Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

# Implementing and troubleshooting certificate deployment in ISA Server 2006

## Abstract

In this article, I will show you some basics about certificates and certificate authorities. I'll also show you how to use certificates in reverse proxy scenarios and how to troubleshoot certificate use and revocation.

## Let's begin

Let's start with some basics about PKI definitions, digital certificates and certificate authorities.

## PKI

In cryptography terms, a public key infrastructure (PKI) is the building block for several other technology aspects with the goal of issuing certificates for users, computers and services from a certificate authority (CA). The PKI role that issued certificates is called the Registration Authority (RA).

## Certificates

In cryptography, a public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with identity information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual. In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). Source:  http://en.wikipedia.org/wiki/Digital_certificate

## Certificate Authority

In cryptography terms, a certification authority (CA) is a server or a set of servers in a CA hierarchy which issues digital certificates for use by users, computers and services. Windows Server 2003 (and older versions) has its own CA implementation.

Certification authorities can be a single server or can be chained into certificate chains where every hierarchy has special tasks like intermediate CA, issuing CA and more. You will see a CA hierarchy in the following picture.

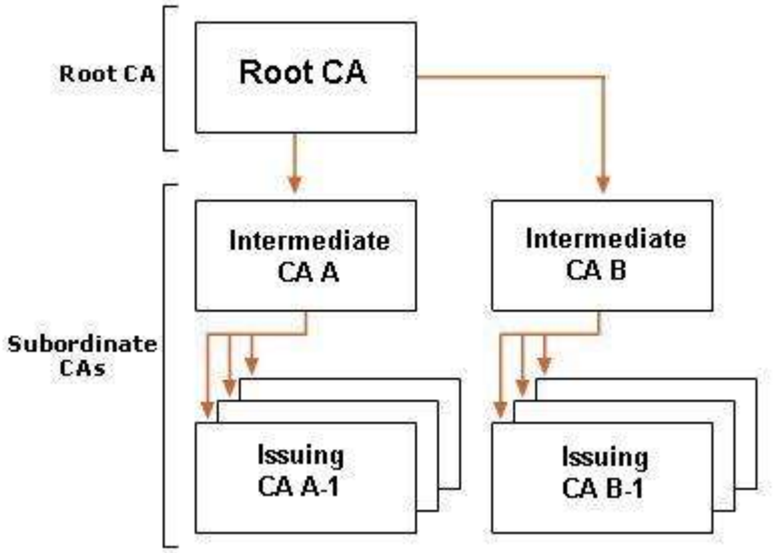


Figure 1: CA Hierarchy

### File extensions used in Cryptography

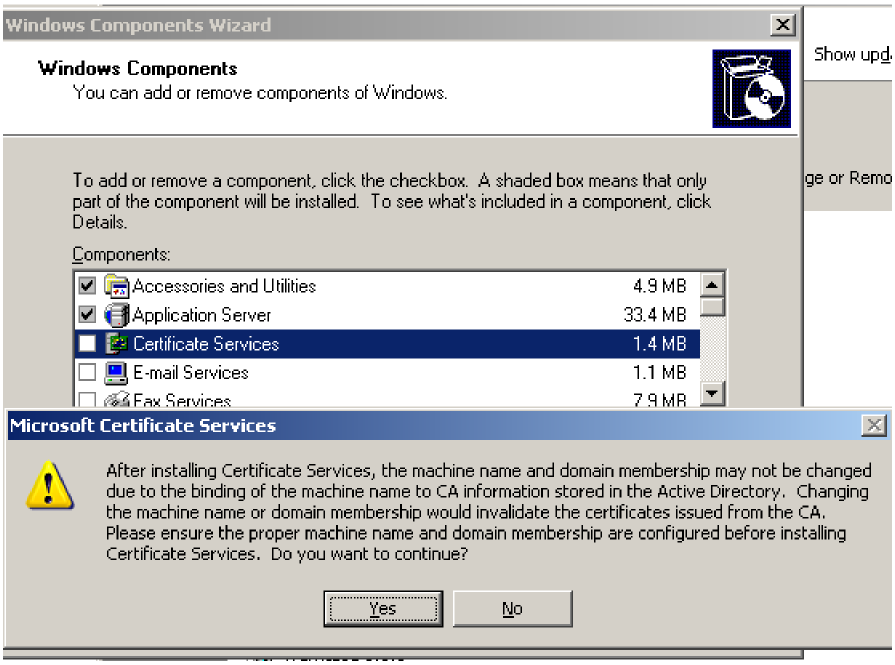
There are several file extension which will be used when you work with ISA Server 2006 and certificates. Here are some examples:

| Key | Description |
|---|---|
| PCKS #12 | Private Information Exchange |
| .PFX | Private Information Exchange |
| .P12 | Private Information Exchange |
| PCKS #7 | Cryptographic Message Syntax Standard |
| .P7B | PCKS #7 certificate |
| .CER | DER-coded-binary X.509<br>Base-64-coded-X.509 |
| .PFX | Private Information Exchange PCKS #12 |
| .CRL | Certification Revocation List |
| .P7C | Digital ID-file |
| .P7M | PCKS #7 MIME-message |
| .P7R | PCKS #7 certificate |
| .P7S | PCKS #7 signature |

Table 1: PKI file extensions

### Installing a CA

Installing and operating a CA is a relative easy process. What make PKI designs complicated are the several applications which use this PKI for several purposes. This article is not designed to show you the whole installation process; I will only cover some pictures.



**Windows Components**
You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

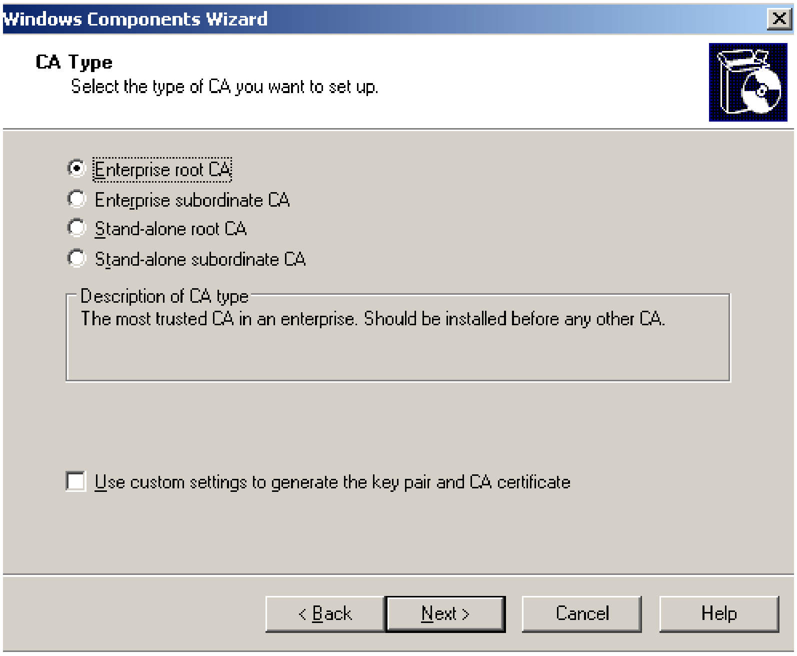
|  |  |  |
|---|---|---|
| ☑ | Accessories and Utilities | 4.9 MB |
| ☑ | Application Server | 33.4 MB |
| □ | Certificate Services | 1.4 MB |
| □ | E-mail Services | 1.1 MB |
| □ | Fax Services | 7.9 MB |

**Microsoft Certificate Services**

After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine name to CA information stored in the Active Directory. Changing the machine name or domain membership would invalidate the certificates issued from the CA. Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want to continue?

Figure 2: Installing a Windows CA

After installing the CA, the Server name and the domain membership shouldn't be changed (If you feel pain: There is a KB article which gives you a chance to move the CA).
There are several types of CA. For this example we select a Enterprise Root CA which integrates into Active Directory.



