SSO for BOC Management Office® Products with Windows Authentication and IIS

www.boc-group.com

Table of Contents

1 Introduction

This document explains how to enable Single Sign-On (SSO) for a BOC Management Office® product with Windows authentication and IIS. It provides step by step instructions how to install the Microsoft Internet Information Services (IIS), connect with a Tomcat web container and forward requests to that container in a way that simulates an IDM scenario.

The currently logged in system (Windows domain) user will be used for authentication (SSO login). This means that the user is logged in automatically when opening the BOC Management Office® product and does not have to enter his credentials again.

2 Prerequisites

For the steps described in the upcoming chapters, the following prerequisites are required:

- The user account that runs the setup must have administrator rights on the target machine.
- The BOC Management Office® product must be installed and running properly.

3 Set Up Users

Single sign-on with Windows authentication and IIS is possible with standard product users and with system users. The following variants are possible:

1. Standard users are created manually in the Administration
2. System users are created on-the-fly when they log in for the first time

If you choose **variant 1**, set up the users in the Administration now. The option *Trusted login* needs to be enabled for all users. The usernames must match exactly with the login names of the Windows users who want to access the BOC Management Office® product.

If you decide to choose **variant 2**, nothing needs to be done now.

Important note: How to create users manually is described in the Administration Help. Please refer to the section "Create Users" for details.

4 Configure Tomcat

This chapter describes how to configure Tomcat for this scenario.

1. In the file `server.xml` in "*<TOMCAT>/conf*", the AJP connector needs to be configured. Look for a comment similar to `<!-- Define an AJP 1.3 Connector on port 8009 -->`.
2. Add the following attributes to the connector:
   - `tomcatAuthentication="false"`,
   - `packetSize="65536"`,
   - `secretRequired="true"` and `secret="<your secret keyword>"`

Note: For the attribute `secret`, choose a strong and secure secret keyword. Only requests from workers with this secret keyword will be accepted.

Make sure you configure the Tomcat AJP connector according to the latest security guidelines of the documentation specific to your Tomcat version. At the time of writing, this is the current recommended way to secure the AJP connector. Please also make sure to protect the used ports from the outside.

Example:

```
<Connector protocol="AJP/1.3" port="8009" redirectPort="8443"
tomcatAuthentication="false" packetSize="65536"
secretRequired="true" secret="<your secret keyword>"/>
```

3. In a browser, navigate to https://downloads.apache.org/tomcat/tomcat-connectors/jk/binaries/windows/ and download the latest version of the Tomcat connector (e.g. `tomcat-connectors-1.2.49-windows-x86_64-iis.zip`).
4. Create a new folder "*<TOMCAT>/connector*", then extract the zip file, and copy the contained file `isapi_redirect.dll` to that new folder.
5. Start **Notepad++** or a similar editor.
6. In the folder "*<TOMCAT>/connector*", create a new file called `isapi_redirect.properties`. Edit it as follows (adapt the path to Tomcat as necessary):

```
# Configuration file for the Jakarta ISAPI Redirector

# 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:\Program Files\Apache Software Foundation\Tomcat
10.1\logs\isapi_redirect.log


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

log_level=info


# Full path to the workers.properties file

worker_file=C:\Program Files\Apache Software Foundation\Tomcat
10.1\connector\workers.properties


# Full path to the uriworkermap.properties file

worker_mount_file=C:\Program Files\Apache Software
Foundation\Tomcat 10.1\connector\uriworkermap.properties
```

7. Again in the folder "*<TOMCAT>/connector*", create a new file called `workers.properties`. Edit it as follows:

```
#

# The workers that jk should create and work with

#

worker.list=myworker

#

# Defining a worker named myworker and of type ajp13

# Note that the name and the type do not have to match.

#

worker.myworker.type=ajp13

worker.myworker.host=localhost

worker.myworker.port=8009

worker.myworker.max_packet_size=65536
```

```
# Enter the secret keyword that you used in the Tomcat AJP configuration

worker.myworker.secret=<your secret keyword>
```

8. Again in the folder "*<TOMCAT>/connector*", create a new file called `uriworkermap.properties`. Edit it as follows if the web application is in a specific path (replacing `<webappname>` with the name of the web application in Tomcat):

```
/<webappname>/* = myworker

/<webappname> = myworker

!/<webappname>/rest/* = myworker

!/<webappname>/oauth2/* = myworker

!/<webappname>/websocket/* = myworker

!/<webappname>/websocket = myworker
```

If the web application is deployed as the ROOT web application, the configuration should look like this:

```
/* = myworker

/*/* = myworker

!/rest/* = myworker

!/oauth2/* = myworker

!/websocket/* = myworker

!/websocket = myworker
```

Done! Tomcat is now ready to cooperate with IIS.

5 Set Up IIS 8/8.5/10

This chapter describes how to install IIS 8/8.5/10 using Windows Server 2012 as an example.

IIS 8 is included in Windows Server 2012 and Windows 8.0. IIS 8.5 is included in Windows Server 2012 R2 and Windows 8.1. IIS 10 is included in Windows Server 2016, Windows Server 2019 and Windows 10.

Important note: If IIS is already installed on the machine, proceed to chapter **6**.

1. Open *Server Manager*.
2. Under *Manage* menu, select *Add Roles and Features*.

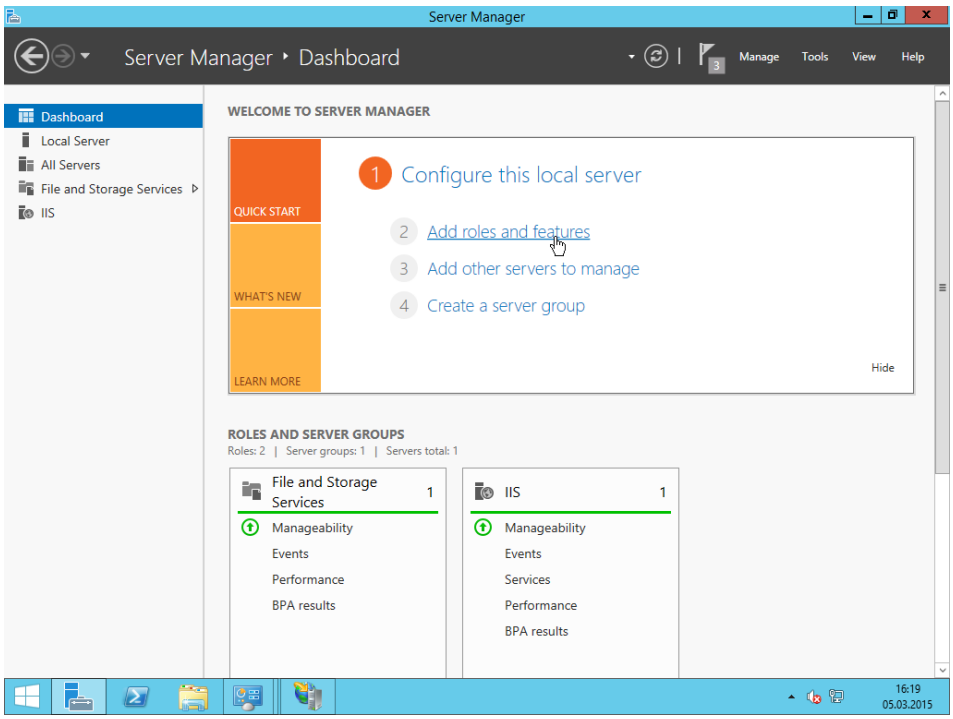

Fig. 1: Server Manager – Select Add Roles and Features

3. Under *Server Roles*, select *Web Server (IIS)*.
4. Under *Web Server Role (IIS) – Role Services*, in addition to the options selected by default, make sure the following entries are checked:

Web Server
- Security
  - ✓ Windows Authentication
- Application Development
  - ✓ CGI
  - ✓ ISAPI Extensions
  - ✓ ISAPI Filters
  - ✓ WebSocket Protocol

5. Click *Install* to finish the installation.

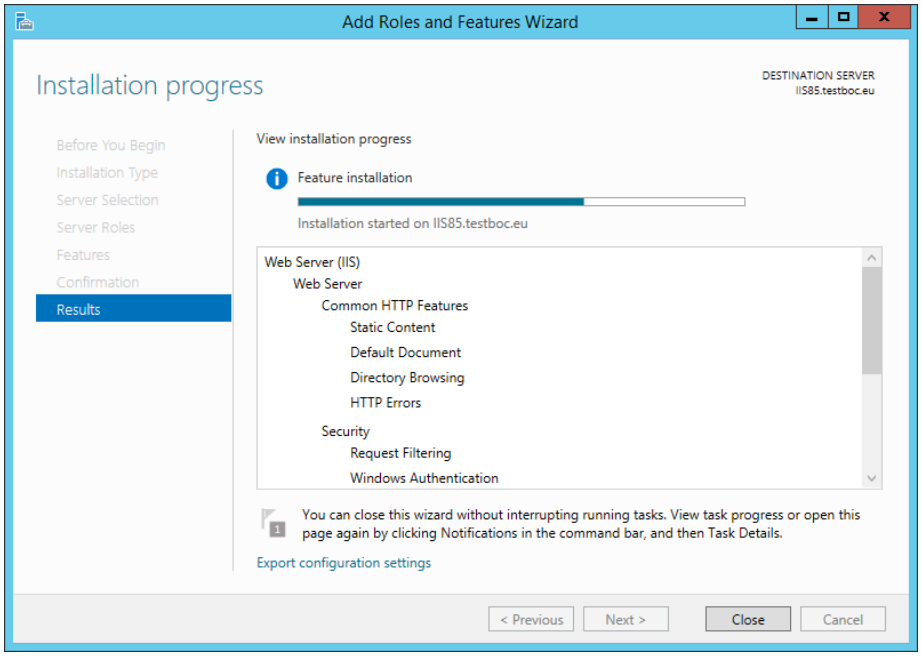

Fig. 2: Server Manager – Installation progress

6. Download and install the following additional modules for IIS:
   - URL Rewrite
   - Application Request Routing
7. Make sure that nothing on your machine is running on port 80, as IIS will try to use that port.
8. After everything is installed you can open a browser and navigate to "*http://localhost*". You should see the following:

