Manage CAs

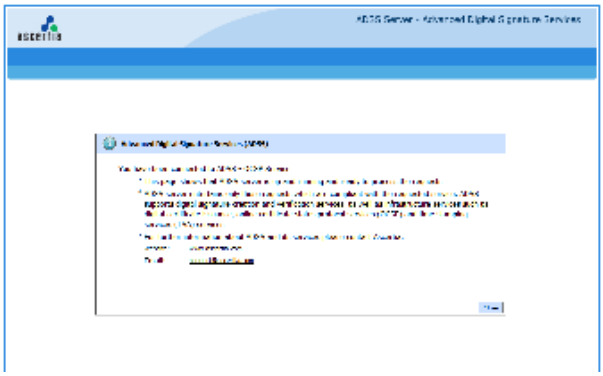
Table of Contents

Configuring public URLs of AIA and CDP addresses if ADSS Server is running in MZ

AIA -> OCSP Responder

If you are running the ADSS Server in MZ (Militarized Zone) and you want to redirect the AIA requests from DMZ (Demilitarized Zone) machine to ADSS Server then follow these instructions:

1. Create a website (e.g. http://ocsp.ascertia.com) in IIS on MZ machine and set the **Physical Path** to **C:\inetpub\wwwroot**
2. Configure the AJP Connector in this website as documented in **Appendix A** of **SigningHub Installation Guide**
3. Now go to **C:\tomcat_iis_connector\conf** directory and edit the file **uriworkermap.properties** and set the worker2 as **/*=worker2** instead of **adss/*=worker2**
4. Edit the **workers.properties.minimal** file and set the value of **worker.worker1.host** and **worker.worker2.host** to your ADSS Server machine name/IP instead of localhost
5. Restart the IIS Service and access the website (e.g. http://ocsp.ascertia.com). If it showing the blue page as below, it means your configurations are correct and send an OCSP request to double check it



CDP and AIA -> CA Cert

If you are running the ADSS Server in MZ (Militarized Zone) and you want to redirect the CDP requests from DMZ (Demilitarized Zone) machine to ADSS Server then follow these instructions:

1. Create a directory on MZ machine file system (e.g. C:\data) and grant **Read** permissions to **IUSR** user on this directory
2. Create a website (e.g. http://downloads.ascertia.com) in IIS on MZ machine and set the **Physical Path** to **C:\data**
3. Create two directories in **C:\data** as **C:\data\crls** and **C:\data\certs**
4. Share the C:\data\crls directory over the network and configure the shared path (e.g. \\mz-server\data\crls) in **Manage CAs > Local CAs** module in the respective CA to publish the CRLs at this path
5. Run the **ADSS Server Console** and **Core Services** under the Windows User who have access to this shared path (e.g. administrator). Click here for details.
6. After services restart publish the CRLs from **Manage CAs > Local CAs** module, the CRLs will be published in the shared directory (e.g. \\mz-server\data\crls)
7. Put the issuer certificates in the **C:\data\certs** directory
8. Access these URLs from the internet to check its working (e.g. http://downloads.ascertia.com/crls/crl-file-name.crl and http://downloads.ascertia.com/certs/ca-cert-file-name.cer)

CRL is not publishing for the Local CA [current and new CRL numbers are same]

This situation is caused when there was a database update failure during the publishing of the last CRL. ADSS Server prints an error in **core.log** t hat the new CRL number must be greater than the current one. The error message will be like the following in core.log:

> **core.log error**
> *[CA Name] CRL invalid because new CRL's CRLNumber '5' is not greater than the current CRL's CRLNumber '5'*
> *Failed to update CRL in database : CRL invalid because new CRL's CRLNumber '5' is not greater than the current CRL's CRLNumber '5'*

Follow these steps to resolve this issue:

1. Connect to the ADSS Server database and execute the following SQL query:
   *Replace the **[**new CRL number]** with next CRL number e.g. 6 in this example and **[CA name from Manage CAs > Local CAs]** accordi ngly:*

   ```
   UPDATE LocalCertificateAuthorities SET CrlNo = [new CRL number] where Id = [CA
   name from Manage CAs > Local CAs]
   ```

2. Now go to **Manage CAs > Local CAs**
3. Click the CA Name for which the problem is occurring. Clicking the **Publish CRL Now** button will publish the CRL with next CRL number
4. Restart the ADSS Server Core from **Server Manager** module for the changes to take effect

What is meant by an external CA?