**CA Type**
Select the type of CA you want to set up.

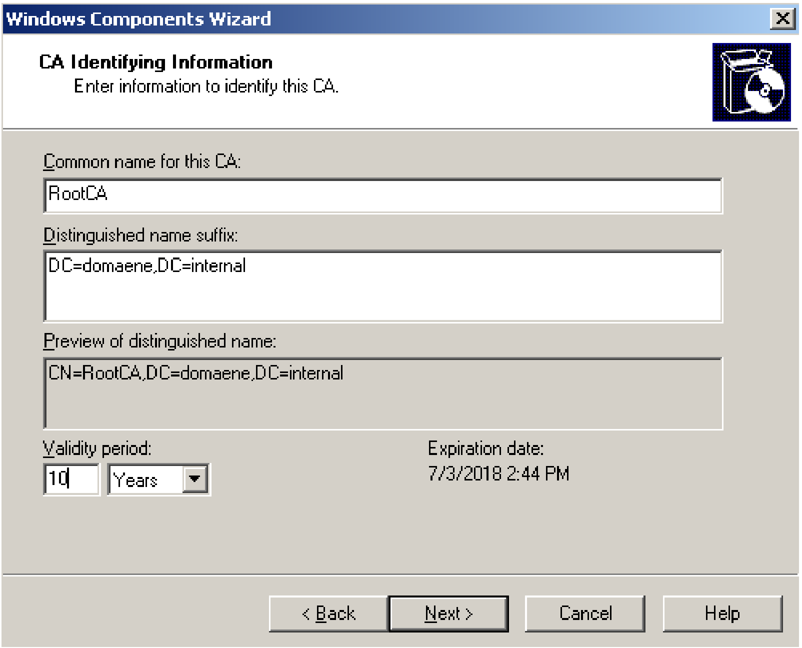
- ● Enterprise root CA
- ○ Enterprise subordinate CA
- ○ Stand-alone root CA
- ○ Stand-alone subordinate CA

Description of CA type
The most trusted CA in an enterprise. Should be installed before any other CA.

□ Use custom settings to generate the key pair and CA certificate

Figure 3: Select CA type

Give the CA a name and a lifetime.



Windows Components Wizard

CA Identifying Information

Enter information to identify this CA.

Common name for this CA: RootCA

Distinguished name suffix: DC=domaene,DC=internal

Preview of distinguished name: CN=RootCA,DC=domaene,DC=internal

Validity period: 10 Years

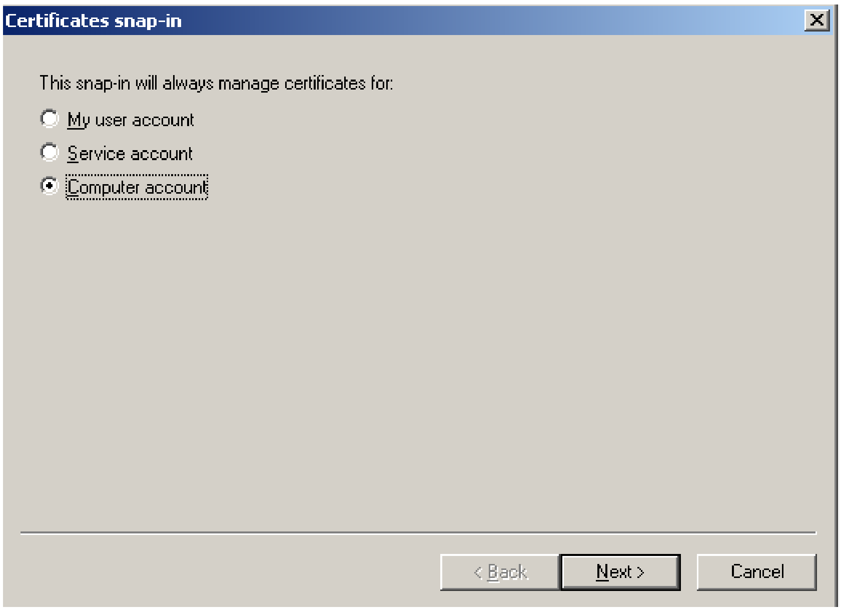
Expiration date: 7/3/2018 2:44 PM

Figure 4: CA Name

After installing the CA, the CA can be used for issuing certificates

### Certificate SnapIn

Every modern Windows version has a certificate snapIn which handles local installed certificates. If you are logged in as an Administrator, you can manage certificates for your own user account, a service account and a computer account.



