MT AG

# SINGLE SIGN-ON

# FOR (APEX) APPLICATIONS

# USING KERBEROS

Author: Niels de Bruijn
Version: 9.0
Date: 31-OCT-2022

# 1 INTRODUCTION

For APEX apps, you normally use a URL like https://<hostname>/ords/f?p=xxx after which by default you have to authenticate yourself using username/password credentials. However, internal users of APEX applications already have authenticated themselves by logging on to the Windows domain, so why authenticate a second time to use the first APEX application? Wouldn't it be nice if you could point your browser to an APEX app and you are instantly authenticated? A secure method to achieve this is to use the Kerberos protocol, which is the same protocol that Windows uses for authentication. In this document we will first describe how to install and setup the Apache module mod_auth_gssapi in a Linux environment that performs the authentication against a Windows domain controller (chapter 3). For those of you who favor a Windows environment, chapter 4 describes how to setup IIS, that is used instead of Apache on Windows.

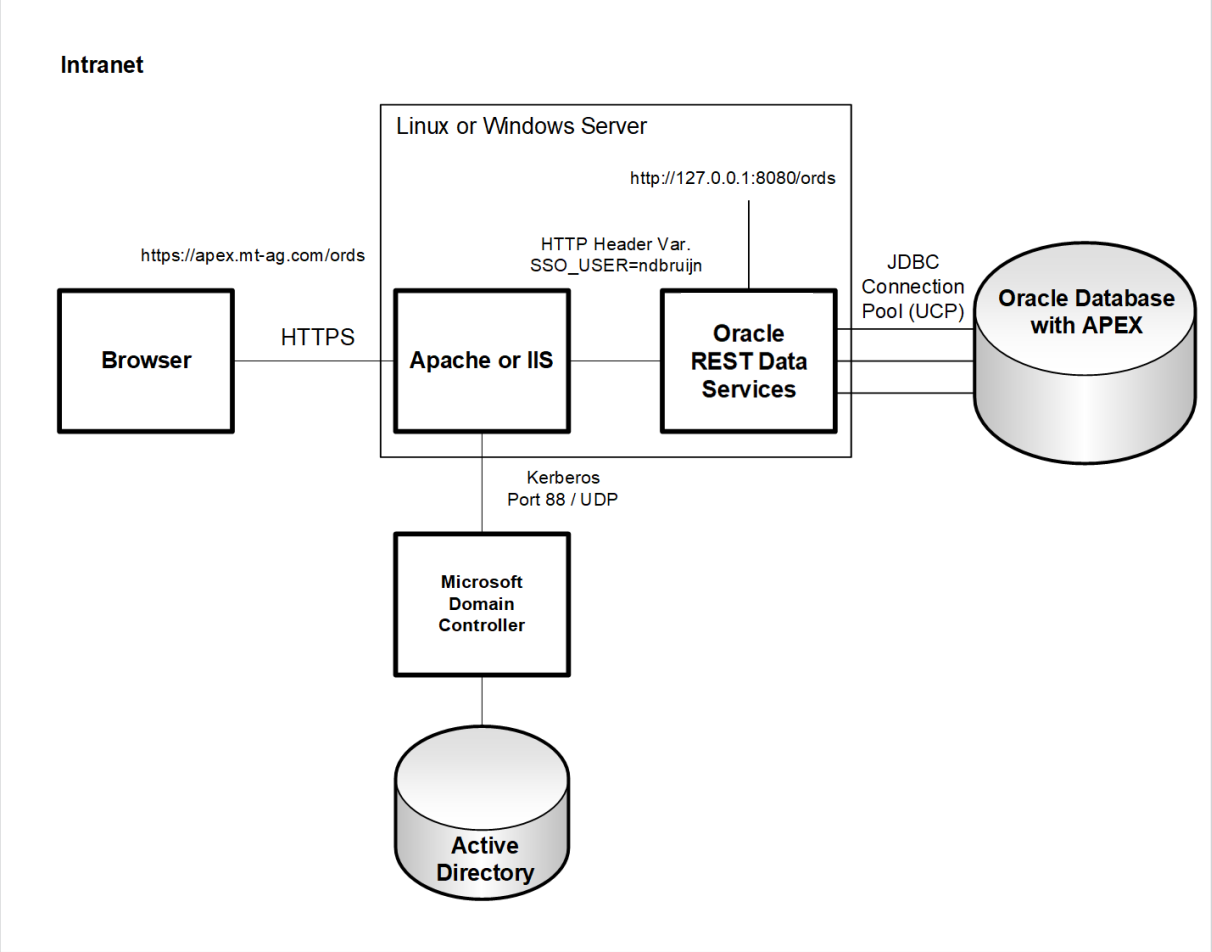



**Image 1: Recommended standard APEX architecture with Apache and ORDS.**

In this document we assume that you have setup a Windows domain controller with Active Directory (Windows Server 20xx) and you have Windows based client-PCs where you have to authenticate against the Windows domain. Also, make sure you have successfully installed and configured the Oracle Database with Oracle Application Express, Oracle REST Data Services (ORDS) and optionally Apache Tomcat.

**Caution:**
There is potentially one major drawback to this setup: if a user belongs to too many groups in Active Directory or the user has a long "history", the Kerberos ticket might become too big. I have seen this only when Apache Web Server was used and "Bad Request" was returned. The "history" may be

deleted by a Windows domain administrator, but if the problem originates in the many user groups, there is not much you can do, as Apache is already configured in a way to accept large tickets. Before running this setup in production, make sure you test with an existing user that belongs to many groups.

You can check the size of the kerberos ticket by running: `klist -v5` (Linux) or `klist tgt` (Windows).

Should you run into this issue, I suggest you implement the OAuth2 authentication method as described here: https://knowledgebase.mt-ag.com/q/apex_sso_oauth2

Remarks:

- A Linux server must not be part of the Windows domain.
- Install Apache Webserver with the mod_auth_gssapi module on a Linux server.
- For Windows environments, I recommend the usage of IIS with the tool ISAPI Rewrite instead of Apache Webserver (see chapter 4).
- Use a firewall to restrict the communication with the server through port 443 (HTTPS). For Linux/Unix environments, you can use Samba 4 as Domain Controller.
- Single Sign-On using Kerberos is one of the most secure authentication methods available. It has the major advantage that the password is not transmitted to the server.
- Although not recommended and not part of the scope of this document: if you are not willing to install Apache, you can also setup Tomcat to get Kerberos authentication in place.
- The described scenario for Single Sign-On in this document works for Desktop-PCs and Laptops having Windows installed. If you are using a smartphone or tablet, you will need to enter your Windows account in a prompted dialog, before you can access the APEX application. If you need a logon screen instead of a prompted dialog, you will need a Single Sign-On Server like Oracle Access Manager or implement something for this on Apache level.
- Please be aware that this document is not about hardening your environment. For instance, you might not need all Apache modules that are installed by default.
- In this case, the APEX URL (/ords) will be protected, but you can protect any other web application with this approach that lies behind the web server.
- It is possible to setup Tomcat to do Kerberos authentication without using a web proxy server in front of it, but this is not part of this document. For maximum flexibility reasons, I prefer using a proxy server in front of ORDS.
- For those of you that would like to use NGINX+ (the paid support version of NGINX) instead of Apache Web Server, there is a Kerberos module available that can be installed directly from the repository, but we didn't test this out yet.

- **Starting with ORDS 22.x, we recommend you to run ORDS in stand-alone using the built-in Jetty web server instead of Apache Tomcat. I would then let communication between the web proxy and ORDS take place using HTTP(S), not AJP as suggested by Eclipse: https://wiki.eclipse.org/Jetty/Howto/Configure_AJP13**

MT AG

# 2 SETUP INDEPENDANT OF OPERATING SYSTEM

## 2.1 CONFIGURATION OF TOMCAT

For those of you that would like to see ORDS running on Tomcat instead of standalone (standalone is recommend with ORDS 22.x or higher), configure it by adding the following attributes in the file `server.xml`:

```
<Server port="8005" shutdown="SHUTDOWN" address="127.0.0.1">
…
<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000"
redirectPort="8443" maxHeaderCount="-1" address="127.0.0.1"
maxHttpHeaderSize="65536" maxPostSize="5242880" URIEncoding="UTF-8"
proxyName="apex.mt-ag.com" proxyPort="8080" />
…
<Connector port="8009" protocol="AJP/1.3" URIEncoding="UTF-8"
packetSize="65536" redirectPort="8443" address="127.0.0.1"
proxyName="apex.mt-ag.com" proxyPort="443" acceptorThreadCount="2"
acceptCount="10" maxConnections="200" maxThreads="200"
minSpareThreads="10" connectionTimeout="30000" maxPostSize="5242880"
disableUploadTimeout="false" connectionUploadTimeout="300000"
secretRequired="false" />
```

Some comments on the attributes:

- `acceptorThreadCount` - The number of threads to be used to accept connections. Increase this value on a multi CPU Core machine.
- `acceptCount` - The maximum queue length for incoming connection requests when all possible request processing threads are in use. Any requests received when the queue is full will be refused. Set to 10 to protect server from getting overloaded.
- `maxConnections` - The maximum number of connections that the server will accept at any given time. When this number has been reached, the server will accept, but not process, one further connection. Connections are passed on to available threads to perform the actual work.
- `maxThreads` - The maximum number of request processing threads to be created by a connector, which therefore determines the maximum number of simultaneous requests that can be handled.
- `maxPostSize` - The maximum size in bytes of the POST which will be handled by the container FORM URL parameter parsing. The limit can be disabled by setting this attribute to a value less than zero. If not specified, this attribute is set to 2097152 (2 megabytes).
- `minSpareThreads` - The minimum number of threads always kept running waiting for new requests.
- `connectionTimeout` - The number of milliseconds a connector will wait, after accepting a connection, for the request URI line to be presented.
- `disableUploadTimeout` - Set to false and use the value in `connectionUploadTimeout` as the upload timeout.
- `connectionUploadTimeout` - Specifies the timeout, in milliseconds, to use while a data upload is in progress. This only takes effect if `disableUploadTimeout` is set to false.
- `secretRequired` – Set this to false, otherwise you will experience errors in Tomcat 9 (as it is set by default to true in that version).

## 2.2 CONFIGURATION OF ORACLE REST DATA SERVICES

By default, the settings for the connection pool used by ORDS are set too small. You need to change these in the file `defaults.xml`:

```
…
<entry key="jdbc.InitialLimit">10</entry>
…
<entry key="jdbc.MaxLimit">40</entry>
…
<entry key="jdbc.MinLimit">10</entry>
…
<entry key="jdbc.MaxConnectionReuseCount">50000</entry>
…
```

Remarks:
- Which initial size you choose for these parameters, depends on your specific use case and might differ.
- Be aware that what you specify in *defaults.xml* applies to all connection pools.
- With ORDS 22.x installed in the CDB, there is only one connection pool created (db user: ords_public_user) that is used as proxy for other db users like apex_listener, apex_rest_public_user and apex_public_user.

## 2.3 CONFIGURATION OF APEX

### 2.3.1 SESSION TIMEOUT

The session timeout is delegated to kerberos, so we have to disable the session timeouts for the APEX session cookie by setting it to 0. You can find this setting in the “security settings” section after logging on in the INTERNAL workspace but be aware that this setting can be overridden on workspace and application level.

