

## **Microsoft ISA Server 2006 – Certificate troubleshooting – Part II**

### **Abstract**

In this article, I will give you some additional information about how ISA Server 2006 uses digital certificates in web chaining and reverse publishing scenarios. This article goes behind my first [article](#) about ISA Server 2006 certificate deployment which was published in July 2008 on [www.isaserver.org](http://www.isaserver.org)

### **Let's begin**

Let us start with a short explanation which type of certificates are used in secure publishing scenarios and specially which functionality SAN certificates (SAN = Subject Alternate Name) provides and which distinguish them from classically certificates like wildcard certificates.

### **Certificate types**

There are three types of often used certificates:

- Normal certificates
- Wildcard certificates
- Subject Alternate Name certificates (SAN)

### **Normal certificates**

A normal certificate is the classically type of certificate. This type of certificate is issued for only one FQDN = Fully Qualified Domain Name aka a DNS hostname like owa.it-training-grote.de.

### **Wildcard certificates**

A Wildcard certificate is often used when a company needs to publish different hostnames with the same domain name. Instead of using multiple normal certificates, it is possible to use this type of certificate. As an example if you buy a wildcard certificate for \*.it-training-grote.de, it is possible to use the certificate to publish webservers with, for example, the names owa.it-training-grote.de and www.it-training-grote.de.

### **SAN certificates**

SAN (Subject Alternate Name) certificates are also often called multi domain certificates or Unified Communication (UC) certificates. With the help of SAN certificates it is possible to publish multiple FQDN with the same or other Top Level Domain (TLD) name. For example:

owa.it-training-grote.de  
www.it-training-grote.de

Server01  
Server01.exchange.internal  
Autodiscover.exchange.internal  
Autodiscover.it-training-grote.de

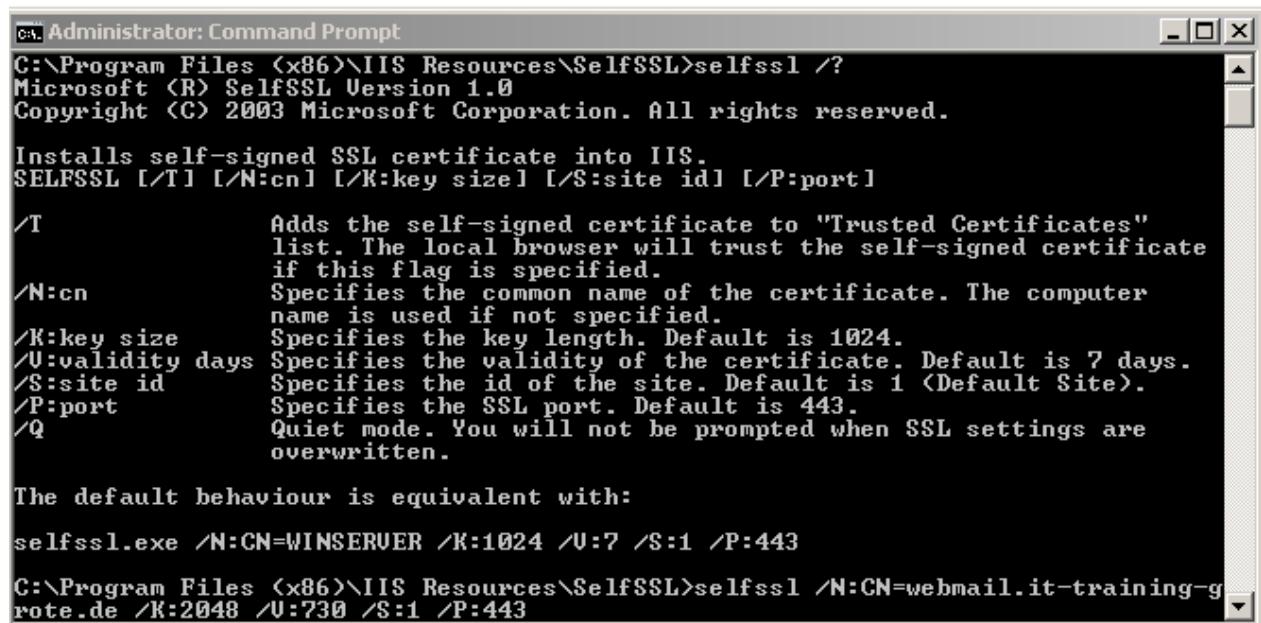
A SAN certificate is widely used in Exchange Server publishing scenarios with or without ISA Server 2006.