The term “External CA” refers to any CA that is operated by an externally managed certificate service provider to issue certificates for business applications or RA managed services. ADSS Server provides support to work with external CAs like Microsoft CA Server 2003, GlobalSign EPKI, EJBCA, Ascertia ADSS CA Server, and offline external CA. Integration of ADSS Server with other CAs is also possible because ADSS Server us es standard data structures for certificate requests and responses, i.e. PKCS#10 for certificate requests and PKCS#7 for certificate responses. Se e **Manage CAs > Configure External CA** for more details.

> Microsoft CA Server 2008 and 2012 are not supported.

How to replace an existing local CA?

When the local CAs have already been used to issue certificates, then ADSS Server would restrict deleting these CAs. As CAs are responsible to publish CRLs (revocation information) along with issuing new certificates. However, there are certain business scenarios, which require replacing a previously configured CA with a new CA, i.e.

- The previously configured CA was used for evaluation purpose, and needs to be replaced before moving into production.
- The old CA key has been compromised, so its usage should be discontinued.
- The existing CA is about to expire. So there is a requirement to add a new CA in place of an existing CA, without extending the license.

Workaround:

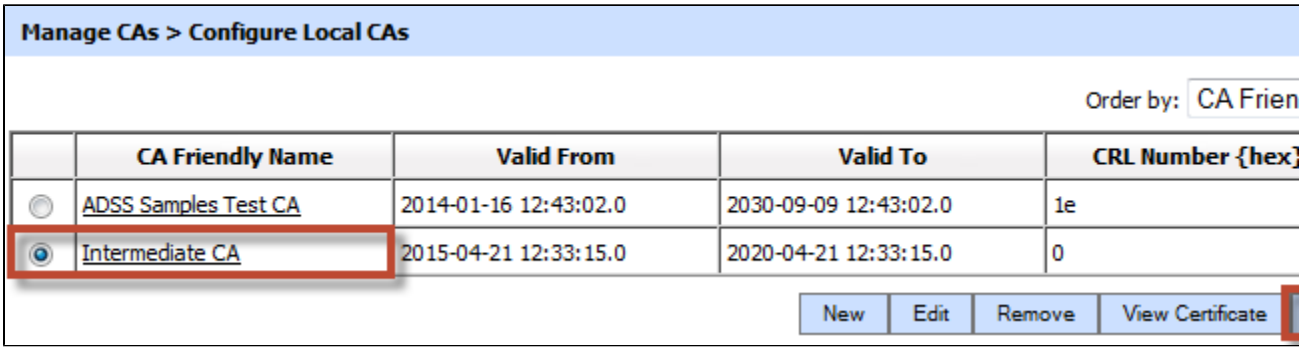
1. Browse the **Key Manager > Service Keys** module and create a new key with the purpose "Certificate/CRL Signing" and self-certify it, or re-certify an existing key with the same purpose.
2. Browse the **Manage CAs > Configure Local CA(s)** module and edit the details of local CA, which is to replace.
3. From the "CA Certificate Info" area, change the certificate for this local CA in the "CA Certificate" drop down. Select the new certificate from the list which was created through step 1.
4. Click the "Update" button to save the changes.

> **Important Considerations**
> - If a CA is renewed with the same details (e.g. Subject Information, Key pair), then all the previously issued certificates by this CA will remain valid.
> - If a new key is used to sign the CA certificate, then all the previously issued certificates by this CA will become invalid.
> - The CA that has been marked as "Default" can not be deleted.

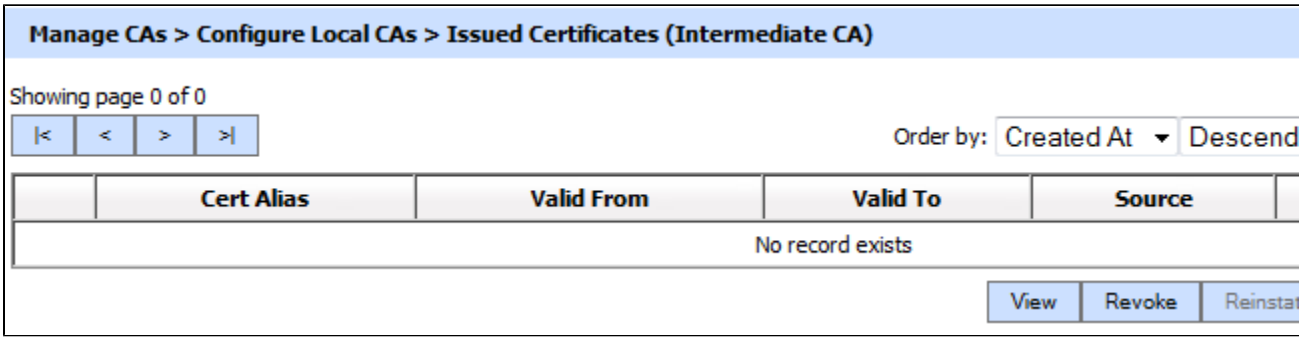
How to import a CA and its issued certificates into ADSS Server?

