160t1, Microsoft Software Key Storage Provider     Show all CSPs	< >	
Key <u>o</u> ptions	*	
Select <u>H</u> ash Algorithm	*	
Select Signature <u>F</u> ormat	•	÷
OK Cancel	<u>A</u> pply	/

**1.18** Expand 'Key Options' and change the Key Size to 2048, and check 'Make Private Key Exportable'

General       Subject       Extensions       Private Key         Select cryptographic service provider (CSP):	^	^
RSA,Microsoft Software Key Storage Provider         DH,Microsoft Software Key Storage Provider         DSA,Microsoft Software Key Storage Provider         ECDH,Microsoft Software Key Storage Provider         ECDH_brainpoolP160r1,Microsoft Software Key Storage Provider         ECDH_brainpoolP160t1,Microsoft Software Key Storage Provider         Storage Provider         ECDH_brainpoolP160t1,Microsoft Software Key Storage Provider         Show all CSPs         Key options         Set the key length and export options for the private key.         Key size:         2048	^	^
RSA,Microsoft Software Key Storage Provider         DH,Microsoft Software Key Storage Provider         DSA,Microsoft Software Key Storage Provider         ECDH,Microsoft Software Key Storage Provider         ECDH_brainpoolP160r1,Microsoft Software Key Storage Provider         ECDH_brainpoolP160t1,Microsoft Software Key Storage Provider         Show all CSPs         Key options         Set the key length and export options for the private key.         Key size:         2048	^	ļ
DH, Microsoft Software Key Storage Provider     DSA, Microsoft Software Key Storage Provider     ECDH, Microsoft Software Key Storage Provider     ECDH_brainpoolP160r1, Microsoft Software Key Storage Provider     ECDH_brainpoolP160t1, Microsoft Software Key Storage Provider     Show all CSPs  Key options Set the key length and export options for the private key. Key size:     2048	^	÷
DSA, Microsoft Software Key Storage Provider     ECDH, Microsoft Software Key Storage Provider     ECDH_brainpoolP160r1, Microsoft Software Key Storage Provider     ECDH_brainpoolP160t1, Microsoft Software Key Storage Provider     Show all CSPs  Key options Set the key length and export options for the private key. Key size:     2048		
ECDH, Microsoft Software Key Storage Provider         ECDH_brainpoolP160r1, Microsoft Software Key Storage Provider         ECDH_brainpoolP160t1, Microsoft Software Key Storage Provider         Show all CSPs         Key options         Set the key length and export options for the private key.         Key size:         2048		
ECDH_brainpoolP160r1,Microsoft Software Key Storage Provider         ECDH_brainpoolP160t1,Microsoft Software Key Storage Provider         Show all CSPs         Key options         Set the key length and export options for the private key.         Key size:         2048		
ECDH_brainpoolP160t1,Microsoft Software Key Storage Provider         Show all CSPs         Key options         Set the key length and export options for the private key.         Key size:         2048		
Show all CSPs         Key options         Set the key length and export options for the private key.         Key size:         2048		
Key options         Set the key length and export options for the private key.         Key size:         2048	~	
Key size: 2048	^	
Make private key exportable		
Allow private key to be archived		
Strong private key protection		
		J

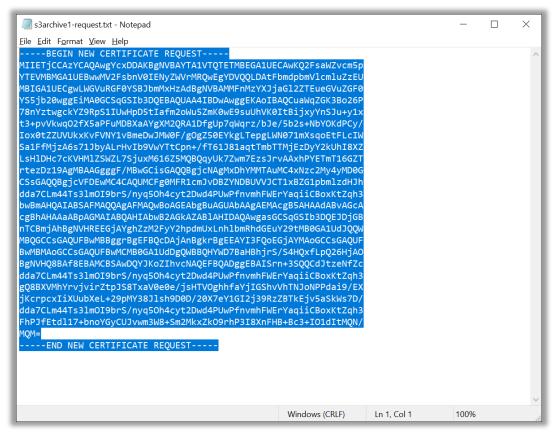
- 1.19 Apply all these settings and click OK
- 1.20 On the Certificate Information dialog, click Next