### **ISA Server 2006 Service Pack 1 certificate enhancements**

ISA Server 2006 Service Pack 1 supports the use of SAN certificates. Prior to ISA Server 2006 Service Pack 1, ISA Server only checked the first name in the certificate and ignored the additional names in the SAN field of the certificate.

### **Using self signed certificates**

One way to use certificates for ISA Server publishing is to use the SELFSSL.EXE tool from the IIS 6 resource kit . With the help of the SELFSSL tool administrators can create certificates which every Common Name (CN) they want.



```
Administrator: Command Prompt
C:\Program Files (x86)\IIS Resources\SelfSSL>selfssl /?
Microsoft (R) SelfSSL Version 1.0
Copyright (C) 2003 Microsoft Corporation. All rights reserved.

Installs self-signed SSL certificate into IIS.
SELFSSL [/T] [/N:cn] [/K:key size] [/S:site id] [/P:port]
/T          Adds the self-signed certificate to "Trusted Certificates"
list. The local browser will trust the self-signed certificate
if this flag is specified.
/N:cn       Specifies the common name of the certificate. The computer
name is used if not specified.
/K:key size Specifies the key length. Default is 1024.
/U:validity days Specifies the validity of the certificate. Default is 7 days.
/S:site id   Specifies the id of the site. Default is 1 (Default Site).
/P:port      Specifies the SSL port. Default is 443.
/Q          Quiet mode. You will not be prompted when SSL settings are
overwritten.

The default behaviour is equivalent with:

selfssl.exe /N:CN=WINSERVER /K:1024 /U:7 /S:1 /P:443
C:\Program Files (x86)\IIS Resources\SelfSSL>selfssl /N:CN=webmail.it-training-g
rote.de /K:2048 /U:730 /S:1 /P:443
```

Figure 1: SELFSSL from the IIS 6 Resource Kit

Because a self signed certificate is not issued by a trusted Root Certificate Authority you must manually place the self signed certificate in the Trusted Root CA store on the local ISA Server.

