



Version 5.10

SSO - IIS

Manual

Document: **Manual - SSO - IIS**

Created: **2017-02-20**

Last changes: **2019-10-31**

Author: **AEgilmez**



COPYRIGHT 2019 BY **FORCAM GMBH**, D-88214 Ravensburg
ALL RIGHTS RESERVED. COPY OR TRANSLATION, ALSO IN EXTRACTS
ONLY WITH WRITTEN PERMISSION BY FORCAM GMBH

Content

1	Concept	3
1.1	General	3
1.2	Solution in FORCAM FORCE™	4
2	IIS	6
2.1	Overview	6
2.2	Installation & Configuration of ISAPI Redirector	6
2.3	Screenshots to Illustrate the IIS Configuration	9
3	Internet Explorer	10
4	FFWorkbench Tomcat	11
5	Localizing the FF.....	13
6	Appendix	14

1 Concept

This document describes the configuration of the Internet Information Server (IIS) and the Internet Explorer (IE) client browser required to integrate the FORCAM FORCE™ (FF) application into an SSO environment.

The configuration described has been tested with IIS Version 7.0 under Windows 2012 Server Enterprise Edition.

1.1 General

With the Single Sign-on procedure (SSO), a user authenticates himself at a Network PC and can then access all computers and services for which he is locally authorized at the same PC. It is no longer necessary to log in each time. If the user changes PCs, authentication and authorization are cancelled.

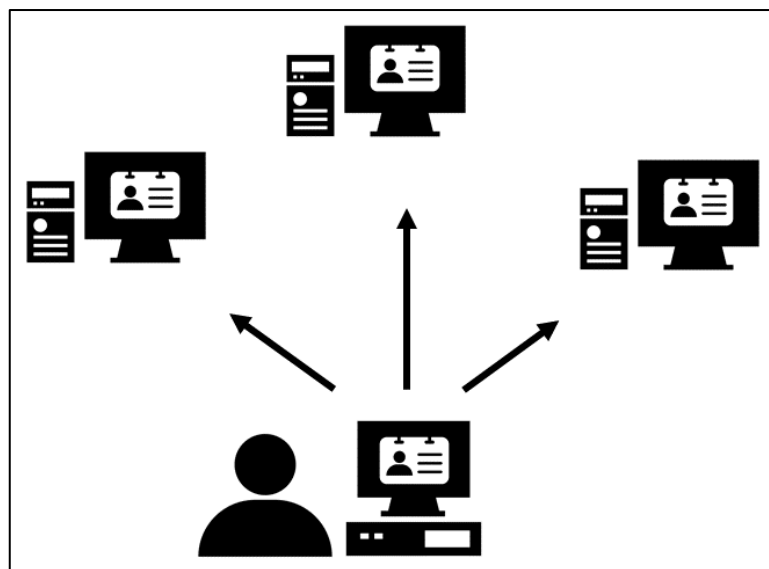


Fig. 1: Principle of Single sign-on

- Ticket system:
Exchanging tickets that identify a user (and services as well as computers)
→ Kerberos (also used in MS AD)
- Portal:
Portal assigns a characteristic to the user that identifies him for the services in Portal.

Authentication is always done through the infrastructure.

1.2 Solution in FORCAM FORCE™

The architecture of SSO is structured as follows:

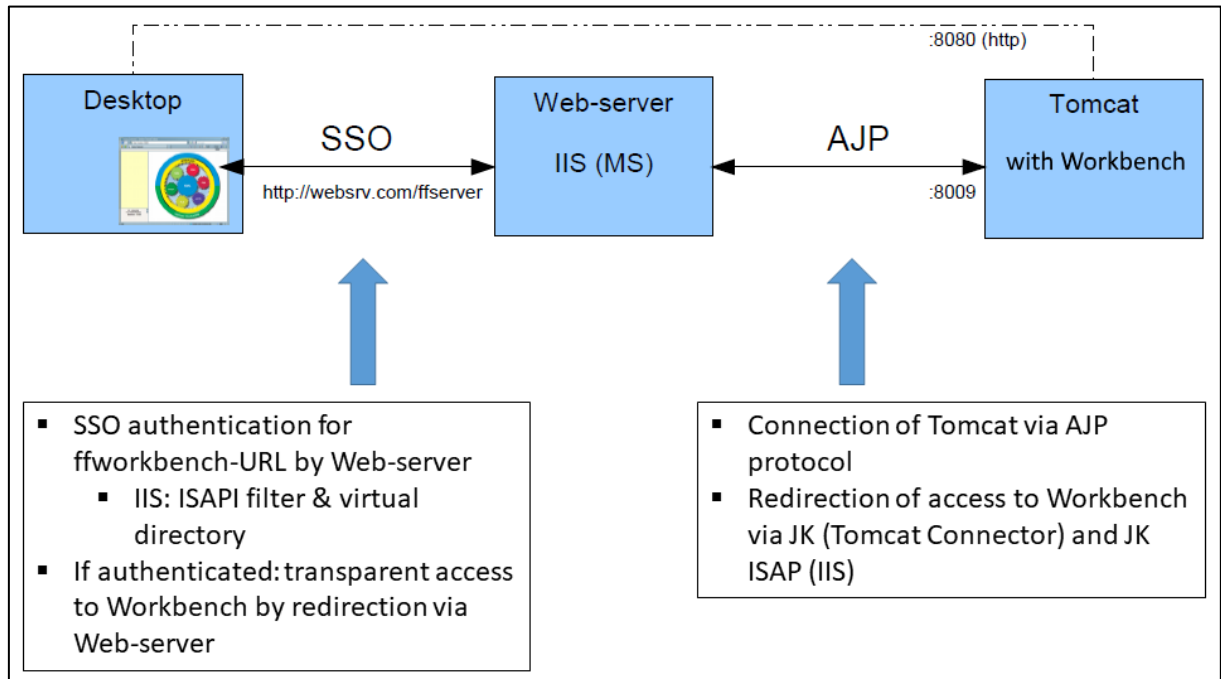


Fig. 2: Overview of the SSO architecture

SSO and ffworkbench:

- AD & IIS
 - IIS is integrated in AD. AD provides the necessary services (Kerberos etc.).
 - Due to domain membership or valid AD login, a desktop client is automatically able to use the SSO functionality → IWA.
 - IIS serves as an authenticator and realizes SSO communication through IWA (ffworkbench is not involved).
 - If authentication is successful, IIS serves as a redirector to Tomcat running ffworkbench.
- REMOTE_USER
 - No IIS is required here. A specific HTTP header is set by a portal environment (such as Sideminder). This usually contains a user name that is already authenticated. This information is used by the Workbench to skip the login. The corresponding user must exist in the local user administration.

Logon scenarios fffoffice:

Table 1: Logon scenarios for fffoffice

With SSO	
Against local user administration	<ul style="list-style-type: none"> External user authentication No logon screen, no password locally maintained User must be maintained simultaneously in local user administration Authorization (permissions & roles) by default No logoff available
Against external directory (AD or LDAP)	<ul style="list-style-type: none"> External user authentication No logon screen, no password locally maintained User does not exist in local user administration Authorization (roles) via customer-specific mapping External groups - Internal roles No logoff available
Without SSO	
Against local user administration (default)	<ul style="list-style-type: none"> Local user authentication Logon screen, password locally maintained User maintained in local user administration Authorization (permissions & roles) by default
Against external directory (AD or LDAP)	<ul style="list-style-type: none"> External user authentication Logon screen, no password locally maintained User does not exist in local user administration Authorization (roles) via customer-specific mapping External groups - Internal roles

2 IIS

2.1 Overview

- IIS is integrated into an AD. The AD provides the services required for SSO. With the AD domain membership and/or valid AD login data and an appropriate IE configuration, client PCs can automatically use the SSO functions → IWA (Integrated Windows Authentication).
- IIS serves as an authenticator handling the complete SSO communication based on an appropriate configuration by means of IWA (see sketch of architecture). This process takes place exclusively between the client (IE) and the IIS.
- When a client is successfully authorized for a specific web site or the virtual directory (FF-URL), IIS uses a web service extension to operate as a redirector for the underlying web application FF under a Tomcat Servlet Container.



IIS Requirements

- IIS requires the ISAPI redirector web service extension (plugin) – (the IIS notation is ISAPI filter).
- Virtual directory in the IIS for the associated FF-URL (for redirect). Its parametrization with the ISAPI filter and IWA directory security.
- Linking Tomcat via AJP protocol is achieved by an appropriately parametrized worker (process).

