ADSS Certification Service

Table of Contents

How one can put custom defined RDNs in the certificates?

Custom RDNs are not supported by the Certification service. However it is still possible to use the RDNs from within the PKCS#10 request by configuring the certification profile as explained below:

1. Go to Certification Service
2. Add/Edit the Certification Profile
3. In the " Distinguish Name Attributes" field, set the attribute "$PKCS10"
4. Save/ Update the profile
5. Restart the Certification Service
6. Send the certification request (PKCS#10) including the custom defined RDNs.

What is an External CA?

The term “External CA” refers to any CA whose private key does not reside on the ADSS Server. A service URL is registered within ADSS Server so that certification requests can be sent to this CA. Any supported CA can be used and these can be operated internally. It can be a CA run by a managed certificate service provider, see **Manage CAs > Configure External CA** for more details.

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.

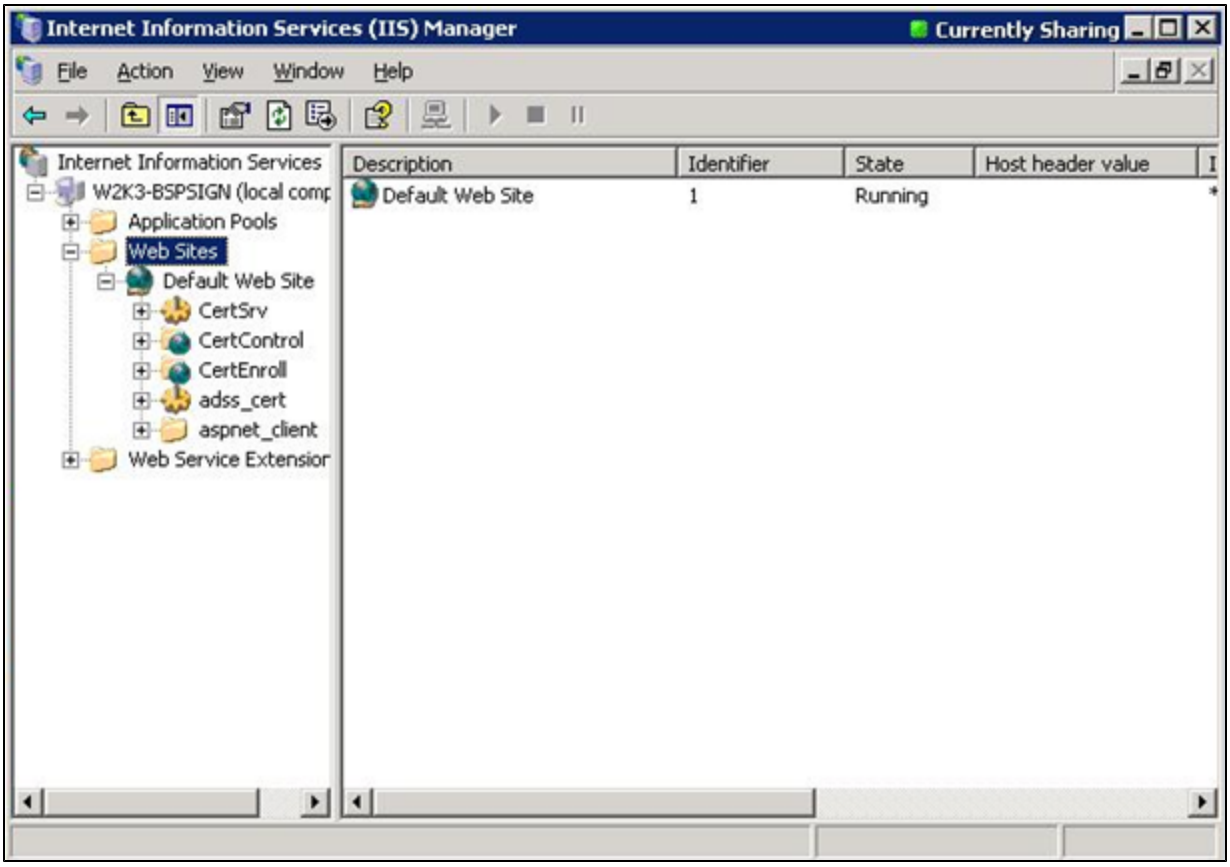
For installation and configuration of Windows 2003 Certification Authority (CA) itself, consult the separate ADSS – Microsoft CA 2003 Installation & Configuration Manual.