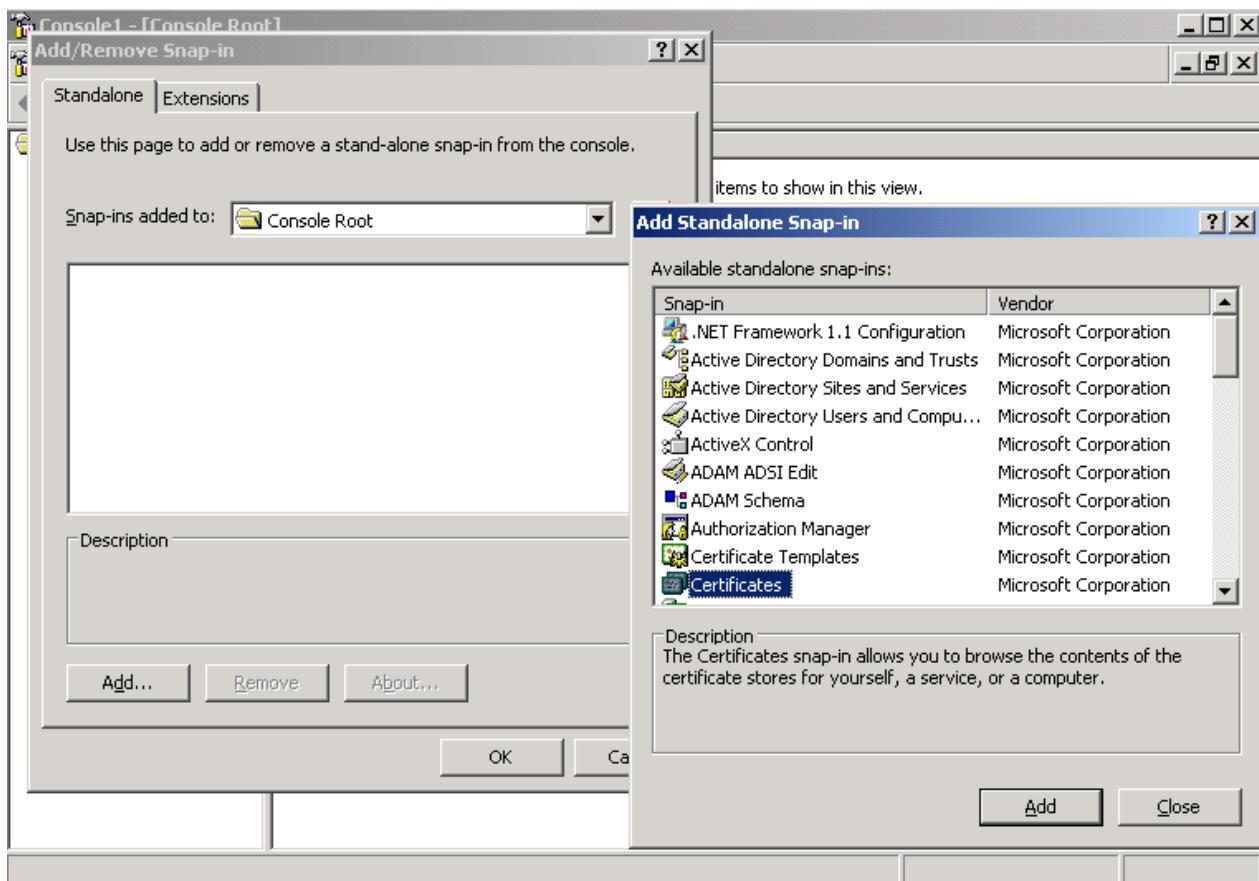


Figure 2: Add certificate Snap-In

Next, select the local Computer account as the certificate store to see all local installed certificates, which ISA Server uses for publishing and webchaining scenarios.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
1	RootCA	8/19/2011	Server Authentication	Webchain
Administrator	RootCA	8/19/2010	Microsoft Trust List S...	webchain
Administrator	RootCA	8/19/2010	Encrypting File Syste...	webchain
ISA2006.ex2k3.dom	RootCA	8/19/2010	Client Authentication...	test
RootCA	RootCA	8/19/2014	<All>	<None>
Webchain	RootCA	8/19/2011	Server Authentication	Webchain

Figure 3: Display certificates in certificate store

## Trusted Root CA certificates

ISA Server ensures that each certificate used can be verified against the issuing Certificate Authority. ISA Server checks the certificate chain of the certificate to the Root CA. The list of trusted Root Certificate Authorities can be found in the local computer certificate store on the ISA Server 2006 machine.

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]					
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	
Equifax Secure Global eBusiness C...	Equifax Secure Global eBusiness CA-1	6/21/2020	Secure Email, Server...	Equifax Secure Glob...	
EUnet International Root CA	EUnet International Root CA	10/2/2018	Secure Email, Server...	EUnet International .	
FESTE, Public Notary Certs	FESTE, Public Notary Certs	1/1/2020	Secure Email, Server...	FESTE, Public Notary	
FESTE, Verified Certs	FESTE, Verified Certs	1/1/2020	Secure Email, Server...	FESTE, Verified Certs	
First Data Digital Certificates Inc. ...	First Data Digital Certificates Inc. Ce...	7/3/2019	Server Authenticatio...	First Data Digital Cer.	
FNMT Clase 2 CA	FNMT Clase 2 CA	3/18/2019	Secure Email, Server...	Fabrica Nacional de .	
GlobalSign Root CA	GlobalSign Root CA	1/28/2014	Secure Email, Server...	GlobalSign Root CA	
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/14/2018	Secure Email, Client ...	GTE CyberTrust Glob	
GTE CyberTrust Root	GTE CyberTrust Root	4/4/2004	Secure Email, Client ...	GTE CyberTrust Root	
GTE CyberTrust Root	GTE CyberTrust Root	2/24/2006	Secure Email, Client ...	GTE CyberTrust Root	
Http://www.valicert.com/	http://www.valicert.com/	6/25/2019	Secure Email, Server...	ValiCert Class 1 Polic.	
Http://www.valicert.com/	http://www.valicert.com/	6/26/2019	Secure Email, Server...	ValiCert Class 3 Polic.	
Http://www.valicert.com/	http://www.valicert.com/	6/26/2019	Secure Email, Server...	ValiCert Class 2 Polic.	
IPS SERVIDORES	IPS SERVIDORES	12/30/2009	Secure Email, Server...	IPS SERVIDORES	
Microsoft Authenticode(tm) Root Au...	Microsoft Authenticode(tm) Root Au...	1/1/2000	Secure Email, Code S...	Microsoft Authentico.	
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Auth.	
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	5/10/2021	<All>	Microsoft Root Certif	
NetLock Expressz (Class C) Tanusit...	NetLock Expressz (Class C) Tanusit...	2/20/2019	Server Authenticatio...	NetLock Expressz (Cl	
NetLock Kozjegyzo (Class A) Tan...	NetLock Kozjegyzo (Class A) Tanusit...	2/20/2019	Server Authenticatio...	NetLock Kozjegyzo (.	
NetLock Uzleti (Class B) Tanusitva...	NetLock Uzleti (Class B) Tanusitvany...	2/20/2019	Server Authenticatio...	NetLock Uzleti (Class.	
NO LIABILITY ACCEPTED, (c)97 V...	NO LIABILITY ACCEPTED, (c)97 Veri...	1/8/2004	Time Stamping	VeriSign Time Stampi.	
PTT Post Root CA	PTT Post Root CA	6/26/2019	Secure Email, Server...	KeyMail PTT Post Ro.	
RootCA	RootCA	8/19/2014	<All>	<None>	
RootCA	RootCA	8/19/2014	<All>	<None>	

Trusted Root Certification Authorities store contains 105 certificates.

