UniversalPlantViewer web server setup

ENGINEERED EFFICIENCY

Contact & information:

CAXperts GmbH
Carl-Zeiss-Ring 4
85737 Ismaning – Germany
P.: +49 89 96 97 72 0
F.: +49 89 96 97 72 11
E.: info@caxperts.com

Copyright

Copyright © 2002 CAXperts GmbH. All Rights Reserved.

Including software, file formats, and audiovisual displays; may be used pursuant to applicable software licence agreement; contains confidential and proprietary information of CAXperts and/or third parties which is protected by copyright law, trade secret law, and international treaty, and may not be provided or otherwise made available without proper authorization.

Restricted Rights Legend

Rights reserved under the copyright laws of the Federal Republic of Germany.

Warranties and Liabilities

All warranties given by CAXperts about equipment or software are set forth in your purchase contract, and nothing stated in, or implied by, this document or its contents shall be considered or deemed a modification or amendment of such warranties. CAXperts believes the information in this publication is accurate as of its publication date.

The information and the software discussed in this document are subject to change without notice and are subject to applicable technical product descriptions. CAXperts is not responsible for any error that may appear in this document.

The software discussed in this document is furnished under a licence and may be used or copied only in accordance with the terms of this licence. THE USER OF THE SOFTWARE IS EXPECTED TO MAKE THE FINAL EVALUATION AS TO THE USEFULNESS OF THE SOFTWARE IN HIS OWN ENVIRONMENT.

Trademarks

CAXperts is a registered trademark of CAXperts GmbH. Intergraph, the Intergraph logo, SmartSketch, FrameWorks, SmartPlant, INtools, MARIAN, PDS, IGDS, RIS and IntelliShip are registered trademarks of Intergraph Corporation. IGDS file formats ©1987-1994 Intergraph Corporation. Microsoft and Windows are registered trademarks of Microsoft Corporation. Bentley, the Bentley logo "B," and MicroStation are registered trademarks of Bentley Systems, Inc. ISOGEN is a registered trademark of Alias Limited. Other brands and product names are trademarks of their respective owners.

Contents

1 How to host UniversalPlantViewer projects

1.1 Prerequisites

Prerequisites: a web server (e.g. IIS, Apache)

IIS is recommended as it is needed for user authentication: only "Basic Authentication" is supported (i.e. Form or Windows integrated authentication are **not** supported; set user and group rights on the local Windows machine as usual)

1.2 How to install IIS 7.5

IIS is one of the Windows Server® server roles. IIS can be installed through the graphical user interface (GUI) by using the new Server Manager interface after the Windows Server operating system is installed.

Server Manager provides a single dashboard to install or uninstall server roles and features. Server Manager also gives an overview of all currently installed roles and features. When IIS is chosen from the Server Manager, the basic components and services needed for IIS are automatically selected.

1. Click **Start** -> **All Programs** -> **Administrative Tools** -> **Server Manager**.
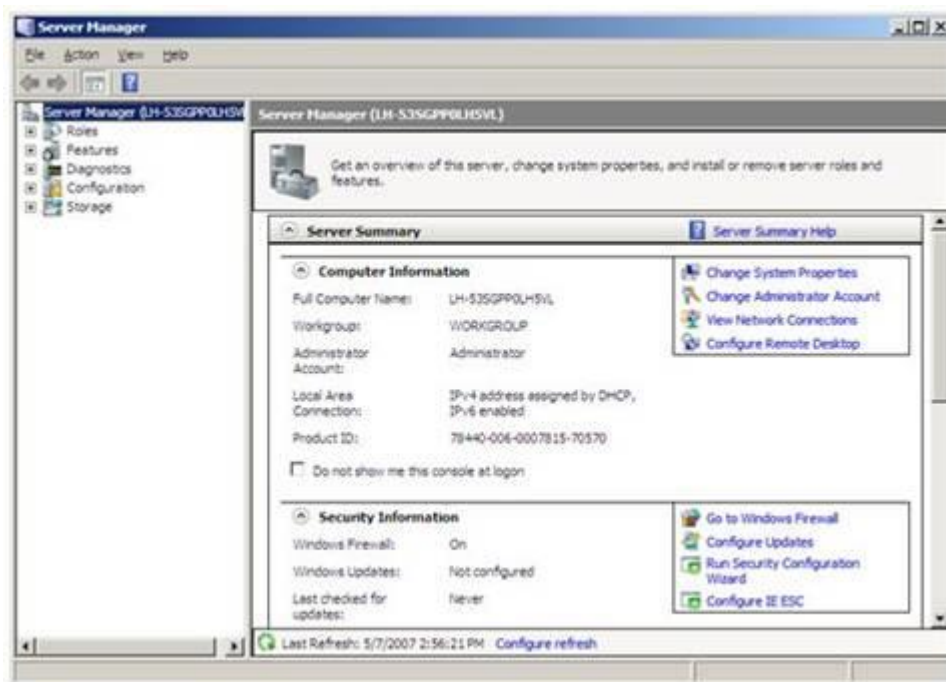