Certificates snap-in

This snap-in will always manage certificates for:

○ My user account

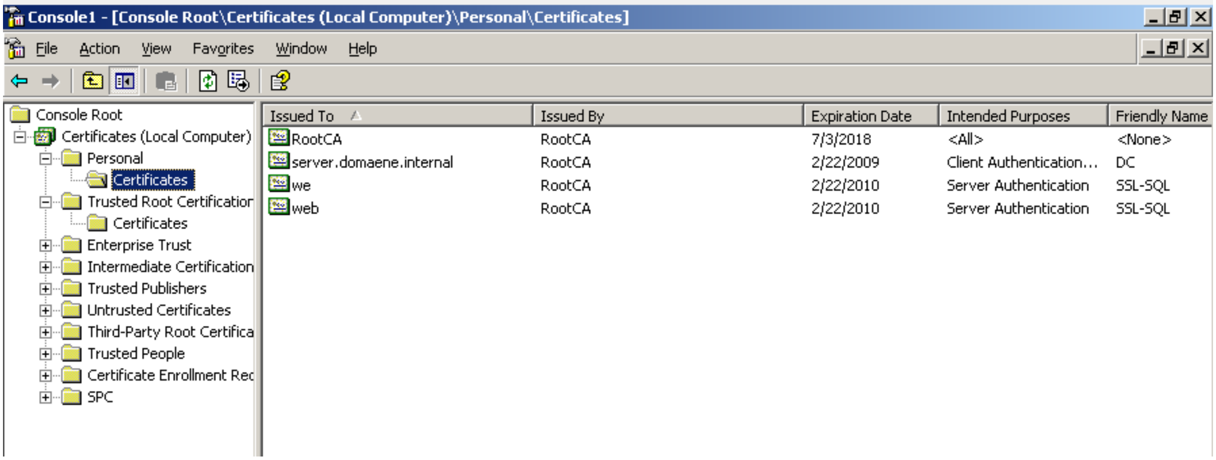
○ Service account

● Computer account

Figure 5: Manage certificates

A normal user account can only open its own certificate store.

Certificates can be managed in the console (Import, export, request new certificates and certificate deletion).