If you need to import a CA and its issued certificates into ADSS Server then follow these instructions:

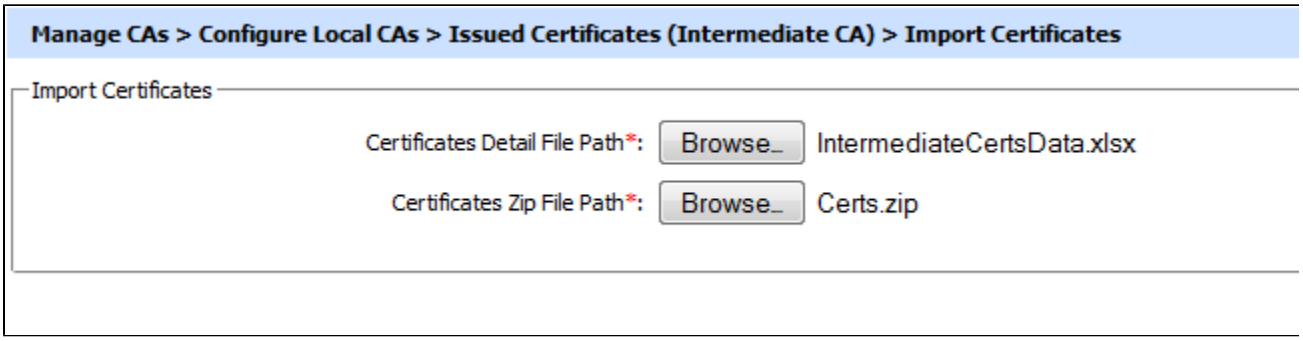
1. If the CA key is held in Hardware Crypto Device then:
    a. Configure that device in ADSS Server. Follow the link for more details:
    http://manuals.ascertia.com/ADSS-Admin-Guide/default.aspx#pageid=creating_a_new_hardware_crypto_profile
    b. Import the key from device in ADSS Server. Follow the link for more details:
    http://manuals.ascertia.com/ADSS-Admin-Guide/default.aspx#pageid=importing_existing_keys
2. If the CA key is held in software (PKCS#12) then import the key in ADSS Server from Key Manager module. Follow the link for more details:
    http://manuals.ascertia.com/ADSS-Admin-Guide/default.aspx#pageid=importing_keys
3. Configure this CA key in Manage CAs module. Follow the link for more details:
    http://manuals.ascertia.com/ADSS-Admin-Guide/default.aspx#pageid=configuring_the_adss_ca_module
4. Go to **Manage CAs > Configure Local CAs**, select the CA and click the **Issued Certificates** button as shown below:



5. On the Issued Certificates page, click the **Import Certificates** button to import the issued certificates of the CA as shown below:



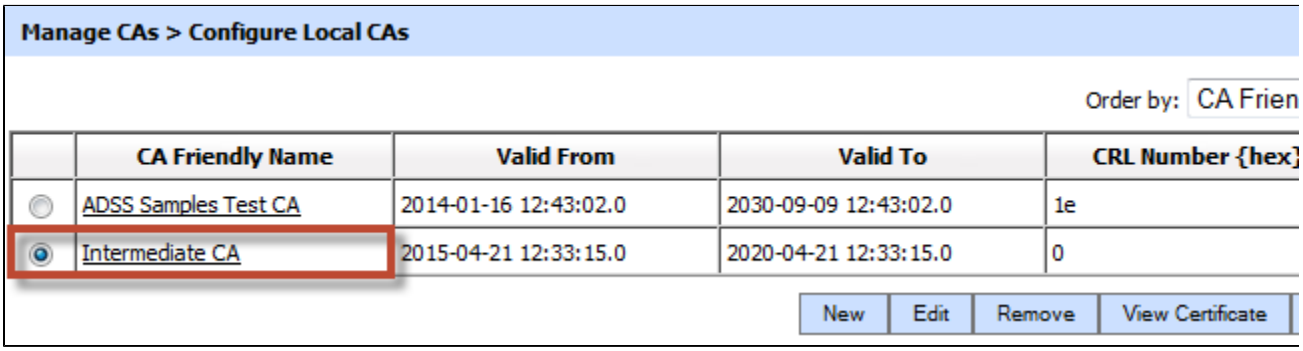
6. Browse the certificates detail file in the **Certificates Detail File Path** field and a zipped certificates in **Certificates Zip File Path** filed.