Figure 1: Server Manager

2. In the **Server Manager** window, scroll down to **Roles Summary**, and then click **Add Roles**. The **Add Roles Wizard** will start with a **Before You Begin** page. The wizard asks for verification of the following:

a. The administrator account has a strong password.

b. The network settings, such as IP addresses, are configured.

3. Select **Web Server (IIS)** on the **Select Server Roles** page. An introductory page will open with links for further information.

Note: When you use the **Add Roles Wizard to install** IIS, you get the default installation, which has a minimum set of role services. If you need additional IIS role services, such as **Application Development** or **Health and Diagnostics**, make sure to select the check boxes associated with those features in the **Select Role Services** page of the wizard.
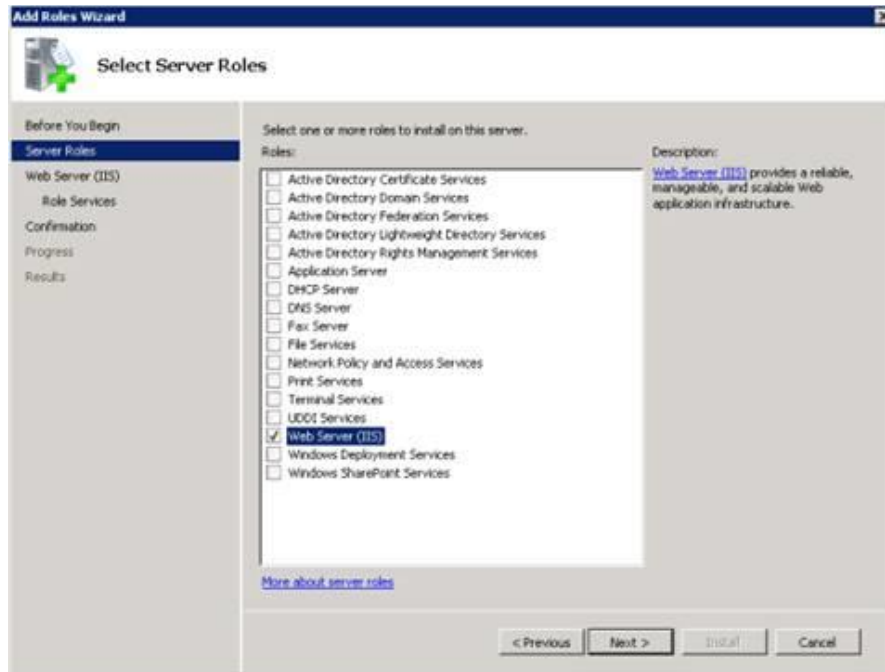