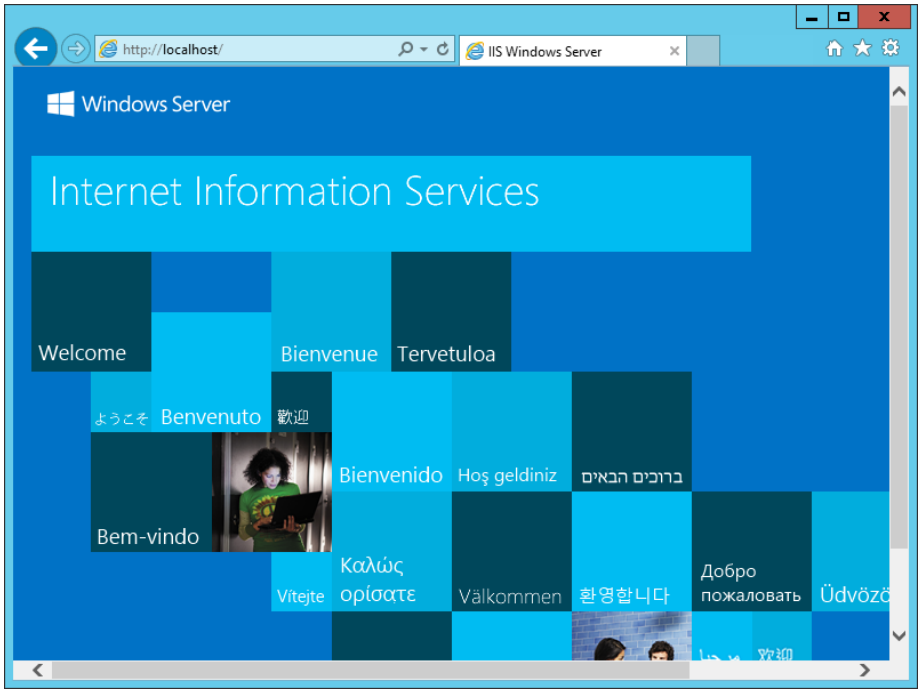

Fig. 3: Navigate to http:/localhost

9. On the *Start* screen, click *Control Panel*, click *Administrative Tools*, and then double-click *Internet Information Services (IIS) Manager*.

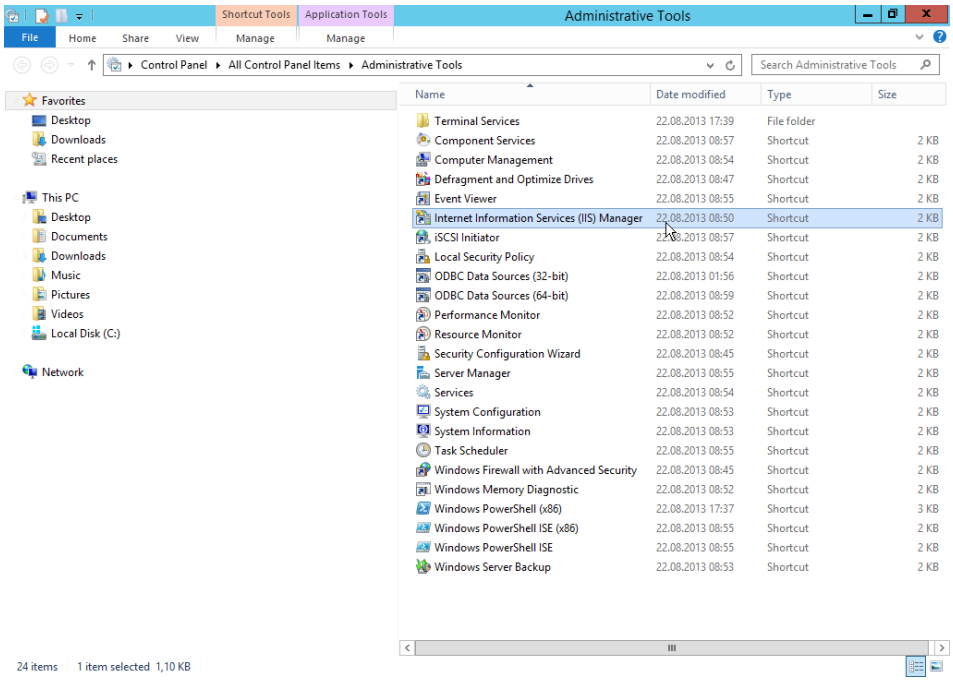

Fig. 4: Open the Internet Information Services Manager

Important note: If during the following steps you find that a required feature is not installed, add it through the Server Manager.

10. In the *Connections* pane, select the root element. In the *Home* pane, open the *ISAPI and CGI Restrictions*.

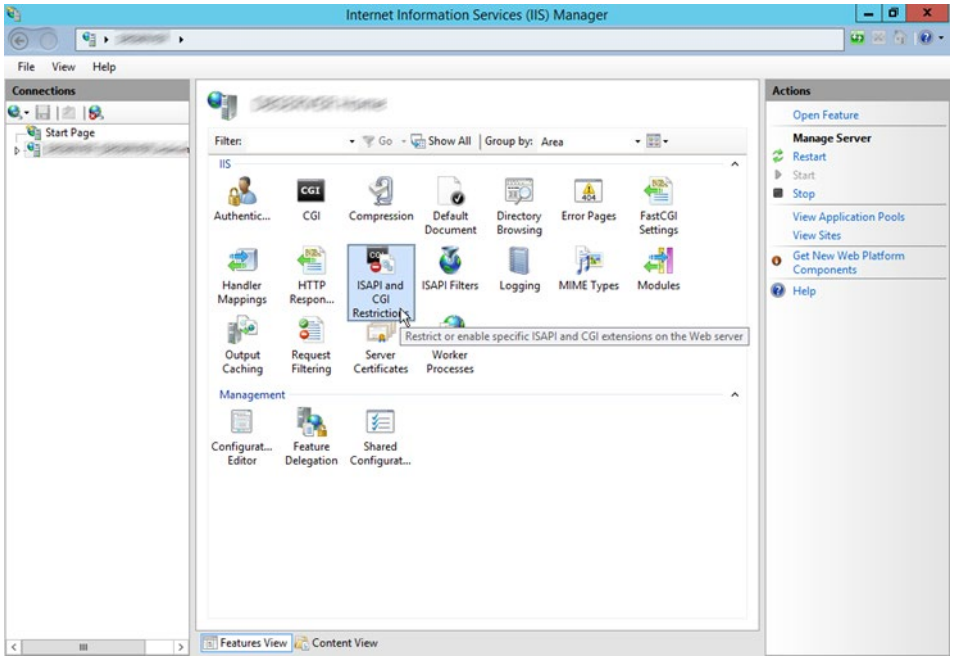

Fig. 5: Open ISAPI and CGI Restrictions

11. In the *Actions* pane, click *Add…* to add the `isapi_redirect.dll`.

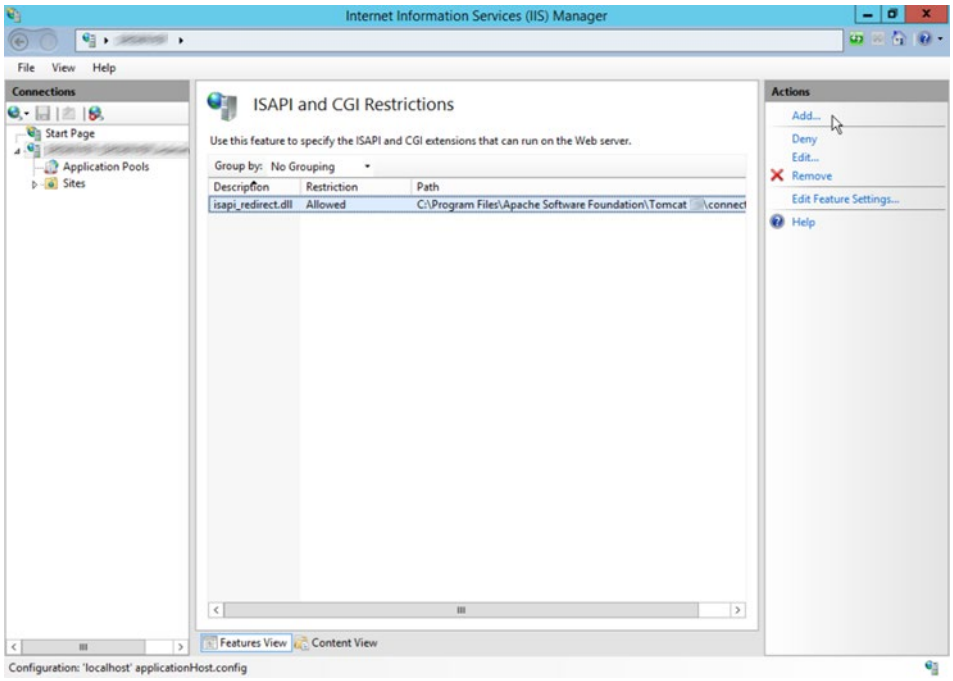

Fig. 6: Add isapi_redirect.dll

12. Choose a *Description* and set *ISAPI or CGI path* to the physical location of the `isapi_redirect.dll`. Select the option "*Allow extension path to execute*".

