

## 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](http://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](http://*.it-training-grote.de), it is possible to use the certificate to publish web servers with, for example, the names [owa.it-training-grote.de](http://owa.it-training-grote.de) and [www.it-training-grote.de](http://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](http://owa.it-training-grote.de)  
[www.it-training-grote.de](http://www.it-training-grote.de)

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

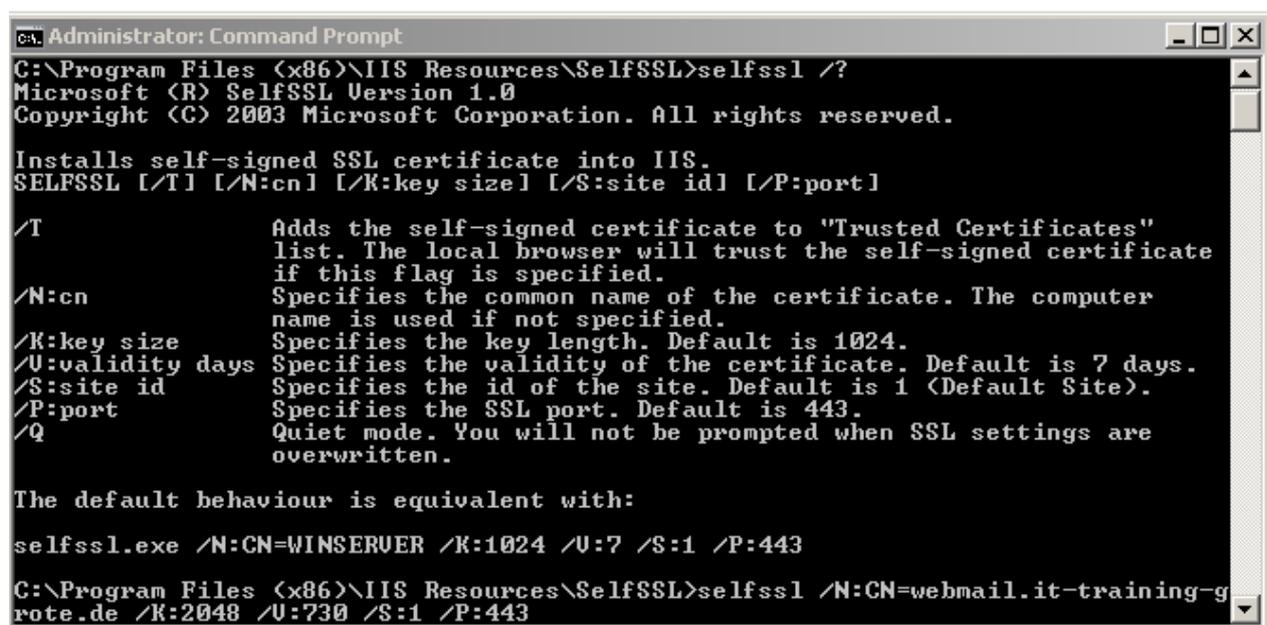
A SAN certificate is widely used in Exchange Server publishing scenarios with or without ISA Server 2006.