Figure 2: Select Server Roles

4. Select the IIS services to be installed on the **Select Role Services** page. Add only the modules necessary. In this case, Basic Authentication. Once desired modules are added, click **Next**.
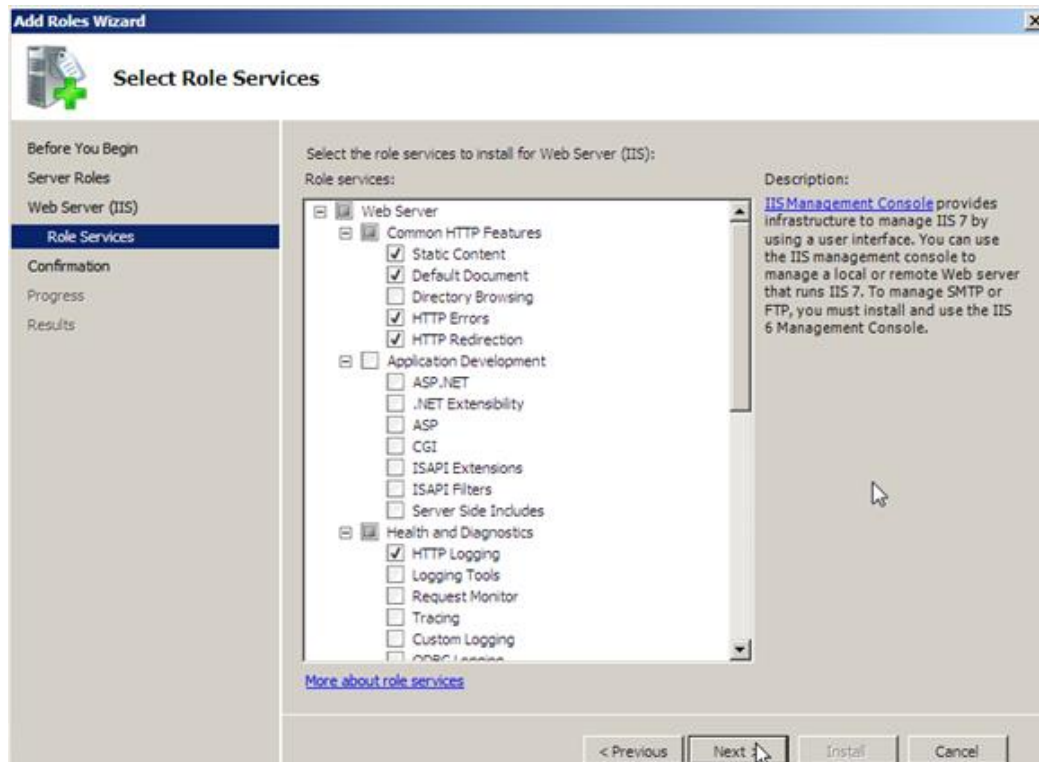
Figure 3: Select Role Services
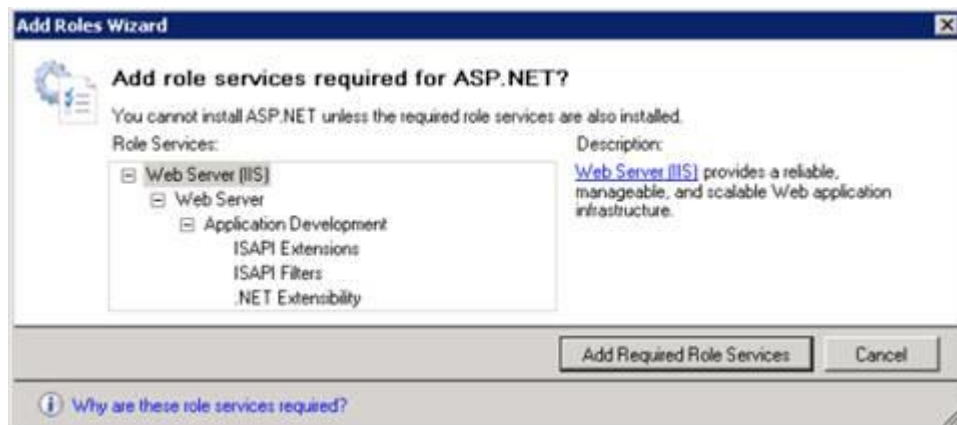
5. Add any required role services.

Figure 4: Wizard warning page

6. IIS is now installed with a default configuration for hosting ASP.NET on Windows Server. Click **Close** to complete the process.
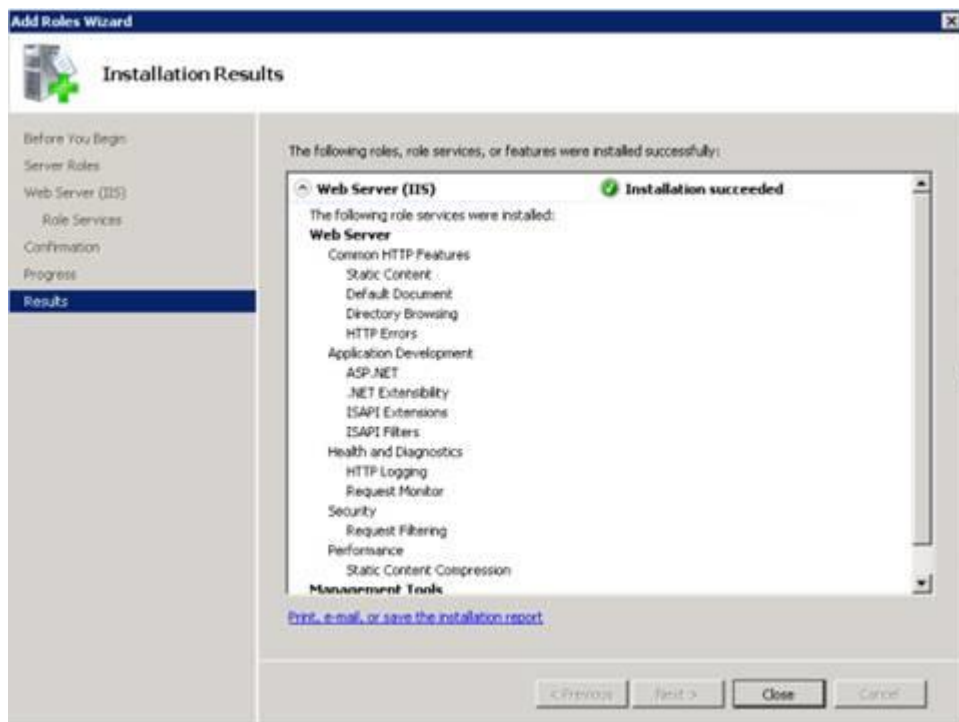
Figure 5: Installation Results page