Figure 4: Trusted Root CA certificates

## Certificates used in Web chaining scenarios

One of the less used features in ISA Server 2006 is the use of certificates in ISA Server web chaining scenarios. Web chaining is used to chain the Web traffic from ISA Server with another Webproxy like ISA Server. To use a certificate in a webchaining scenario, the following prerequisites must be present:

- Be a client authentication certificate
- Be trusted to the issuing Root Certificate Authority
- Have a private key installed in the local computer certificate store
- Be installed in the Firewall service account personal certificate store

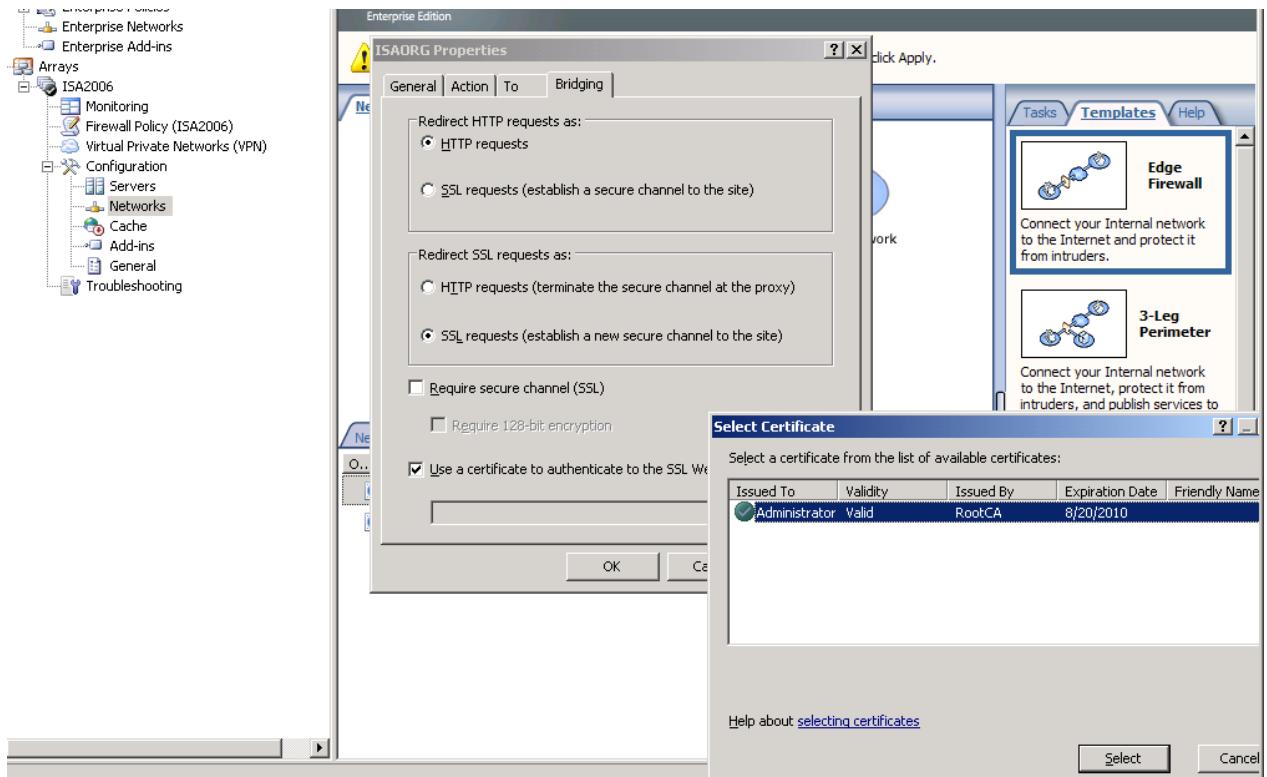


Figure 5: Select certificates in web chaining scenarios

## Exchange Remote Connectivity Analyzer

The Microsoft Exchange Remote Connectivity Analyzer is a helpful tool for testing different type of Exchange Server publishings with and without ISA Server without the use of the required tools like Microsoft Outlook. The Exchange Remote Connectivity Analyzer is also very helpful for verifying the correct Deployment of certificates on the Exchange Client Access Server (CAS) or/and on the ISA Server.