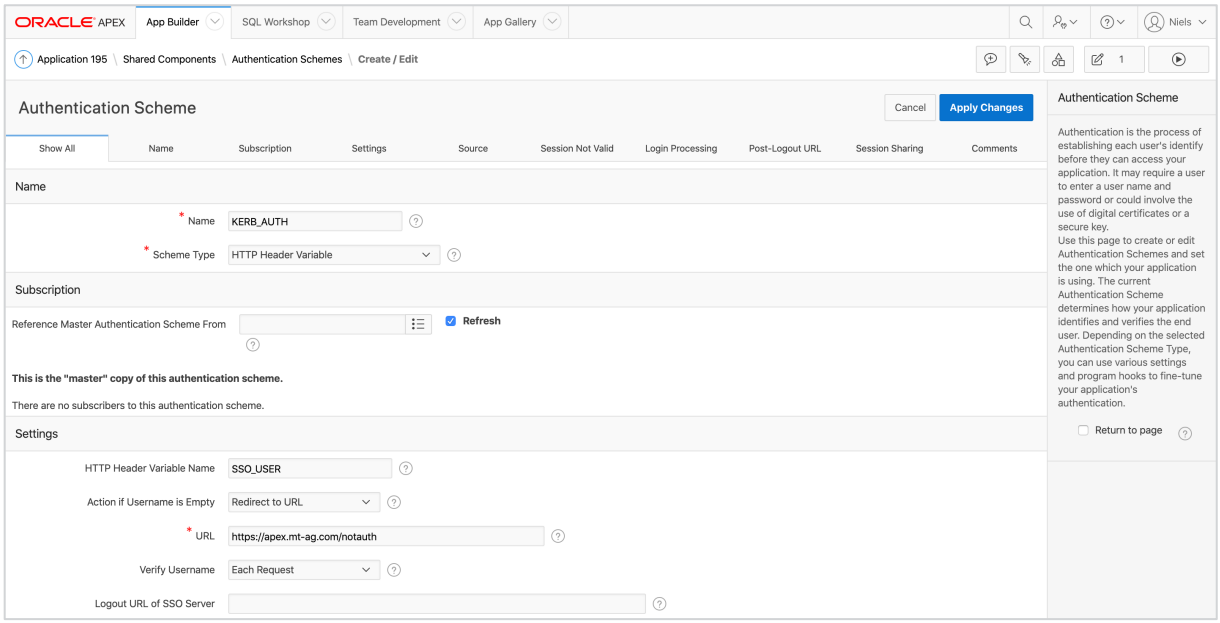
There is also the attribute “Maximum Session Idle Time in Seconds”. By setting this to 0, you get the maximum session idle time, which is 12 hours. Even if you specify a value in seconds that exceeds 12 hours, APEX still enforces 12 hours, because it needs to clean up the sessions table once in a while.

You can verify this by executing the following query in SQL Workshop:

```
select   to_char(session_idle_timeout_on, 'DD.MM.RRRR HH24:MI:SS') session_idle_timeout_on
,        session_max_idle_sec
from     apex_workspace_sessions
order by session_idle_timeout_on desc
```

### 2.3.2 AUTHENTICATION SCHEME

For each APEX application (including APEX itself), configure a authentication scheme that reads out the HTTP header variable „SSO_USER“.

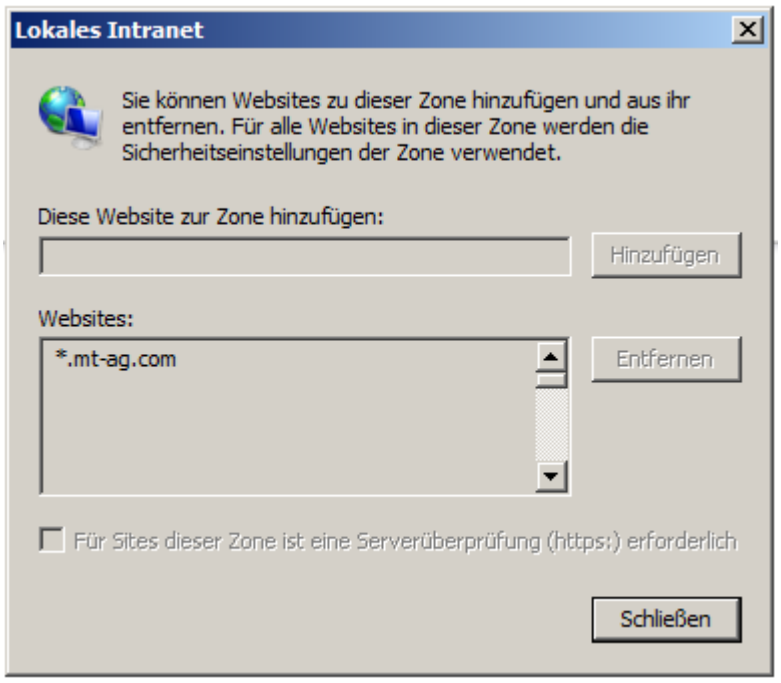



Wenn SSO_USER is empty, the user will be redirected to a static HTML page (index.html) hosted by Apache informing the user not being logged on to the Windows domain.

Note: if you would like to see all HTTP header variables in APEX, just create a region of type “PL/SQL dynamic content” and enter the PL/SQL code: `owa_util.print_cgi_env;`.

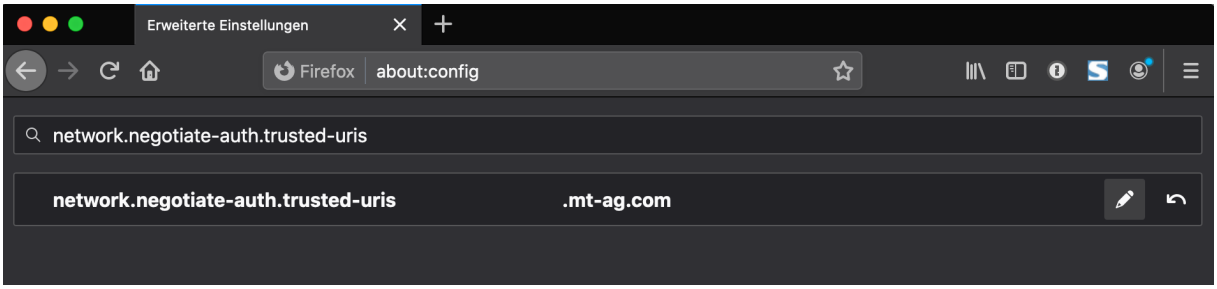
## 2.4 CONFIGURATION OF A WINDOWS CLIENT PC

The web address of Apache should be listed in the intranet zone in Internet Explorer, otherwise you will be prompted to enter your Windows credentials if you try to access your APEX application:



Remark: first go to the server address using a Windows client with IE and then check if the “Local Intranet” zone is highlighted within Internet Options.

When you are using Firefox, go to the URL `about:config` and set the attribute `network.negotiate-auth.trusted-uris` to `.mt-ag.com`.




When you are using Google Chrome on Windows, make sure that the domain is registered in the Windows Registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome
AuthSchemes = "negotiate,basic"
AuthNegotiateDelegateWhitelist = *.mt-ag.com
AuthServWhitelist = *.mt-ag.com
```

Important: make sure that all browser requests aren’t routed through a proxy server. So, if your browser was configured to use a proxy server, make sure that an exception for apex.mt-ag.com exists, otherwise you will get a “page not found” error, because the Kerberos ticket got lost along the way.

## 2.5 CONFIGURATION OF A LINUX CLIENT PC

By default, users running Linux will be prompted to enter username/password each time a new browser instance was started. This is because a kerberos ticket wasn’t created after starting the operating system. To request a kerberos ticket, enter `kinit <AD user>@<Domain>`, for example `kinit joe.foo@MT-AG.COM`.

When using Firefox, go to the URL `about:config` and set the attribute `network.negotiate-auth.trusted-uris` to `.mt-ag.com`. After this, you can start Firefox und work with your APEX apps without being confronted with an authentication dialog.

For Google Chrome, you will have to start Chrome using the parameter `auth-server-whitelist`:

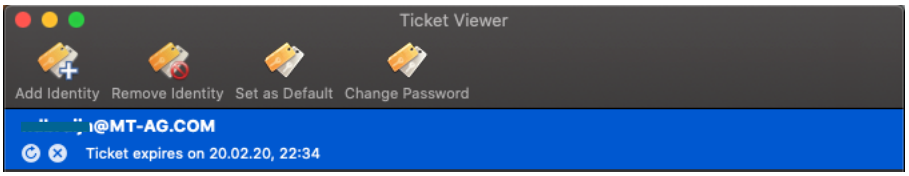
```
google-chrome -auth-server-whitelist=".MT-AG.COM"
```

Alternatively, you can add the following in `kerberos.json` to prevent providing parameter during startup:

```
$ cat /etc/opt/chrome/policies/managed/kerberos.json
{
  "AuthServerWhitelist": ".MT-AG.COM",
  "AuthNegotiateDelegateWhitelist": ".MT-AG.COM"
}
```

## 2.6 CONFIGURATION OF A MACOS CLIENT PC

By default, users running MacOS will be prompted to enter username/password each time a new browser instance was started. This is because a kerberos ticket wasn't created after starting the operating system. By starting the built-in app "Ticket Viewer" you can request a kerberos ticket. If your AD credentials are stored in your Apple keychain, you won't even have to logon to get the ticket.




After this, you can start Safari und work with your APEX apps without being confronted with an authentication dialog.

When using Firefox, go to the URL `about:config` and set the attribute `network.negotiate-auth.trusted-uris` to `.mt-ag.com` before accessing the APEX application.

For Google Chrome, you will have to start Chrome using the parameter `auth-server-whitelist`:

```
open /Applications/Google\ Chrome.app --args -auth-server-whitelist=".MT-AG.COM"
```

Have a look at the following blog post on how to configure a shortcut that starts Google Chrome with this attribute:
https://wpguru.co.uk/2016/11/how-to-launch-a-mac-app-with-command-line-parameters-from-the-dock/

# 3 CONFIGURATION WHEN USING LINUX

## 3.1 ADD AN ENTRY IN DNS FOR THE WEBSERVER

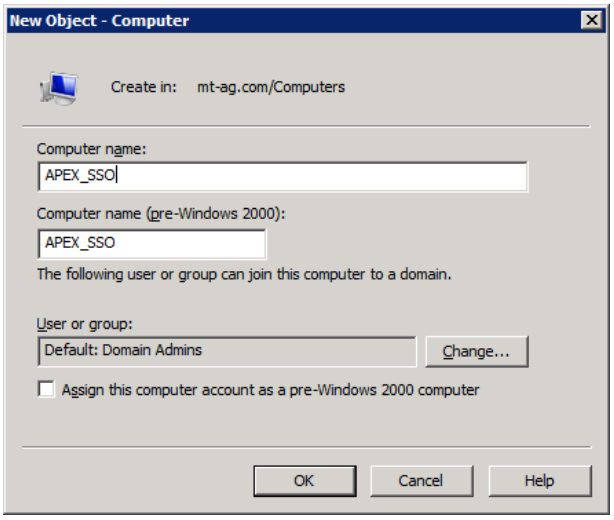
First add the fully qualified domain name (FQDN) as A-record (not as alias!) in your internal DNS server. In our example, we entered apex.mt-ag.com. You can verify this by executing nslookup apex.mt-ag.com.

Remarks:

- If the FQDN was registered as alias, the end user needs to authenticate himself through the Basic Authentication protocol and is requested to enter his username/password combination. The Kerberos authentication will not work in this case!
- A PTR-record for the IP address of the physical host should exist (reverse lookup).
- In our case, the physical server name equals the web address. Should the physical server name differ from the web address, register the physical server name as A-record and the web address as CNAME-record that points to the physical host (A-record). **Only for the physical server name you will need to go through the various steps below. So for instance, execute `ktpass` with the physical server name as `-princ` parameter. You can setup many additional CNAME-records if required.**

## 3.2 CREATE A SERVICE USER IN ACTIVE DIRECTORY

Add a computer account, like APEX_SSO in Active Directory.



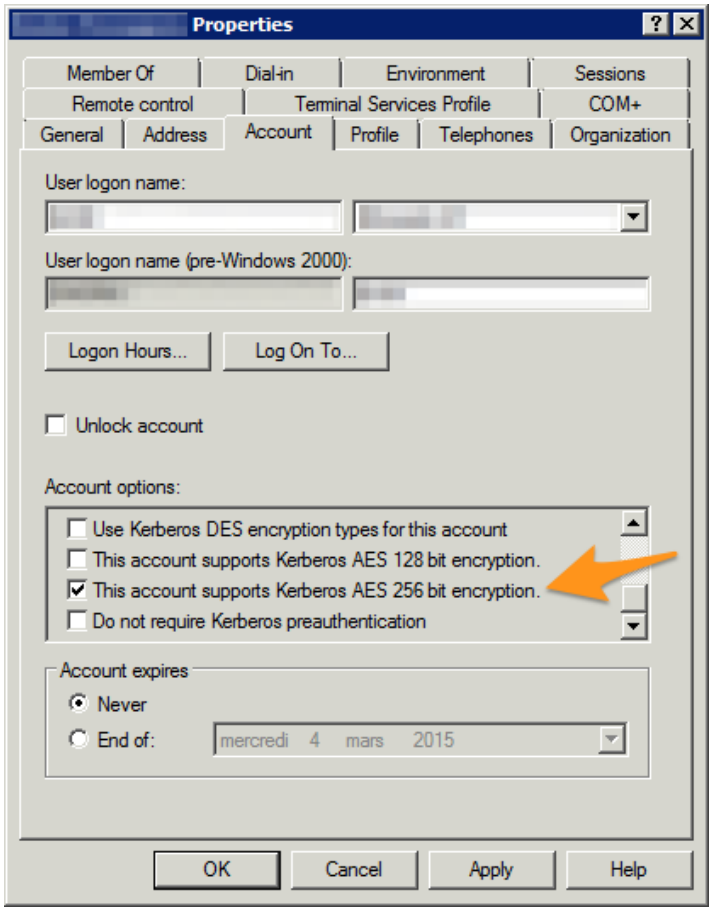

Use this account to create a keytab file with which Apache may verify if users are authenticated:

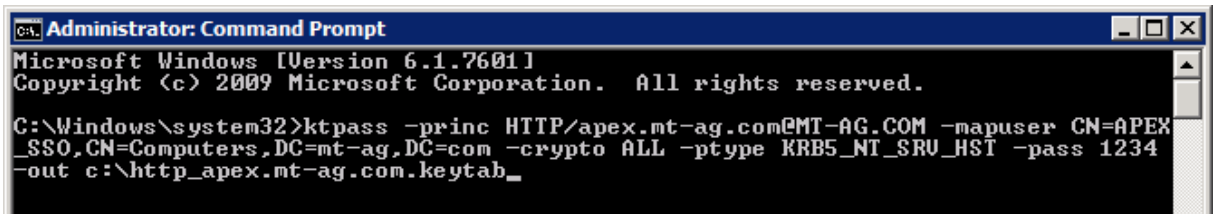
```
ktpass -princ HTTP/apex.mt-ag.com@MT-AG.COM -mapuser
"CN=APEX_SSO,CN=Computers,DC=mt-ag,DC=com" -crypto All -ptype
KRB5_NT_SRV_HST -pass <password> -out c:\http_apex.mt-ag.com.keytab
```

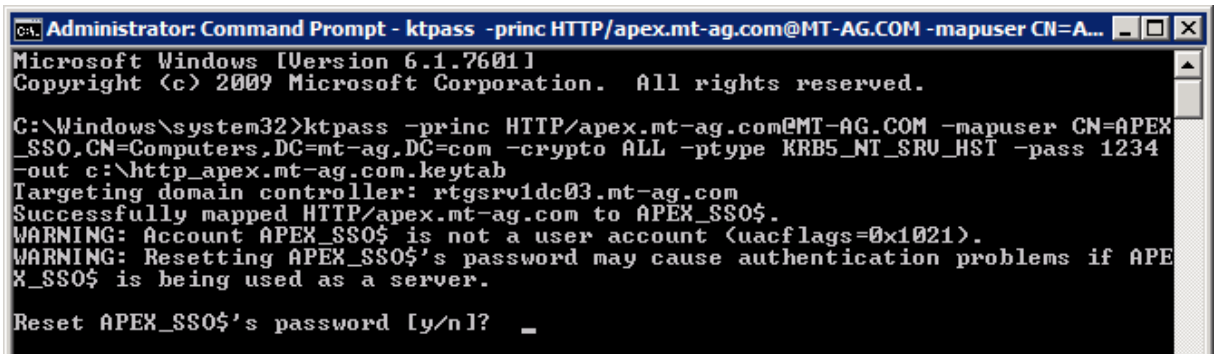
Remarks:

- Although it is also possible to use a user account, we recommend the usage of a computer account, since with this account type it is not possible to logon on a client pc that is registered in a windows domain.

- Our domain in this example is called MT-AG.COM and the web address we use to access APEX through Apache is https://apex.mt-ag.com. Make sure that the domain is written in uppercase. You can find the domain in the “Computer properties” dialog on your Windows client.
- Run the command prompt in administrator mode on the domain controller, otherwise you will get a strange “abort” error message.
- The password can be whatever you like it to be.
- The address apex.mt-ag.com behind HTTP/ is the A-record in the DNS (in this case the physical host name).
- Although we access APEX by using HTTPS, you still need to specify HTTP behind –princ.
- The filename of the keytab-file can be chosen freely.
- Windows 2003 Server is not aware of the option –crypto all, so use the legacy -crypto RC4-HMAC-NT instead. If possible, set -crypto to AES256-SHA1 to enforce a strong encryption. By doing so, make sure that the Windows (user) account supports it:






Copy over the keytab file to the Linux server where you want to install Apache. In our example, this is the directory /opt/httpkeytab.

## 3.3 INSTALL NTP

The time on the Apache server should be kept in sync with the domain controller. You can achieve this by installing the NTP service:

```
yum install ntp
```

Make sure that it starts automatically upon server reboot:

```
chkconfig ntpd on
```

## 3.4 INSTALL APACHE WITH MOD_AUTH_GSSAPI

By installing the module mod_auth_gssapi, Apache will be installed as well:

```
yum install mod_auth_gssapi
```

Make sure that Apache starts upon server reboot:

```
chkconfig httpd on
```

Remark: `ntpq -p` will show you the difference between times on the domain controller and the local server.

This document does not describe how to configure Apache so it can be accessed through Port 443 using a valid SSL server certificate. We strongly recommend using HTTPS as the fallback authentication method “basic authentication” is otherwise insecure.

## 3.5 CONFIGURE KERBEROS ON THE APACHE SERVER

Edit the file `/etc/krb5.conf`:

```
[libdefaults]
default_realm                    = MT-AG.COM
dns_lookup_realm                 = false
dns_lookup_kdc                   = false
ticket_lifetime                  = 24h
renew_lifetime                   = 7d
forwardable                      = true

[realms]
MT-AG.COM = {
kdc                              = mt-ag.com
```

```
admin_server                    = MT-AG.COM
default_domain                  = MT-AG.COM
}

[domain_realm]
.mt-ag.com                      = MT-AG.COM
mt-ag.com                       = MT-AG.COM
```

Remarks:

- After kdc you can also state multiple hostnames, separated by a space.
- The domain must be written in uppercase.
- No reboot of Apache is needed since this configuration is read each time the authentication process takes place.
- A good documentation of this file can be find here: http://web.mit.edu/Kerberos/www/krb5-1.12/doc/admin/conf_files/krb5_conf.html

## 3.6 APACHE CONFIGURATION

Add the following lines to the file `/etc/httpd/conf/httpd.conf`:

```
# Load all necessary modules if not already loaded
LoadModule auth_gssapi_module           /etc/httpd/modules/mod_auth_gssapi.so
LoadModule proxy_module                 /etc/httpd/modules/mod_proxy.so
LoadModule proxy_ajp_module             /etc/httpd/modules/mod_proxy_ajp.so
LoadModule headers_module               /etc/httpd/modules/mod_headers.so
LoadModule rewrite_module               /etc/httpd/modules/mod_rewrite.so

# If Apache runs with a different address, enable the following line
# LoadModule proxy_http_module          /etc/httpd/modules/mod_proxy_http.so


# The default maximum size for a HTTP request header with 8190 is set too small and may result # into a Bad Request error message in the browser. As with Tomcat, we need to explicitly set # this value to 65536 to avoid problems.
LimitRequestFieldSize 65536

# Depending on the version of Apache, you might need to have “RewriteEngine on” outside the
# location block.
RewriteEngine On

# Enforce usage of https instead of http, no http access is allowed any
# more and all requests are transparently rewritten as https.
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI} [NC,R,L]

ProxyIOBufferSize 65536

# Protect all APEX specific requests
<Location /ords>
  AuthType              GSSAPI
  AuthName              "Kerberos Login"
  GssapiCredStore       keytab:/opt/httpkeytab/http_apex.mt-ag.com.keytab
  GssapiBasicAuth       On
  GssapiLocalName       On
  require valid-user

  RewriteEngine On

  # disable/enable the following lines if you want to pass the domain name as well
```

```
  # RewriteCond %{LA-U:REMOTE_USER} (.+)$
  RewriteCond %{REMOTE_USER} (.+)@.*
  RewriteRule . - [E=RU:%1]

  # Introduce a new HTTP header variable SSO_USER as REMOTE_USER is overwritten by ORDS
  RequestHeader set SSO_USER %{REMOTE_USER}s

  # If Apache runs with a different address, enable the following line
  # ProxyPreserveHost On

  ProxyPass ajp://127.0.0.1:8009/ords connectiontimeout=2100 timeout=2100

  # If Apache runs with a different hostname as Tomcat, enable the following line
  # and enable communication between the two using either AJP or HTTP(S)
  # ProxyPassReverse http://<hostname_tomcat>:8080/ords

  # Add this line to prevent an error message “” from ORDS
  RequestHeader unset Origin

  # Display a nice message to end users when Tomcat is down due to maintenance
  ErrorDocument 503 /msgs/my_nice_maintenance_message.html
</Location>

# Static files of APEX
Alias /i/ "/srv/www/htdocs/images/"

# enable caching of static images
<Directory "/srv/www/htdocs/images/">
    AllowOverride None
    Order allow,deny
    Allow from all
    Options Indexes
    <IfModule mod_expires.c>
      ExpiresActive on
      ExpiresDefault "access plus 8 hours"
    </IfModule>
    IndexOptions FancyIndexing
</Directory>

# enable compression of static files
<IfModule mod_deflate.c>
  AddOutputFilterByType DEFLATE text/html application/javascript text/plain text/css text/xml
</IfModule>
```

Save the file and restart Apache.

Remarks:

- All static files of APEX were copied to /srv/www/htdocs/images. You can find these in /images within the software directory of the APEX software.

Optionally, you can additionally require that the user is also a member of a certain group in Active Directory:

```
...
# Load the required module
LoadModule authz_ldap_module                    /etc/httpd/modules/mod_authz_ldap.so
...
```

```
# LDAP server and search filter
AuthLDAPUrl  "ldap://myldapserver.mt-ag.com/OU=Rollen,DC=MT-ag,DC=com?userPrincipalName?sub?(objectClass=user)"

# User used for the inquiry
AuthLDAPBindDN  "CN=myldapuser,OU=Rollen,DC=mt-ag,DC=com"
AuthLDAPBindPassword  "mypassword"

# The LDAP group the user hast to be member of
require ldap-group "CN=myldapgruppe,OU=Gruppen,DC=mt-ag,DC=com"
# require valid-user
. . .
```

# 4 CONFIGURATION WHEN USING WINDOWS

## 4.1 ADDITIONAL COMPONENTS

To get SSO for APEX with IIS in front of it, the following components are required:

- Nonstandard IIS components
  - Windows Authentication (under Security)
  - ISAPI Extensions (under Application Development)
  - ISAPI Filters (under Application Development)

- Additional Software
  - Helicon ISAPI Rewrite (http://www.helicontech.com/isapi_rewrite)
  - Tomcat Connector (http://tomcat.apache.org)

### 4.1.1 INSTALL NON-STANDARD IIS COMPONENTS

If not installed by default already, install the necessary IIS components by opening a PowerShell as administrator and executing the following command:

```
Install-WindowsFeature -Name Web-Windows-Auth,Web-Basic-Auth,Web-ISAPI-Ext,Web-ISAPI-Filter
```

### 4.1.2 INSTALL HELICON ISAPI REWRITE

The installation of the ISAPI Rewrite component is pretty straightforward, so there is no need to document this.

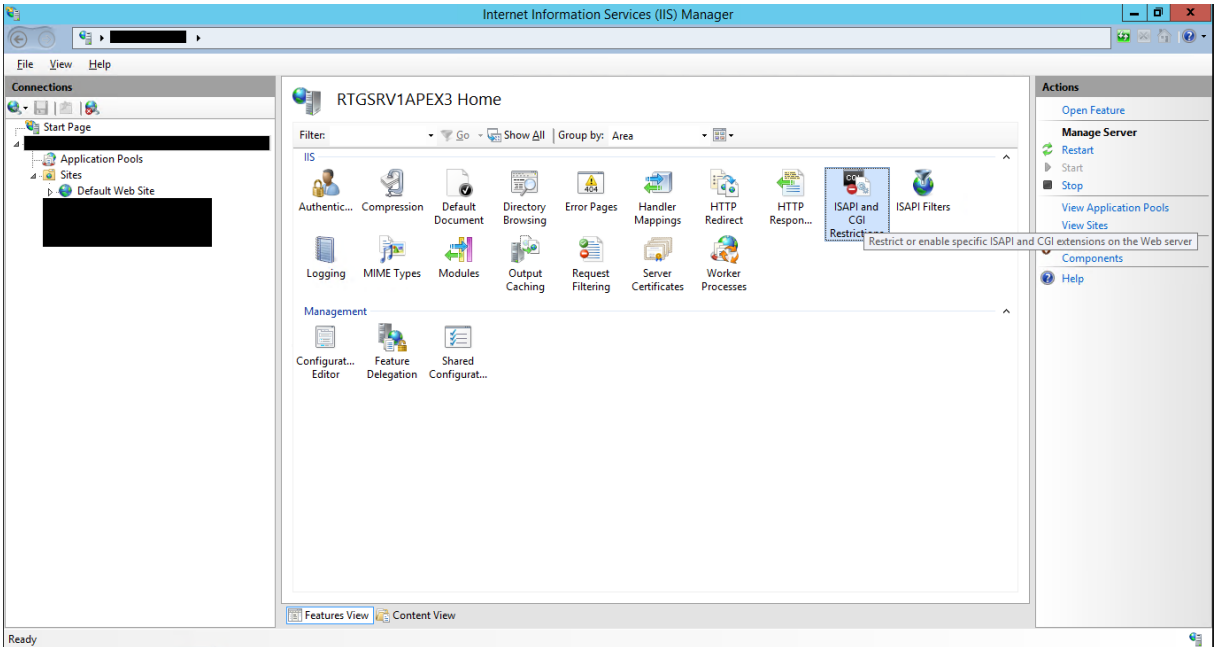
Remarks: This product is needed to set the AD username in the HTTP header after authentication.

### 4.1.3 INSTALL TOMCAT CONNECTOR

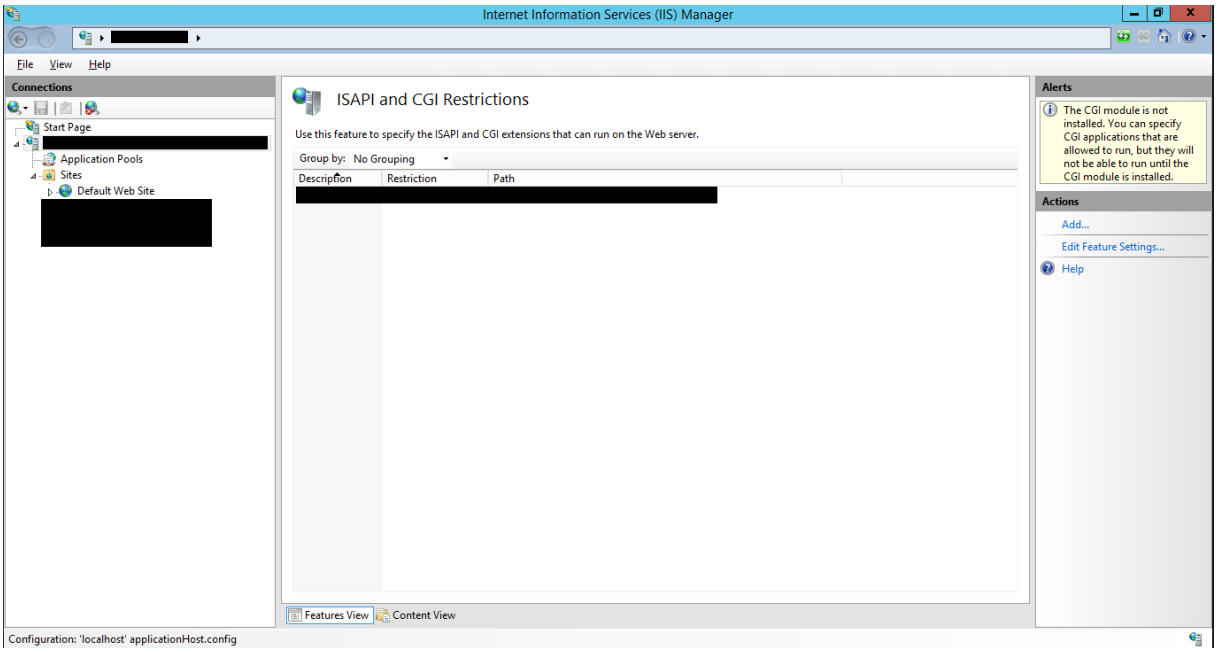
To use the better AJP protocol of Tomcat you need to install the Tomcat Connector for IIS. The installation of the Tomcat Connector is completely manual, so please follow the next steps to install it.
First, we need to download the Tomcat Connector for Windows 64 bit. You can get the latest version from the Tomcat website
http://tomcat.apache.org/download-connectors.cgi > „Binary Releases for selected versions“.
In the downloaded zip file is one dll which is need. In this documentation this file is present under following location:
c:\inetpub\tomcat-connector\isapi_redirect.dll

### 4.1.3.1 ALLOW THE ISAPI EXTENSION TO RUN

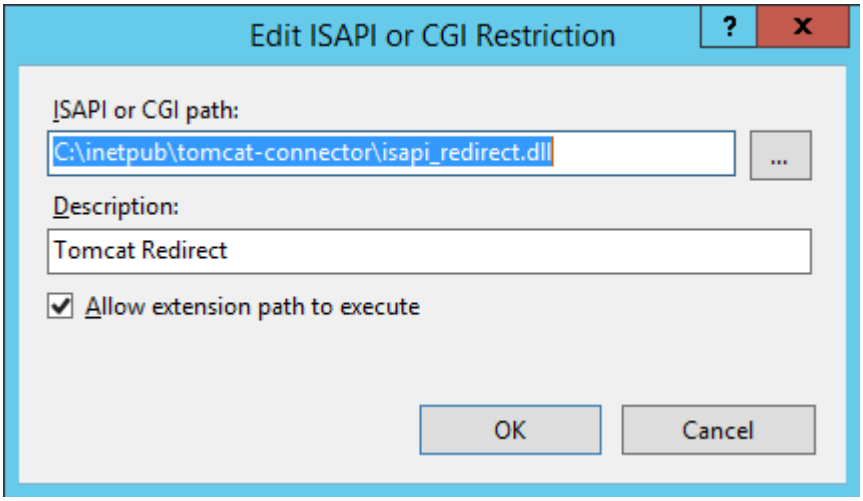
- To get Tomcat Connector working we need to do some things in the IIS Manager
- Mark the webserver in the ‘Connections’ panel
- Double click the ‘ISAPI and CGI Restrictions’ icon




- Click ‘Add’ in the ‘Actions’ panel

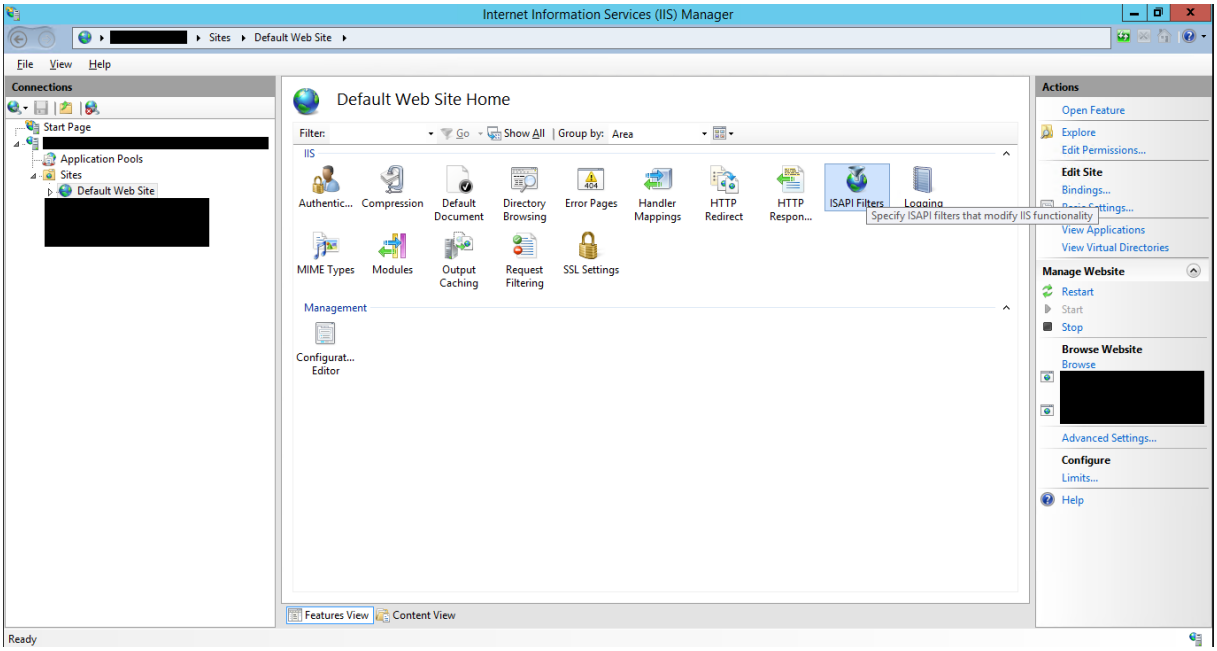


- Browse to the isapi_redirect.dll in the Tomcat Connector folder, enter a description and enable ‘Allow extension path to execute’

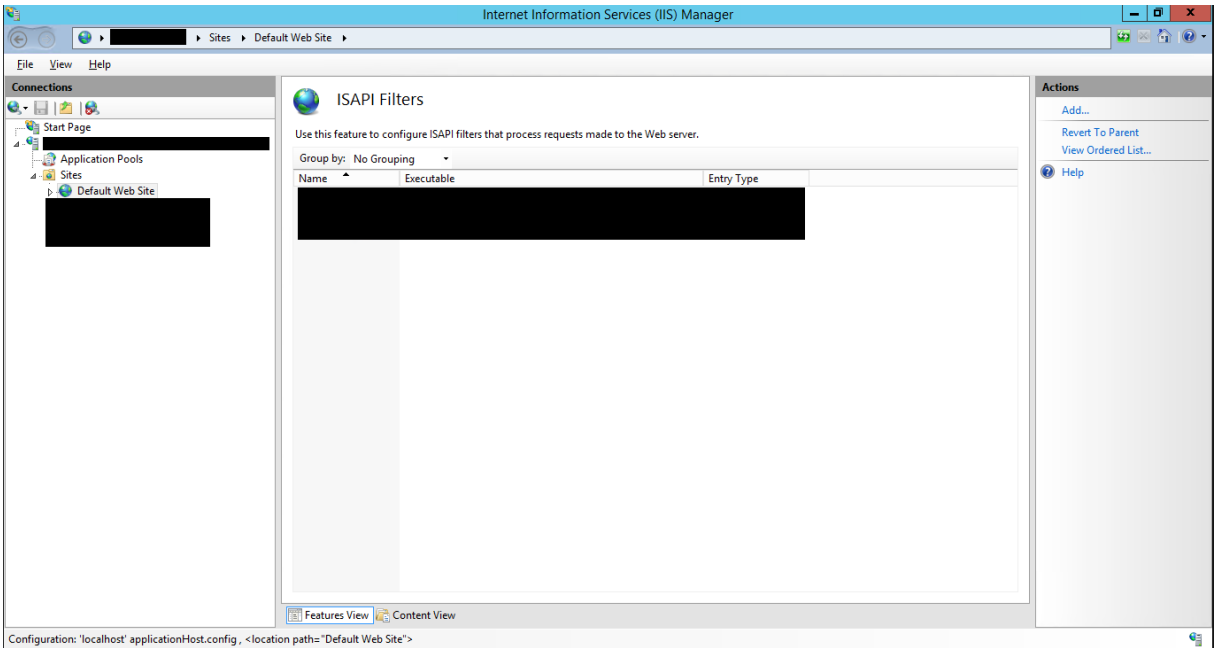



### 4.1.3.2 ADD ISAPI FILTER

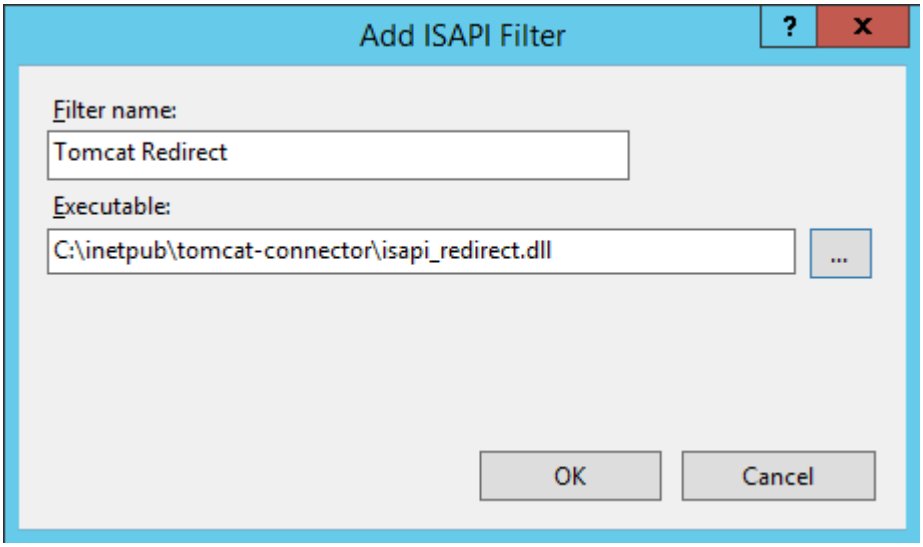