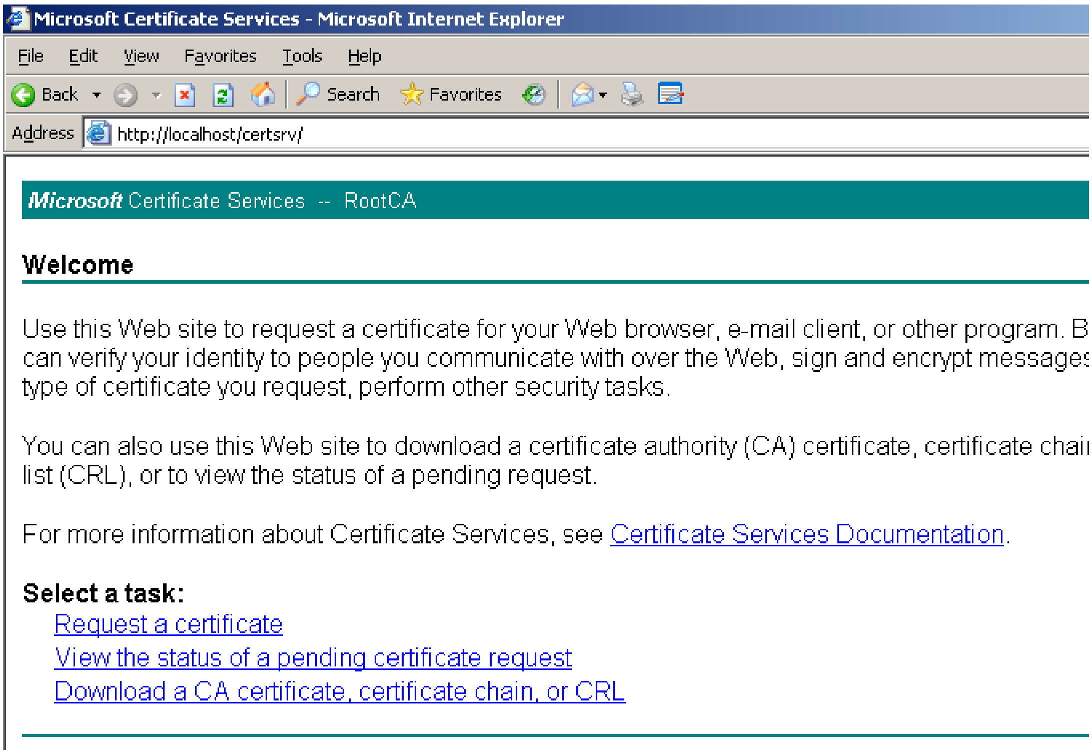

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help

Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification
Certificates
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certifica
Trusted People
Certificate Enrollment Rec
SPC

| Issued To | Issued By | Expiration Date | Intended Purposes | Friendly Name |
|---|---|---|---|---|
| RootCA | RootCA | 7/3/2018 | <All> | <None> |
| server.domaene.internal | RootCA | 2/22/2009 | Client Authentication... | DC |
| we | RootCA | 2/22/2010 | Server Authentication | SSL-SQL |
| web | RootCA | 2/22/2010 | Server Authentication | SSL-SQL |

Figure 5: Manage certificates

There is also a website which can be used by users to request new certificates or to download CA root certificates.


Microsoft Certificate Services - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address

http://localhost/certsrv/

*Microsoft* Certificate Services -- RootCA

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. B
can verify your identity to people you communicate with over the Web, sign and encrypt messages
type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chai
list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

**Select a task:**

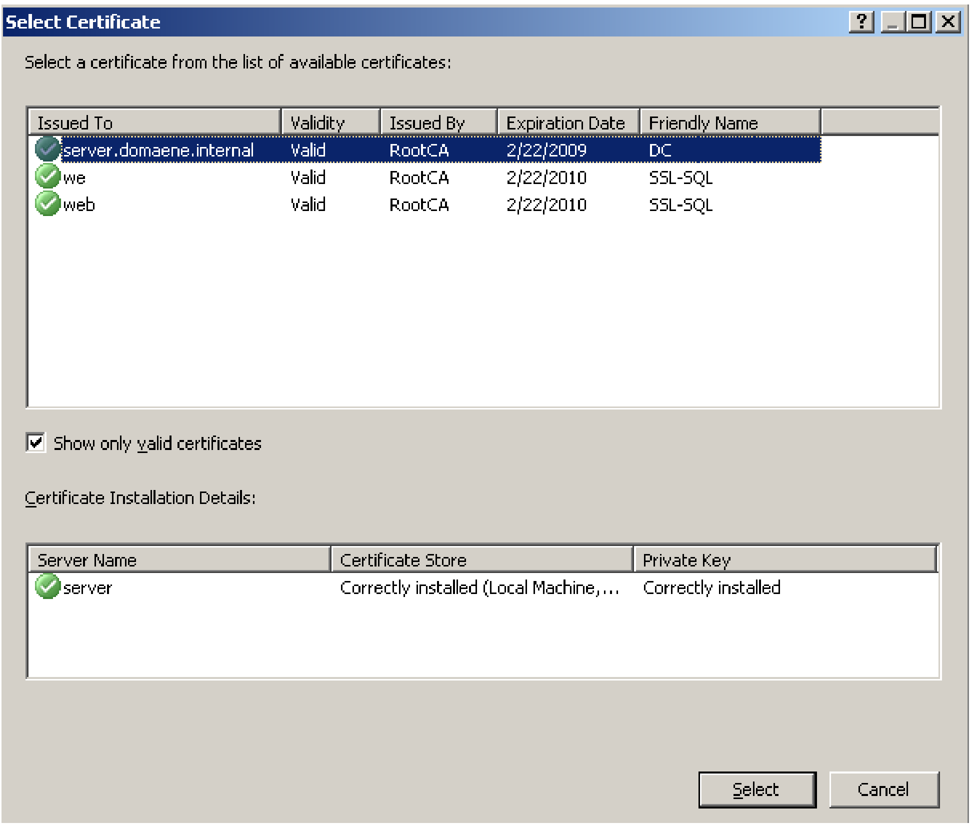
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Figure 6: CA website

