Creating a new SSL certificate on the First Node

Because the FQDN used to access the Client Access servers in our NLB cluster doesn't match the FQDN specified in the common name field nor the subject alternative names field in the default self-signed SSL certificate that automatically is installed on each Client Access server during Exchange 2007 setup (**Figure 3.5** and **3.6**), we must create a new certificate.

rtificate Seperal	Details	<u>?</u>]
<u>S</u> how:	<all></all>	<u>•</u>
Field	Value	
DNS Na DNS Na	pject Alternative Name DNS Na hanced Key Usage Server / Usage Digital S sic Constraints Subject umbprint algorithm sha1 umbprint ce b9 d me=CAS01 me=CAS01.ehlo.dk	ame=CASO1, DNS Name=CASO1 Authentication (1.3.6.1.5.5.7.: 5ignature, Key Encipherment (a : Type=End Entity, Path Length I1 d0 60 b6 6b 08 9b 53 49 20 € ✔
	<u>E</u> dit Pro	operties ⊆opy to File

Figure 3.5: Subject Alternative Names on CAS01 Certificate Property page

Rachine: CAS01 Scop	e: ehlo.dk	
[PS] C:\>Get-Exchan	geCertificate FL	-
AccessRules CertificateDomains HasPrivateKey IsSelfSigned Issuer NotAfter NotBefore PublicKeySize SerialNumber Status Subject Thumbprint	<pre>: (System.Security.AccessControl.CryptoKeyAccessRule,</pre>	Systen
[PS] C:>>_		-1

Figure 3.6: Subject Alternative Names on CAS01 via the Exchange Management Shell

For the purpose of this article series, we'll generate a new certificate using an internal Microsoft certificate authority server, but in a corporate production environment, you would in most situations want to submit the certificate request to a 3rd party certificate authority.

Note:

Because we need a certificate in which multiple FQDNs have to be specified, we must use a subject alternative name (SAN) certificate. At the time of this writing only a handful 3rd party CAs offer these types of certificates, most of which are listed in the following KB article: <u>http://support.microsoft.com/kb/929395</u>.

As we're going to generate a request for a new SAN certificate, we must use the New-ExchangeCertificate cmdlet for this purpose, as the IIS Manager isn't capable of creating requests for SAN certificates. To do this launch the Exchange Management Shell, then type the following command (replace the names with your own):

New-ExchangeCertificate –GenerateRequest –SubjectName "C=dk, O=EHLO organization, CN=mailehlo.dk" –DomainName mail.ehlo.dk, autodiscover.ehlo.dk, cas01.ehlo.dk, cas02.ehlo.dk –FriendlyName "CAS SAN Certificate" –KeySize 1024 –Path c:\CAS_SAN_cert.req –PrivateKeyExportable:\$true

After hitting Enter, the thumbprint for the new certificate request will be listed as shown in **Figure 3.7**.



Figure 3.7: Generating a request for a new SAN Certificate

Submitting the SAN Certificate to a Microsoft Certificate Authority

With the SAN SSL certificate request generated, we can submit it to our Microsoft CA, or almost that is. The reason I why I say so, is because by default a Microsoft CA cannot handle certificates with the SAN field properly. To fix this issue log on to the Domain Controller and open a command prompt window, then type the following command:

Certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2

After hitting Enter, you should see the old and new value as in Figure 3.8.

es Command Prompt	
C:\>certutil -setreg policy\EditFlags -EDITF_ATTRIBUTESUBJECTALTNAME2 SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\EHLO Root CA\PolicyMo es\CertificateAuthority_MicrosoftDefault.Policy\EditFlags:	odul
Old Ualue: EditFlags REG_DWORD = 11014e (1114446) EDITF_REQUESTEXTENSIONLIST 2 EDITF_DISABLEEXTENSIONLIST 4 EDITF_ADDOLDKEYUSAGE 8 EDITF_BASICCONSTRAINTSCRITICAL 40 (64) EDITF_ENABLEAKIKEYID 100 (256) EDITF_ENABLEDEFAULTSMIME 100000 (65536) EDITF_ENABLEDEFAULTSMIME 100000 (1048576)	
New Value: EditFlags REG_DWORD = 11014e (1114446) EDITF_REQUESTEXTENSIONLIST 2 EDITF_ADDOLDKEYUSAGE 4 EDITF_ADDOLDKEYUSAGE 8 EDITF_BASICCONSTRAINTSCRITICAL 40 (64) EDITF_ENABLEAKIKEYID 100 (256) EDITF_ENABLEDEFAULTSMIME 10000 (65536) EDITF_ENABLEDEFAULTSMIME 100000 (1048576) CertUtil: -setreg command completed successfully. The CertSvc service may need to be restarted for changes to take effect.	
C:\>_	-1

Figure 3.8: Changing the EditFlags on the Microsoft CA

Now restart Certificate Services (CertSVC) service on the Microsoft CA server (Domain Controller) in order to have the changes applied (**Figure 3.9**).