## 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.

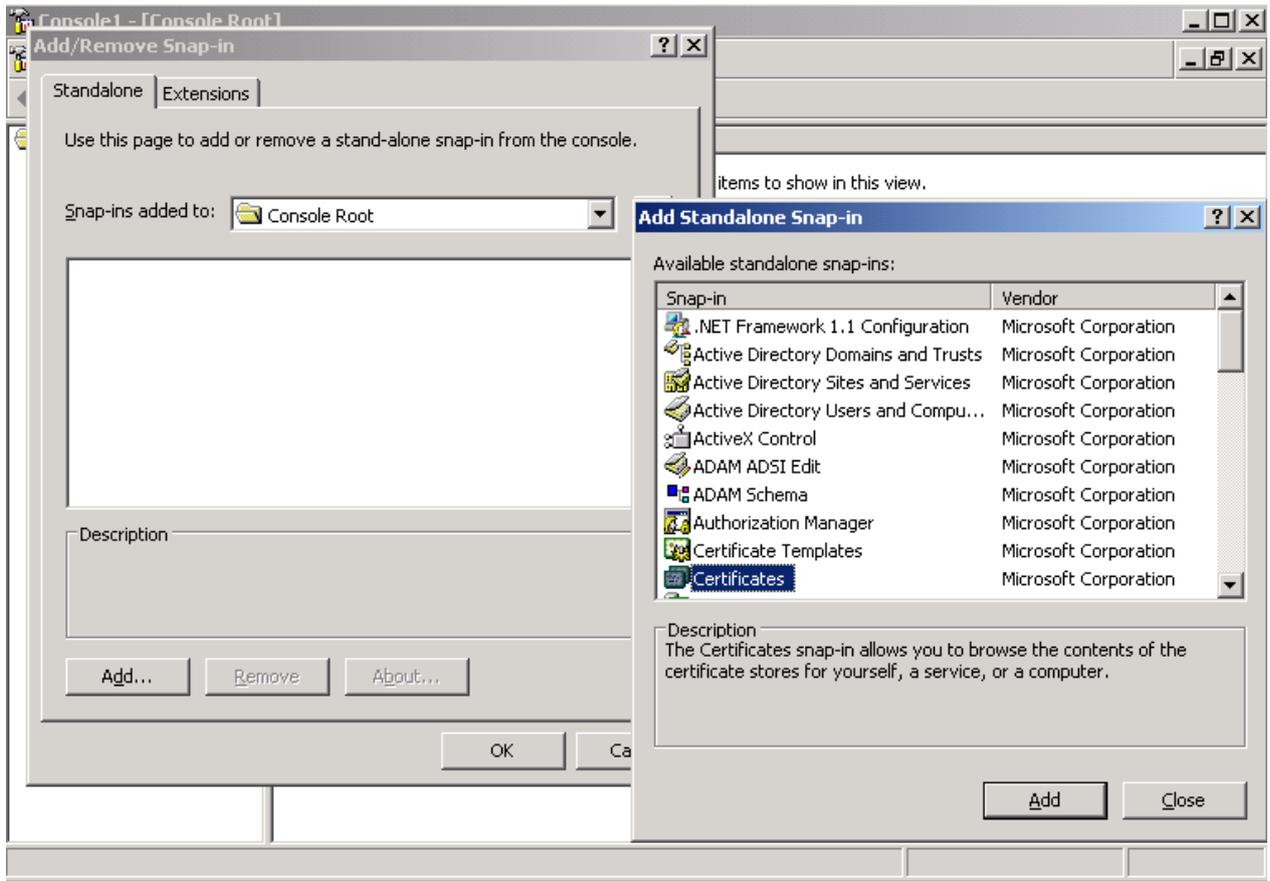


Figure 2: Add certificate Snap-In

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.