- Mark the website you want to use for APEX in the ‘Connections’ panel
- Open the ‘ISAPI Filters’



- Click ‘Add’ in the ‘Actions’ panel

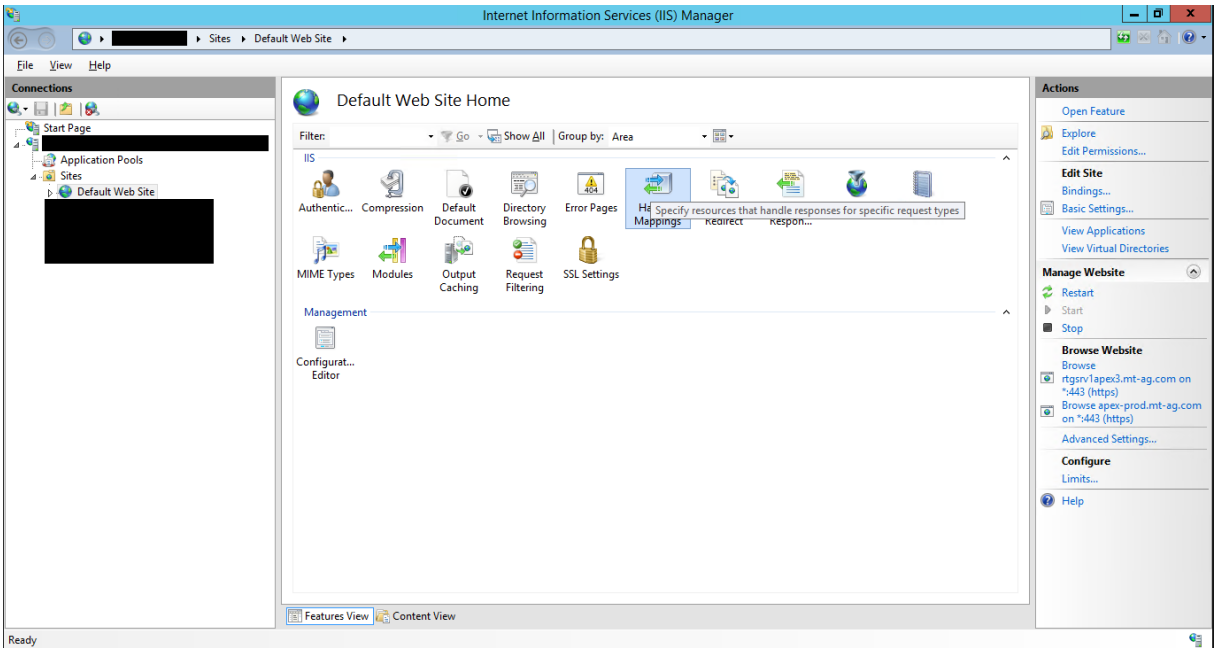



- Set a ‘Filter name’ and browse to the isapi_redirect.dll in the Tomcat connector folder
- Click on ‘OK’ to insert the filter

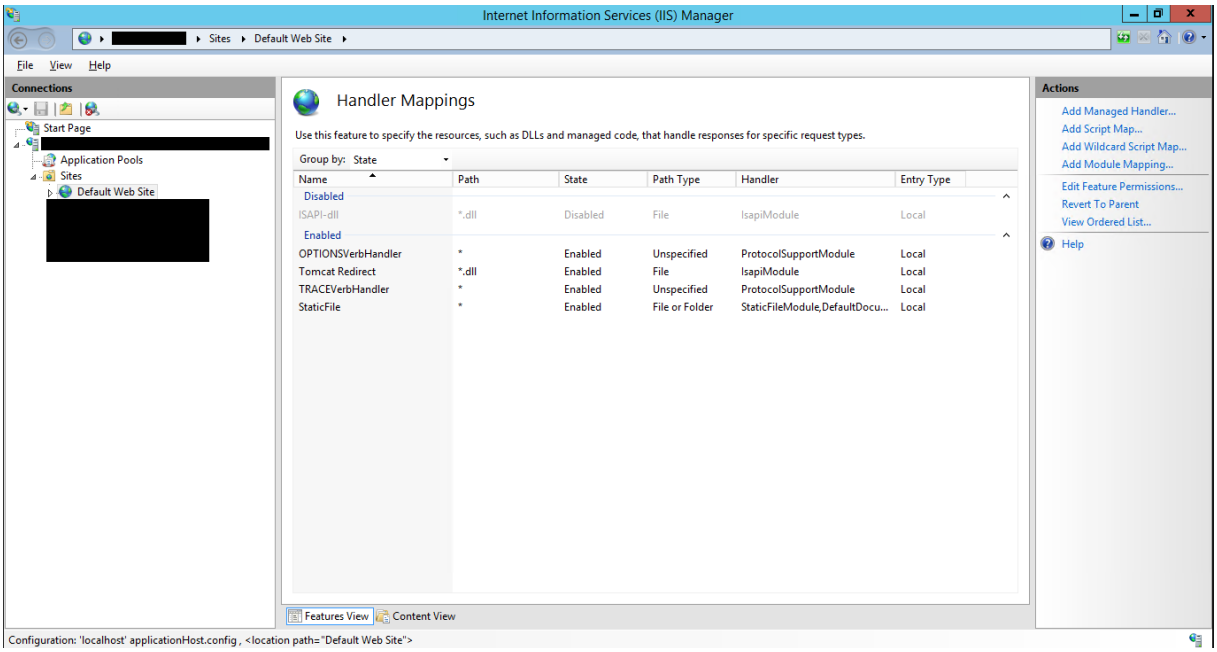


### 4.1.3.3 ADD SCRIPT MAP

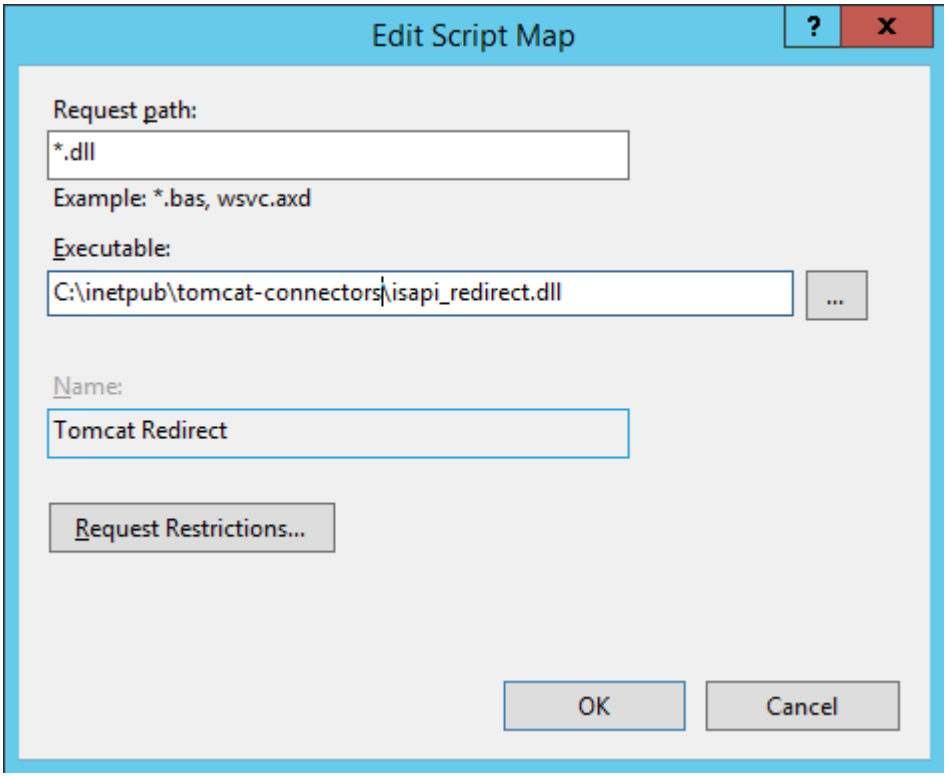
- In IIS Manager in ‚Connections' select the default website
- Double click on ‚Handler Mappings'




- Click on ‚Add Script Map…' in the ‚Actions' panel

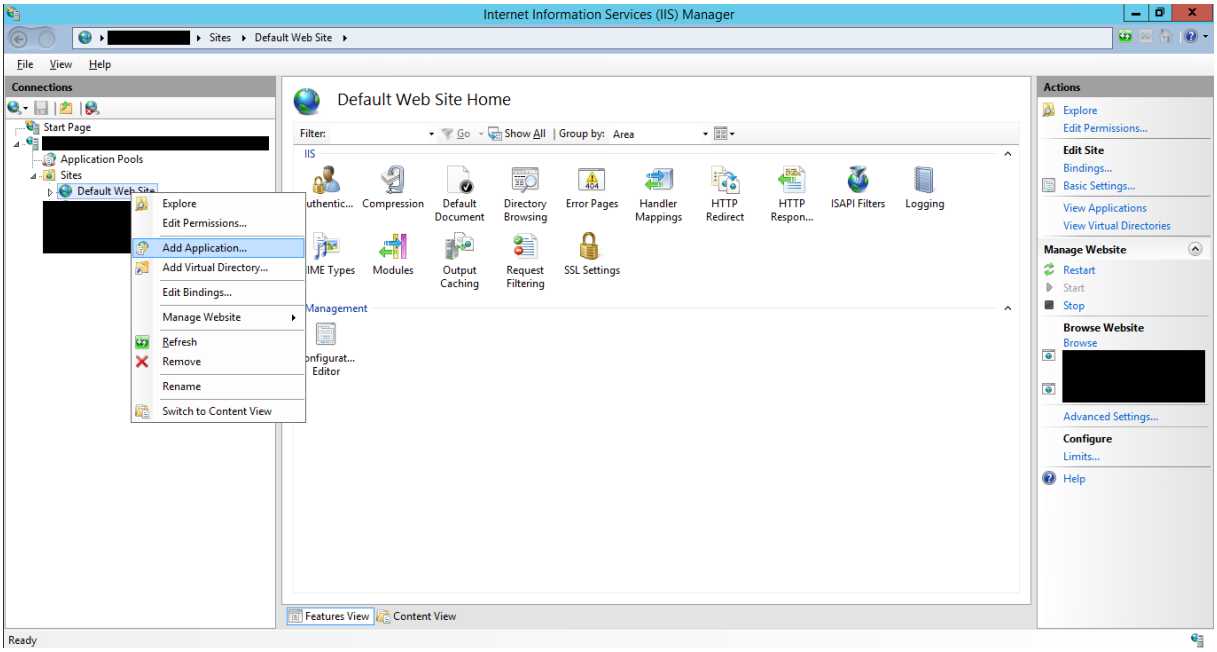


- In the dialog, enter *.dll as ‚Request path‘ and the location oft he DLL file. Click on ‚OK‘.

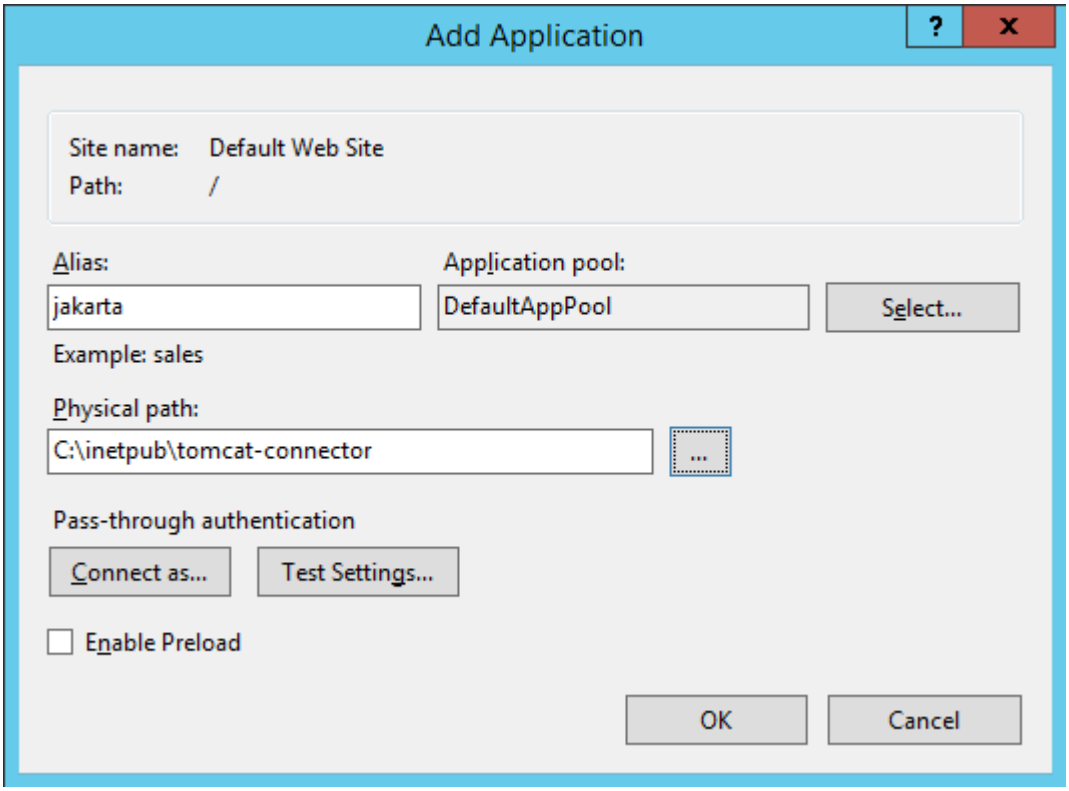



### 4.1.3.4 ADD APPLICATION

- Right click the Website and click ‘Add Application’

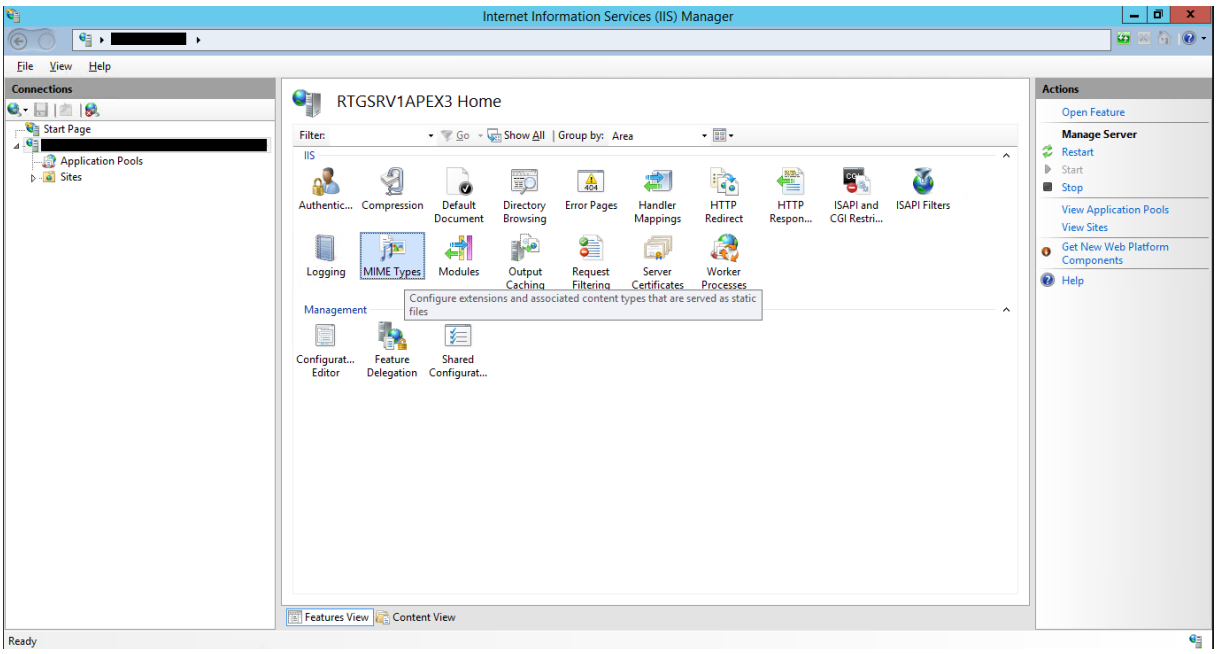


- Set the Alias to ‘jakarta’ (this name doesn’t show up in any URL or something but it is important for this documentation that you enter exactly this name) and browse to the Tomcat Connector folder
- Click on ‘OK’ to create the Application



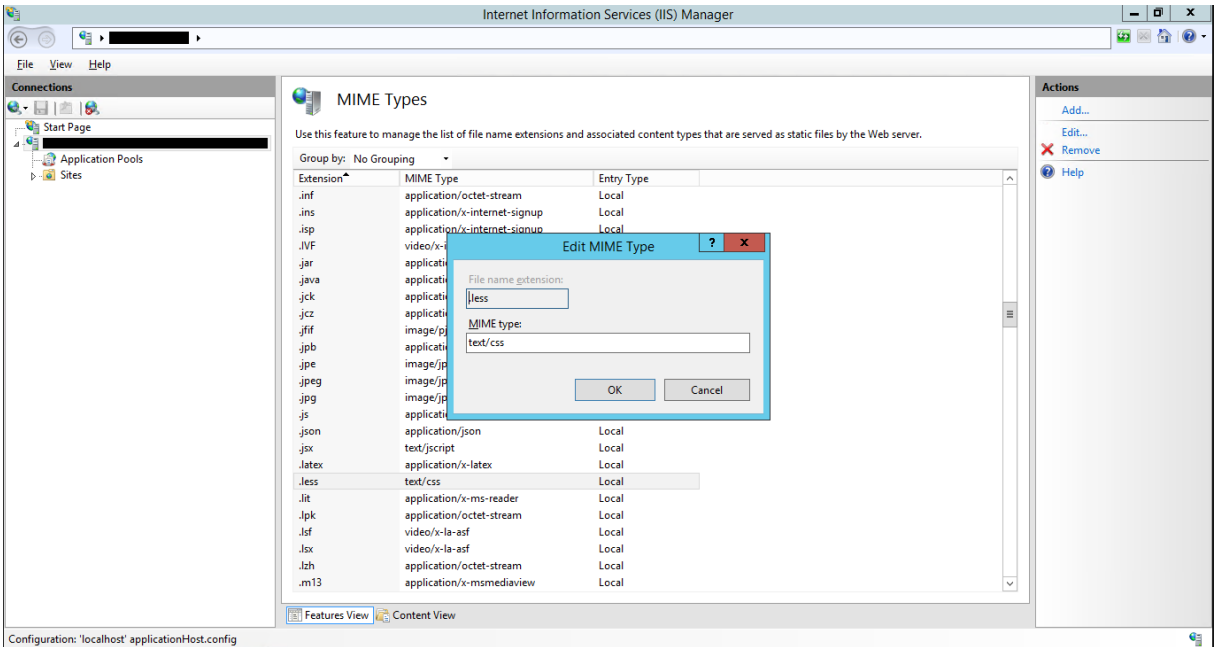
### 4.1.3.5 MIME TYPE FOR .LESS FILES

- APEX uses .less files; unfortunately, IIS on Windows Server 2012 does not support this file type by default, so you have to insert this file type in the ‘MIME Types’.




Please also check if other MIME type extensions used by APEX like *.json, *.woff and *.woff2 are also registered. Depending on your Windows version, this might not be the case, although they are present by default on Windows Server 2016.