Services							
Ele Action View	Help						
⇔ → 🗊 🔐							
Services (Local)	Name /		Description	Status	Startup Type	Log On As	
	Alerter Application Experience Lookup Ser Application Layer Gateway Service Application Management Automatic Updates Background Intelligent Transfer Se	vice	Notifies sel Process ap Provides s Processes i Enables th Transfers f	Started Started	Disabled Automatic Manual Manual Automatic Manual	Local Service Local System Local Service Local System Local System Local System	
	COM+ Event System COM+ Event System COM+ System Application Computer Browser Cryptographic Services DCOM Server Process Launcher DHCP Client DHCP Client Distributed File System	Stop Payse Restart All Todys Refresh	Enables Cl Supports S Manages t Provides th Provides th Provides la Registers a Integrates	Started Started Started Started Started Started	Disabled Automatic Manual Automatic Automatic Automatic Automatic Automatic	Local System Local System Local System Local System Local System Local System Network S Local System	-
	\Extended \Standard /	Properties					12
Stop and Start service (erblicate Services on Local Computer	Help					

Figure 3.9: Restarting the Microsoft Certificate Service

We're now ready to submit the certificate request to the Microsoft CA. One way to do this is to open a browser and type http://dc_name/certsrv. On the Welcome page, click **Request a certificate** (Figure 3.10).

Microsoft Certificate Services - Microsoft Internet Explorer	
Ble Edit Yew Pavorites Iools Help	2
🔾 Back + 🔾 - 💽 🐒 🐔 🔎 Search 🔮 Favorites 🔗 🗇 - 📡 🗔	
Address 🗿 http://dc01/certsrv/	💌 🛃 Go Links **
Microsoft Certificate Services EHLO Root CA	Home
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or you can verify your identity to people you communicate with over the Web, sign a depending upon the type of certificate you request, perform other security tasks.	r other program. By using a certificate, and encrypt messages, and,
You can also use this Web site to download a certificate authority (CA) certificat revocation list (CRL), or to view the status of a pending request.	te, certificate chain, or certificate
For more information about Certificate Services, see Certificate Services Docu	mentation
Select a task: Request a certificate	
View the status of a pending certificate request	
Download a CA certificate, certificate chain, or CRL	
	O Trusted sites

Figure 3.10: Microsoft Certificates Welcome page

On the Request a Certificate page, click advanced certificate request (Figure 3.11).

Microsoft Certificate Services - Microsoft Internet Explorer	and the second	
Ele Edit Yew Figvorites Iools Help		27
🔾 Back + 🖒 - 💽 👔 🛟 🔎 Search 👷 Favorites 🔗 🗇 - 🖕 🗔		
Address 🖓 http://dc01/certsrv/certrgus.asp		💌 🛃 Go 🛛 Links 🏁
Microsoft Certificate Services EHLO Root CA		Home
Request a Certificate		
Select the certificate type: User Certificate		
Or, submit an advanced certificate request		
		2
۵)		Trusted sites

Figure 3.11: Requesting a Certificate

On the Advanced Certificate Request page, click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file (Figure 3.12)**.



Figure 3.12: Selecting the second option on the Advanced Certificate Request page

Now paste the content of the certificate request file into the Base-64-encoded window as shown in **Figure 3.13**. Then select **Web Server** in the certificate template drop-down menu and click **Submit**.