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:

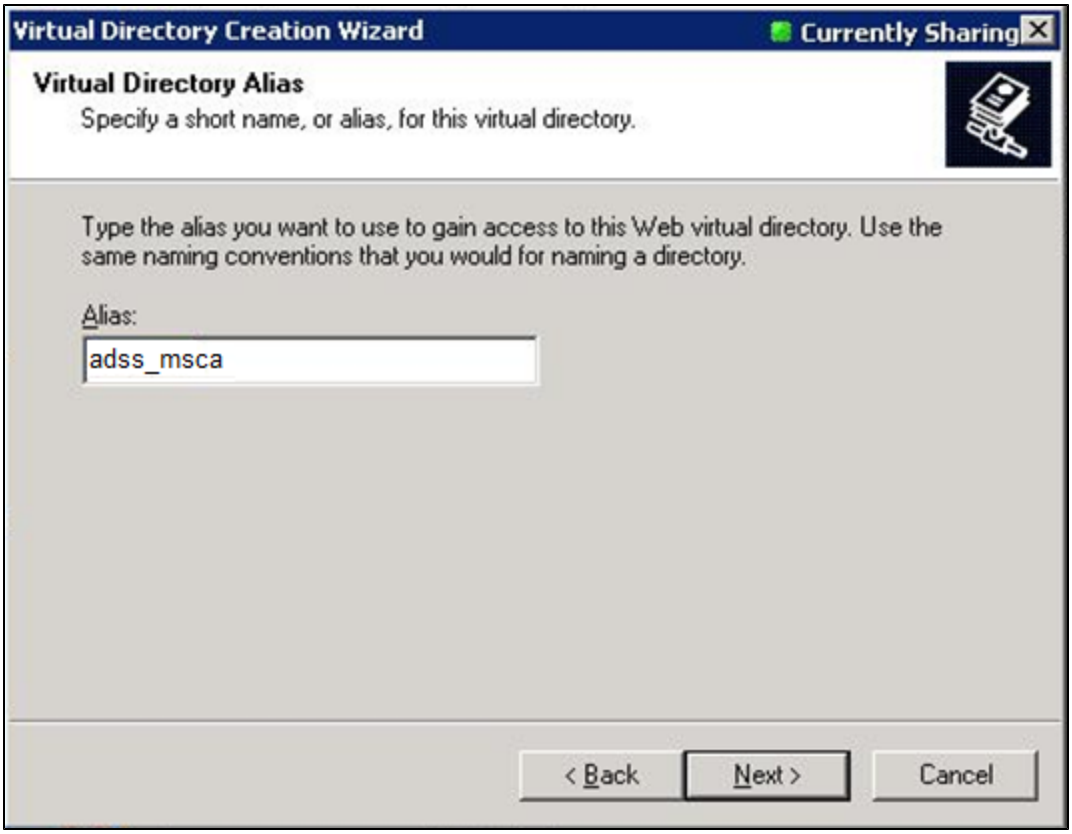
The following steps are required to configure the ADSS_MSCA module with IIS:

- 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 middleware between the ADSS Server which requests certificates and the Windows 2003 CA which accepts these certificate requests and generates corresponding certificates
- Click on **Start** button >> **Control Panel** >> **Administrative Tools** >> **Internet information Services Manager (IIS).** The Internet Information Services window opens.
- Expand Web Sites (as shown below):