### Settings in a reverse publishing scenario

If you want to use ISA Server as a reverse publishing proxy to publish services like Outlook Web Access (OWA) or Outlook Anywhere (OA), it is possible to enable SSL Bridging to enhance the security of ISA Server. When SSL Bridging is enabled, ISA Server terminates the SSL connection from the Server to the client; ISA then inspects the traffic and encrypts the traffic to HTTPS again. This is the most secure scenario. In this scenario, ISA server needs the Root CA certificate from the internal CA that has issued certificates for the server to publish. ISA Server also needs a certificate for the ISA listener which Common Name (CN) has the same entry as the public name which clients enter when they try to establish a connection with the published server.

During the publish process, ISA Server 2006 has a new certificate assistant that helps you to select the correct certificate. For troubleshooting purposes read the SSL troubleshooting article at the end of this article.
The certificate must be issued from a trusted CA, the certificate must be valid and keep a closer look at the Common Name of the certificate. The CN must match the public name that clients use to connect to the server.



Select Certificate

Select a certificate from the list of available certificates:

| Issued To | Validity | Issued By | Expiration Date | Friendly Name |
|---|---|---|---|---|
| server.domaene.internal | Valid | RootCA | 2/22/2009 | DC |
| we | Valid | RootCA | 2/22/2010 | SSL-SQL |
| web | Valid | RootCA | 2/22/2010 | SSL-SQL |

☑ Show only valid certificates

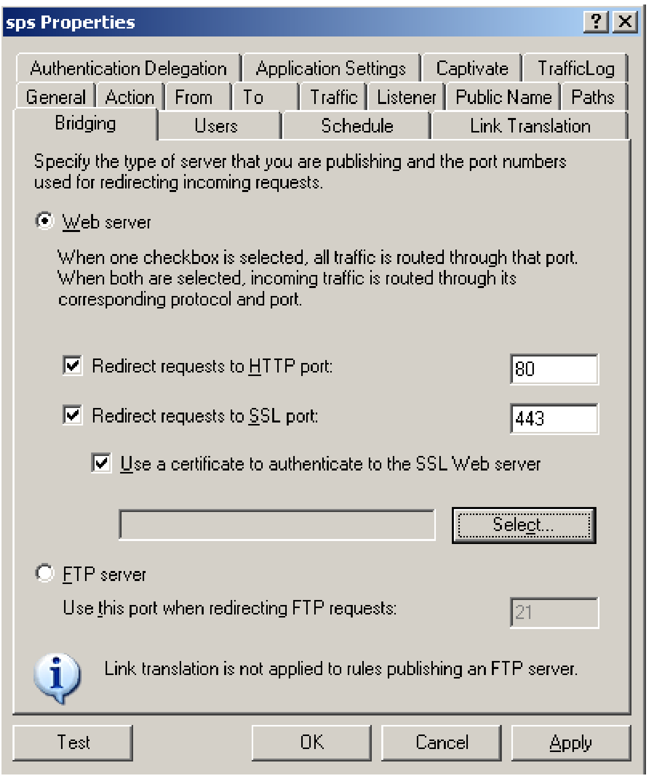
Certificate Installation Details:

| Server Name | Certificate Store | Private Key |
|---|---|---|
| server | Correctly installed (Local Machine,... | Correctly installed |

Figure 7: Certificate assistant

## What is the Bridging Tab in ISA Server 2006?

Have you ever tried to use the Bridging feature in the publishing rule? If you try to select the certificate, ISA often says that there is no certificate right?
To get this working you must issue a user certificate for a normal user. This issued certificate must be imported (with the private key) into the local certificate store of the Microsoft ISA Server Firewall service. After that you can use the certificate to redirect incoming request to the internal server which requires certificate authentication.



sps Properties

Specify the type of server that you are publishing and the port numbers used for redirecting incoming requests.

● Web server

When one checkbox is selected, all traffic is routed through that port. When both are selected, incoming traffic is routed through its corresponding protocol and port.