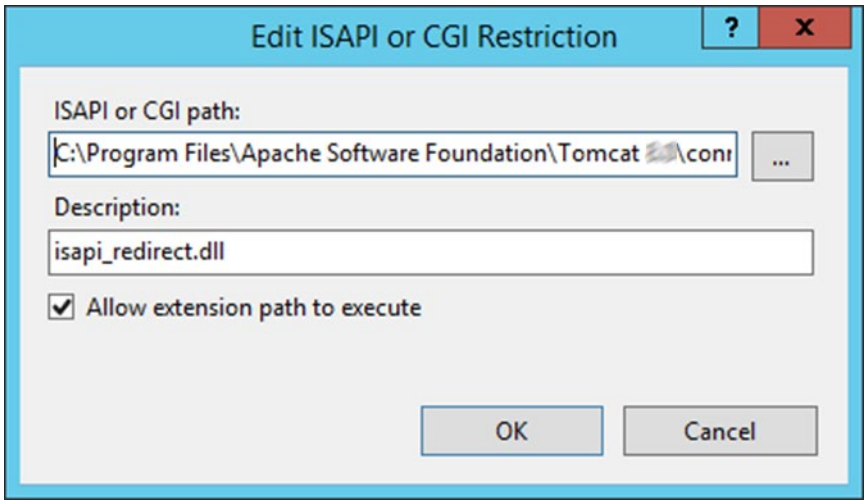

Fig. 7: Select the option "Allow extension path to execute"

13. In the *Connections* pane, select the *Default Web Site*. In the *Home* pane open *ISAPI Filters*.

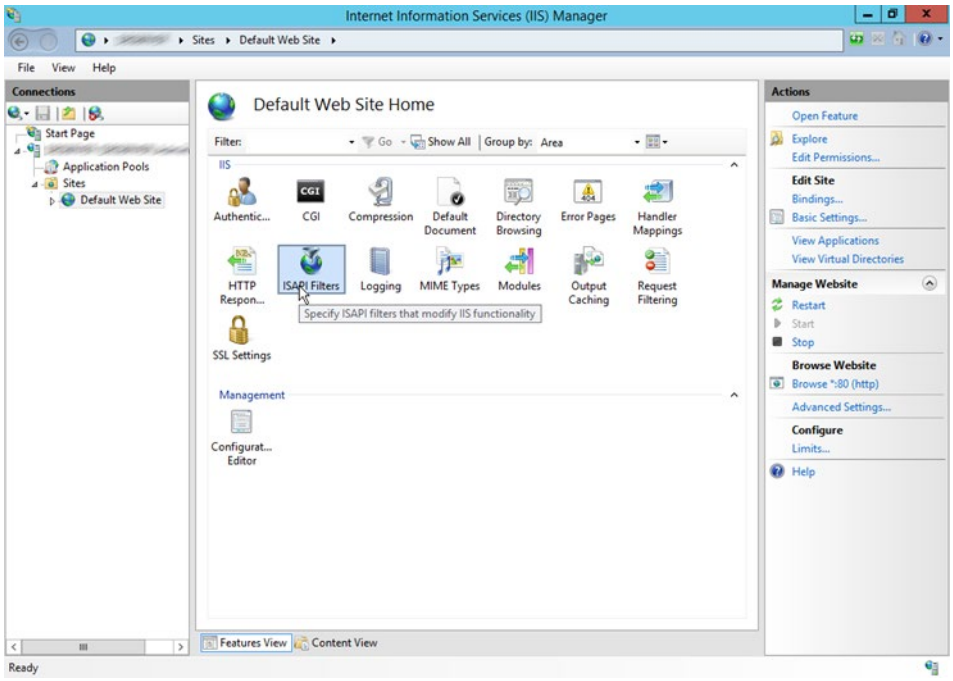

Fig. 8: Select the Default Web Site and in the Home pane open the ISAPI-Filter

14. In the *Actions* pane, click *Add…* to create an ISAPI filter. Choose a *Filter name*. Set *Executable* to the physical location of the `isapi_redirect.dll`.

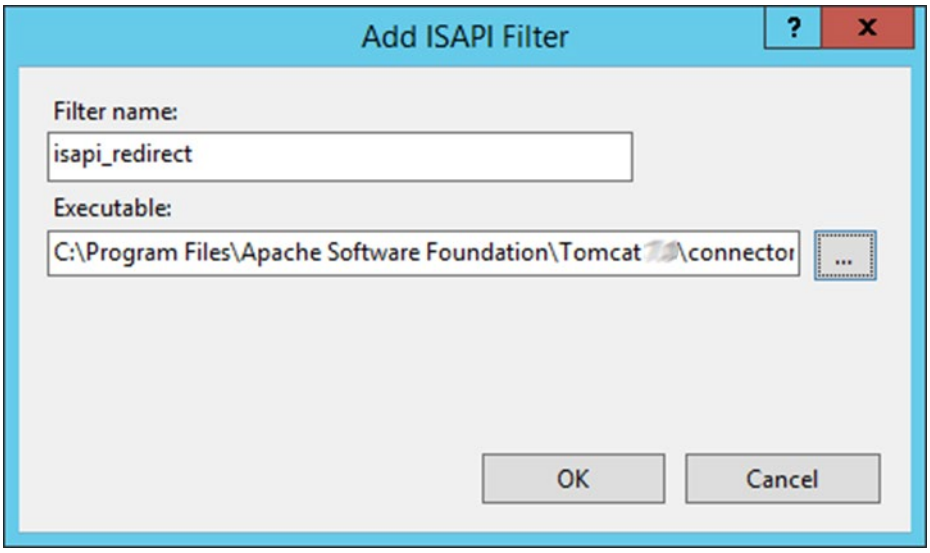

Fig. 9: Create an ISAPI filter

15. In the *Connections* pane, right click the *Default Web Site* and click *Add Virtual Directory…*. The *Alias* of this directory should be *Jakarta*. The *Physical path* should point to the directory where you have placed the `isapi_redirect.dll`:

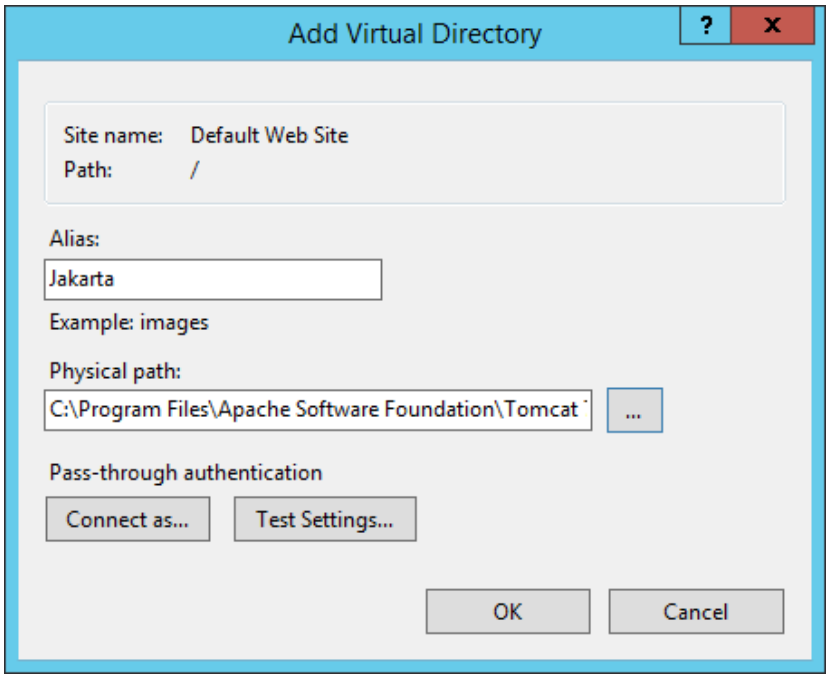

Fig. 10: Create virtual directory "Jakarta"

