

EXCHANGE 2007 – CERTIFICATO SCADUTO

If your **Exchange 2007** is nearing its first birthday, there is a good chance you will soon come across some event log warnings concerning the expiry of an internal transport certificate.

If you ignore these, users will start chasing you!! Outlook 2007 is now popping an expired certificate warning dialog.

With so many changes, it is easy to overlook some of the less shiny Exchange 2007 improvements, especially if you haven't been using earlier Exchange versions. **Exchange 2007** automatically installs a self-signed certificate.

Amongst other benefits, this certificate immediately secures **OWA** access enabling users to login to their mailbox using HTTPS.

One may replace this with the one issued by a **Certification Authority**. In any case earlier Exchange users will certainly appreciate that starting from the security of a self-signed certificate is much better than starting from the no security of port **80** HTTP.

ONE YEAR LATER...

Those choosing to continue working with the self-signed certificate will have the opportunity to appreciate how time flies!! In fact Exchange will remind you of its first anniversary with events of the type:

Event Type: WarningEvent Source: MSExchangeTransportEvent Category: TransportServiceEvent ID: 12018Date: 13/04/2008Time: 09:01:00User: N/AComputer: EXSERVERDescription:The STARTTLS certificate will expire soon: subject: exserver.domain.local, hours remaining:157700393E5D76615E855A773CFA08AB5842DFB0. Run the New-ExchangeCertificate cmdlet to create a newcertificate.

Event Type: Warning Event Source: MSExchangeTransport Event Category: TransportService Event ID: 12017 Date: 13/04/2008 Time: 09:01:00 User: N/A Computer: EXSERVER Description:



An internal transport certificate will expire soon. Thumbprint:157700393E5D76615E855A773CFA08AB5842DFB0, hours remaining: 295

The events are informative enough to point you to the right direction for resolving the issue i.e. calling the **New-ExchangeCertificate** cmdlet. **Exchange** is also kind enough to alert you days in advance. In the above event example we have 295 hours left, approximately 12 days.

You do check the event logs right? If not, or you simply ignore these events someone else will remind you! Most commonly **Outlook 2007** users will be amongst the first to start knocking at your door. If the certificate expires, opening Outlook will cause an annoying dialog saying:

exserver.domain.local Information you exchange with this site cannot be viewed or changed by others. However, there is problem with the site's security certificate...

GENERATING A NEW CERTIFICATE

Solving the problem is simple. To begin let see the currently installed certificate by running:

```
Get-ExchangeCertificate | List
```

[PS] C:\Documents a	and Settings\Administrator>get-exchangecertificate List
AccessRules	: {System.Security.AccessControl.CryptoKeyAccessRule, System .Security.AccessControl.CryptoKeyAccessRule, System.Securi ty.AccessControl.CryptoKeyAccessRule>
	: (bark, bark.spark.local)
lasPrivateKey	True
lsSelfSigned Issuer	: True : CN=bark
NotAfter	: 14/04/2009 13:14:21
NotBefore	: 14/04/2008 13:14:21
PublicKeySize	: 2048
RootCAType	: None
SerialNumber	: 7DA4B7F7FF262BAC40301508F36E3578
Services	: IMAP, POP, IIS, SMTP
Status Subject	: Valid : CN=bark
Subject Thumbprint	= 157700393E5D76615E855A773CFA08AB5842DFB0

Note that here I am taking screen shots from a test machine whose certificate is not about to expire! Some properties worth noticing include:

NotAfter - shows the certificate expiry date Services - shows that the certificate applies to IMAP, POP, IIS and SMTP Thumbprint - will use this to identify and make changes to this certificate

Creating a new certificate is just a matter of running the cmdlet:

New-ExchangeCertificate

Data: 09/10/2012 Total Chars: 3430



This will warn you about overwriting the SMTP certificate.

[PS] C:\Documents and Settings\Administrat	tor>New-Exc	hangeCert	tificate
Confirm Overwrite existing default SMIP certifica '157700393E5D76615E855A773CFA08AB5842DFB0 certificate 'F7A8FLB443A0E7266C72CDE060334 10:21:59>? [Y] Yes IA] Yes to All IN] No IL] No to (default is "Y"):9	02C07B85607	'6' (expir	09 13:14:21), with ∿es 08/06/2009 [?] Help
Thunbprint	Services	Subject	
F788F1B443A0E7266C72CDE0603302C07B856076		CN=bark	

To be honest the first time I ran into this, I thought that was it. After all there were no more event log warnings. However this is not the case.

Re-running **Get-ExchangeCertificate** we see that the **IIS** service is still using the old certificate. This means **Outlook** users will still be knocking at our door.

🔀 Machine: bark Scope:	
[PS] C:\Documents	and Settings\Administrator>get-exchangecertificate List
AccessRules	: (System.Security.AccessControl.CryptoKeyAccessRule, System .Security.AccessControl.CryptoKeyAccessRule, System.Securi ty.AccessControl.CryptoKeyAccessRule>
CertificateDomains HasPrivateKey	: (bark, bark.spark.local) : True
Issuer	: CN-hark
NotAfter	: 08/06/2009 10:21:59
NotBefore	: 08/06/2008 10:21:59
PublicKeySize	: 2048
RootCAType	: True : CN-bark : O8/06/2009 10:21:59 : 08/06/2008 10:21:59 : 2048 : None : None : C910C59981D99CB64929337D359DBB3C : IMAP, POP, SMTP : Valid
SerialNumber	: C910C59981D99CB64929337D359DBB3C
Services	= IMAP, POP, SMTP
status	: Valid
Status Subject Fhunbprint	: CN=bark : F788F1B44380E7266C72CDE0603302C07B856076
Inunoprint	: F7H8F1B443H0E7266C72CDE0603302C07B856076
AccessRules	: (System.Security.AccessControl.CryptoKeyAccessRule, System .Security.AccessControl.CryptoKeyAccessRule, System.Securi ty.AccessControl.CryptoKeyAccessRule>
CertificateDonains	: {bark, bark.spark.local}
lasPrivateKey IsSelfSigned	: True
IsSelfSigned	: True
lssuer NotAfter	- ON-DOLN
NotHiter	: 14/04/2009 13:14:21 : 14/04/2008 13:14:21
NotBefore PublicKeySize	: 2048
RootCATupe	- 2018 : None
RootCAType SerialNunber Services Status	= 7DA4B7F7FF262BAC40301508F36E3578
Services	: IMAP, POP, IIS, SMTP
Status	= Valid
Subject Fhunbprint	: CN=bark
Thumbprint	: 157700393E5D76615E855A773CFA08AB5842DFB0

We need to move the **IIS** service using **Enable-ExchangeCertificate**. To do this we need thethumbnail value of the newly created certificate. In my case I used this command:

Enable-ExchangeCertificate -Thumbprint F7A8F1B443A0E7266C72CDE0603302C07B856076 -Service IIS



With the new certificate in place we may now remove the old certificate using **Remove-ExchangeCertificate** with the thumbprint value of the old certificate:

Remove-ExchangeCertificate -Thumbprint 157700393E5D76615E855A773CFA08AB58

Data: 09/10/2012 Total Chars: 3430

