## Publishing OWA/Outlook Anywhere with Self Signed Certificate

OM February 11, 2013 Exchange Hosted 7 Comments

My boss recently acquired a small company. Now he wants to permit the users, remote access via OWA/Outlook Anywhere. The user base is around 50, so he doesn't want to spend on SAN certificate. They doesn't have a PKI either, so only possible option left is to use a Self Signed Certificate for both OWA/Outlook Anywhere.

So, before deploying it to Production, I gave it a try on my Lab and it passed with flying colors.

When you install Exchange 2010, a self-signed certificate is automatically configured. A self-signed certificate is signed by the application that created it. The subject and the name of the certificate match. The issuer and the subject are defined on the certificate.

Machine: TESTEXCH.con	toso.com
[PS] C:\>Get-Exchar	geCertificate  fl
AccessRules CertificateDomains HasPrivateKey IsSelfSigned Issuer NotAfter NotBefore PublicKeySize RootCAType Services Status Subject Thumbprint	: (System.Security.AccessControl.CryptoKeyAccessRule, System.Security.AccessControl.CryptoKeyAccessR ule, System.Security.AccessControl.CryptoKeyAccessRule) : (TESTEXCH, TESTEXCH.contoso.com) : True : True : CN-TESTEXCH : 2/9/2018 12:33:22 AM : 2/9/2013 12:33:22 AM : 2048 : None : 6DF3DAFD676E73AD4C6CE446F1C0E867 : MAPP. POP. IIS, SMTP : Ualid : CN-TESTEXCH : 38BA31BB622FD9818FED1AF8868C6CF0D24357B6
(F8) (FV_	

If you launch OWA at this point, you will be prompted with the Certificate error as the certificate was not a trusted root certificate.



I also tried to configure Outlook Anywhere and as expected, it also throws Security error.

Configuring       Security Alert         Configuring e-mail server set       Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.         Search for on Log on to server       Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.         X       The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.         X       The security certificate date is valid.         X       The name on the security certificate is invalid or does not match the name of the site.	Online search for your	server settings
Establish netw     Search for or     Log on to serv     Search for or     Log on to serv     The security certificate was issued by a company you have     not chosen to trust. View the certificate to determine whether     you want to trust the certifying authority.     The security certificate date is valid.     The name on the security certificate is invalid or does not     match the name of the site.	Configuring	Security Alert
Do you want to proceed?           Yes         No         View Certificate	<ul> <li>Establish n</li> <li>Search fo</li> <li>Log on to s</li> </ul>	etw       Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.         erv       X       The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certificate to determine whether the security certificate date is valid.         X       The security certificate date is valid.         X       The name on the security certificate is invalid or does not match the name of the site.         Do you want to proceed?       Yes         Yes       No

Once you accept this warning, you will be prompted with credential, but as the certificate is not a trusted one, a secure channel won't be initiated and it will throw a proxy error.

0	contoso\onat	h			
	Remember my o	redentials			
	Use another a	account			
- 0		ОК	Cancel	_	×
8	There is a problem with the security certificate is Outlook is unable to commail.contoso.com. (Error	he proxy server's security not from a trusted certifyi iect to the proxy server Code 18).	certificate. ing authority.		

So, you won't be able to configure Outlook Anywhere with the default Self Signed Certificate.

The solution is to generate a new Self Signed Certificate with the following names on it.

- mail.contoso.com
- autodiscover.contoso.com

We need this do this via Power Shell,

New-ExchangeCertificate -FriendlyName "SelfSigned Certificate" -KeySize 2048 -SubjectName "c=IN, s=, l=, o=CONTOSO, ou=IT, cn=CONTOSO.COM" -DomainName MAIL.CONTOSO.COM, AUTODISCOVER.CONTOSO.COM -PrivateKeyExportable \$True



Once the certificate is generated, we have to enable the certificate for IIS, (SMTP) services.

At this point, we need to delete the original self signed certificate which was generated during the installation.



Now, if we launch OWA, we can see the new certificate with all the necessary names on this required for proper functioning of OWA/Outlook Anywhere.

look Web App	🗿 • 🖾 • 📼	🙀 Favorites 🛛 🙀 🔊 Suggested Sit	tes 🔹 🙋 Web Slice Gallery 👻	
ificate	×	Outlook Web App		<u>6</u> • 6
Image: Certification Path       Image: Certificate Information       This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.		Certificate General Details Certification Pe Show: CAII> Field Version Serial number Signature aboothm	th ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	×
Issued to: CONTOSO.COM	omputer	Signature hash algorithm Issuer Valid from Valid to Subject	Sha1 CONTOSO.COM, IT, CONTOS Saturday, February 09, 2013 1 Friday, February 09, 2018 12: CONTOSO.COM, IT, CONTOS V	omputer
Issued by: CONTOSO.COM Valid from 2/ 9/ 2013 to 2/ 9/ 2018		CN = CONTOSO.COM OU = IT O = CONTOSO L = S = C = IN		ook Web App
Instal Certificate Issuer Statement arn more about <u>certificates</u>	s reserved.	Learn more about <u>certificate deta</u>	Edit Properties	s reserved.