16. Select the new virtual directory *Jakarta* in the *Connections* pane. In the *Home* pane, open *Handler Mappings*.

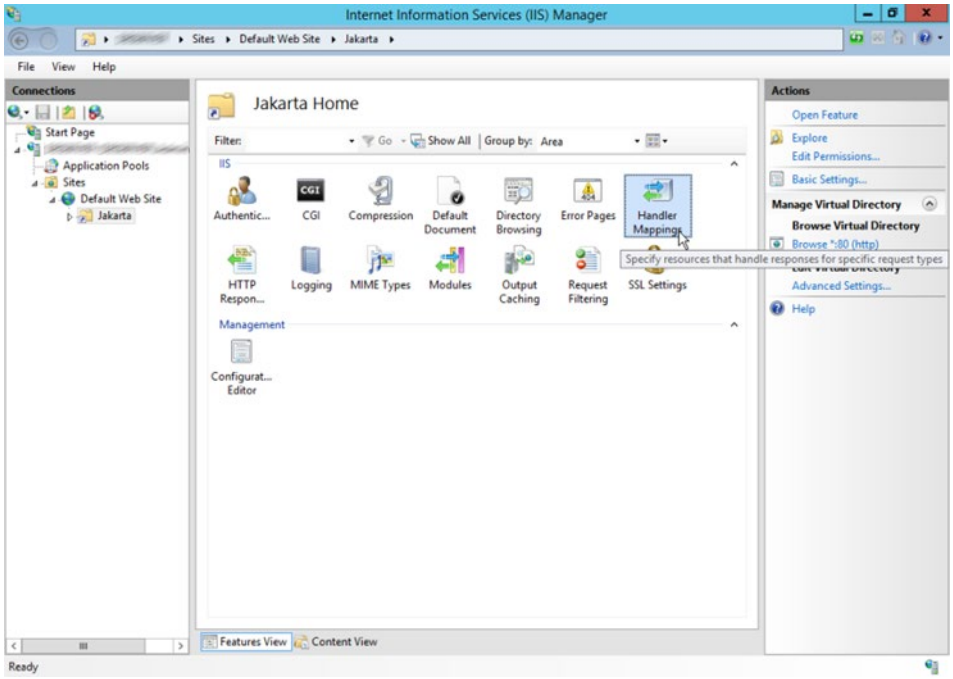

Fig. 11: Select virtual directory "Jakarta" and open the Handler Mappings

17. In the *Actions* pane, click *Edit Feature Permissions*….

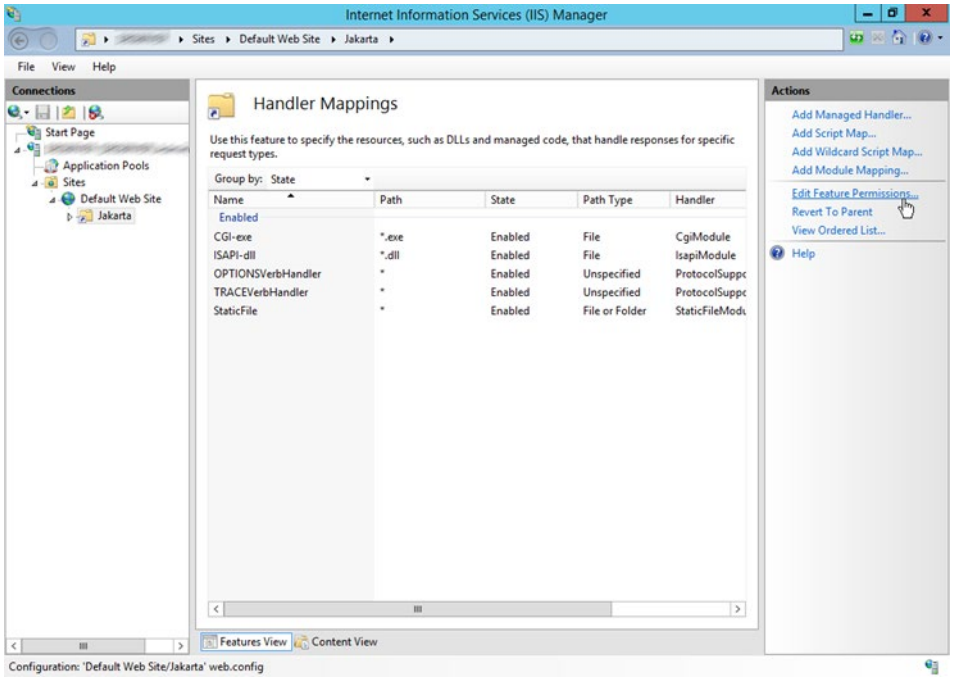

Fig. 12: Edit Feature Permissions

18. Make sure that all check boxes are ticked as you need the right to execute scripts.

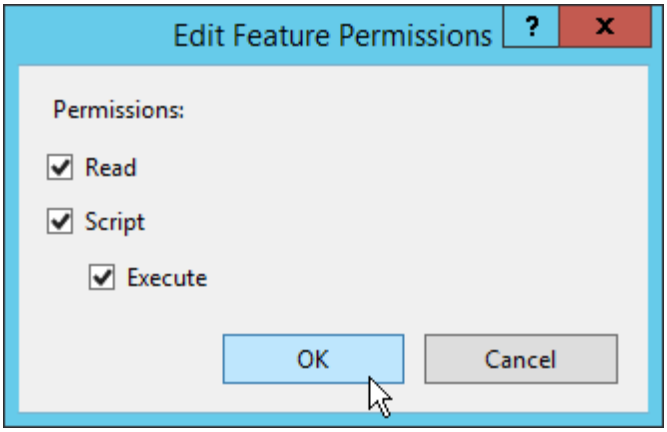

Fig. 13: Select all check boxes

19. In the *Actions* pane, click *Add Module Mapping*….

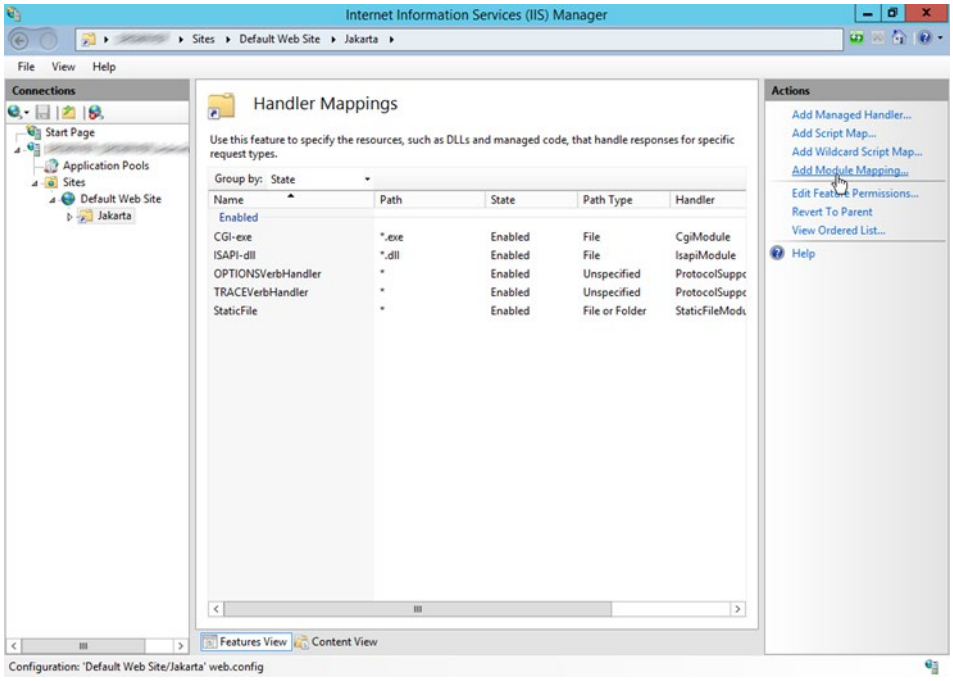

Fig. 14: Add Module Mapping

20. Type the file name extension `*.dll` in the *Request path* box. Click *IsapiModule* in the *Module* drop-down list. Set *Executable (optional)* to the physical location of the `isapi_redirect.dll`. Choose a *Name* for the module mapping.

