

Outlook Web Access – Guide to Installing Root Certificates, Generating CSR and Installing SSL Certificate

Copyright[©] Trustis Limited 2010. All rights reserved.



Trustis Limited

Building 273 New Greenham Park Greenham Common Thatcham RG19 6HN

E: info@trustis.com W: www.trustis.com Registered in England No: 03613613



Table of Contents

1	Introduction	3
2	Install Root and Intermediate Certificates	3
	2.1 Installing the Root CA Certificate	
	2.2 Installing the Issuing CA Certificate	5
3	Certificate Signing Request (CSR) Generation	7
4	Installing your SSL Server Certificate	12

1 Introduction

This document specifies instructions for Installing the Root and Intermediate certificates, generating your CSR, and Installing your certificate.

2 Install Root and Intermediate Certificates

Firstly, you need to download the CA certificates (both Root CA certificate and Issuing CA certificate) as individual files

- <u>DER format Root CA certificate</u> found at http://www.tructic.com/oki/beathagea/apa/fag
- http://www.trustis.com/pki/healthcare/ops/fpsroot-der.crt
 <u>DER format Healthcare TT Issuing Authority certificate</u> found at
- http://www.trustis.com/pki/healthcare/ops/healthcarett-der.crt

To install these certificates, you must first enable the certificates Snap-in for the Microsoft Management Console (mmc)

- 1. Click the Start Button then select Run and type mmc
- 2. Click File and select Add/Remove Snap in
- 3. Select Add, select Certificates from the Add Standalone Snap-in box and click Add
- 4. Select Computer Account and click Next
- 5. Select Local Computer and click Finish
- 6. Close the Add Standalone Snap-in box, click OK in the Add/Remove Snap in
- 7. Return to the MMC

2.1 Installing the Root CA Certificate

1. Right click the *Trusted Root Certification Authorities*. Select **All Tasks**, select **Import**.

🚡 Console 1			
∫ <u>C</u> onsole <u>W</u> indow <u>H</u> elp ∫) 🖻 🖥 💷		
🚡 Console Root			
Action ⊻iew Eavorites	← → 🛍 💽	🖪 😫	
Tree Favorites		Name	
Console Root		🗐 Certifical	es (Local Computer)
📄 🗑 Certificates (Local Computer)		
Emiliar Personal Final Trusted Root Certificatio	n Authorities		
🕀 🛄 Enterprise Trust	Find Certificate	s	
	All Tasks	Þ	Find Certificates
	New Window fr	om Here	Import
	Refresh		
	Help		
Add a certificate to a store			1.

This starts the certificate import wizard

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.	
	To continue, click Next.	
		_
	< Back Next > Cancel	

2. Click Next.

3. The File to Import dialog is shown

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)	
	_
< <u>B</u> ack <u>N</u> ext > Cancel	

Locate the Root CA Certificate file you downloaded earlier and click Next.

4. When the wizard is completed, click **Finish**.

2.2 Installing the Issuing CA Certificate

1. Right click the Intermediate Certification Authorities. Select All Tasks, select Import.

🚡 Console1		
∫ <u>C</u> onsole <u>W</u> indow <u>H</u> elp ∫ 🗋	🖻 🔒 🗉	
🚡 Console Root		
$Action View Eavorites \downarrow \leftarrow$	· -> 🛍 💽 🖶 😫	
Tree Favorites	Name	
Console Root	🗐 Certifical	es (Local Computer)
E- Certificates (Local Computer)		
	Authorities	
Enterprise Trust	Authorities	
	Find Certificates	
EE.R EE.REQUEST	All Tasks 🔹 🕨	Find Certificates
É 🧰 SPC	New Window from Here	Import
	Refresh	
	Help	
Add a certificate to a store		

2. Complete the import wizard again, but this time locating the **Issuing CA Certificate** when prompted for the Certificate file.