tificate		Contraction of the second s
		×
eneral Details Certification P	ath ]	
ibow:		1
usin Teas		
Field	Value	
Issuer	CONTOSO.COM, IT, CONTOS	
Valid from	Saturday, February 09, 2013	
Valid to	Friday, February 09, 2018 12:	
Subject	CONTOSO.COM, IT, CONTOS	
Public key	R5A (2048 Bits)	mouter
Subject Alternative Name	Server Authentication (1.2.6	(in process)
Key Licage	Digital Signature Key Engineer	
ME Key Usage	Digital Digitature, Key Encipher	and Male Anna
DNS Name=MAIL.CONTOSO.CC	M	LOOK WED APP
DNS Name=AUTODISCOVER.CO	INTOSO.COM	
DNS Name=AUTODISCOVER.CO	ONTOSO.COM	
DNS Name=AUTODISCOVER.Co	ONTOSO.COM	
DNS Name=AUTODISCOVER.Co	NITOSO.COM	
DNS Name=AUTODISCOVER.Co	INTOSO.COM	
DNS Name=AUTODISCOVER.Co	INTOSO.COM	Sign in
DNS Name=AUTODISCOVER.Co	Edit Properties	Sign in
DNS Name=AUTODISCOVER.Co	Edit Properties	Sign in
DNS Name=AUTODISCOVER.Co	Edit Properties	Sign in

The Self-signed certificates must be manually copied to the trusted root certificate store on the client computer or mobile device. When a client connects to a server over SSL and the server presents a self-signed certificate, the client will be prompted to verify that the certificate was issued by a trusted authority. The client must explicitly trust the issuing authority. If the client confirms the trust, then, SSL communications can continue.

Now, we have to install this certificate in the local trusted certificate store on every machine which will be using OWA/Outlook Anywhere.



At this point if we launch OWA, no longer we will get the certificate error and our OWA site will now be a trusted.



Now, if we start configuring Outlook Anywhere, it will be completed without any security/proxy error.

Add New Account Online search for your server settings	1
OK Cancel	÷
Add New Account Online search for your server settings	÷
Online search for your server settings	7
Configuring	
Configuring e-mail server settings. This might take several minutes:	
<ul> <li>Establish network connection</li> </ul>	
Search for omprakash.nath@contoso.com server settings	
Log on to server	



In my test, Outlook Anywhere was fully functional without any issues and was able to contact with CAS without any issues.

eral Local Mailbox							Categorize *	Address Boo
Server name mail.contoso.com mail.contoso.com mail.contoso.com	Type Directory Mail Mail Directory	Interface Local Area Local Area Local Area Local Area	Conn HTTPS HTTPS HTTPS HTTPS	Status Established Established Established Established	Reg/Fail 17/0 17/0 24/0 1/0	Avg Resp 605 458 324 0	➤ Febr Su Mo Tu 27 28 29 3 4 5 10 11 12 17 18 19 24 25 26 3 4 5 No upcomin	uary 2013     ▶       We Th Fr Sa     30 31 1 2       6 7 8 9     13 14 15 16       20 21 22 23     27 28 1 2       6 7 8 9       uary 2013     1 2       9 7 8 9       10 21 22 3       27 28 1 2       6 7 8 9       9 7 8 9

The OOF/OAB/Free Busy was fully functional along with Autodiscover Service.

Search Inbox (Ctrl+E)		Q	Test
Arrange By: Date		Newest on top	SuperCoach
▲ Tuesday	Test E-mail Au	toConfiguration	×
<ul> <li>Tuesday</li> <li>SuperCoach Test</li> </ul>	E-mail Address Password Legacy DN Results Log Protocol: Exc Server: mail. Login Name: a SSL: Yes Mutual Authe Availability Se OOF URL: htt OAB URL: htt Unified Messa Auth Package Certificate Pr Exchange Co	Image: AutoDiscover         Image: AutoDisco	com Use Guessmart Secure Guessmart Authentication Test Cancel so.com/ews/exchange.asmx xchange.asmx '99cdff6-e466-4c03-afa7-9afab0b036bc/ contoso.com/ews/UM2007Legacy.asmx oso.com contoso.com/ecp/
	ECP Sub URL ECP Sub URL ECP Sub URL ECP Sub URL ECP Sub URL	: ?p=customize/voicemail.asp) : ?p=personalsettings/EmailSu : ?p=sms/textmessaging.slab? : PersonalSettings/DeliveryRe; : ?p=organize/retentionpolicy!	x&exsvurl=1 ubscriptions.slab&exsvurl=1 &exsvurl=1 port.aspx?exsvurl=1&IsOWA= <isowa>&amp;MsgID=<msgid>&amp;Mbx=<mbx> tags.slab&amp;exsvurl=1</mbx></msgid></isowa>

Frequently, small organizations decide not to use a third-party certificate or not to install their own PKI to issue their own certificates. They might make this decision because those solutions are too expensive, because their administrators lack the experience and knowledge to create their own certificate hierarchy, or for both reasons. The cost is minimal and the setup is simple when you use self-signed certificates. However, it's much more difficult to establish an infrastructure for certificate life-cycle management, renewal, trust management, and revocation when you use self-signed certificates.