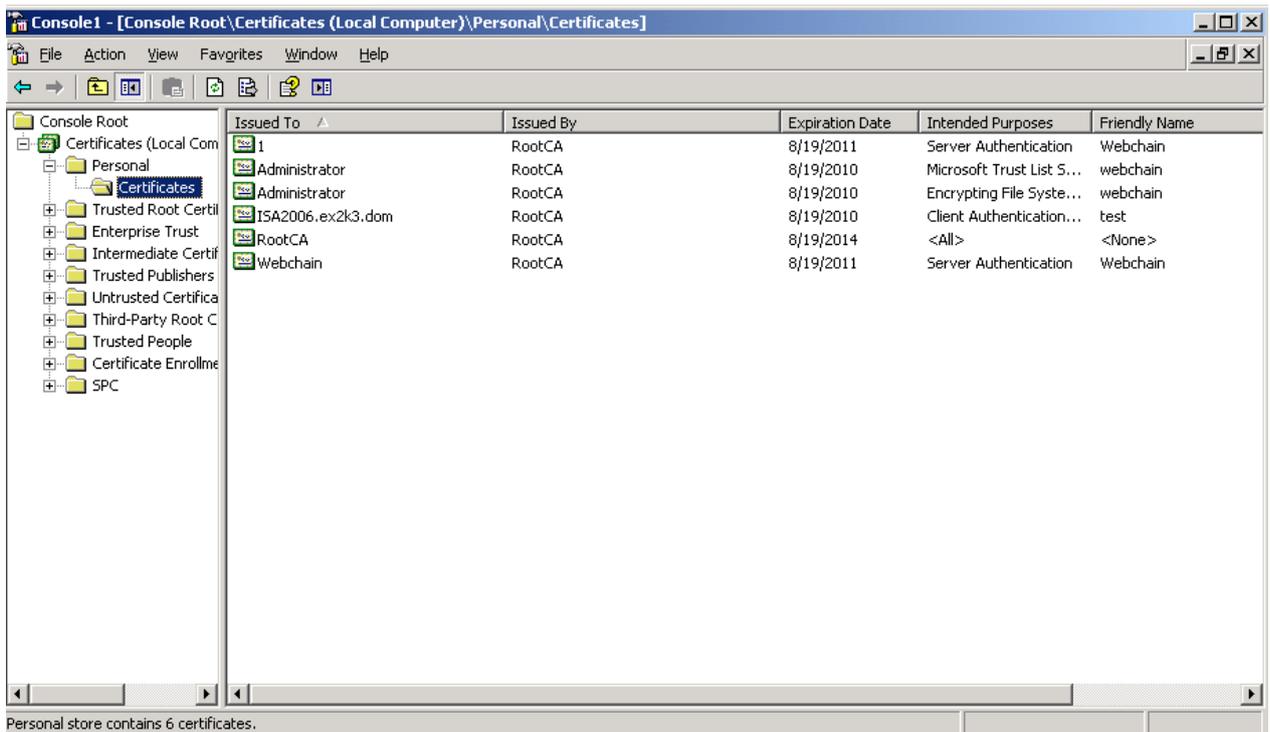


Figure 3: Display certificates in certificate store

## 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.

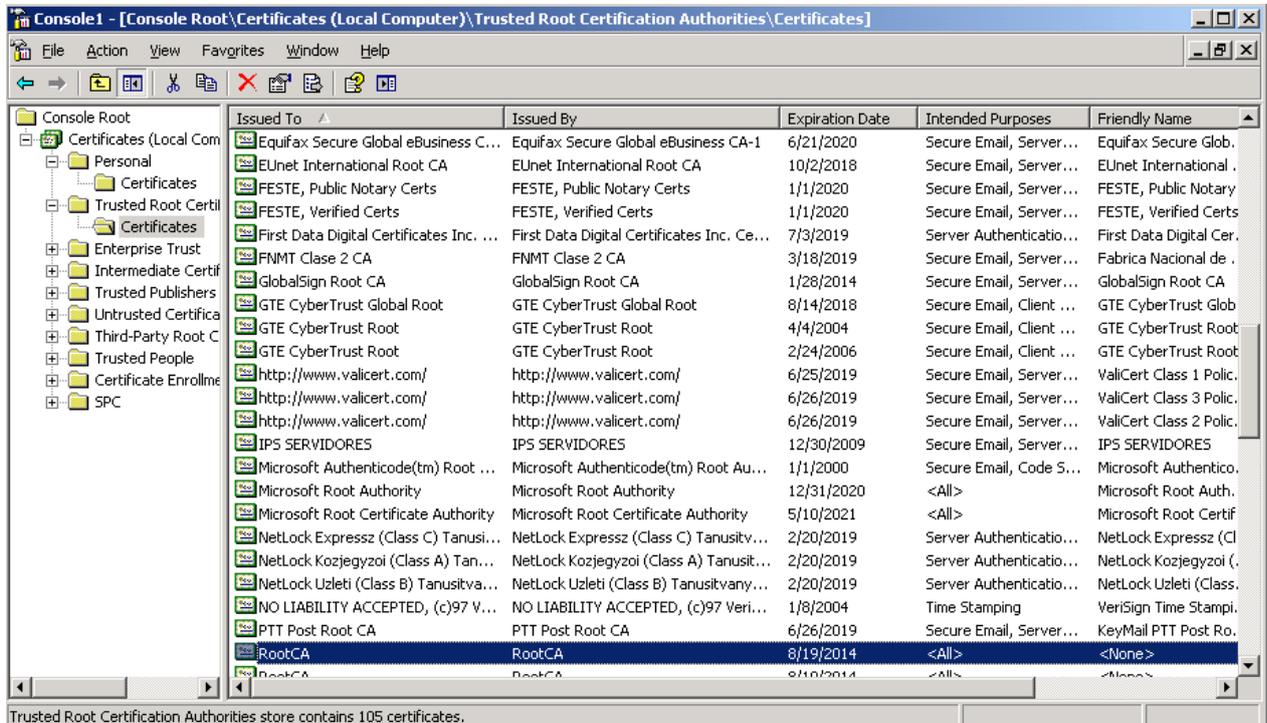


Figure 4: Trusted Root CA certificates