Certificate Enrollment		
Certificate Information		
Click Next to use the options al request, and then click Next.	Iready selected for this template, or click Details to cus	tomize the certificate
✓ Custom request	😲 STATUS: Available	Details <b>^</b>
Key usage:	scribe the uses and validity period that apply to this ty Server Authentication Client Authentication );	pe of certificate:
		Next Cancel

**1.21** Save the file in Base 64 file format with a .txt extension and select Finish

Certificate Enrollment	
Where do you want to save the offline request?	
If you want to save a copy of your certificate request or want to process the req your hard disk or removable media. Enter the location and name of your certific Finish.	
File Name: s3archive1-request	Browse
File format:	
Base 64	
⊖ Binary	
	Finish Cance

**1.22** Open the saved file, select all and copy, this is the CSR which can be used when requesting an SSL certificate from the Certificate Authority

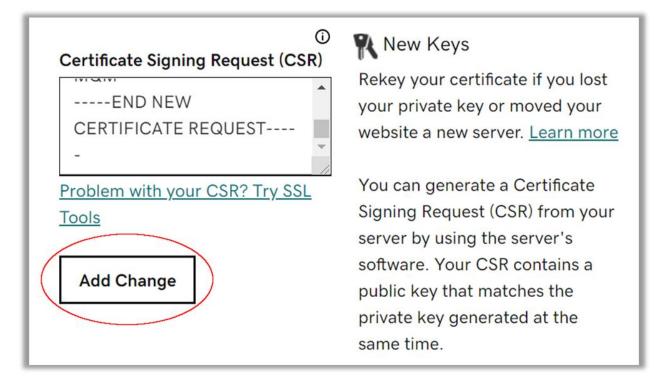


**1.23** Download your SSL certificate. If prompted for Server type, choose "IIS" and download the Zip file. After saving the Zip file, copy it to the server and extract it to a known location

# 2. Submitting a Re-Key Request for an Existing SSL Cert

If an SSL certificate has already been purchased, the CSR can be used to request a re-key for the server on which you want to install the certificate. The following instructions describe the process used to re-key a certificate where the Certificate Authority is GoDaddy; equivalent functionality should be found on the websites of other Certificate Authorities.

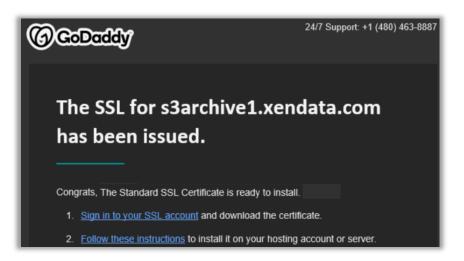
- 2.1 Navigate to the SSL Cert management console
- **2.2** Paste the CSR content into the SSL certificate providers SSL Certificate Signing Request (CSR) tool and click 'Add Change'



**2.3** Submit the certificate request (response times vary from a few minutes to a week or more, depending on the certificate type)

If domain ownership verification is required for these changes, you may choose how you would like to prove you have control of the domain(s).				
Domain Control Options	]			
Cancel	Submit All Changes			

2.4 Your Certificate Authority should email you once the certificate is ready



**2.5** Download your SSL certificate. If prompted for Server type, choose "IIS" and download the Zip file. After saving the Zip file, copy it to the server and extract it to a known location

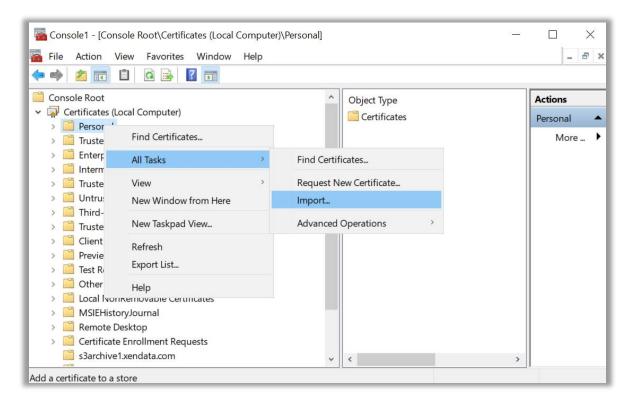
Certificate Details		Download Certificate
Туре	Standard SSL Certificate	To secure your site that's hosted elsewhere, download the Zip file that matches your hosting server type. Then, install all of the
Status	Certificate issued ( <u>Revoke</u> )	certificates in the Zip file on your hosting server, including any intermediate certificates that might be needed for older browsers or
Domain name	s3archive1.xendata.com	servers.
Certificate Issuer	GoDaddy SHA-2	First time installing a certificate? <u>View Installation Instructions for the selected</u> server.
Request Date	7/12/2021 10:13	
Request Submission Type	Rekey	Server type IIS  Download Zip File
Current Certificate Validity Period	7/12/2021 - 4/8/2022	
Subscription Period	4/8/2021 - 4/8/2022	
Serial Number	c6:25:f2:1f:b3:9a:26:17	