When both certificates have been installed:

- Ensure that the **Root CA** certificate appears under **Trusted Root Certification Authorities**
- Ensure that the **Issuing CA** certificate appears under **Intermediate Certification Authorities**

3 Certificate Signing Request (CSR) Generation

- 1. Using the Internet Services Manager.
- 2. Right click on the website that is hosting your OWA component (this is by default the "**Default Web Site**") and open its properties.

Internet Information Services
 Internet Information Services
 Internet Information
 Internet

- 3. Select the "Directory Security" tab and then click on "Server Certificates". The "Web Server Certificates Wizard" will now be displayed, click Next.
- 4. On the "Server Certificate" dialogue box (below), we are going to select "Create a new certificate", click Next.

IIS Certificate Wizard	21 (1) 21		X
Server Certificate There are three methods for assigning a certifica	ate to a Web si	te.	
Select the method you want to use for this web	site:		
Create a new certificate.			
C Assign an existing certificate			
C Import a certificate from a Key Manager bac	kup file.		
	< <u>B</u> ack	<u>N</u> ext>	Cancel
그는 것은 이번에 가지 않는 것은 것은 것이 같이 있는 것이 없다.			

5. In the "Delayed or Immediate Request" dialogue box (below) select "Prepare the request now, but send it later", click Next.

IS Certificate Wizard		X
Delayed or Immediate Request You can prepare a request to be sent later, immediately.	or you can send one	
Do you want to prepare a certificate reques immediately to an online certification author	st to be sent later, or do you ity?	want to send it
Prepare the request now, but send it lat	er	
C Send the request immediately to an onli	ne certification authority	
	< Back Ne	ext > Cancel

6. Next you are presented with the "**Name and Security Settings**" dialogue box (below). Give your new certificate a name and also select the level of security you would like to use – choose 2048 bit, click **Next**.

IIS Certificate Wiza	d	×
Name and Securi Your new certifi	Settings te must have a name and a specific bit length.	2
Type a name fo remember.	he new certificate. The name should be easy for you to refer to and	
Na <u>m</u> e:		
Your Company	ame	
The bit length o The greater the decrease perfor Bit length:	he encryption key determines the certificate's encryption strength. t length, the stronger the security. However, a greater bit length may ance.	
bicieng <u>(i</u> .	2048	
C Select crypt	graphic service provider (CSP) for this certificate	
	< <u>B</u> ack <u>N</u> ext > Cancel	

7. In the "**Organisation Information**" dialogue box (below), enter the name of your organisation. This should be as you want it to appear on any legal documents as this is the name that will appear in your certificate. The organisational unit can be a location, department or business unit within your company.

IS Certificate Wizard		X
Organization Information Your certificate must include informa distinguishes it from other organizatio	ation about your organization that ons.	
Select or type your organization's na legal name of your organization and	ame and your organizational unit. This is typically th the name of your division or department.	e
For further information, consult certifi	ication authority's Web site.	
Organization:		
Northwind Traders	•	
Organizational <u>u</u> nit:		
IT		
	< <u>B</u> ack <u>N</u> ext> (Cancel

8. In the "**Common Name**" dialogue box (below), you must enter the FQDN of our web server.

Your Site's Common Name	Ilu gualified domain name	10
Todi web site s common name is its to	ny quained domain name.	Ŵ
Type the common name for your site. I name. If the server is on the intranet, y name.	f the server is on the Internet, use a valid DNS iou may prefer to use the computer's NetBIOS	
If the common name changes, you will	need to obtain a new certificate.	
Common name:		
london.nwtraders.msft		
	c Back Nevto	Cancel

9. You are now presented with the "Geographical Information" dialogue box (below). It is important to make sure you enter the State in full, for example "New York" not just "NY". Abbreviating State names will be rejected at the end of the Certificate Wizard.

ographical Information	and the second se	
The certification authority requires the	ne following geographical information.	
Country/Region:		
US (United States)		
State/province:		
New York		•
City/Jocality:		
Rochester		-
State/province and City/locality mus abbreviations.	st be complete, official names and may not co	ntain

10. The last step is to specify the location of the Certificate Request File, remember where and what you called this as you will need it later.