7. Confirm that the Web server works by using http://localhost.

To open port 80 on Windows Server 2008 R2

1. From the **Start menu**, click **Control Panel**, click **System and Security**, and then click **Windows Firewall**. Control Panel is not configured for 'Category' view, you only need to select **Windows Firewall**.
2. Click **Advanced Settings**.
3. Click **Inbound Rules**.
4. Click **New Rule** in the Actions window (upper right corner).
5. Click Rule Type of **Port**.
6. Click **Next**.
7. On the Protocol and Ports page click **TCP**.
8. Select Specific Local Ports and type a value of **80**.
9. Click Next.
10. On the Action page click **Allow the connection**.
11. Click **Next**.
12. On the Profile page I am leaving **Domain** turned on and turning off private and public. You should check the appropriate options for your environment.
13. Click **Next**.
14. On the Name page enter a name of such as Allow ReportServer (TCP on port 80)
15. Click Finish.
16. You may want to repeat the steps to open port 443 if you are using https for anything.

1.3 Copying UniversalPlantViewer files to the webserver

On IIS, the UniversalPlantViewer files should be copied to c:\inetpub\www\UPV, also rename the UPV.web.html to index.html

1.4 Accessing UPV on the webserver

Navigate to http://ip-address/UPV or http://servername/upv using a browser or the UniversalPlantViewer app.

1.5 How to expose the webserver to the internet (optional)

Basic port forwarding

If the computer already has a public IP address then no port forwarding is needed.

If the computer is behind a firewall: You will need to setup port forwarding on the router. Ports to forward: 80. If you use SSL you will also need to forward Port 443. Those ports need to be forwarded to the computer which is running the IIS.

1.6 Setting up HTTPS / SSL (optional)

1. From the **Start menu**, click **Control Panel**, click **System and Security**, and then click **Windows Firewall**. Control Panel is not configured for 'Category' view, you only need to select **Windows Firewall**.
2. Click **Advanced Settings**.
3. Click **Inbound Rules**.
4. Click **New Rule** in the Actions window (upper right corner).
5. Click Rule Type of **Port**.
6. Click **Next**.

7. On the Protocol and Ports page click **TCP**.

8. Select Specific Local Ports and type a value of **443**.

9. Click Next.

10. On the Action page click **Allow the connection**.

11. Click **Next**.

12. On the Profile page I am leaving **Domain** turned on and turning off private and public. You should check the appropriate options for your environment.

13. Click **Next**.

14. On the Name page enter a name of such as Allow ReportServer (TCP on port 443)

15. Click Finish.

1.7   Enable basic authentication (optional)

- Open the MMC and select the site or directory you wish to protect
- Right click and select properties on that site / directory
- Select the directory security tab
- Click the "edit" button on authentication control
- Enable basic authentication
- Now your site is setup to support basic authentication you need to change the NTFS permissions for the directory you want to protect and add any users or groups you wish to have access

When IUSR_MACHINENAME does not have access to a directory or you disable anonymous access the basic authentication windows will popup.

Or in IIS Manager:

Choose your Site (Default Site)
>Authentication
> Disable Anonymous Authentication
> Enable Basic Authentication
>.net Authorization Rules
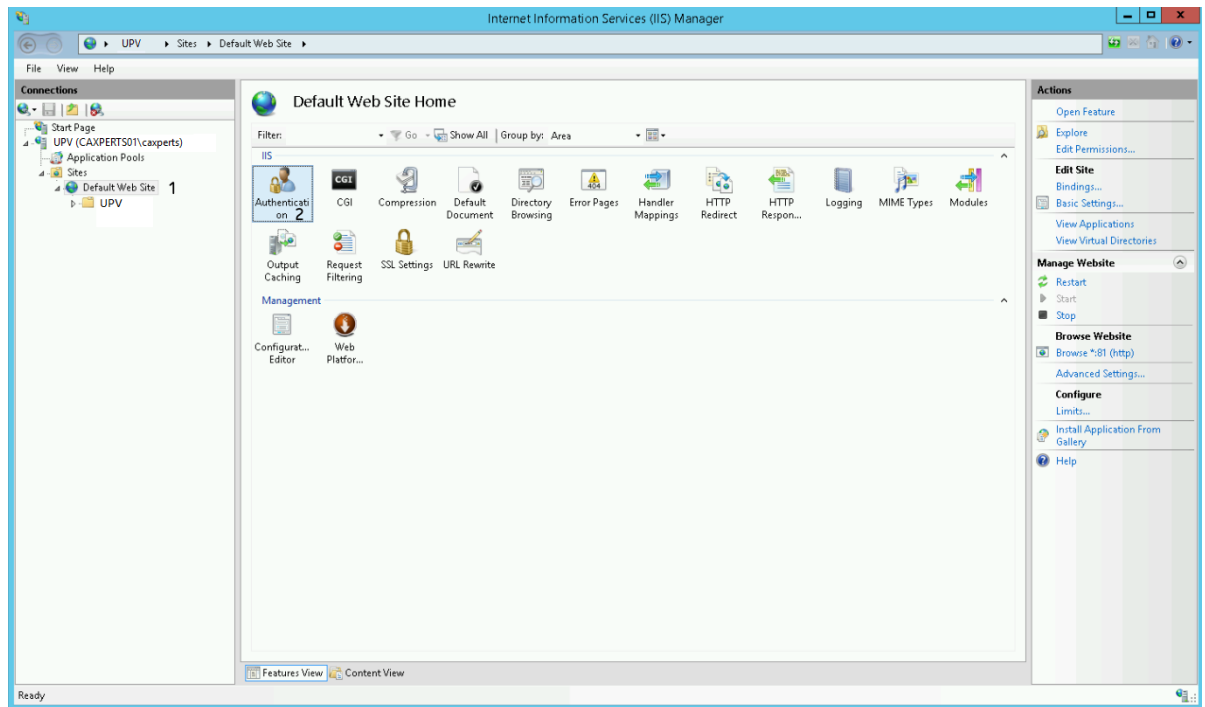>Add Deny Rules
All users
>Add Allow Rules
Your Windows Group or Windows User
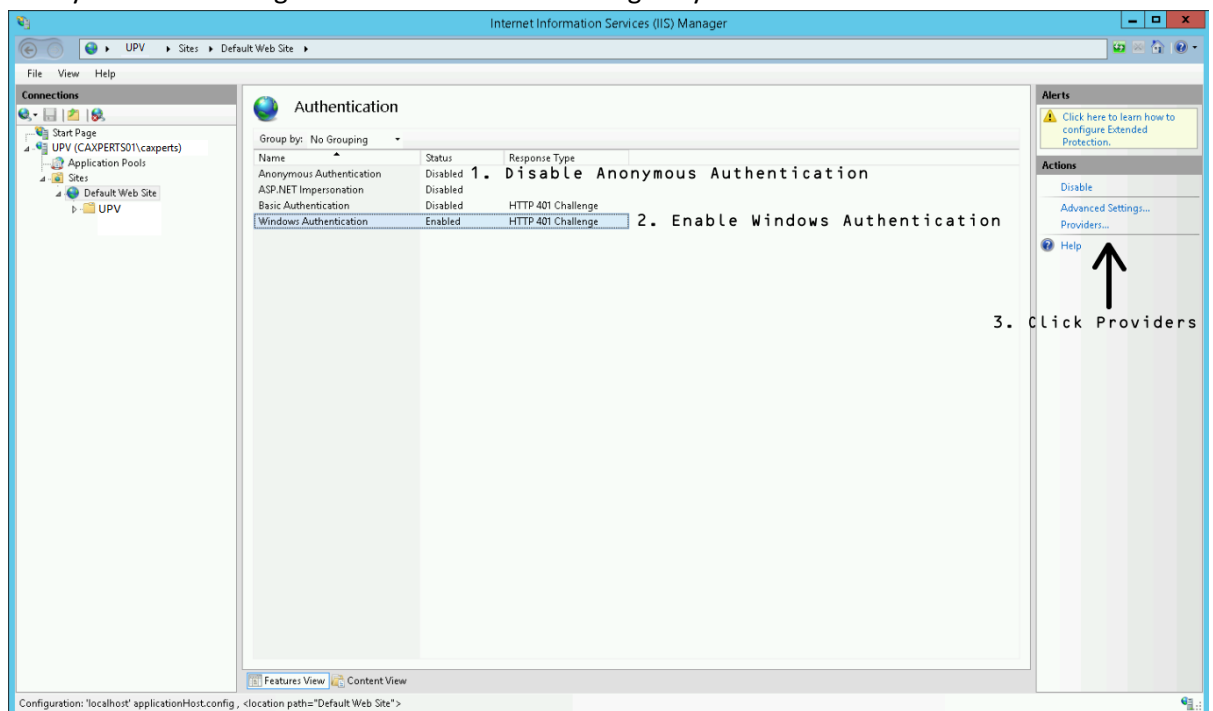
16. Click Finish.

