

XenData S3 Server Interface Requesting and Installing an SSL Certificate

Table of Contents

1. Creating a Certificate Signing Request (CSR)	3
2. Submitting a Re-Key Request for an Existing SSL Cert	12
3. Installing the Certificate on the Server	14

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-microsoft-servers-using-digicert-utility.htm</u>

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



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	
< <u>B</u> ack <u>N</u> ext > Ca	ncel

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:	
◯ <u>A</u> nother computer:	B <u>r</u> owse
Allow the selected computer to be changed when launching from the only applies if you save the console.	e command line. This
< <u>B</u> ack	Finish Cancel

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

Add or Remove Snap-ins	his console from th	ose	available on vou	r computer and configure the selected s	×
snap-ins, you can configure	which extensions a	re e	nabled.	, ,	
Available <u>s</u> nap-ins:				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 <u>U</u> p
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				
	Microsoft Corp				
	Microsoft Corp				
IP Security Policy Ma	Microsoft Corp				
Link to Web Address	Microsoft Corp				
Local Backup	Microsoft Corp				Advanced
Local Lisers and Gro	Microsoft Corn	~			Advanced
Description:					
The Certificates shap in allo	we you to browce t	ha	contents of the c	artificate stores for vourself a sonice o	r a computer
	ws you to browse	ine (eruncate stores for yoursen, a service, o	r a computer.
					OK Cancel
				L	Citro

- 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



- **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
	Proceed without enrollment policy			
		<u>N</u> ext	Cano	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		~	
	<u>Suppress default extensions</u>			1
Request format:	• <u>P</u> KCS #10			
	<u>○ <u>c</u>mc</u>			
Note: Key archival is	not available for certificates based on a custom certificate request,	even w	hen this	
option is specified in	the certificate template.			
	<u>N</u>	ext	Can	cel

1.13 Expand the details pane and select Properties

		_		×
🔄 Ce	rtificate Enrollment			
	Certificate Information			
	Click Next to use the options already selected for this template, or click Details to cu request, and then click Next.	stomize th	e certifica	ate
	Custom request 😲 STATUS: Available	(Details	~
	The following options describe the uses and validity period that apply to this ty	pe of certi	ficate:	
	Key usage: Application policies:			
	Validity period (days):			
		<u>P</u> (operties	
		Next	Can	cel
		<u>n</u> ext	Curr	

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

General	Subject	Extensions	Private Key			
A friend	lly name	and descript	ion will make it ea	asier to identify	and use a certifica	ate.
Friendly	/ <u>n</u> ame:					
s3arch	ive1.xend	ata.com				
<u>D</u> escrip	tion:					
XenDa	ta Archive	e Server				

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

General	Subject	Extensions	Private Key			
The sub can ente can be u	ject of a c er inform used in a	certificate is t ation about certificate.	the user or co the types of	omputer to w subject name	which the certificate is issued. e and alternative name value:	You s tha
Subject	of certific	ate				
The use	r or comp	outer that is i	receiving the	certificate		
Subject	name:					
Туре:					CN=s3archive1.xendata	i.con
Count	ry	~		Add >	O=XenData Inc OU=Engineering	
Value:				_	L=Walnut Creek	
			<	Remove	S=California	
Alternat	tive name	- '			C=USA	
Type:					DNS	
DNS		~			s3archive1.xendata.com	1
Value:						
				Add >		
			<	Remove		

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

Certificate Properties		×
General Subject Extensions	Private Key	
The following are the certification	ate extensions for this certificate type.	^
Key usage	۲	
Extended Key Usage (applic	 ation policies)	
An application policy (called certificate can be used. Selec certificates issued by this ter	enhanced key usage in Windows 2000) defines how a t the application policy required for valid signatures of mplate.	
Available options: Code Signing Secure Email Time Stamping Microsoft Trust List Signii Microsoft Time Stamping IP security end system IP security unnel termina IP security unnel termina IP security user Encrypting File System Make the Extended Key User	Add > Add > < Remove	
Basic constraints	ب	~
	OK Cancel Apply	