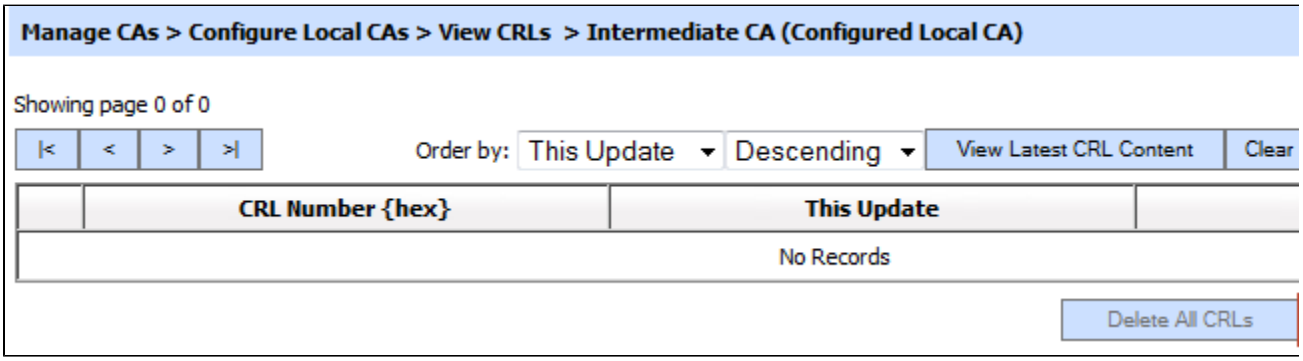
The certificates details file should be a CSV in the following format:

ALIAS	ISSUANCE_DATE	CERT_FILE	EXPIRY_DATE	REVOCATION_D
sample-1	21/04/2015	sample-01.cer	23/02/2018 21:59:59	
sample-2	21/04/2015	sample-02.cer	23/02/2018 21:59:59	
sample-3	21/04/2015	sample-03.cer	23/02/2018 21:59:59	21/04/2015 13:5
sample-4	21/04/2015	sample-04.cer	03/04/2018 21:59:59	21/04/2015 13:5
sample-5	21/04/2015	sample-05.cer	14/04/2018 21:59:59	21/04/2015 13:0
sample-6	21/04/2015	sample-06.cer	14/04/2018 21:59:59	21/04/2015 13:0
sample-7	21/04/2015	sample-07.cer	10/01/2018 21:59:59	21/04/2015 13:0
sample-8	21/04/2015	sample-08.cer	10/01/2018 21:59:59	21/04/2015 13:0
sample-9	21/04/2015	sample-09.cer	23/02/2018 21:59:59	21/04/2015 13:0
sample-10	21/04/2015	sample-10.cer	23/02/2018 21:59:59	21/04/2015 13:0

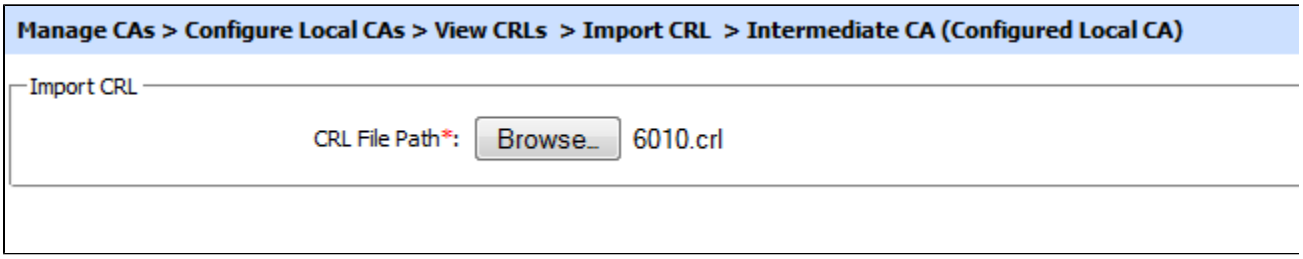
7. Click **OK** to complete the action.
8. To import CRL, go to **Manage CAs > Configure Local CAs** sub-module, select the CA and click the **View CRLs** button as shown below:



9. Now click the Import CRL button as shown below:



10. Browse the latest CRL for this from the file system as shown below:



11. Click **OK** to proceed.
12. See **details** as how to configure the CRL publishing settings for this CA

How to configure a Microsoft CA with ADSS Server?

This section describes how business applications can register users, have ADSS Server generate keys and then have an external Microsoft CA certify these.

This section describes the steps required to configure the ADSS Server certification module (ADSS_msca) within the Internet Information Services (IIS) on the Windows 2003 CA server so that this CA can be used by ADSS Server Certification Service.

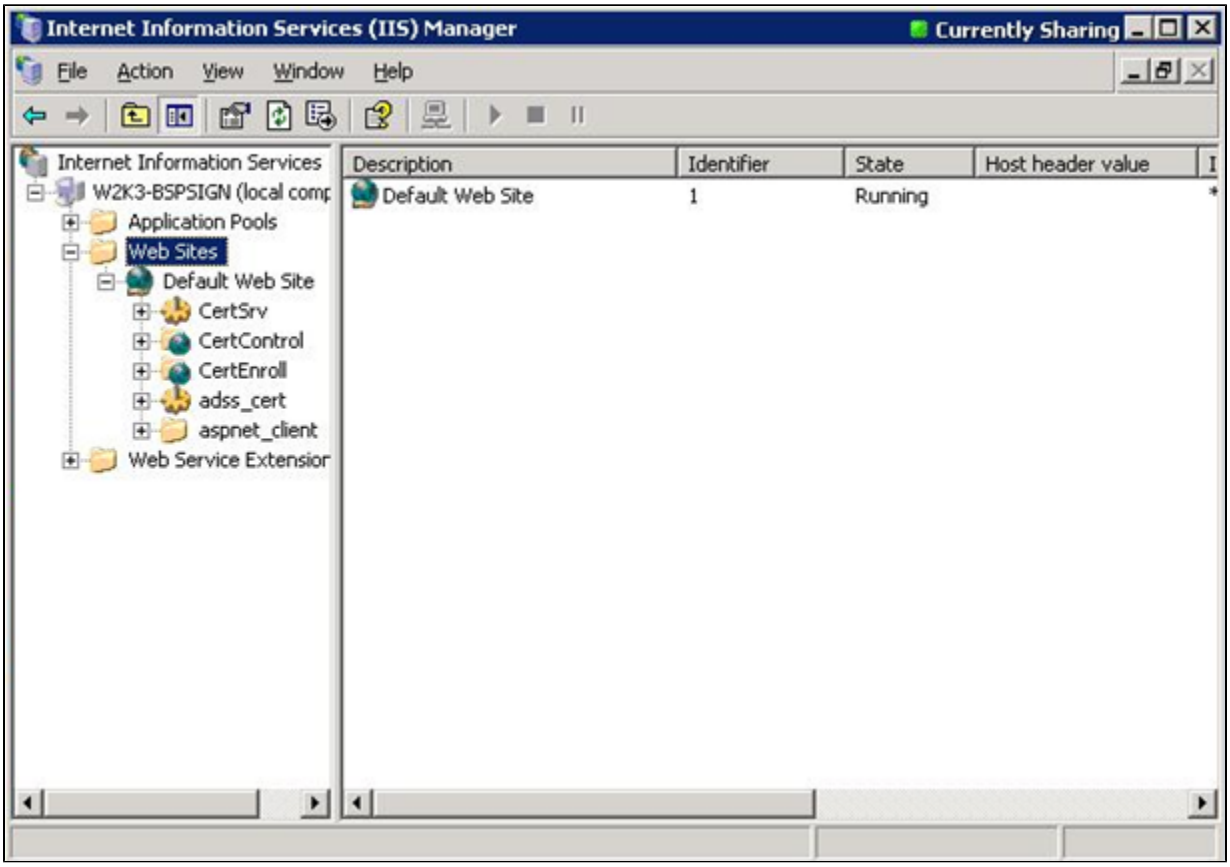
For installation and configuration of Windows 2003 Certification Authority (CA) itself, consult the separate ADSS – Microsoft CA 2003 Installation & Configuration Manual.