- ✓ Testing SSL Certificate for validity.  
The certificate passed all validation requirements.
  - ▲ Test Steps
    - ✓ Validating certificate name  
Successfully validated the certificate name
    - ▲ Additional Details  
Found hostname mail.hex2007.net in Certificate Subject Common name
  - ✓ Validating certificate trust  
Certificate is trusted and all certificates are present in chain
    - ▲ Additional Details  
The Certificate chain has been validated up to a trusted root. Root = E=server-certs@thawte.com, CN=Thawte Server CA, OU=Certification Services Division, O=Thawte Consulting cc, L=Cape Town, S=Western Cape, C=ZA
  - ✓ Testing certificate date to ensure validity  
Date Validation passed. The certificate is not expired.
    - Additional Details

Figure 6: Exchange Remote Connectivity Analyzer checks

## ISA Server 2006 Best Practice Analyzer

On helpful troubleshooting utility for certificate issues with ISA Server 2006 is the well known ISA Server 2006 Best Practice Analyzer which analyzes the ISA Server

installation against a database with best practices from Microsoft to find possible missconfigurations or other problems. For certificate troubleshooting purposes, ISABPA checks the ISA Server configuration and looks if certificates are used in publishing or web chaining scenarios and if the corresponding certificates can be found in the local computer certificate store.

The screenshot shows the Microsoft ISA Server Best Practices Analyzer Tool interface. On the left, there's a sidebar with navigation links: Welcome, Start a scan, Select a Best Practices scan to view, View a report (which is selected), Start BPA2Visio, and Schedule a scan. Below that is a 'See also' section with links to the Help, About the ISA Server Best Practices Analyzer, Send us your feedback, and Updates and Customer Feedback. The main area is titled 'View Best Practices Report' and 'Certificate'. It shows a list of issues under the 'All Issues' tab (7 items). The issues listed are:

- Only the Default policy rule is used
- The secure channel to the domain controller cannot be verified
- NLB integration is disabled, but the registry contains BDA settings
- The Configuration error warning alert was signaled 1 times
- There are no certificates in the local computer store. A note states: "There are no certificates in the local computer store. Secure Web publishing cannot be implemented when no certificate is available in the local computer store. This warning can be safely ignored if you do not want to publish a Web server with SSL certificate authentication." With two buttons: "Tell me more about this issue and how to resolve it." and "Do not show me this item again for all instances."
- DNS search order is blank
- ISA Server is running on a virtual server

Figure 7: ISA Server Best Practices Analyzer

To give you some information about how ISABPA displays certificate related issues, I deleted all certificates from the local computer store.

## Conclusion

In this article, I tried to give you some more information about ISA Server 2006 certificate deployment and troubleshooting. We also covered some new features of ISA Server 2006 Service Pack 1 which extends ISA Server 2006 capabilities to use SAN certificates in webserver publishing scenarios.

## Related links

Implementing and troubleshooting certificate deployment in ISA Server 2006  
<http://www.isaserver.org/tutorials/Implementing-Troubleshooting-Certificate-Deployment-ISA-Server-2006.html>

Exporting Your SSL Certificate from IIS 6.0 and Importing To ISA Server 2004  
<http://www.isaserver.org/articles/exportsslcert.html>

Digital Certificates for ISA Server 2004  
<http://technet.microsoft.com/en-us/library/cc302649.aspx>

Certificate Revocation and Status Checking  
<http://technet.microsoft.com/en-us/library/bb457027.aspx>

How to install and use certificates for SSL connections in ISA Server 2006  
<http://support.microsoft.com/kb/840614/en-us>

Troubleshooting Outlook Web Access Publishing

<http://technet.microsoft.com/en-us/library/bb794843.aspx>

Exchange Remote Connectivity Analyzer

<https://www.testexchangeconnectivity.com/Default.aspx>

Internet Information Services (IIS) 6.0 Resource Kit Tools

<http://www.microsoft.com/downloads/details.aspx?familyid=56FC92EE-A71A-4C73-B628-ADE629C89499&displaylang=en>

Microsoft Internet Security and Acceleration (ISA) Server Best Practices Analyzer (BPA) Tool

<http://www.microsoft.com/downloads/details.aspx?FamilyId=D22EC2B9-4CD3-4BB6-91EC-0829E5F84063&displaylang=en>