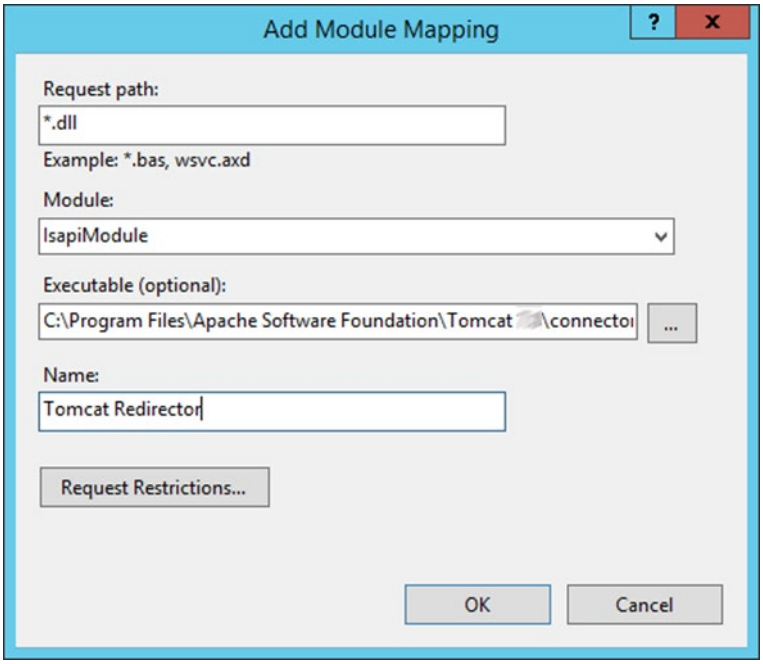

Fig. 15: Add Module Mapping II

21. To the question *Do you want to allow this ISAPI extension?*, click *Yes*.

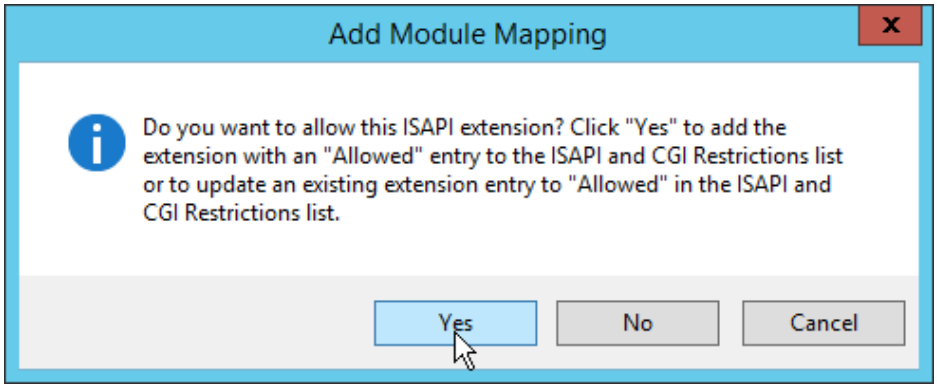

Fig. 16: Add Module Mapping III

22. In the *Connections* pane, select the root element. In the *Home* pane, open *Feature Delegation*.

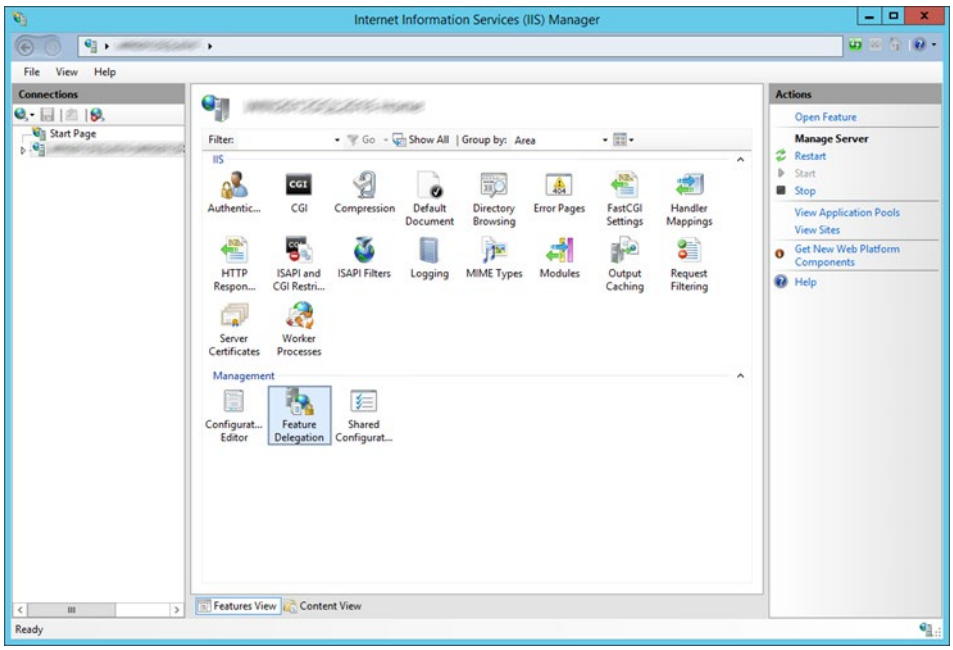

Fig. 17: Open Feature Delegation

23. Make sure that the default delegation state for *Handler Mappings* is *Read/Write*.

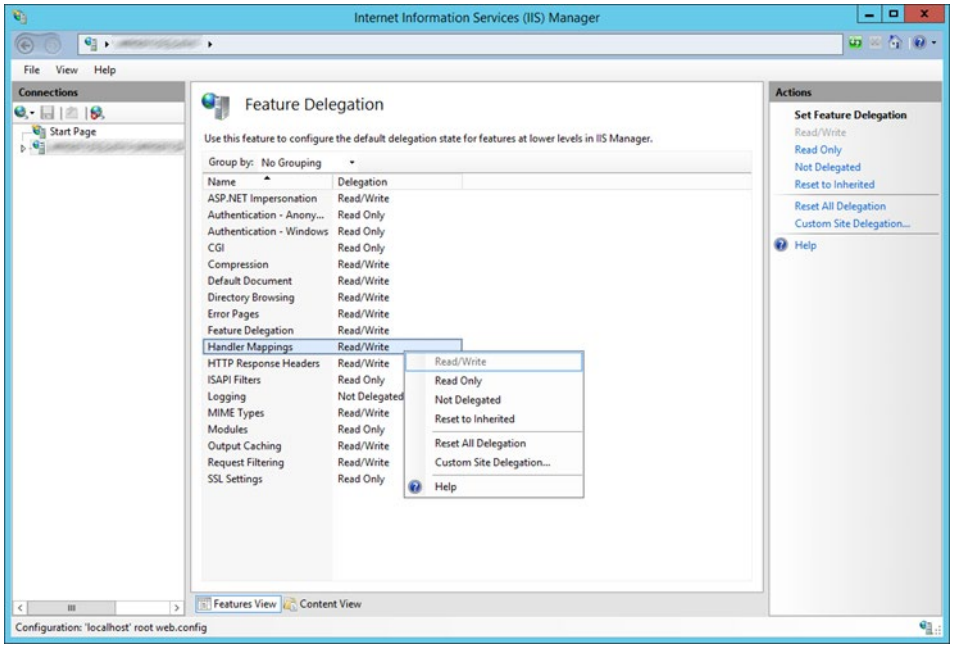

Fig. 18: Set the default delegation state for the feature "Handler Mappings" to "Read/Write"

24. Select the virtual directory *Jakarta* in the *Connections* pane. In the *Home* pane, open *Authentication*.

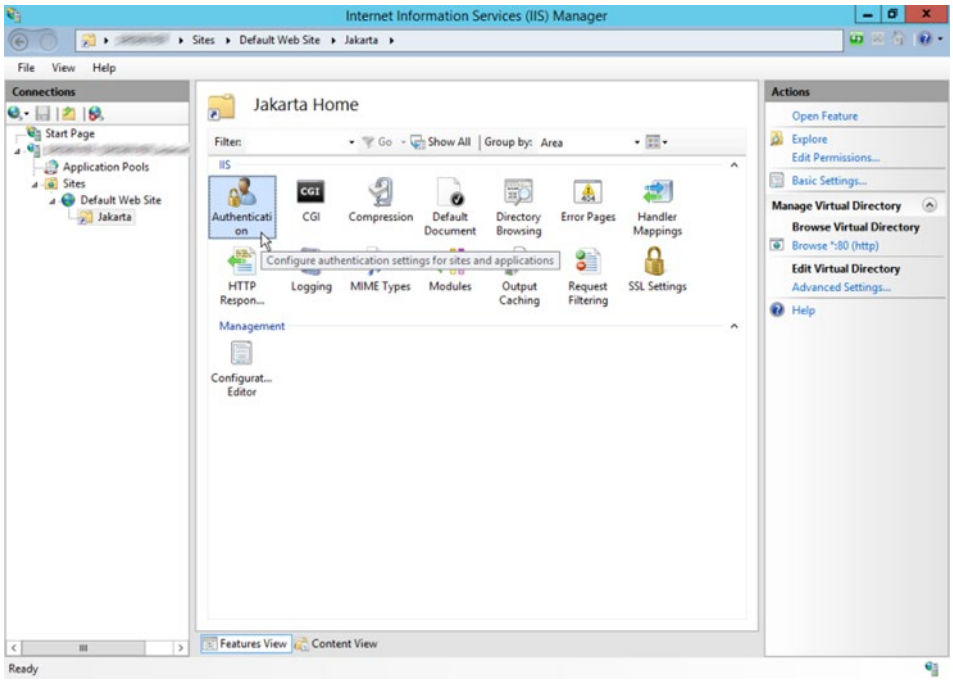

Fig. 19: Open Authentication

25. Disable everything but *Windows Authentication*:

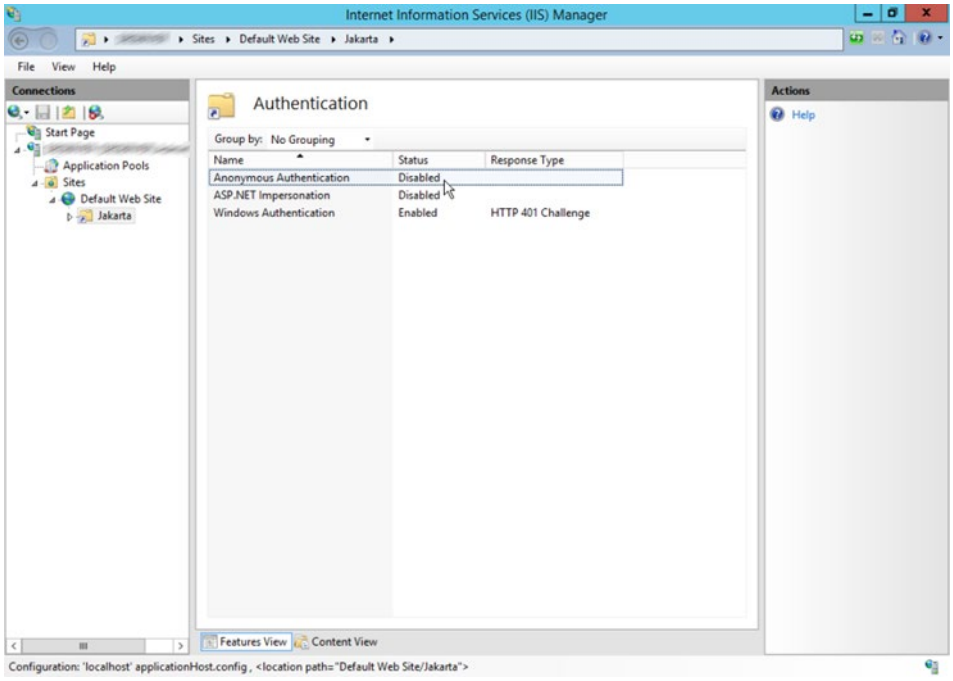

Fig. 20: Deactivate everything but "Windows Authentication"

26. Next, *Authentication* settings for the *Default Web Site* need to be created. Repeat steps **24** - **25**. Make sure to select the *Default Web Site* in the *Connections* pane before you start. On the *Authentication* page, disable everything but *Anonymous Authentication*.
27. In the *Connections* pane, select the *Default Web Site*. In the *Home* pane, open *Request Filtering*.