## 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

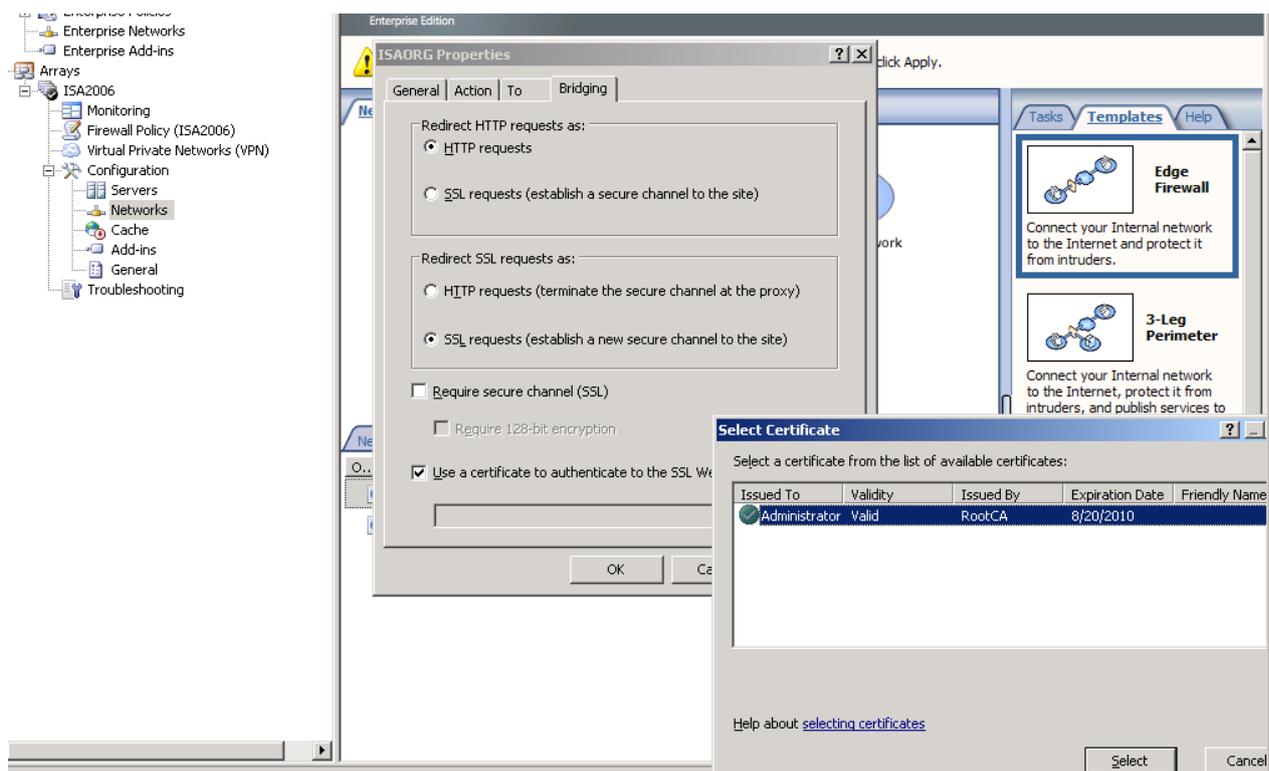


Figure 5: Select certificates in web chaining scenarios

## 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 be 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 misconfigurations 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.