☑ Redirect requests to HTTP port: 80

☑ Redirect requests to SSL port: 443

☑ Use a certificate to authenticate to the SSL Web server

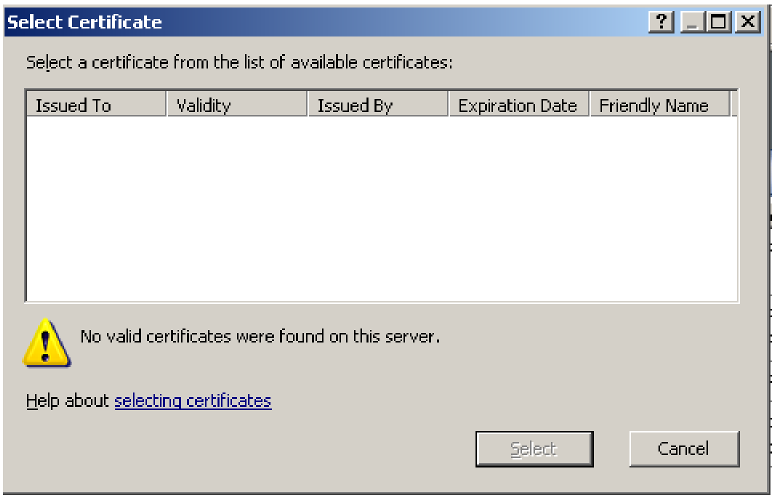
○ FTP server

Use this port when redirecting FTP requests: 21

Link translation is not applied to rules publishing an FTP server.

Figure 8: SSL Bridging

There are no certificates that are available because there is no certificate installed in the local certificate store of the ISA Server Firewall service.



Select Certificate

Select a certificate from the list of available certificates:

| Issued To | Validity | Issued By | Expiration Date | Friendly Name |
|---|---|---|---|---|

No valid certificates were found on this server.