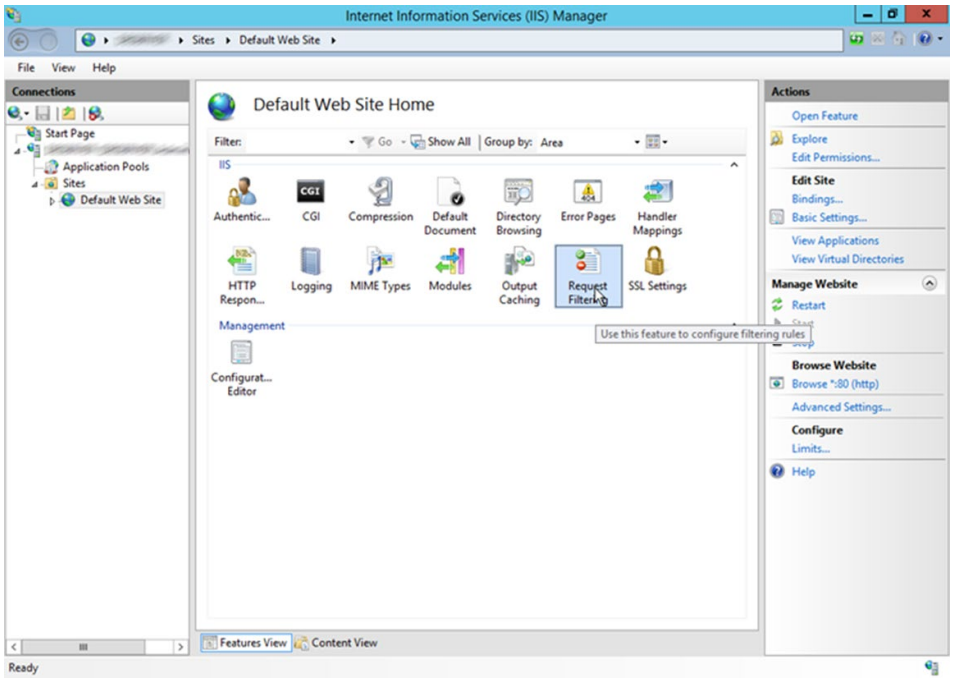

Fig. 21: Open Request Filtering

28. In the *Actions* pane, select *Edit Feature Settings*.

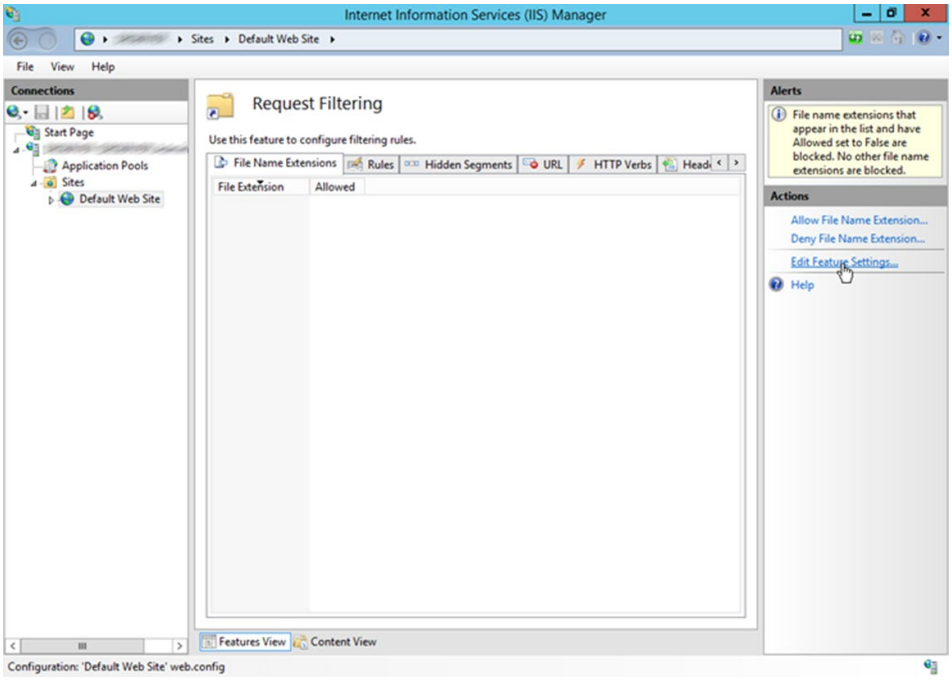

Fig. 22: Edit Feature Settings

29. Make sure that *Allow double escaping* is allowed. Set *Maximum allowed content length (Bytes)* to the maximum size of data that IIS should accept, such as for file uploads. To calculate the value in bytes, use the formula `1 MB = 1.048.576 bytes`. For example, to allow the import of a 100 MB migration package, set the value to *104857600* bytes. Confirm your changes with *OK*. These settings will automatically apply to the virtual directory *Jakarta* as well, unless they are explicitly modified there.

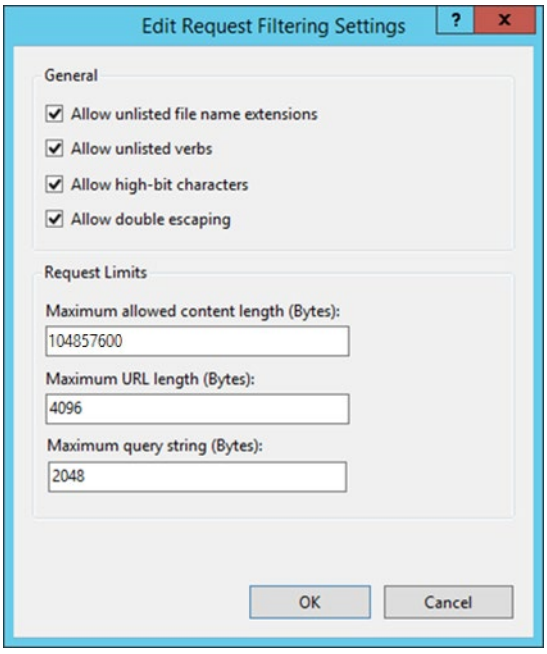

Fig. 23: Edit Request Filtering Settings

30. In the *Connections* pane, select the root element. In the *Home* pane, open *Application Request Routing Cache*.

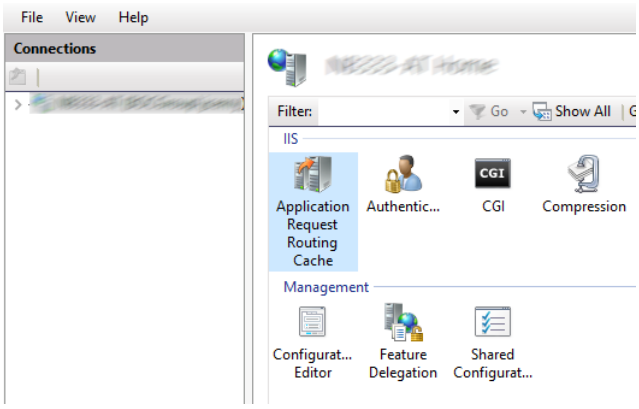

Fig. 24: Open Application Request Routing Cache

31. In the *Actions* pane, select *Server Proxy Settings*.

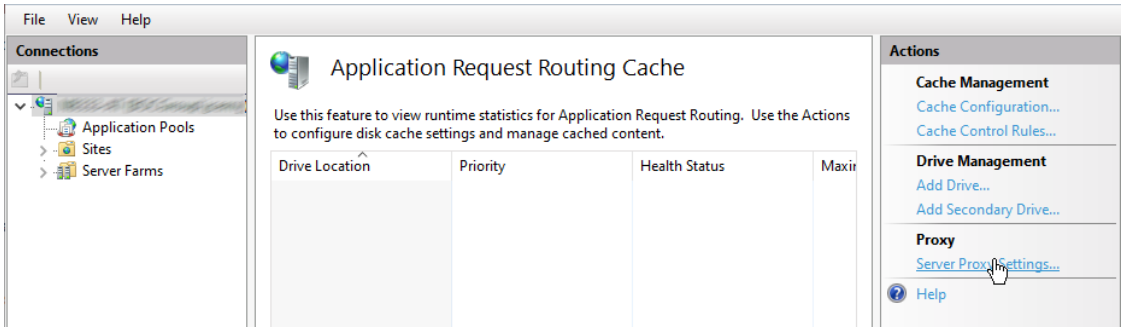

Fig. 25: Select Server Proxy Settings

32. Select *Enable proxy*. Under *Custom Headers*, disable *Include TCP port from client IP*. Leave the other settings unchanged. Confirm with *Apply*.