- Click on ‘Add’ in the ‘Actions’ panel and insert the ‘File name extension’ .less and as ‘MIME type’ text/css.

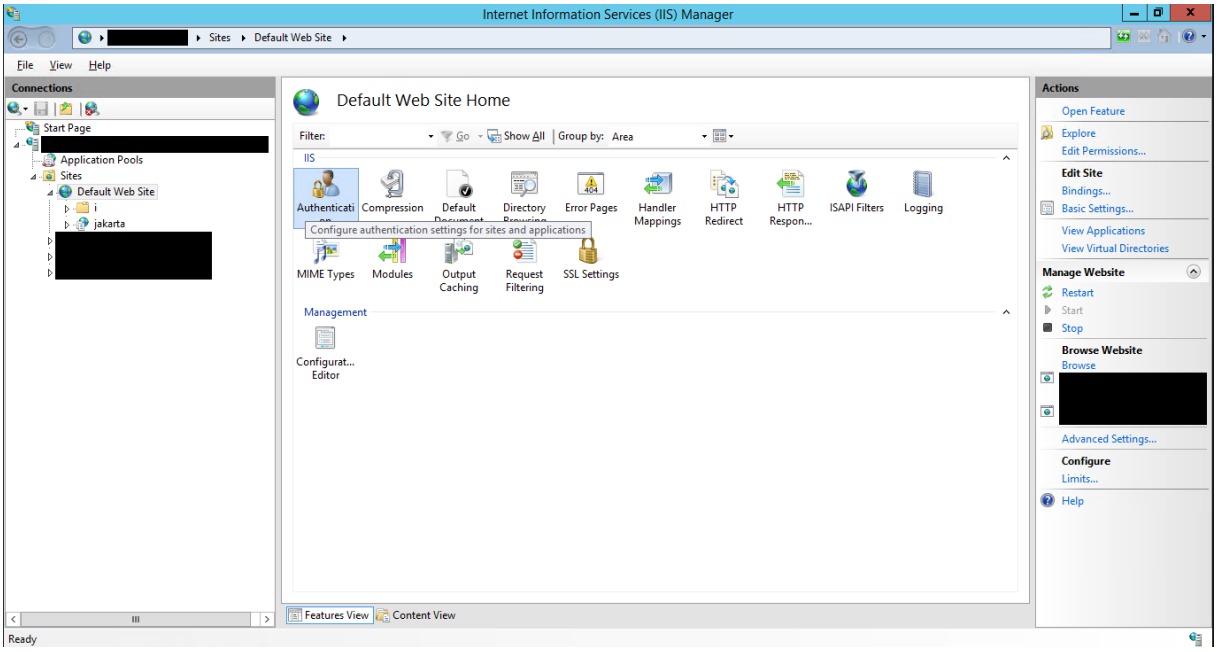


## 4.2 CONFIGURE ADDITIONAL COMPONENTS

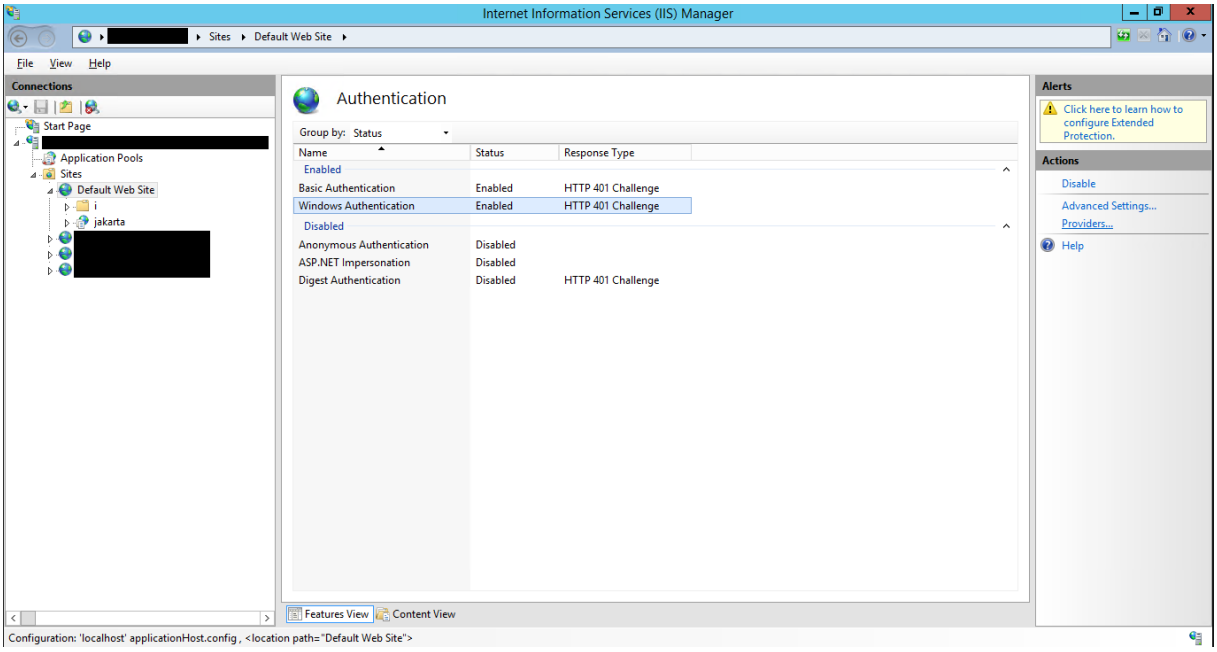
### 4.2.1 IIS AUTHENTICATION

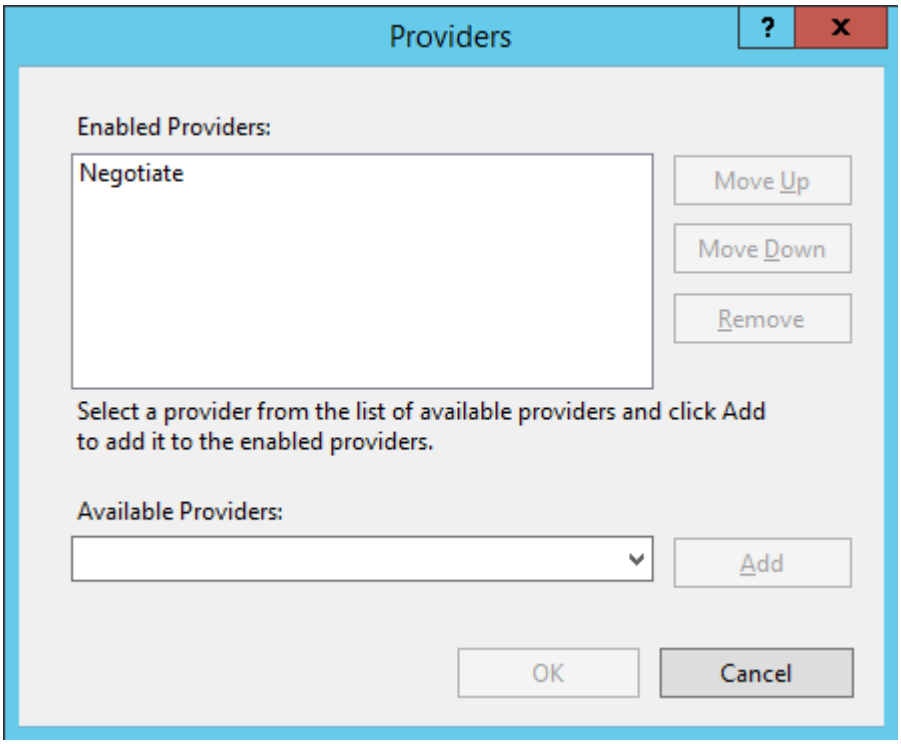
#### 4.2.1.1 KERBEROS FOR WEBSITE

To achieve SSO we need to enable Kerberos authentication for the website. For mobile devices and non-domain clients we enable Basic authentication, too. To encrypt the password, it is important to secure the channel via SSL.




To prevent ‚Windows Authentication' to work with NTLM you can delete it in the ‚Providers' list (Mark ‚Windows Authentication' – ‚Actions' Panel – ‚Providers')

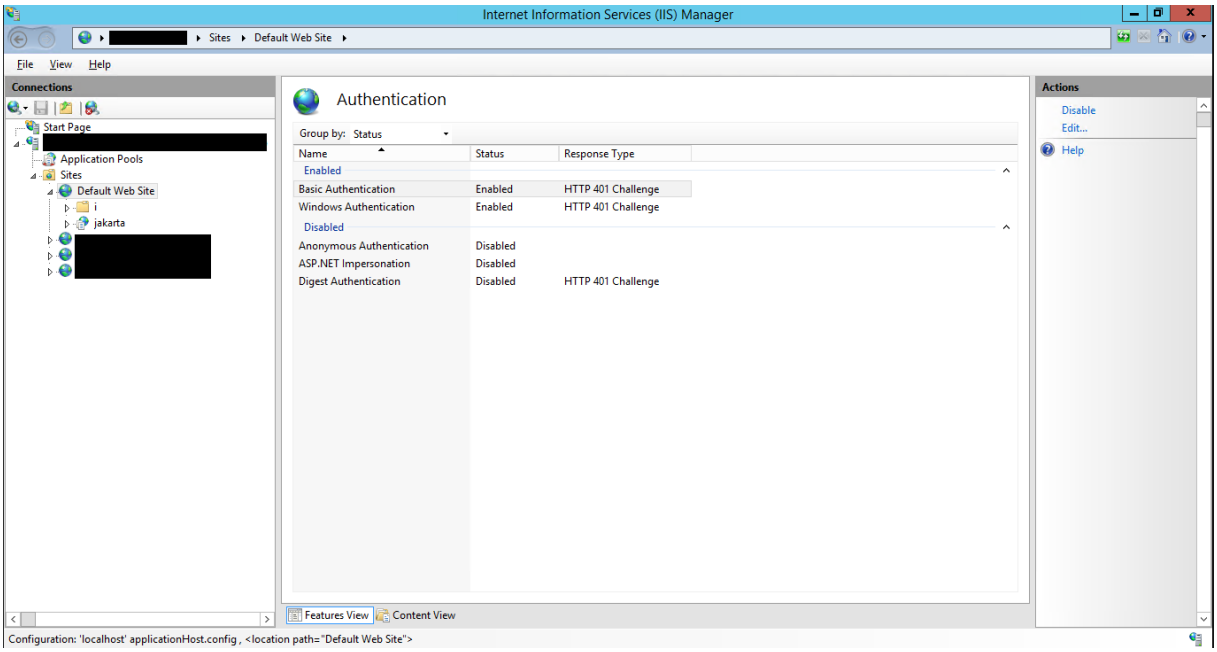





You just need “Negotiate”. You may ignore other providers, even though you will find “Negotiate:Kerberos” listed in “Available Providers”.

#### 4.2.1.2 FOR BASIC AUTHENTICATION SET DEFAULT DOMAIN

To make it easier for non-domain clients we edit the ‘Basic Authentication’ component (Mark ‘Basic Authentication’ – ‘Actions’ panel – ‘Edit’) and enter the NETBIOS Domain name in the ‘Default domain’ field.



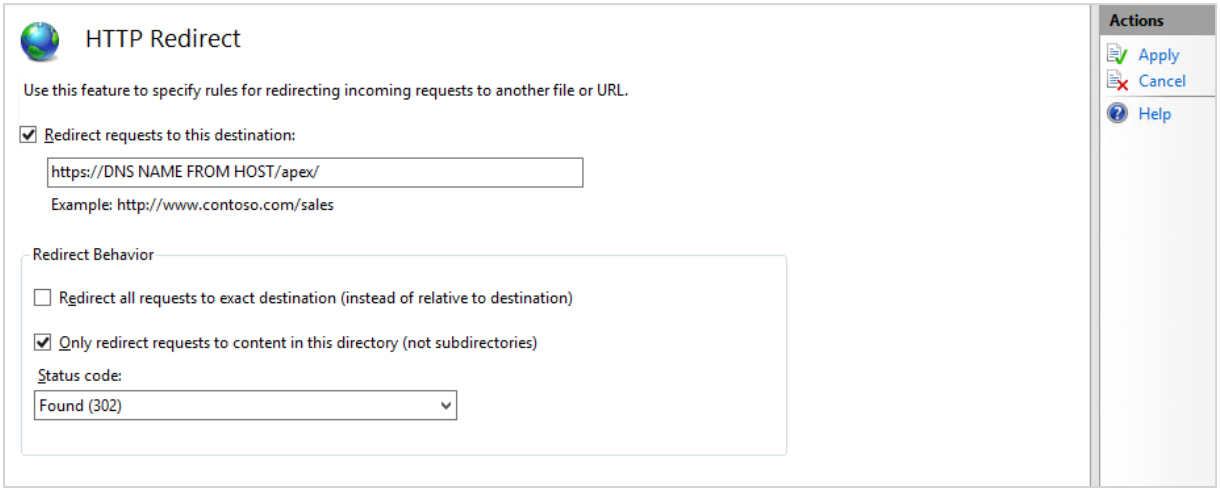
#### 4.2.1.3 ANONYMOUS AUTHENTICATION FOR APEX STATIC IMAGES FOLDER

To get better performance for ‘i’ (copy of ‘images’ folder from APEX) enable only ‘Anonymous Authentication’ for this subfolder.

Remarks: the images directory is automatically being cached. If possible, any file is also sent compressed over the network.

#### 4.2.1.4 REDIRECT / TO /APEX

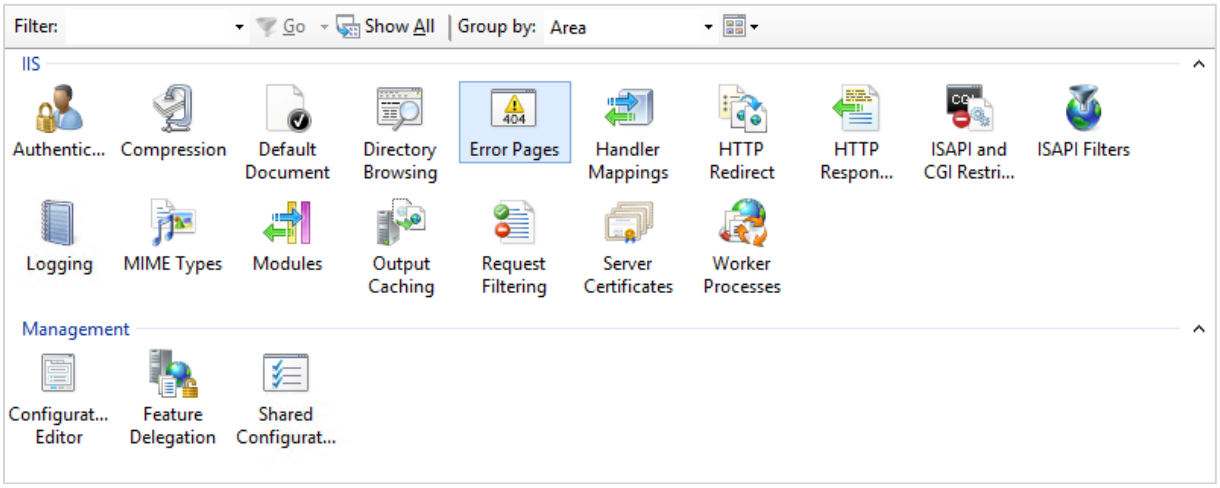