Microsoft .NET framework is needed to be installed on the target server in order to run the ADSS_msca module.

Configuration of ADSS_MSCA module in IIS:

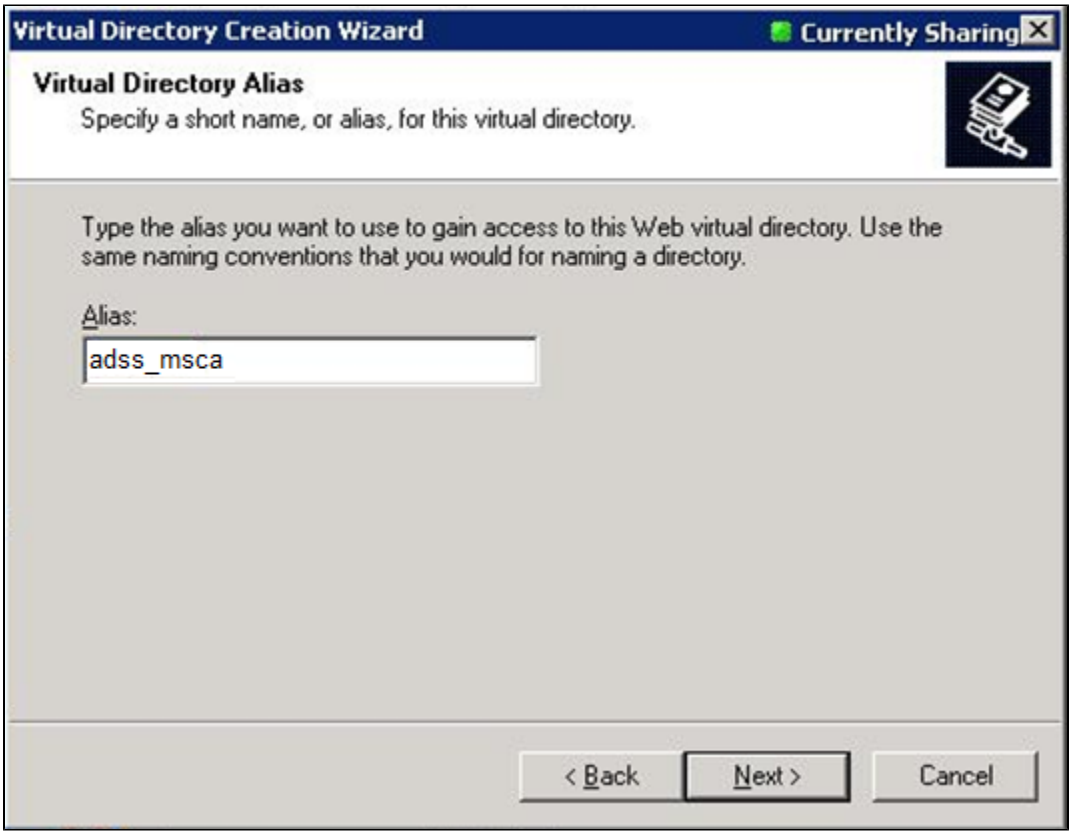
The following steps are required to configure the ADSS_msca module with IIS:

- Unzip and extract the "ADSS_msca.zip" contents in a folder e.g. "C:\ADSS_msca". This module is present at the location: “<ADSS Server installation directory>/support”. ADSS_msca is an application built using ASP.Net. This application acts as middle-ware between the ADSS Server which requests certificates and the Windows 2003 CA which accepts these certificate requests and generates corresponding certificates.
- Click the "Start" button > Control Panel > Administrative Tools > Internet information Services Manager (IIS)**.** The Internet Information Services window opens.
- Expand Web Sites (as shown below):