Microsoft Certifica	te Services - Microsoft Internet Explorer	aloi x
Ele Edit Yew F	prorites Iools Help	20
3 Back + 🔿 - 🖻	👔 🏠 🔎 Search 😭 Fevorites 🕑 🎲 - 🖓 🗔	
gdress 🛃 http://dc0	f/certsrv/certrgxt.asp	💌 🛃 Go Links *
Microsoft Certific	ite Services - EHLO Root CA	Home
Submit a Certi	ficate Request or Renewal Request	
To submit a sav renewal reques Saved Request:	ed request to the CA, paste a base-64-encoded CMC or PKC generated by an external source (such as a Web server) in the	S #10 certificate request or PKCS #7 Saved Request box
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	KpIlozYwJschxUdvH+TKG1v3zT4140hBkFHeH3V8 AfnNVZ5/cpfsXyXObVdX19zceNrE4mA6YyG/17bH zJcnPZLB6v5qQIOMyHdtQFoHZBrLb2tZcsgdjPrd aM5ovuynSeJGjeknD6vKqfAGa49p0hbsf33ZpNHx 8LEw9J9mn+fOfbtI5np1P7IIC+LQWw11U042+b4J 	
Certificate Temp	Browse for a file to insert. ate:	
Additional Attribu	Web Server	
Attributes:	× ×	
	Submit >	
Done		Trusted stes

Figure 3.13: Submitting the Certificate Request

The certificate has been issued and you can download a DER or Base 64 encoded version by clicking Download certificate or Download certificate chain. Let's select **Base 64 encoded** followed by clicking **Download certificate chain** (**Figure 3.14**).

Microsoft Certificate Services - Microsoft Internet Explorer	
Ele Edit Yew Favorites Icols Help	
🔾 Back • 🔘 • 💽 😰 🟠 🔎 Search 🔅 Favorites 🙆 🔂 • 😓 🗔	
Address a http://dc01/certsrv/certfnsh.asp	💌 🛃 Go 🛛 Links 🍟
Microsoft Certificate Services EHLO Root CA	Home
Certificate Issued	
The certificate you requested was issued to you.	
C DER encoded or C Base 64 encoded	
Download certificate Download certificate chain	
	-
e	O Trusted sites

Figure 3.14: Downloading the issued Certificate

It's time to import the issued certificate using the Import-ExchangeCertificate cmdlet. We do this by typing the following command:

Import-ExchangeCertificate –Path c:\certnew.p7b

The certificate has now been imported to the personal certificate store.



Figure 3.15

To verify the certificate looks like expected, let's now type the following command:

Get-ExchangeCertificate -Thumbprint <thumbprint> | FL

Aachine: CAS01 Scop	e:	ehlo.dk		_OX
[PS] C:\>Get-Exchar	ng	eCertificate		-
Thumbprint			Services	Subject
D3D87858F9249CBF8C CEB9D1D060B66B089B	3A) 53	262871D54A25CØEC391B 4920A9E462713479A3B5	:ip::	CN=mail.ehlo.dk, 0=EHLO CN=CASØ1
[PS] C:\>Get-Exchar C391B FL	ng	eCertificate -Thumbpr	int D3D878	58F9249CBF8C3A262871D54A25C0E
AccessRules	:	(System.Security.Acc	essControl	CryptoKeyAccessRule, System
Security.AccessCont CertificateDomains : (mail.ehlo.dk, autor			iscover.eh	lo.dk, cas01.ehlo.dk, cas02.
HasPrivateKey	:	True		
IsSelfSigned		CN=FHLO Root CA. DC=	eblo DC=d	i.
NotAfter		26-06-2009 13:10:03	chaop no a	
NotBefore	-	27-06-2007 13:10:03		
PublicKeySize SepialNumber		2048 61906601888888888888		
Status	-	Valid		
Subject		CN=nail.ehlo.dk, O=E	HLO organi	zation, C=dk
Thumpprint	1	D3D87858F9249CBF8C3H	262871D54H	25C9EC391B
(PS] C:>_				
				*

Figure 3.16: SAN Certificate - Detailed Information

Finally we need to enable the certificate for the client services, our end-users will use to connect to their mailboxes. In this setup I'll enable the certificate for OWA, EAS, Outlook Anywhere, POP3 and IMAP4. To do so we need to type:

Enable-ExchangeCertificate – Thumbprint < thumbprint > -Services "IIS, POP, IMAP"



Figure 3.17: Enabling the SAN certificate

The certificate has now been enabled for these services but only on the first Client Access server in our NLB cluster.