To access the APEX system easier a redirect from the root directory to the /apex is a good solution. This means that the user only has to enter the hostname into the browser and get the APEX website. To archive this, you have to insert a ‘HTTP Redirect’ on the website. (Double klick ‘HTTP Redirect’ – ‘Actions’ panel – ‘Edit’) In the next screenshot you can see the settings.

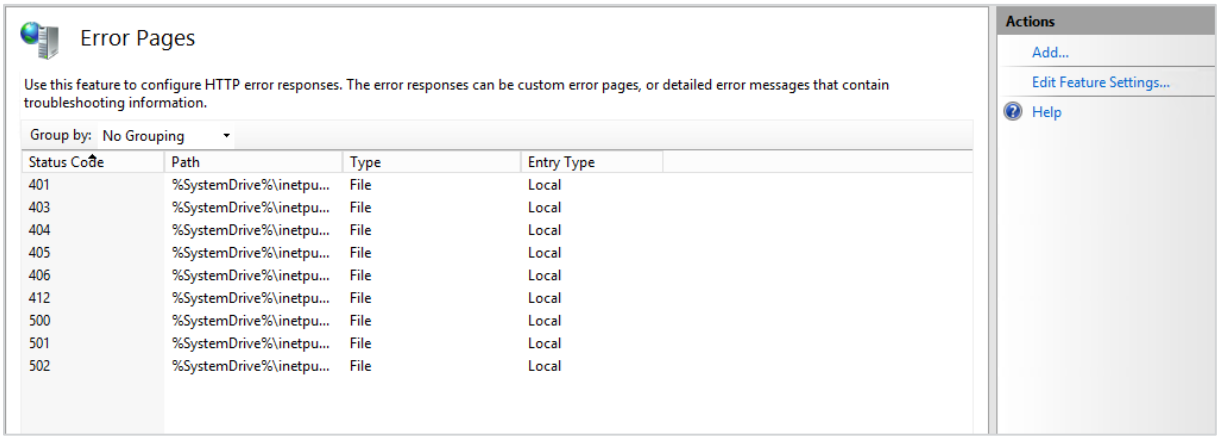



To finish this step klick ‘Apply’.

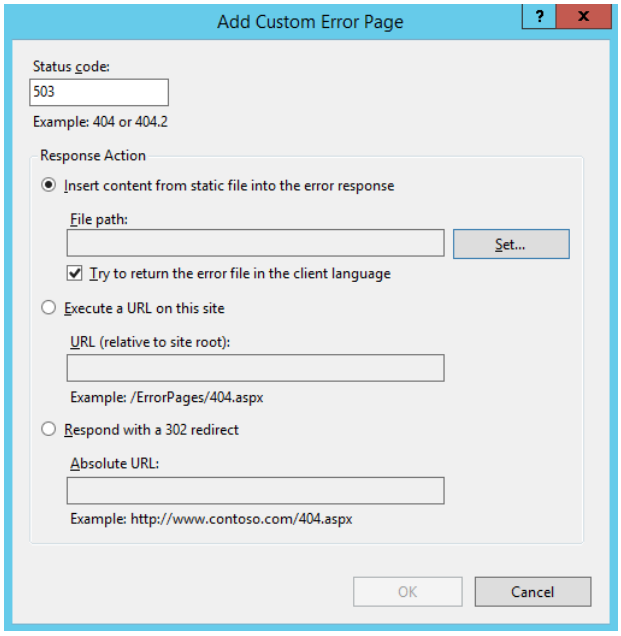
#### 4.2.1.5 FRIENDLY ERROR MESSAGE DURING MAINTENANCE OF TOMCAT

To get a specific error page for maintenance work you have to insert an additional error code in the IIS config. Select the server (not the website!) and double klick ‘Error Pages’ – ‘Actions’ panel – ‘Add’.

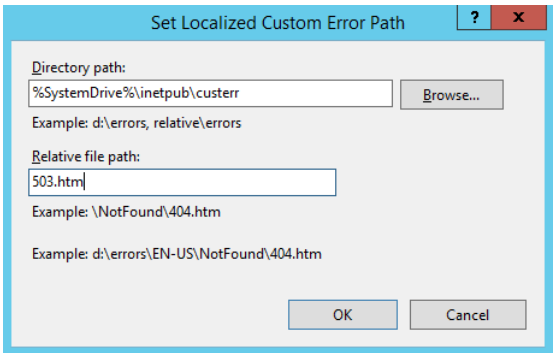


- In the next window you have to insert the ‘Status code’ 503 activate ‘try to return the error file in the client language’ and press the ‘Set’ button.




- The settings for the next window you can see in the following screenshot.




- Close both windows with ‘OK’

- You need to create the HTML page for the error code 503. To do this you have to go to ‘C:\inetpub\custerr\en-US\‘ and make a copy of the file ‘502.html’. After that rename the copy to ‘503.html’ and open it in an editor. The changes you have to make are marked bold.

Filename: C:\inetpub\custerr\en-US\503.htm

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>Maintenance</title>
<style type="text/css">
<!--
```

```
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Maintenance</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>Maintenance</h2>
  <h3>Currently the APEX System is not available</h3>
 </fieldset></div>
</div>
</body>
</html>
```