Certificate Wizard		
ertificate Request File Name Your certificate request is saved as a text file with the file name you	and a second	E.
specify.		
Enter a file name for the certificate request.		
Eile name:		
c:\cettreq.txt	Browse	

11. The "**Request File Summary**" will now appear (below). Make sure all details are correct and then click **Next** to process the request.

Certificate Wizard equest File Summary You have chosen to ge	nerate a request file.		
To generate the followin	g request, click Next.		
File name: c:\certreq.t	xt		
Your request contains th	e following information:		
Issued To Friendly Name Country / Region State / Province City Organization Organizational Unit	london.nwtraders.msft SSL Certificate for DWA US New York Rochester Northwind Traders IT		
	< <u>B</u> ack	<u>N</u> ext>	Cancel

You have now created a "Certificate Signing Request" which will be needed when you apply for your certificate.

4 Installing your SSL Server Certificate

You will receive an email from the Registration Authority when your certificate request has been approved that contains a link to a location where your certificate may be obtained. Clicking on this link will bring up a browser window that contains the details of your issued certificate and includes a section that looks something like the following:

-----BEGIN CERTIFICATE-----

MIAGCSqGSIb3DQEHAqCAMIACAQExADALBgkqhkiG9w0BBwGggDCCAmowggHXA hAF

UbM77e50M63v1Z2A/5O5MA0GCSqGSIb3DQEOBAUAMF8xCzAJBgNVBAYTAIVTMS Aw

(.....)

È+cFEpf0WForA+eRP6XraWw8rTN8102zGrcJgg4P6XVS4l39+l5aCEGGbauLP5W6 K99c42ku3QrlX2+KeDi+xBG2cEIsdSiXeQS/16S36ITclu4AADEAAAAAAAA -----END CERTIFICATE-----

Copy everything you see **between and including** the lines that look like -----BEGIN CERTIFICATE-----

and

-----END CERTIFICATE-----

and paste it into an appropriately named text file e.g. myserver.cert

Certificate Installation

- 1. Open Internet Services Manager from your Administrative Tools.
- 2. Open the Properties for the Web Site that is hosting OWA (normally the Default Web Site).
- 3. Select the "Directory Security" tab and then click on the "Server Certificates" button.
- You will now be presented with the "Pending Certificate Request" dialogue box. Select "Process the pending request and install the certificate" Click Next.
- 5. The "**Process a Pending Request**" dialogue box will appear Navigate to the site certificate that you received and click Next.
- 6. You will now be presented with the "Certificate Summary" Click Next.

You have now installed the SSL certificate into your web site, the next step is to enable SSL for OWA - this is a pretty simple task.

1. Using the Internet Services Manager, open the properties for the "**Exchange**" virtual directory.



- 2. Select the "**Directory Security**" tab and the click on the "**Edit**" button in the Secure Communication section.
- In the "Secure Communications" dialogue box (below), check the box "Require Secure Channel (SSL)", you could also check the box "Require 128-bit encryption", if you do check the 128-bit checkbox, any browsers that do not support 128-bit encryption will be unable to connect to OWA.

Secure Communications		×
Require secure channel (SSL)	and the second	
E Require 128-bit encryption		
Client certificates		
Ignore client certificates		
C Accept client certificates		
C Require client certificates		
Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.	E <u>d</u> it	
OK Cancel	<u>H</u> elp	

When users enter http://ahost.adomain.com/exchange, they will receive an "HTTP 403.4 - Forbidden: SSL required Internet Information Services" error message, because OWA is configured to require SSL. SSL uses the HTTPS protocol, so users would need to enter the url as https://ahost.adomain.com/exchange. Please see the Microsoft article regarding forcing the use of SSL with OWA:

http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q279681

One final step that you may need to take is to ensure that your Firewall is configured to allow HTTPS (port 443 by default) to pass through.