Importing and Enabling the SAN SSL certificate on the Second Client Access Server in the NLB Cluster

To import the SAN certificate on the second Client Access server in the NLB cluster, we first need to export it from the first Client Access server. When doing so, we need to make sure we export the certificate with its private key. This is done by opening the Certificates snap-in. To open the Certificates snap-in, click **Start > Run** and type **mmc.exe** to first open an empty MMC window. Now click **File > Add/Remove Snap-in > Add > Select Certificates >** Click **Add > Select Computer Account >** Click **Next > Finish > Close** and finally **OK**. Expand **Certificates (Local Computer) > Personal,** then right-click on the certificate that should be exported. On the context appearing menu, select **All Tasks > Export (Figure 3.18)**.



Figure 3.18: Selecting Export on the Context Menu

In the Certificate Export Wizard, click **Next**. On the Export Private Key page, select **Yes**, **export the private key** as shown in **Figure 3.19** then click **Next**.

rtificate Export Wizard	
Export Private Key You can choose to export the private key with the certificate	
You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key v certificate, you must type a password on a later page.	vith the
Do you want to export the private key with the certificate?	
• Yes, export the private key	
C No, do not export the private key	
< Back Next >	Cancel

Figure 3.19: Exporting the private key

On the **Export File Format** page, select **Personal Information Exchange – PKCS #12** (.**PFX**) and tick **Include all certificates in the certificates path if possible** as shown in **Figure 3.20**. Click **Next**.

Certificates c	an be exported in a variety of file formats.
Select the for	mat you want to use:
C DER 6	ncoded binary X.509 (,CER)
C Base-	64 encoded X.509 (,CER)
C ⊆rypt	ographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
🗖 In	clude all certificates in the certification path if possible
• Perso	nal Information Exchange - PKCS #12 (.PFX)
🔽 In	clude all certificates in the certification path if possible
🗖 Er	able strong protection (requires IE 5.0, NT 4.0 SP4 or above)
E De	elete the private key if the export is successful

Figure 3.20: Selecting the format to use

Enter a password and click Next (Figure 3.21).

Note:

Make sure you remember this password as you need it when importing it on the second Client Access server.

To maintain security, you must i	protect the	orivate kev bv	using a passwo	rd.
ro maintain pocanty) you mast	protoccano	, , , , ,	asing a passing	
Type and confirm a password.				
Password:				
•••••				
, Confirm password:				
•••••				

Figure 3.21: Enter a password in order to protect the private key

Now specify the path to where you want to save the .PFX file (Figure 3.22), then click Next.

ificate Export Wizard	
ile to Export Specify the name of the file you (want to export
Eile name:	
C:\exported_cert.pfx	Browse

Figure 3.22: Specifying the path for the .PFX file

Finally click **Finish**.

Okay with the certificate exported, let's copy it to the C: drive of the second Client Access server, and then open the Exchange Management Shell on that server. To import the certificate, type the following command:

Import-ExchangeCertificate –Path c:\exported_cert.pfx –Password:(Get-Credential).password

When pressing Enter, you'll be prompted for the password you specified earlier on as shown **Figure 3.23**. It doesn't matter what username you specify as this isn't used in this type of authentication.

Machine: CAS02 Scope: ehlo.dk		_ []	×
[PS] C:\>Inport-ExchangeCertificate edential>.password	-Path c:\exported_c	ert.pfx -Password:(Get-Cr	-
cmdlet Get-Credential at command pi Supply values for the following par Credential	peline position 1 ameters:		
Windows Power	Shell Credential Request	<u>? × </u>	
R			
Please enter you	r credentials.		
<u>U</u> ser name:	🖸 sometext	×	
Password:	•••••		
	ОК	Cancel	
			-1

Figure 3.23: Importing the certificate

After clicking OK, the certificate has been imported (Figure 3.24).



Figure 3.24: Certficate imported

Now copy the certificate thumbprint to the clipboard, then enable the certificate for the required services by typing the following command (just like we did on the first Client Access server):

Enable-ExchangeCertificate – Thumbprint < thumbprint > -Services "IIS, POP, IMAP"



Figure 3.25: Enabling the SAN certificate on the second Client Access Server

The SAN certificate has now been properly enabled on both servers, and if the clients trust the root CA from our internal Microsoft CA, we should no longer get security warnings, when accessing OWA via the NLB cluster name as shown in **Figure 3.26**.



Figure 3.26: Accessing OWA 2007 without security warnings