Help about selecting certificates

Figure 9: SSL Bridging – select a certificate

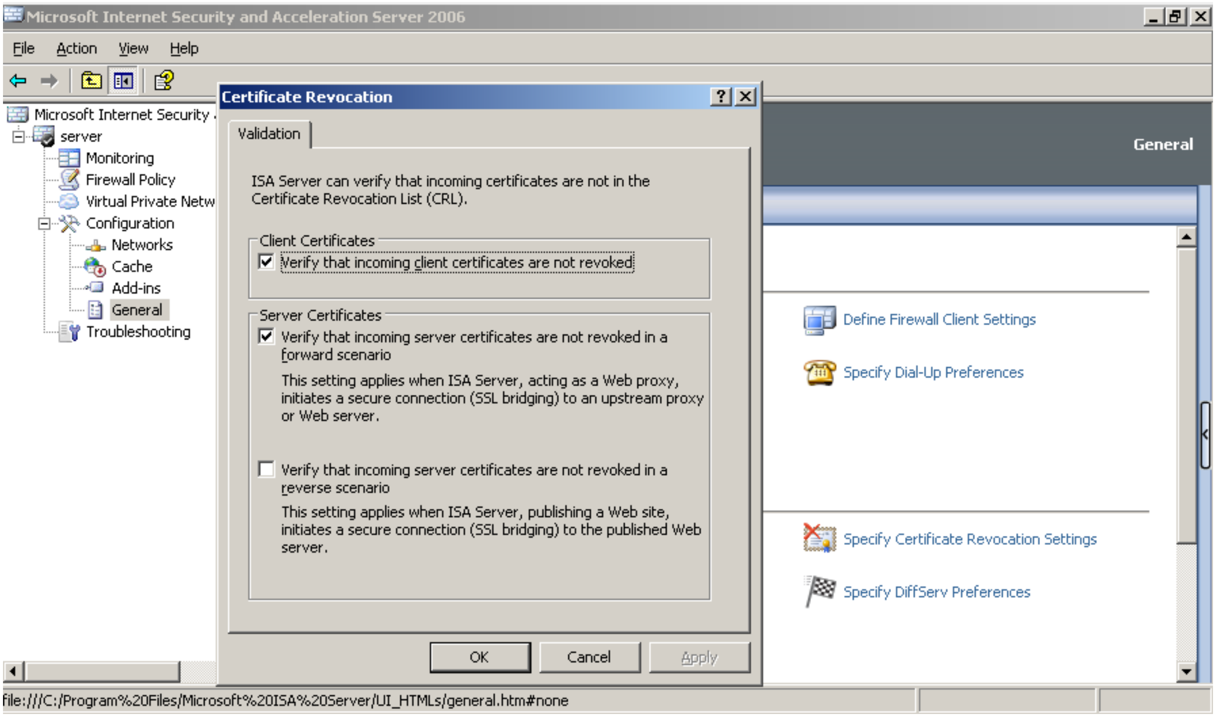
### Certificate revocation

Certificate revocation is the process when an application requests the certificate chaining engine to evaluate a certificate, the validation is performed on all certificates in that certificates chain. This includes every certificate from the issuing CA to the issued certificate. As a first step the certificate chain will be evaluated. If the certificate chain is intact, the process checks that:

- The certificates signature is valid
- Verify that the current date and time from the certificate falls into the valid time period of the certificate.
- Verify that each certificate is not corrupt or malformed

A certificate revocation list contains no more valid certificates. A process or Software like ISA Server can check the requested certificate against the certificate revocation list.

It is possible to configure ISA Server for several validation requests. ISA Server can verify that incoming certificates are not in the Certificate Revocation List (CRL).


Microsoft Internet Security and Acceleration Server 2006
File
Action
View
Help
Microsoft Internet Security
server
Monitoring
Firewall Policy
Virtual Private Netw
Configuration
Networks
Cache
Add-ins
General
Troubleshooting
General
Define Firewall Client Settings
Specify Dial-Up Preferences
Specify Certificate Revocation Settings
Specify DiffServ Preferences
Certificate Revocation
Validation
OK
Cancel
Apply

ISA Server can verify that incoming certificates are not in the Certificate Revocation List (CRL).

Client Certificates

☑ Verify that incoming client certificates are not revoked

Server Certificates

☑ Verify that incoming server certificates are not revoked in a forward scenario

This setting applies when ISA Server, acting as a Web proxy, initiates a secure connection (SSL bridging) to an upstream proxy or Web server.

☐ Verify that incoming server certificates are not revoked in a reverse scenario

This setting applies when ISA Server, publishing a Web site, initiates a secure connection (SSL bridging) to the published Web server.

file:///C:/Program%20Files/Microsoft%20ISA%20Server/UI_HTMLs/general.htm#none

Figure 10: Certificate revocation

### Verify that incoming client certificates are not revoked

You must select this certificate if you want to let ISA Server to perform a check of the incoming certificate against the Certificate revocation List (CRL) to see if the certificate is revoked. If the certificate is revoked, the client request will be denied.

### Verify that incoming server certificates are not revoked in a forward scenario

This option is a little different from the scenario above. In this scenario, ISA server checks to see if the incoming Server certificate in an SSL Bridging scenario is revoked. If the certificate is revoked, the request will be denied.

### Verify that incoming server certificates are not revoked in a reverse scenario

Select this check box to specify that ISA Server will automatically check the Certificate Revocation List (CRL) to see if server certificates, in a Web publishing scenario, are revoked. If the certificate is revoked, the request will be denied.

## Conclusion

In this article I tried to show you all aspects of certificate use in ISA Server 2006 for reverse publishing scenarios for Outlook Web Access (OWA), Outlook Anywhere (OA) and more. I also tried to give you some basics about certificates, certificate authorities and certificate checks.

## Related links

Troubleshooting SSL Certificates in ISA Server 2004 Publishing
http://technet.microsoft.com/en-us/library/cc302619.aspx
Troubleshooting Outlook Web Access Publishing
http://technet.microsoft.com/en-us/library/bb794843(TechNet.10).aspx
Certificate Revocation and Status Checking
http://technet.microsoft.com/en-us/library/bb457027.aspx
Public key infrastructure - Wikipedia, the free encyclopedia
http://en.wikipedia.org/wiki/Public_key_infrastructure