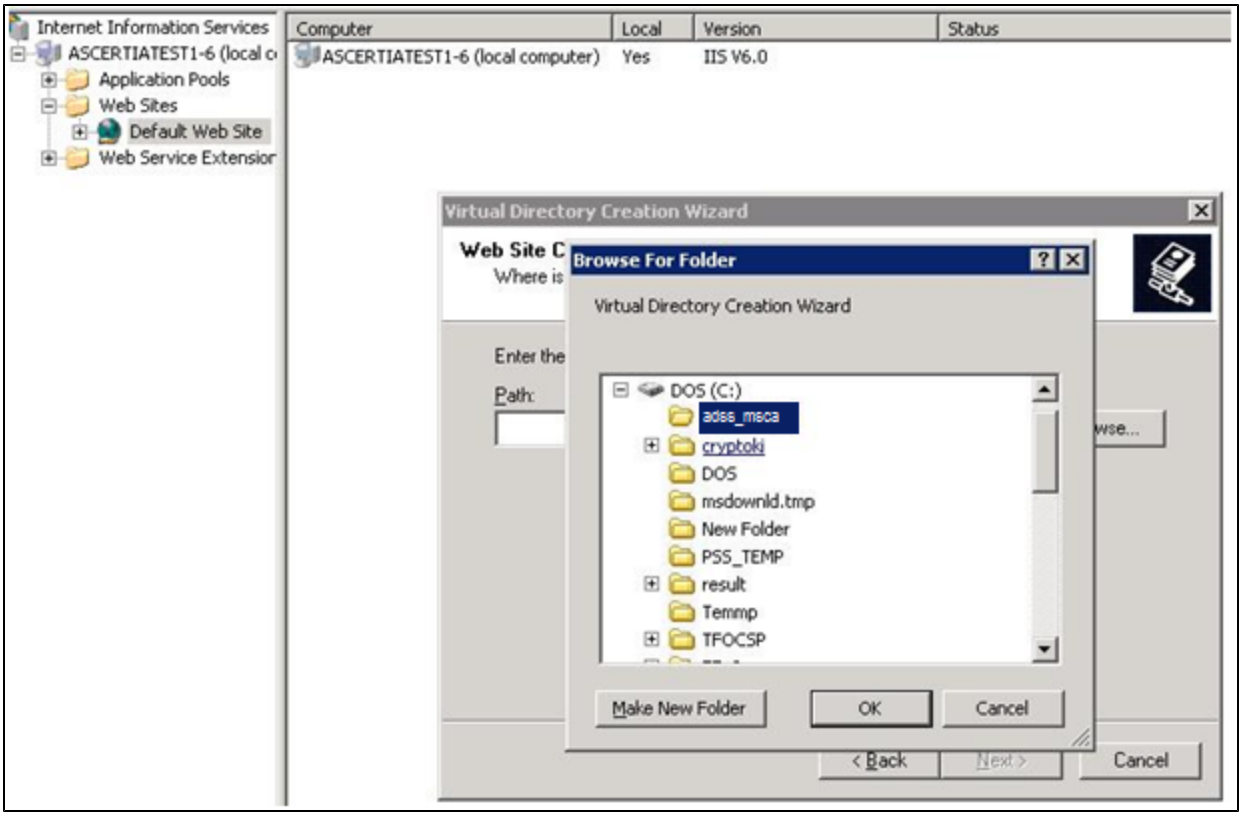


- Right click the Default web Site > click New > Virtual directory. The Directory Creation wizard will pop-up, click the "Next" button below to start the process:

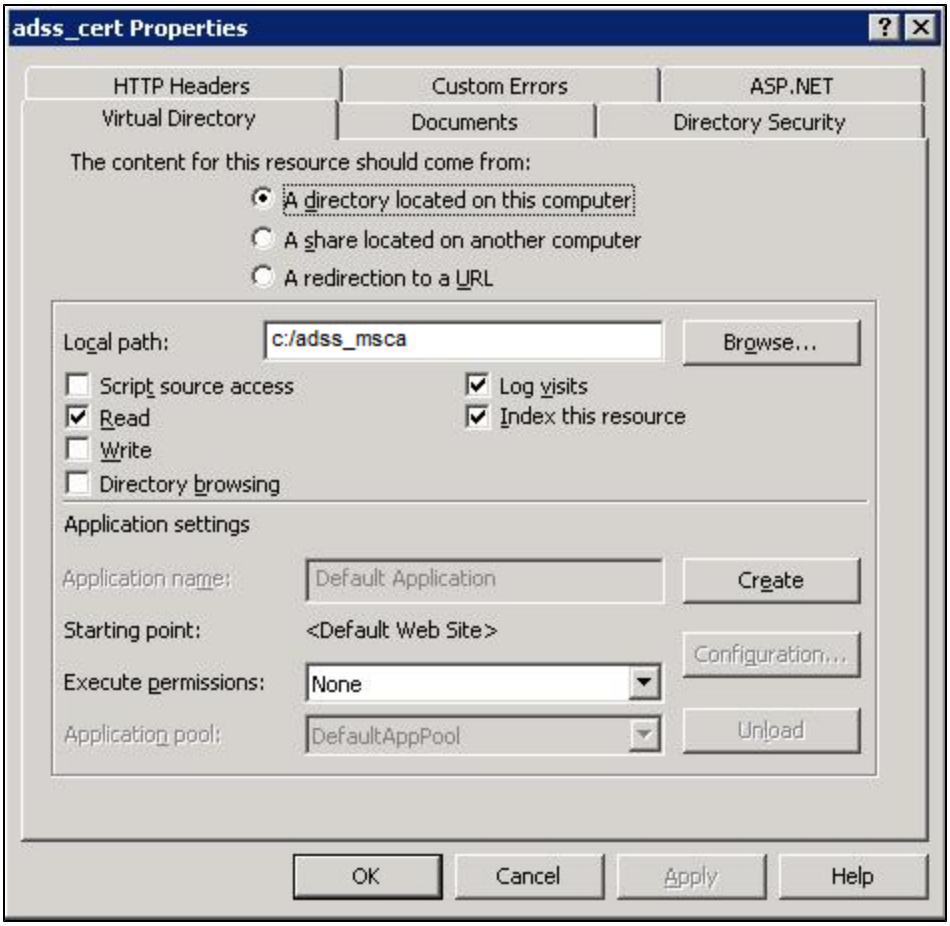
- On the next screen, type alias "ADSS_msca" and click the "Next" button:



- Browse "C:\ADSS_msca" for the contents to publish for this virtual directory and click OK to select the path. Click Next to complete the procedure, when done click Finish in next window to complete virtual directory creation wizard.



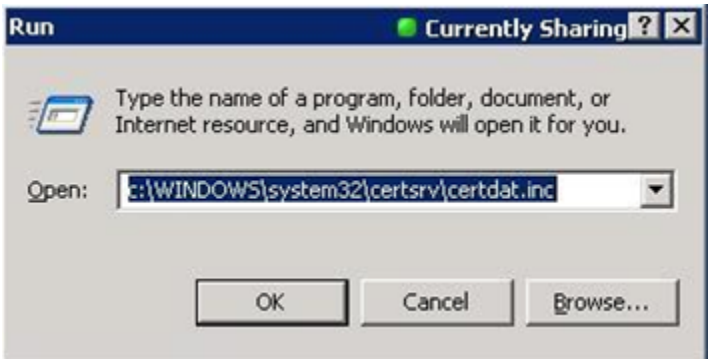
- Right click the "adss_msca" virtual directory in IIS and click on properties and change the executable permissions to Scripts only then click OK:



- You will now need to restart Microsoft Internet Information Service.

Configuring ADSS_msca module to work with Windows 2003 CA Server:
The following steps are needed to use Windows 2003 CA server with ADSS Server and they are performed where the CA is installed:

- Make sure Microsoft Windows .NET framework runtime v1 or greater is installed on the machine where Windows 2003 CA server is deployed.
- Click the "Start" button in task bar and then click "Run" and type "C:\windows\system32\certsrv\certdat.inc" and copy the value of "ServerConfig" global state.



- Edit c:\ADSS\adss_msca\Web.config extracted in step 1 (in Section A.1) and paste the above value to the add tag as value of the key "CertificateServer". e.g. if the value of "CertificateServer" is "W2K-BSPSIGN.AD.UK\Test CA" then the add tag in Web.config. It will look like this:

```
<appSettings>
<add key="CertificateServer" value="W2K-BSPSIGN.AD.Test.UK\Test CA"> </add>
</appSettings>
```

- Save and close this file.
- Restart the IIS service

- The Windows 2003 CA server can be installed on the same machine where ADSS Server is running.
- Make sure to change the policy module inside the Windows 2003 CA server to issue certificates automatically before any requests are sent by the ADSS Server. Restart the CA service if this setting is updated.
- You will need to configure the ADSS certification policy to point to this web application running on IIS for the ADSS Server to connect to the Windows 2003 CA server. This is described in the ADSS Admin Manual.