# **3. Installing the Certificate on the Server**

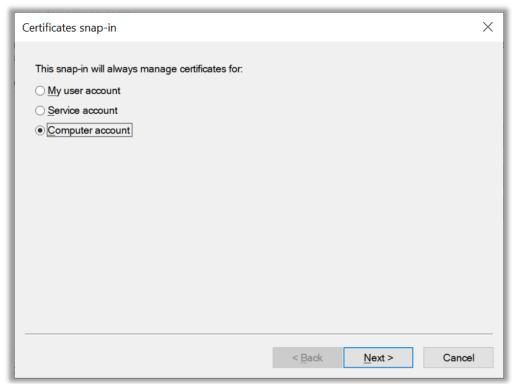
- 3.1 Right-Click Start, select Run
- 3.2 Type MMC in the Run box and press Enter
- 3.3 Click on the Files menu, then click Add/Remove Snap-in
- 3.4 From the available snap-ins list, click Certificates then click Add

Console1 - [Conso	ole Root]						-	- 🗆 X
🚡 File Action Vi	Add or Remove Snap-ins						Х	- 8 ×
Console Root	You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.							
	Available snap-ins:				Selected snap-ins:			<b>^</b>
	Snap-in	Vendor	^		Console Root	Edit Extensions		•
	ActiveX Control	Microsoft Corp Microsoft Corp				Remove		
	Certificates	Microsoft Corp Microsoft Corp				Move Up	e.	
	Computer Managem	Microsoft Corp Microsoft Corp		• • • •		Move Down		
	Disk Management     Event Viewer	Microsoft and Microsoft Corp		Add >				
	Folder	Microsoft Corp Microsoft Corp						
	IP Security Monitor	Microsoft Corp Microsoft Corp						
	Link to Web Address	Microsoft Corp Microsoft Corp	~			Advanced		
	Description:	Microsoft Corn						
	The Certificates snap-in allo	ws you to browse	the c	ontents of the c	ertificate stores for yourself, a service,	or a computer.		
					[	OK Cancel		

**3.5** Under the Certificates – Local Computer Section, Select Personal, then right-click and select and expand All Tasks, then select Import



#### 3.6 Select Computer account, then click Next



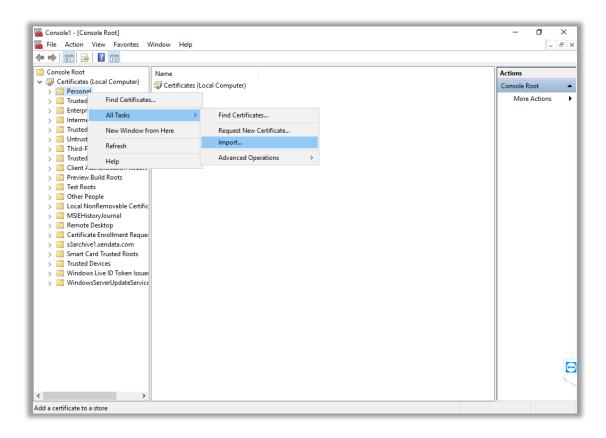
3.7 Select Local computer and click Finish

Select Computer	$\times$
Select the computer you want this snap-in to manage. This snap-in will always manage: [Local computer: (the computer this console is running on)	
Another computer:     Browse      Allow the selected computer to be changed when launching from the command line. This	
only applies if you save the console.	
< <u>B</u> ack Finish Cano	el

## 3.8 On the Add or Remove Snap-ins dialog, click on OK

vailable <u>s</u> nap-ins:			Selected snap-ins:			
Snap-in ActiveX Control Authorization Manager Certificates Component Services Compouter Manager Device Manager Disk Management Event Viewer Tolder	Vendor Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp	^	Add >	Edit Extensions  Edit Extensions  Remove Move Up Move Down		
Group Policy Object P Security Monitor IP Security Policy Ma Link to Web Address Local Backup	Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp Microsoft Corp	*		Ad <u>v</u> anced		
Description: The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.						