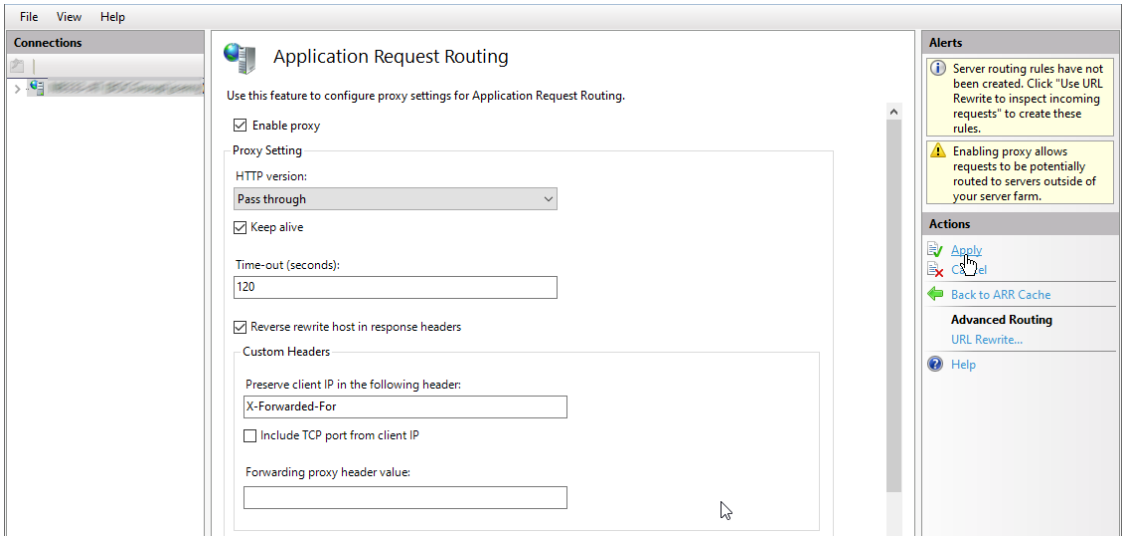

Fig. 26: Select Enable Proxy and Apply

33. In the *Connections* pane, select the *Default Web Site*. In the *Home* pane open *URL Rewrite*.

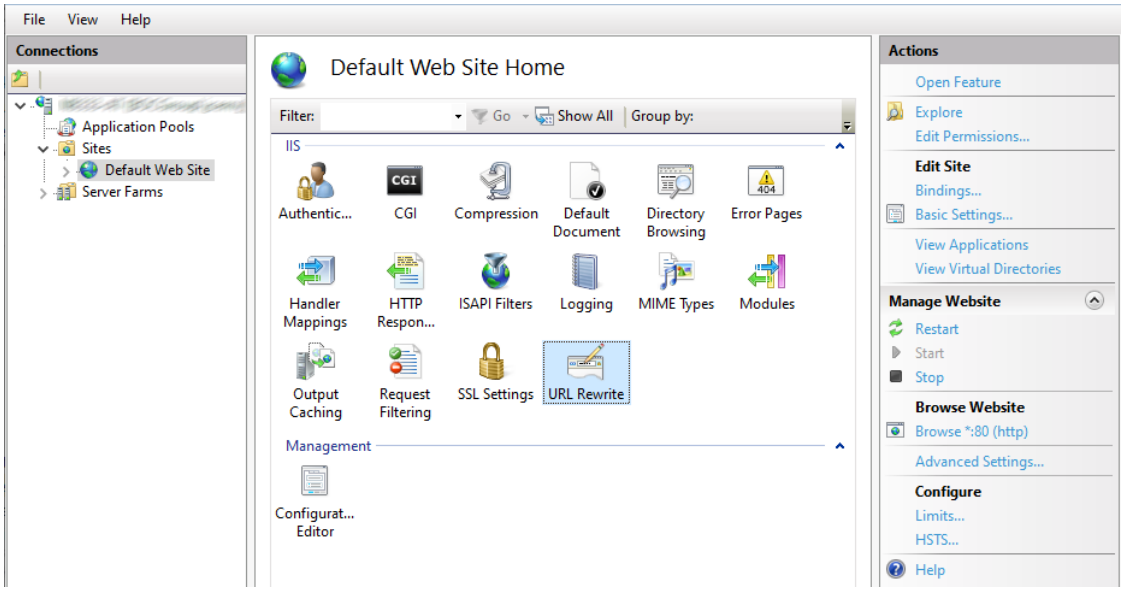

Fig. 27: Open URL Rewrite

34. In the *Actions* pane, select *Add Rule(s)*.

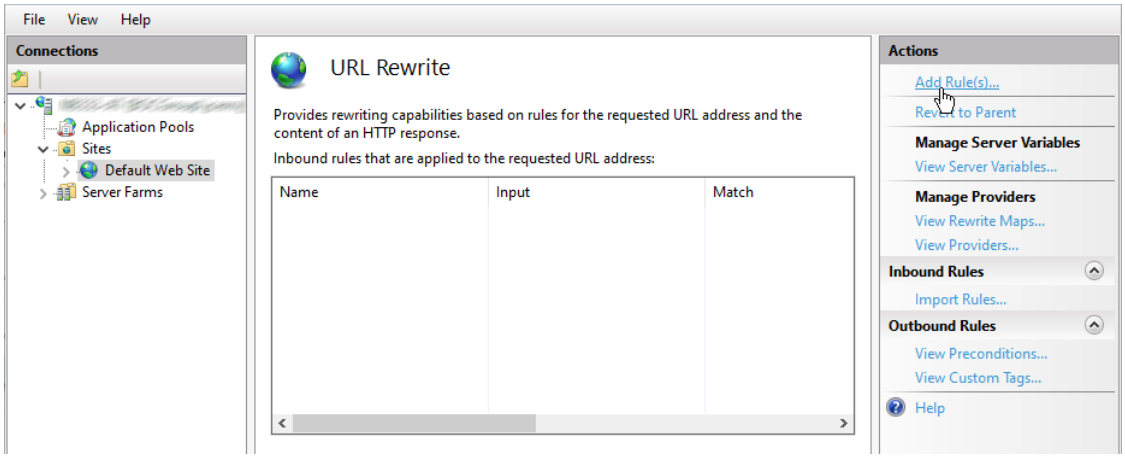

Fig. 28: Select Add Rule(s)

35. Now, an inbound rule for REST requests needs to created so those specific requests are not processed with the AJP protocol and Windows authentication, but directly forwarded via HTTP to Tomcat. Select *Blank rule* and confirm with *OK*.

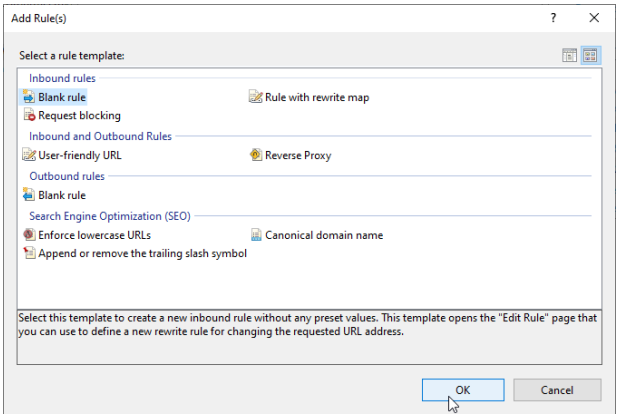

Fig. 29: Select Blank Rule and OK

36. Enter a name for the new rule, such as "*REST to Tomcat*". From the *Using* list, select *Wildcards*. In the *Pattern* box, enter `ADO*/rest/*` if the web application is in a specific path or `rest/*` if the web application is deployed as the ROOT web application. Under *Action Properties*, in the *Rewrite URL* box, enter the Tomcat URL, including the protocol, host, and port, followed by `{PATH_INFO}` which dynamically appends the path after the host and port. For example, for a local Tomcat setup with the HTTP/1.1 connector port set to "8000", the URL would be: `http://localhost:8000{PATH_INFO}`. Confirm with *Apply,* and then click *Back to Rules*.