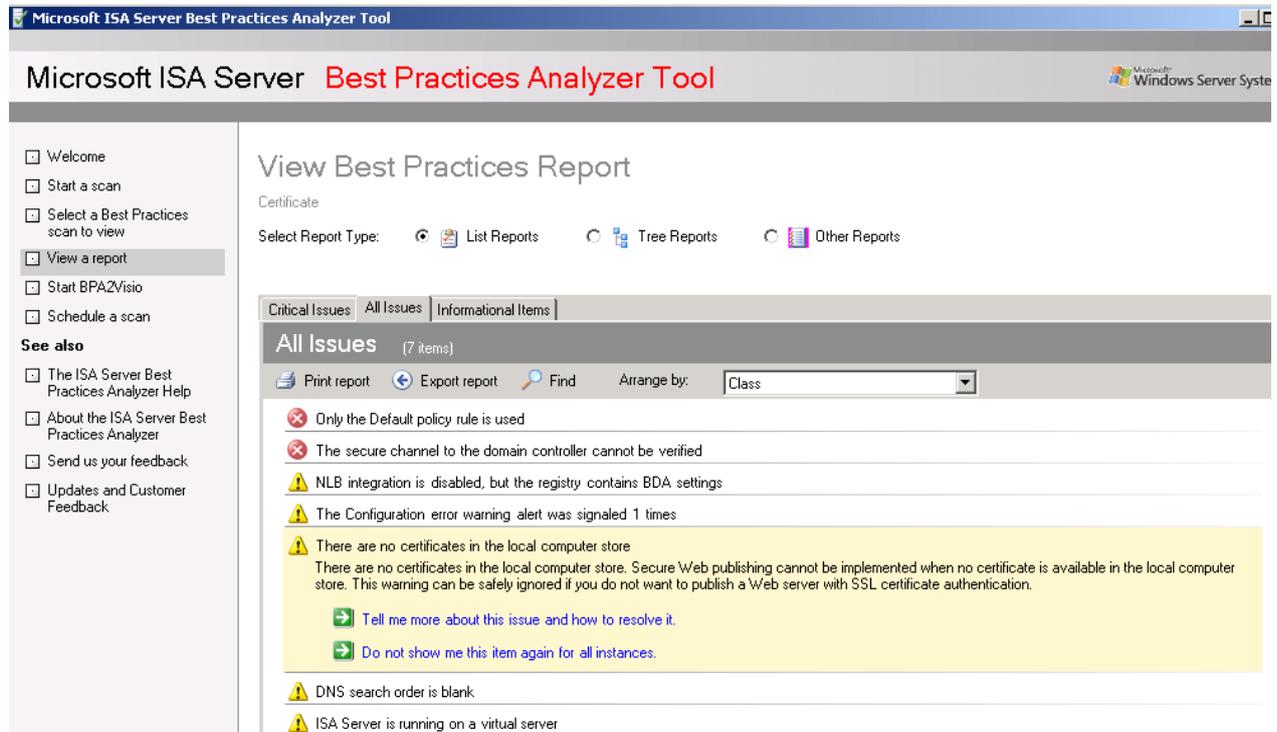


Figure 7: ISA Server Best Practices Analyzer

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

[B628-ADE629C89499&displaylang=en](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>