1.8   SSO with IIS on Windows

Enable Windows Authentication

Open the IIS Manager and select the site under which your UPV environment runs. In our case we use the "Default Web Site".

After that double click "Authentication"
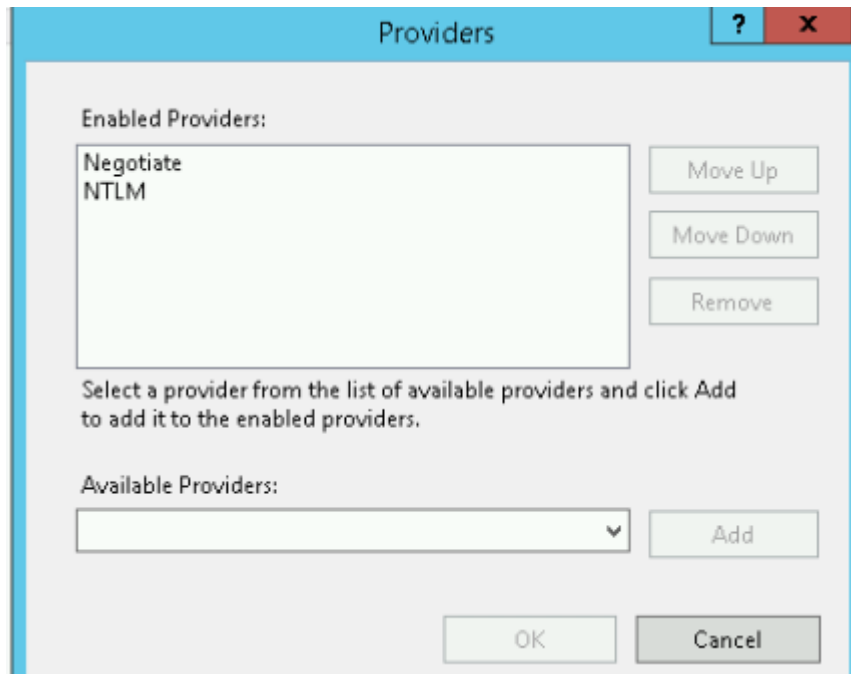Now you have to configure the authentication settings of your site.
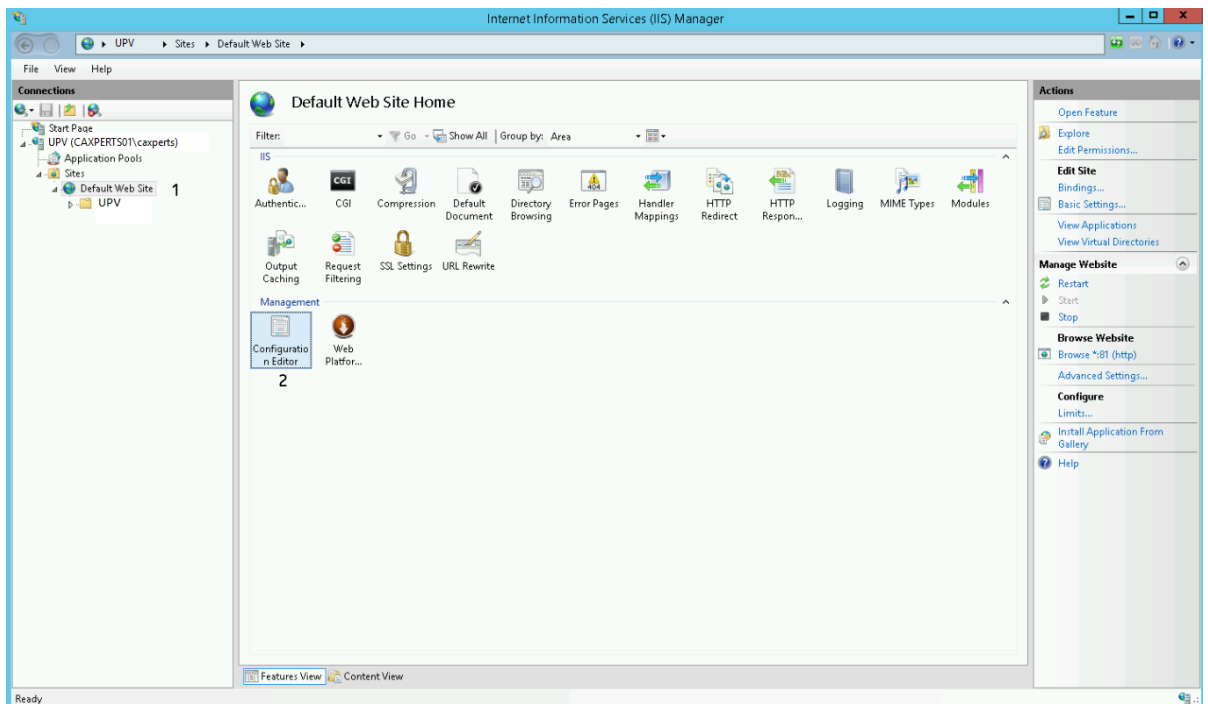
Disable *Anonymous Authentication*