#### 4.2.1.6 FRIENDLY ERROR MESSAGE SHOULD AUTHENTIFICATION FAIL

If authentication in APEX fails because the HTTP header variable wasn't set, the user is redirected to the file 'C:\inetpub\notauth\index.html'. To create this file, copy the file 'c:\inetpub\custerr\en-US\503.htm' to the folder 'C:\inetpub\notauth' and rename it to 'index.html'. After that open the file in an editor and change the marked entries.

Filename: C:\inetpub\notauth\index.html

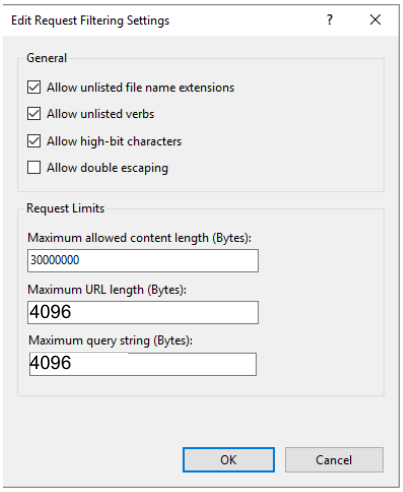
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>Authentification Error</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-
serif;background:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana,
sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>Authentification Error</h2>
  <h3>Please ask your local IT department.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

- You have to change the authentication method for the the 'notauth' folder (Mark website/notauth and double klick 'Authentication')
- Enable 'Anonymous Authentication' and disable all other

#### 4.2.1.7 INCREASE URL & CONTENT LENGTH

When opening Theme Roller as a developer from within the developer toolbar at the bottom of an APEX app, the URL used by APEX is 3,600 bytes long. By default, IIS allows only URLs that are 2048 bytes long. To increase this value, select the server and click on 'Request Filtering'. Enter 4096 for "Maximum URL length (Bytes)" and 4096 for "Maximum query string (Bytes)".

The allowed content length (Bytes) determines how large ie. an imported APEX app may be, so set it at least to 30,000,000 bytes.




### 4.2.2 CONFIGURE ISAPI REWRITE

To configure ISAPI Rewrite start ISAPI_Rewrite Manager. In the free edition you can only use the root folder ‚IIS Web Sites'. Click on ‚Edit' to enter the config file.

The following lines enables the rewrite engine of ISAPI Rewrite and transfer the REMOTE_USER to the SSO_USER header variable for Kerberos and Basic authentication.

```
# Helicon ISAPI_Rewrite configuration file

## Acivates rewrite mechanism
RewriteEngine  On
LogLevel error
RewriteLogLevel 0

## Set header variable "SSO_USER" if user authenticates via basic authentication
RewriteCond    %{REMOTE_USER} (.*)
RewriteHeader  SSO_USER: (.*) %1

## Set header variable "SSO_USER" if user authenticates via kerberos authentication
RewriteCond    %{REMOTE_USER} \\(.*)
RewriteHeader  SSO_USER: (.*) %1
```

### 4.2.3 CONFIGURE TOMCAT CONNECTOR

The last step to get this work is to create the following config files in the Tomcat Connector folder.

#### 4.2.3.1 ISAPI_REDIRECT.PROPERTIES

```
# The path to the ISAPI Redirector Extension, relative to the website
# This must be in a virtual directory with execute privileges
extension_uri=/jakarta/isapi_redirect.dll

 # Full path to the log file for the ISAPI Redirector
log_file=C:\inetpub\tomcat-connector\log\isapi.log

# Log level (debug, info, warn, error or trace)
log_level=error

# Full path to the workers.properties file
worker_file=C:\inetpub\tomcat-connector\workers.properties
```

```
# Full path to the uriworkermap.properties file
worker_mount_file=C:\inetpub\tomcat-connector\uriworkermap.properties
```

#### 4.2.3.2 URIWORKERMAP.PROPERTIES

```
/ords = ords
/ords/* = ords
```

#### 4.2.3.3 WORKERS.PROPERTIES

```
worker.list=ords
worker.ords.type=ajp13
worker.ords.host=127.0.0.1
worker.ords.port=8009
worker.ords.max_packet_size=65536
```

# 5 WHATS HAPPENING?

## 5.1 APACHE WEBSERVER

If you would like to see what's happening in the background, you can set the log level of Apache to debug and inspect the log files.

Edit the file: `/etc/httpd/conf/httpd.conf` and change the row containing „LogLevel warn" to „LogLevel debug". Save the file and restart Apache: `service httpd restart`

The log files you need to inspect are called `ssl_access_log` and `ssl_error_log`.

If the Kerberos authentication works, you should see the username appear in the access_log file:

```
192.168.2.106 - niels.de.bruijn [06/Feb/2017:09:55:06 +0100] "GET /apex/f?p=432:210:8679059367105 HTTP/1.1" 200 52939
192.168.2.106 - niels.de.bruijn [06/Feb/2017:09:55:07 +0100] "POST /apex/wwv_flow.ajax HTTP/1.1" 200 13
```

An extensive blog post about Kerberos based authentication can be found here:
http://www.grolmsnet.de/kerbtut

To check if kerberos without mod_auth_gssapi works, just run the following commands on the server where the Apache web server is running:

```
kinit joe.foo@MT-AG.COM
kinit -k -t /opt/httpkeytab/http_apex.mt-ag.com.keytab HTTP/apex.mt-
ag.com
klist
```

## 5.2 WINDOWS CLIENT

With the Windows client utility `klist`, you can find out which Kerberos tickets the Windows Domain User currently has. If all was setup correctly, you should see a ticket for `apex.mt-ag.com` in the output.

# 6 OTHER USEFUL LINKS

Alternative setup to use IIS as reverse proxy in front of Tomcat
(without passing a HTTP header variable):
https://medium.com/@rammelhofdotat/iis-and-oracle-apex-ords-437908c79e2

General guidelines to install/configure Apache, ORDS and Tomcat without SSO:
http://www.opal-consulting.de/downloads/presentations/2015-11-DOAG-ORDS-Setup

Authentication with mod_auth_gssapi not working with AD users that are member too many groups? Have a look here for more information:
http://blogs.technet.com/b/surama/archive/2009/04/06/kerberos-authentication-problem-with-active-directory.aspx

https://www.msxfaq.de/windows/kerberos/kerberosticketsize.htm (DE)

Should you encounter any HTTP 413 “request entity too large” errors, this document might help you out:
https://www.techpaste.com/2016/12/413-request-entity-large

**Disclaimer:**
Just to make sure: MT AG is not responsible for any damage, outages or loss of profit resulting from the usage of this document. Use it at your own risk. Have fun!