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

certificat	eriopen	103			
General	Subject	Extensions	Private Key		
Crypt	ographic	Service Provi	der		^
A CSP certific	is a progr ate-relate	am that gen d processes.	erates a public and private key pair used in man	у	
Select	cryptogra	phic service	provider (CSP):		
RS/	A, Microso	ft Software H	(ey Storage Provider	^	
DH	,Microsof	ft Software K	ey Storage Provider		
	A, Microso	oft Software	Key Storage Provider		
	DH, Micro	soft Software	Key Storage Provider		
	DH_brain	poolP160r1,N	1icrosoft Software Key Storage Provider		
	DH_brain	poolP160t1,N	ficrosoft Software Key Storage Provider	~	
Sho	w all CSPs	5			
Key <u>o</u>	ptions			*	
Select	<u>H</u> ash Alg	jorithm		*	Ì
Select	Signature	e <u>F</u> ormat		*	~
			OK Cancel	<u>A</u> pply	y

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

Certificate Properties	×
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	~ I
Lishow all CSPs	
Set the key length and export options for the private key.	^
Key size: 2048	
Make private key exportable	
Allow private key to be archived	
Strong private key protection	
	¥
OK Cancel	Apply

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 a request, and then click Next.	lready selected for this template, or click Details to	o customize the certificate
Custom request	i status: Available	Details ^
The following options de Key usage: Application policies: Validity period (days)	scribe the uses and validity period that apply to t Server Authentication Client Authentication):	his type of certificate: <u>Properties</u>
		<u>N</u> ext 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 request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.
File Name: s3archive1-request Browse
File format: Base 64 Binary
Finish Cancel

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 choose how you would like to p	n is required for these changes, you may rove 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

		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
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	<u>361761.</u>
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]						_		\times
🔚 File Action Vi	Add or Remove Snap-ins					:	×	-	8 ×
Console Root	You can select snap-ins for t snap-ins, you can configure	his console from th which extensions a	nose a are er	available on you nabled.	r computer and configure the selected	set of snap-ins. For extensible	-		
	Available snap-ins:				Selected snap-ins:				•
	Snap-in	Vendor	^		Console Root	Edit Extensions			►
	ActiveX Control	Microsoft Corp Microsoft Corp				Remove			
	Component Services	Microsoft Corp Microsoft Corp				Move Up			
	Computer Manager Device Manager Disk Management	Microsoft Corp Microsoft Corp Microsoft and		Add >		Move Down			
	Event Viewer Folder	Microsoft Corp Microsoft Corp							
	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	the c	ontents of the c	ertificate stores for yourself, a service, o	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	×
Select the computer you want this snap-in to manage. This snap-in will always manage: [_ocal 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 Cance	.

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

able snap-ins:			Selected shap-ins:	
ap-in	Vendor	^		Edit Extensions.
ActiveX Control	Microsoft Corp		Certificates (Local C	Bomovo
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		Add >	
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 Lisers and Gro	Microsoft Corp	~		Adyanced
ription:				
Cautification on an in alla		h	stanta of the contificate starse for using of	
Cautificantes amon in all-	we you to browse t	he c	ntents 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 revoca lists from your disk to a certificate store.	ition
A certificate, which is issued by a certification authority, is a confirmation of your ic and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	lentity
Store Location	
Current User	
Local Machine	
To continue, dick Next.	
Next	Cancel

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	×
	Certificate Store 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	
	D <u>r</u> owse	
	<u>N</u> ext Cance	į

3.13 Click on Finish

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

Certificat	×	
1	The import was successful.	
	ОК	

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

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates] Elle Action View Favorites Window Help									
Console Root	Issued To Go Daddy Root Certificate Auth Go Daddy Secure Certificate Au Sarchive1.xendata.com	Issued By Go Daddy Class 2 Certification Au Go Daddy Root Certificate Author Go Daddy Secure Certificate Auth	Expiration Date 5/29/2031 5/2/2031 8/4/2022	Intended Purposes <all> <all> Server Authenticati</all></all>	F < s	Actions Certificates A More Actions			
Personal store contains 3 certificates.									

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> C</u> ertifica	ate				×
General [Details	Certification Path	1		
Show: <	All>		\sim		
Field Field Field Subje Subje SCT I Field Subje Field Subje Field Subje Thur Field Subje Field Subje Thur Field Subje Field Subje Field Subje Field Field Subje Field Fiel	ority Ke ect Alte ect Key List Constr Jsage bprint	ry Identifier rnative Name Identifier aints ffb5bbf143f	Value KeyID=40c2bd2 DNS Name=s3ar 076160fb05a1c: v1, 2979bef09e Subject Type=E Digital Signature f558c8b0f6ffb5t 372524829b2	278ecc348330 rchive 1. xenda 1863ad2fd2e0 393921f05673 nd Entity, Pat c, Key Encipher obf143f37252 2dda8a159 2dda8a159	^
				O	<

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 S3 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=s3archive1.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