Enable *Windows Authentication*

With *Windows Authentication* selected, click on the *Providers* link in the right *Action* panel

Now the following window should appear. Please add the providers as shown in the picture. The order has to be **Negotiate over NTLM**!
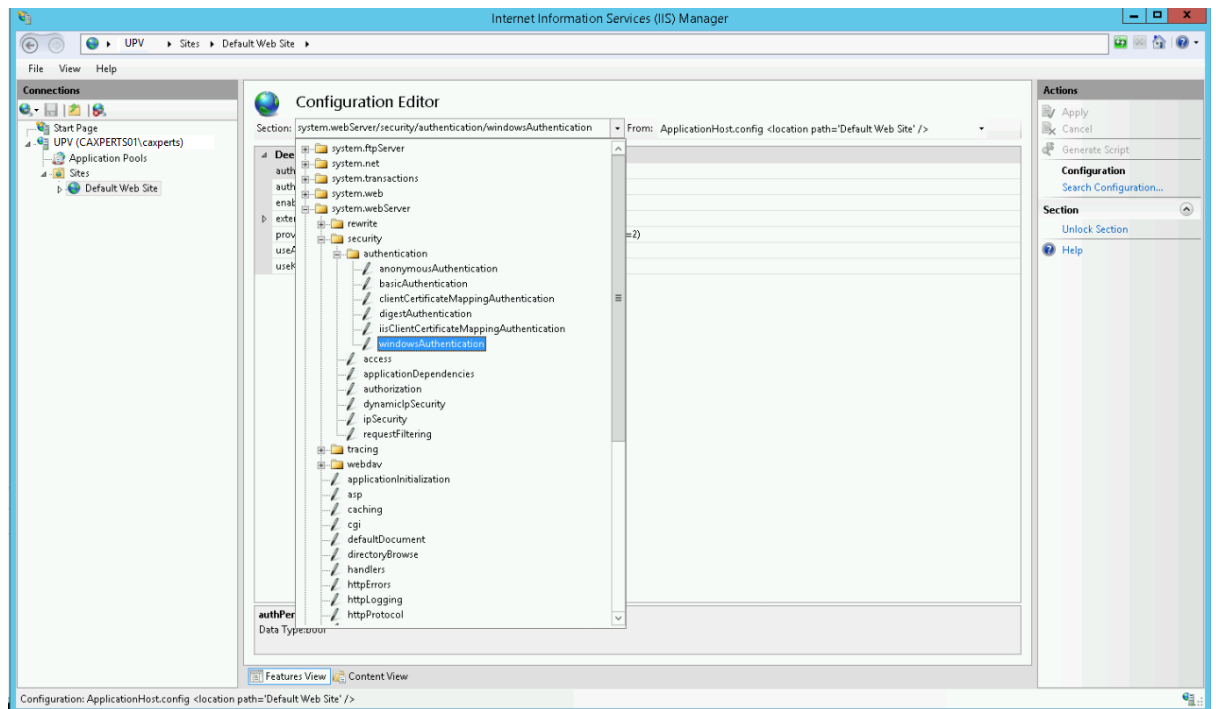