**3.9** Under the Console Root folder, expand Certificates (Local computer). Right-click the Personal folder and select All Tasks - Import



3.10 Click Next on the Welcome to the Certificate Import Wizard dialog

🔶 🛿 🐉 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 Qurrent User Local Machine	
To continue, click Next.	
<u>N</u> ext Can	cel

**3.11** Browse to the location you extracted the SSL certs ZIP file and select the .CRT file and click Next

🗧 🐉 Certificate Import Wizard
File to Import Specify the file you want to import.
File name: Browse
Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B) Microsoft Serialized Certificate Store (.SST)
Next Cancel

**3.12** Choose to place all certificates into the Personal Certificate store and click Next

÷	🛃 Certificate Import Wizard	×
	<b>Certificate Store</b> Certificate stores are system areas where certificates are kept.	
	Windows can automatically select a certificate store, or you can specify a location for the certificate.	
	Place all certificates in the following store     Certificate store:	
	Personal B <u>r</u> owse	
	<u>N</u> ext Cance	el l

### 3.13 Click on Finish

÷	Certificate Import Wizard	×
	Completing the Certifica	te Import Wizard
	The certificate will be imported after y	
	You have specified the following settin Certificate Store Selected by User	Personal
	Content File Name	Certificate C:\Users\Administrator\Documents\s3archive1.xendat
	٢	>
		<u>F</u> inish Cancel

Certificate Import Wizard					
The import was successful.					
	OK				

3.14 Repeat steps 3.9 through 3.13 for the .P7B file

**3.15** After importing the CRT and P7B files, the certificate should be visible in the Personal Certificate store

See Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]       -       X         See Eile Action View Favgrites Window Help       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -       -								
Console Root  Certificates (Local Computer)  Personal  Certificates  Certificates  Certificates  Certificates  Certification  Certificates  Certification  Certificates  Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates		Issued By Go Daddy Class 2 Certification Au Go Daddy Root Certificate Author Go Daddy Secure Certificate Auth	5/2/2031	Intended Purposes <all> <all> Server Authenticati</all></all>	<	Actions Certificates A More Actions		

**3.16** Double click on the imported certificate and open the Details tab. Scroll to the bottom and then select and copy the contents of the 'Thumbprint' field

<u> </u> Certif	icate				$\times$
General	Details	Certification Path			
Show:	<all></all>		$\sim$		
Su Su Su SC Ba Re Th	bject Alte bject Key T List sic Constr y Usage umbprint	ffb5bbf143f	DNS Name=s3a 076160fb05a1c v1, 2979bef09e Subject Type=E Digital Signature f558c8b0f6ffb5	278ecc348330 rchive 1.xenda 1863ad2fd2e0 393921f05673 ind Entity, Pat e, Key Encipher bbf143f37252 2dda8a159 2dda8a159	<ul> <li></li> </ul>
				OK	:

3.17 Open a PowerShell session with the "Run as Administrator" option

**3.18** Generate a GUID using the following command:

## [guid]::NewGuid().ToString("B")

**3.19** To add the SSL cert to the DNS name, enter the following **netsh** command, replacing:

YOUR\_DNS\_NAME with your DNS name THUMBPRINT with the thumbprint acquired in step 3.16\* \*Remove any spaces and/or any strange characters in the copied thumbprint. GUID with the GUID created in step 3.18

**netsh** http add sslcert certstorename=MY hostnameport=**YOUR\_DNS\_NAME**:443 certhash=**THUMBPRINT** appid='{**GUID**}'

Example:

netsh http add sslcert certstorename=MY hostnameport=archive1.xendata.com:443
certhash=f558c8b0f6ffb5bbf143f372524829b2dda8a159 appid='{6dd8738a-b7b1-46af-a18424cde77be7b2}'

If successful, the command will return the following message:

#### SSL Certificate successfully added

3.20 Add the chosen DNS to your hosts file in windows, the file is located in: C:\Windows\System32\drivers\etc\hosts and can be opened with Notepad
3.21 Open a web browser and point to the DNS. You should be able to access it