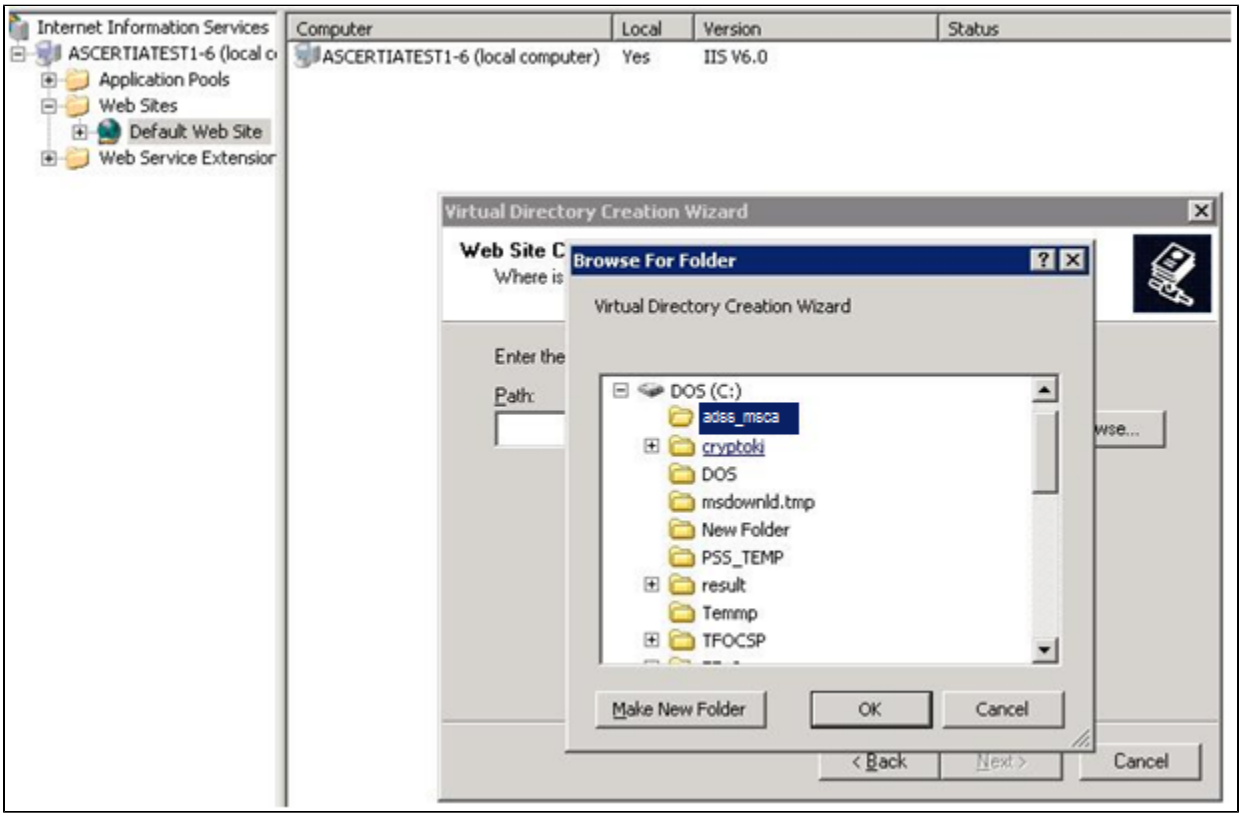


- Right click on Default web Site >> click on **New** >> **virtual directory**. The Directory Creation wizard will start, click on the **Next** button below to start the process:

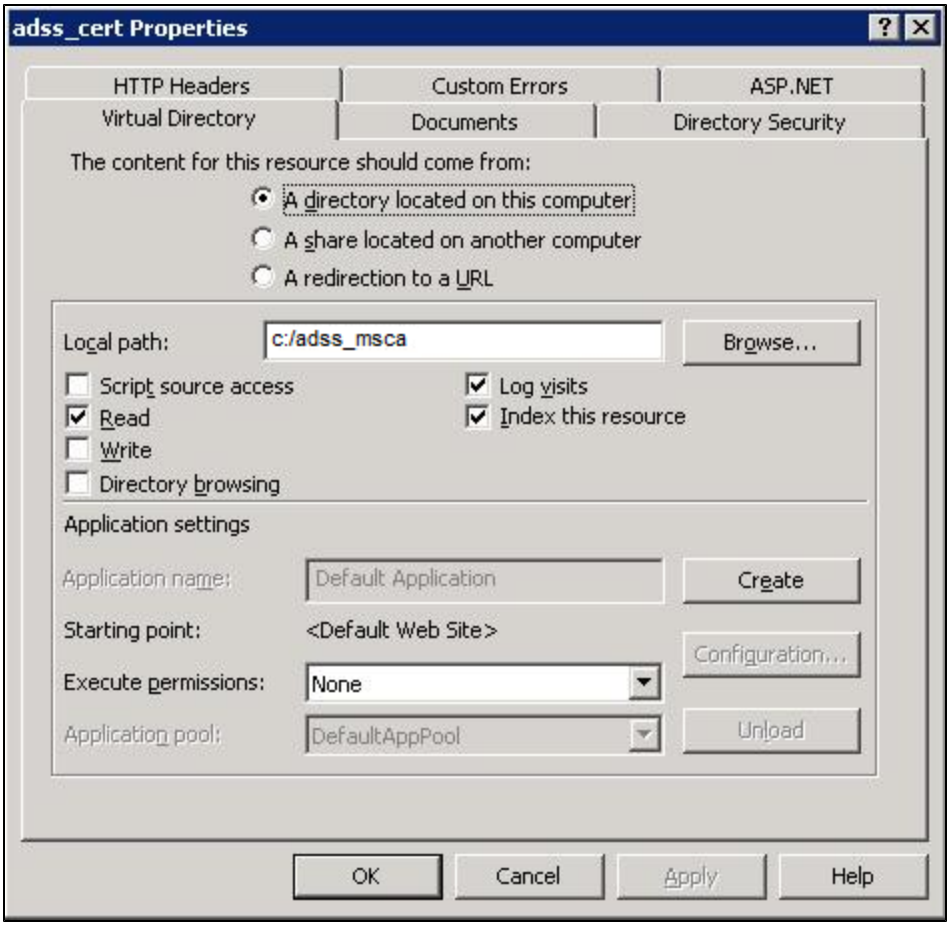
- In the next screen type alias **ADSS_msca** and click on the **Next** button:



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



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

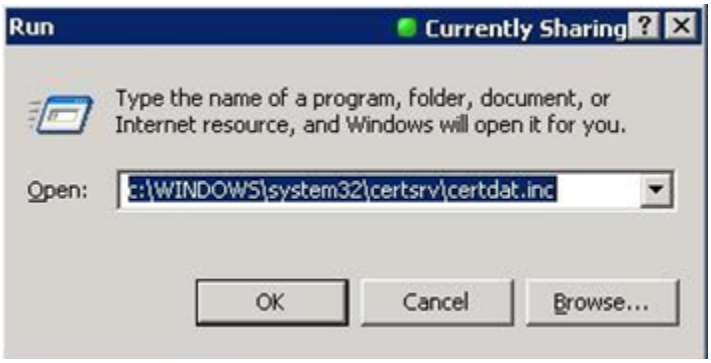


- You will now need to restart Microsoft Internet Information Service.

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 on **Start** button in task bar and then click on Run and type **C:\windows\system32\certsrv\certdat.inc** and copy the value of**Server Config** 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.configwill 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 in order to ADSS Server to connect to the Windows 2003 CA server. This is described in the ADSS Admin Manual.

How to use delta CRLs published by the Microsoft CA within ADSS Server?

With the default Microsoft CA configurations ADSS Server fails to download the delta CRLs as the delta CRL file name contains a + sign. You can tune the Microsoft CA configurations so that it does not include the + sign in the delta CRL file names. Follow these instructions to make required configurations in the MS CA:

- Go to the Start Menu > Control Panel > Administrative Tools and launch the Certification Authority
- Right click on the CA certificate node and click on Properties
- In the Properties dialog, go to the Extensions tab
- For the CRL Distribution Point (CDP) extension, by default a CRL file publishing address is configured like this:
    - C:\WINDOWS\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
- By default the options to publish both the CRL and the delta CRL to this location are selected. Note the variable <DeltaCRLAllowed> is the reason why MS CA adds a + sign in the delta CRL file name while it doesn't add any such character in the full CRL file name.
- Remove this default address and add two separate addresses out of which one is for publishing the full CRL where the option to publish CRL to this location is selected. The other address is specifically for delta CRLs for which only the option to publish delta CRL to this location is selected. The example addresses are listed below:
    - C:\WINDOWS\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix>.crl
    - C:\WINDOWS\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix>_DELTA.crl

As in the second address listed above, the fixed string "_DELTA" is used instead of the variable "<DeltaCRLAllowed>" to avoid inclusion of + sign in the CRL file name.

- Apart from the CRL publishing path currently there is a default CRL Distribution Point configured for both the full and delta CRLs like this:
    - http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
- This should also be removed and two new CRL addresses should be added likewise:
    - http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix>.crl (used as the CDP Extension within issued certificates)
      http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix>_DELTA.crl (used as Freshest CRL Extension within the issued CRLs)

How to configure a certification profile to override subject Distinguished name in the issued certificates?

ADSS Certification Service provides a flexible format for specifying the subject DName. It can be configured to use either a hard-coded subject DName for all user certificates or use the DName information requested by the client application in the certificate request message. Here are the examples on how to configure the subject DName value:

- If the DName value is configured as “CN=$CN, OU=$OU, O=$O, C=$C” this means that the values for

CN, OU, O and C attributes will be taken from the ones provided in the request message sent by the client application. Suppose if there will be multiple OUs or other attributes in the request then all RDNs will be put in the certificate.

- If the subject DName is configured as “CN=$CN, OU=$OU, O=Ascertia, C=GB, C=US” it means that values for the CN and OU attributes will be taken from the request message sent by the client application and values for O is fixed as "Ascertia"and C attribute is fixed as “GB” and "US". Other supported elements are Locality (L), State (S), Serial Number (Sr) and E-mail address (E).

In a specific scenario if this is required to use the full subject distinguished name as it is provided in the certificate request (PKCS#10) then only provide the text "$pkcs10" in the "Distinguished Name Attributes" field. This way even if some of the attributes coming in the PKCS#10 are not supported, these will be used as they are provided in the request.