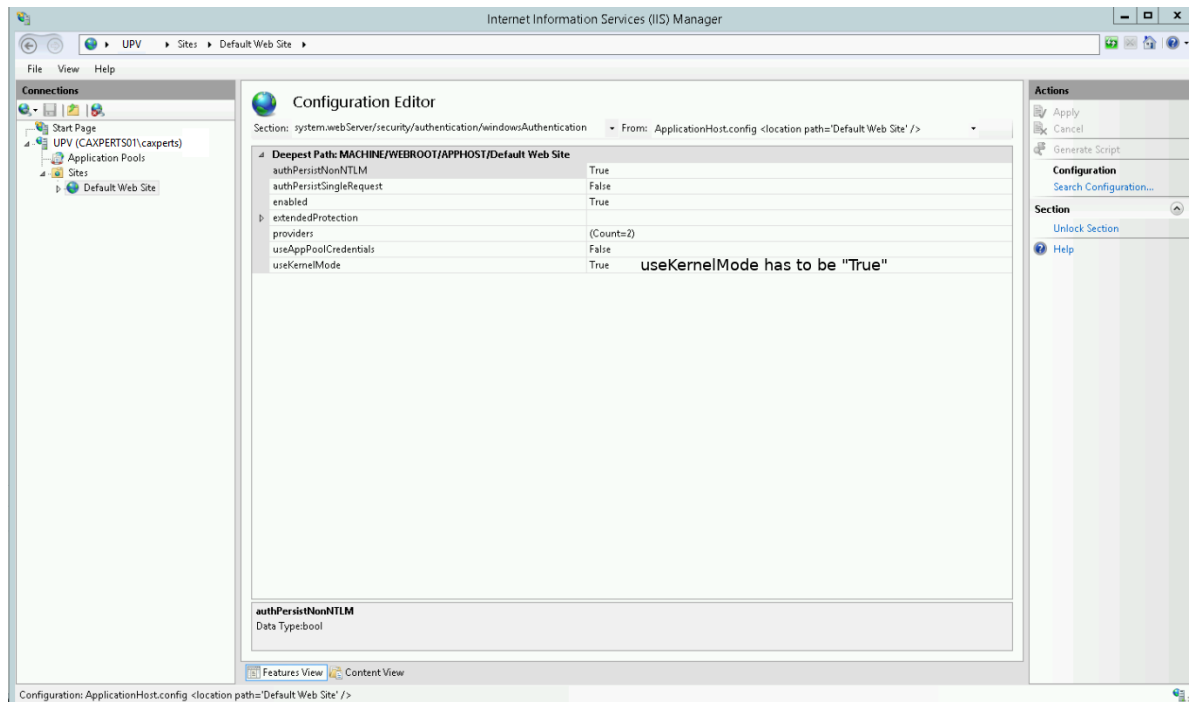After that close the window by pressing OK.

For the next step please select your site on the *left* panel

After that double click the *Configuration Editor*

Now please select *windowsAuthentication* from the dropdown menu

Please change *useKernelMode* to *True* and save the settings by pressing *Apply* button in the upper right corner.

Finally, please restart your IIS.

Configure SPNs

In our example we imagine the following scenario

Hostname	Domain	FQDN hostname
UPV	*caxperts01*	*UPV.caxperts01*

Open a console and type *hostname* in order to see the hostname of your machine.

Now type the following to receive a list of all SPNs registered for your machine

setspn -L yourMachineName

You now have to add a HOST and a http SPN for the address of your UPV environment which has to equal the hostname. To do this type the following commands:

setspn -a HOST/yourHostName yourMachineName

setspn -a http/yourHostName yourMachineName

Check if the SPNs were added successfully by typing

setspn -L yourMachineName

```
C:\Users\caxperts>setspn -L upv
Registered ServicePrincipalNames for CN=UPV,OU=VM,OU=CAXperts Computers,DC=CAXperts01:
        HTTP/dns2upv.caxperts01
        HTTP/dns2upv
        HTTP/upv.caxperts01
        Http/upv
        TERMSRV/UPV
        TERMSRV/UPV.CAXperts01
        WSMAN/UPV
        WSMAN/UPV.CAXperts01
        RestrictedKrbHost/UPV
        HOST/UPV
        RestrictedKrbHost/UPV.CAXperts01
        HOST/UPV.CAXperts01
```

If your hostname contains a port (e.g. *nadi-ts.test.ad:81/wordpress*) do __not__ add the port to the SPNs. This is only required for older environments up to Windows 7 and Windows Server 2008.

2   Technical support

Need more help? Contact CAXperts support by email, online, or phone:

mailto:support@caxperts.com

http://www.caxperts.com/contact/