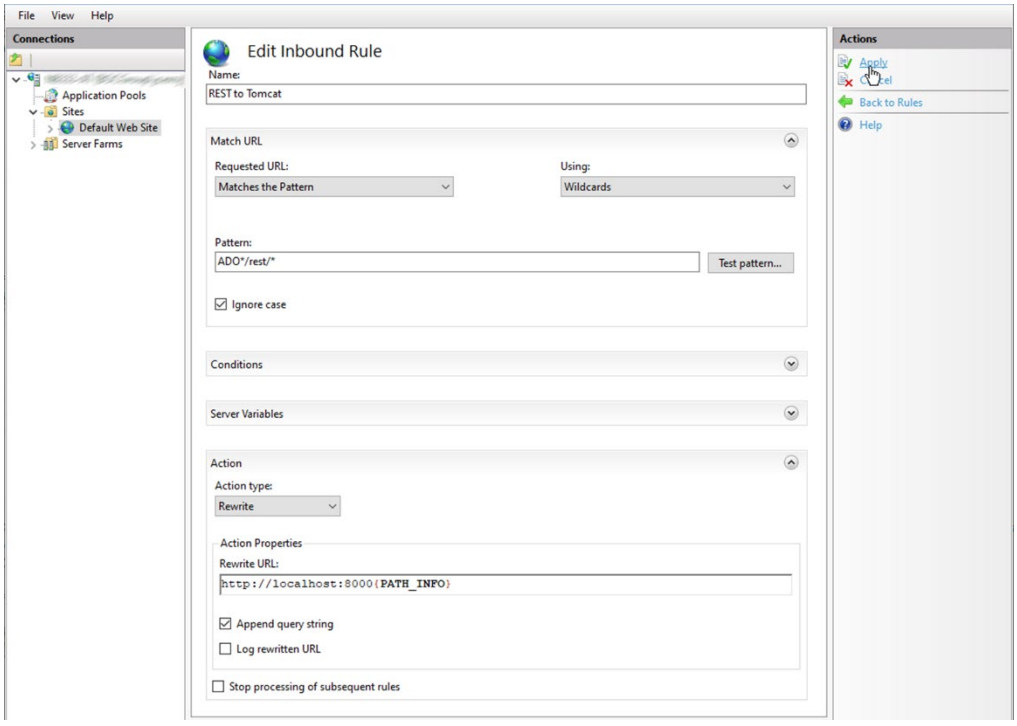

Fig. 30: Edit REST Rule

37. Next, inbound rules for OAuth2 and WebSocket need to be created. Repeat steps **34** - **36** and enter the following data:
    - **OAuth2 rule**: *Name* e.g. "*OAuth2 to Tomcat*". For *Using*, select *Wildcards*. For *Pattern*, enter `ADO*/oauth2/*` or `oauth2/*` if the web application is deployed as ROOT. For *Rewrite URL*, enter the Tomcat URL followed by `{PATH_INFO}`.
    - **WebSocket rule**: *Name* e.g. "WebSocket *to Tomcat*". For *Using*, select *Wildcards*. For *Pattern*, enter `ADO*/websocket` or `websocket` if the web application is deployed as ROOT. For *Rewrite URL*, enter the Tomcat URL followed by `{PATH_INFO}?_axx_socket_fwd=true`.

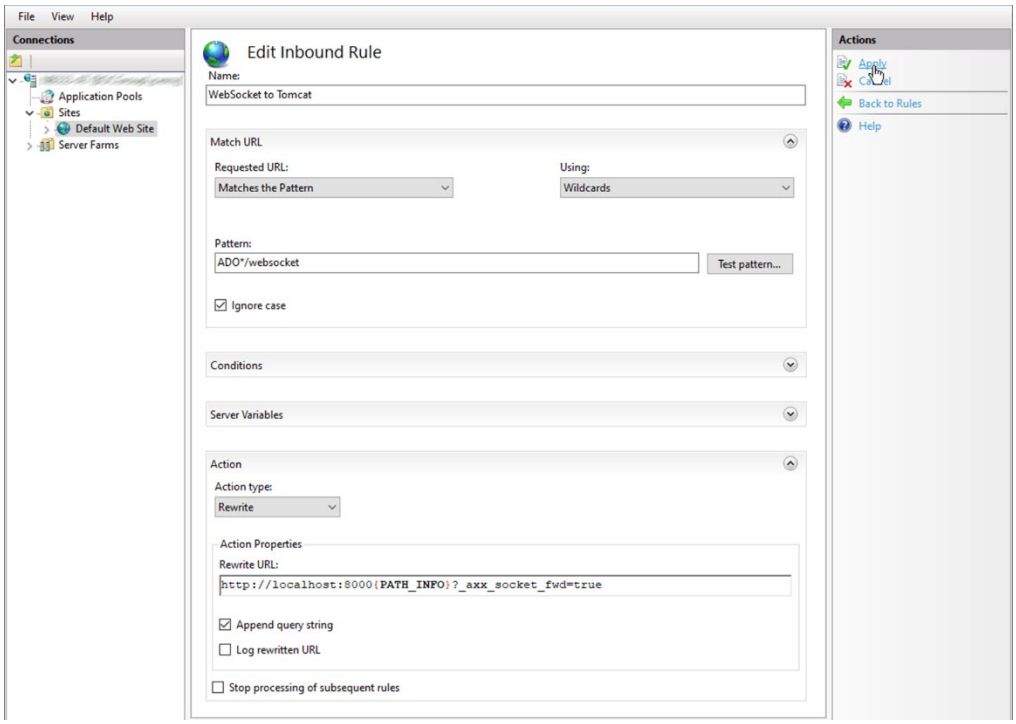

Fig. 31: Edit OAuth2 and WebSocket Rules

IIS is now configured and can be used as reverse proxy for Tomcat.

38. To finalize the configuration, restart IIS. Select the root folder in the *Connections* pane. In the *Action* pane, click *Restart*.
39. Also restart Tomcat.

6 Adapt Authentication Configuration of the Web Application

The setup of for a BOC Management Office® product using Windows authentication and IIS requires the configuration of certain connection parameters and directory service specific properties in the *Administration*:

1. Enter the URL where the BOC Management Office® product is available, click *Administration*, enter your credentials and log in.

Note: The user must have access rights to the "Administration Toolkit" component.

2. Go to *Authentication* > *Connectors*, and then click *Create*.
3. In the *ID* box, enter a unique name for your connector.
4. From the *Select type* list, select *IDM*.
5. Click *Create*. Once you have created the connector, you can start working on the configuration right away.
6. On the IDM connector's *Properties* page, modify the following parameters:
   - Make sure the *Crop the domain extension of the remote username* check box is selected.
   - In the *Regular expression to replace strings in the username with another string* box, enter the following regular expression: "^.*\\" (without the quotation marks). This cuts the domain identifier from the passed user name because the login procedure only takes user names without domain names. By specifying this, the user name "<DOMAIN NAME>\user" becomes just "user ".

Note: We assume that the users that we want to log in are in one domain, so the usernames that are passed to the BOC Management Office® product by IIS will e.g. be "<DOMAIN NAME>\user", "<DOMAIN NAME>\test" etc.

7. On the IDM connector's *User mapping* page, modify the following parameters:
   - Under *Roles*, specify the *Default roles* that should be assigned to automatically created users (**variant 2**). Define any number of such elements.
   - Under *Groups*, specify the *Default groups* that should be assigned to automatically created users (**variant 2**). If none of the user groups exists, users are assigned to the standard group.
   - Under Repositories, specify the *Baseline assignments* i.e. repositories that will be automatically assigned to every user.
   - Under *Synchronize user*, set *Create user automatically* as follows:

- Disable this option if you set up the users manually in the Administration (**variant 1**)
- Enable this option if users should be created on-the-fly in the database when they log in for the first time (**variant 2**).

8. Click *OK* to return to the *Connectors* page.
9. Find the IDM connector and select the *Connector enabled* check box.
10. Use the drag handle (☰) to move the IDM connector to the top of the list, prioritising it as the primary authentication mechanism.

IDM-based authentication is now activated and will be used as the default connector. The standard connector ("Standard Login", the standard login page) is activated as well and can be used in case that additional constraints are defined for the IDM connector. Do not disable the standard connector.

Note: In this chapter, we focus on the minimum essential parameters needed for IDM authentication setup. For a comprehensive overview of all configurable parameters, please refer to the "Authentication" chapter in the Administration Help.

For instance, the login process can be configured to support a hybrid approach with multiple connectors, allowing specific connectors only for requests originating from certain IP addresses. Additionally, LDAP properties can be mapped to BOC Management Office® product user groups and system roles, enabling the assignment of tailored permissions based on the user's role and department within the organisation. The IDM connector must be configured to use LDAP coupling in this case.

Done! Restart the Apache Tomcat web server. For users logged in with their domain accounts in a domain which the IIS service can access, SSO is now supported.

7 Using the Reverse Proxy to Automatically Log In to the BOC Management Office® Product

Prerequisites

The following prerequisites must be met so that a user can log in to the BOC Management Office® product using Windows authentication and IIS:

- IIS must be reachable for all users that should have access to the BOC Management Office® product.
- IIS must have access to the user management component (e.g. Active Directory).
- The web browser must be configured to send the login credentials of the currently logged in users to IIS. This works out of the box for Google Chrome and Microsoft Edge. For other browsers the browser configuration needs to be adapted.

Login

In order to access the BOC Management Office® using Windows authentication and IIS:

- Navigate to "*http://localhost/<PRODUCT><VERSION>*" (again, no port as IIS is running on port 80).

The currently logged in Windows user should be directly logged in to the BOC Management Office® product.

If you set up the users manually in the Administration (**variant 1**), a user with a name exactly matching the name of the Windows user must exist in the database. *Trusted login* needs to be enabled for this user.

If users should be created on-the-fly in the database when they log in for the first time (**variant 2**), a new user is created automatically. The mapping of user attributes (group assignment etc.) is synchronized on each subsequent login.

8 Frequently Asked Questions

The log file for the ISAPI redirector *isapi_redirect.log* is not created. What should I do?

Specify a path without blanks, e.g. create a new folder “C:\Temp”, and then adapt the path to the log file in the file `isapi_redirect.properties` accordingly.

How can I deploy the web application as the ROOT application

1. Stop the Apache Tomcat web server.
2. Remove the folder *\webapps\ROOT* in the Tomcat installation directory.
3. Rename the WAR file to ROOT.war.
4. In the file `uriworkermap.properties`, remove the name of the web application:

```
/* = myworker

/*/* = myworker
```

5. Restart IIS and the Apache Tomcat web server.