2.2 Installation & Configuration of ISAPI Redirector

1. Load the required files into a suitable directory which can be accessed by the IIS, for example, C:\Inetpub\ff_redirect. An appropriate ZIP file containing the files is available; these are the individual files:
 - isapi_redirect.dll
 - isapi_redirect.properties
 - uriworkermap.properties
 - workers.properties
2. Adjust the configuration files with the extension ***.properties** to the local circumstances. The entries that usually need to be adjusted appear on a yellow background, the other entries can normally be left as they are as shown in the example.

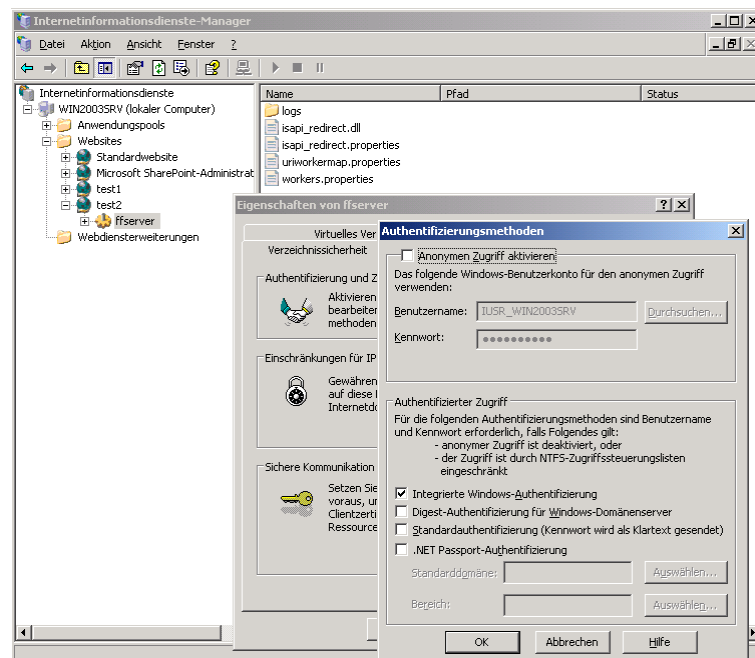
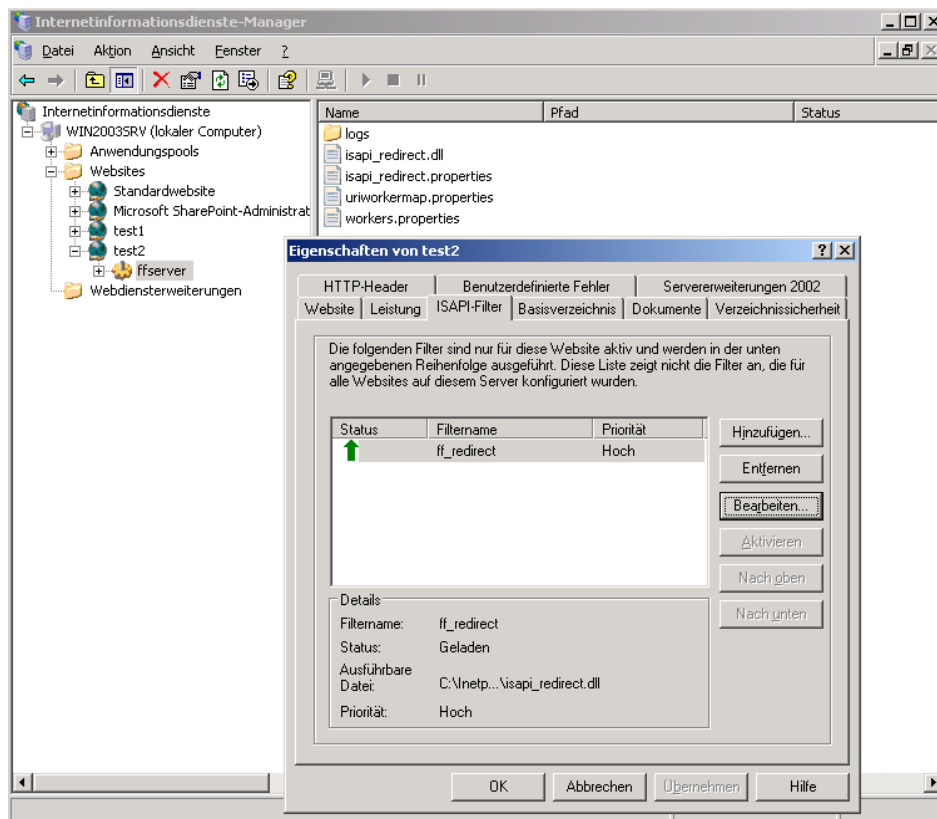
The attributes of the various files are as follows:

File: isapi_redirect.properties
extension_uri=/ffserver/isapi_redirect.dll The <i>ffserver</i> part of the path must be exactly identical with the name of the virtual IIS directory.
log_file=c:\inetpub\ff_redirect\logs\ff_redirect.log Specifies a user-defined path for the log file.
log_level=info  Higher log levels may produce huge log files and have a negative impact on performance. Hence, it is recommended to set warn or info in productive operations.
worker_file=c:\inetpub\ff_redirect\workers.properties Specify the appropriate path.
worker_mount_file=c:\inetpub\ff_redirect\uriworkermapping.properties Specify the appropriate path.
File: uriworkermapping.properties
/ffserver/*=ajp13 Mapping of the FF-URL to the Tomcat Worker, i.e. the process performing the Redirect operation.  The URL to be passed must match the virtual directory name in the IIS.
File: workers.properties Note: The entries for the Tomcat Worker must match those of the AJP Connector in the <i>server.xml</i> file of Tomcat.
worker.list=ajp13 Specifies the Tomcat Worker.
worker.ajp13.port=8009 Port of Tomcat with FF. 8009 is the default.
worker.ajp13.host=claudius_2.ibb.local Host address of Tomcat with FF. The FQDN must be specified accordingly.
worker.ajp13.type=ajp13 Specifies the protocol.

- In the IIS Manager, set up a virtual directory for Redirect to FF. It is recommended to set up a separate web site for Redirect to FF (in the example, test2). However, it is also possible to create the virtual directory in an existing web site.
Specify an alias, e.g. *ffserver* (must match *extension_uri* from *isapi_redirect.properties*). The path refers to the directory of 1., i.e. C:\inetpub\ff_redirect. Assign access rights, i.e. **Read**, **Execute Scripts** and **Execute**.
- In the IIS Manager, define *isapi_redirect.dll* from 1. as an ISAPI filter for the test2 web site. Enter a filter name, for example, **ff_redirect**. The executable file refers to *isapi_redirect.dll* from 1.


5. In the IIS Manager, define the ISAPI filter as a new web service extension. Enter an extension name, for example, **ff_redirect**. Specify isapi_redirect.dll from 1. as the required file. Set the extension status to **Valid**.
6. Make sure that the host address of Tomcat with FF is available to the IIS (DNS lookup, etc.). If this is not ensured, the ISAPI filter cannot be started correctly. The log file shows any related notes.
Restart the IIS service. The ISAPI filter of the relevant web site must have a green status arrow.
7. You can now test the fundamental function of routing by IIS to Tomcat with FF initially without SSO. For this purpose, enter the appropriate URL in the browser, i.e. in this example <DN_IIS>:<Port_IIS_Website>/ffworkbench. The FF login page appears.
8. Set up the SSO functions for FF routing. In the IIS Manager, go to the properties of the virtual directory, deselect **Anonymous Access** on the **Directory Security** tab and select **Integrated Windows Authentication** instead.
Set up the client browser for SSO; see the section on "Internet Explorer". A user accessing the system is now implicitly authenticated by SSO and the FF start page appears.

2.3 Screenshots to Illustrate the IIS Configuration



3 Internet Explorer

The IE must be parametrized with the relevant URL for using SSO (FF Redirect-URL). Authentication is negotiated implicitly for the URL specified in this way when called.

-  If these parameters should not be set, usually a lower-level procedure (NTLM) is used in Windows.

Activating IWA (SSO):

1. Go to Internet Options>Extended>Security and select **Integrated Windows authentication**.
2. Go to Internet Options>Security (Local Intranet)>Sites>Extended and add the FF-URL (via web server) to the zone.

4 FFWorkbench Tomcat

In order for SSO to work with the FFWorkbench Tomcat, the following steps are necessary:

1. Move the JAR file named **common-modules.jndi-X.X.X*.jar** from "ffworkbench-tomcat\webapps\ffworkbench\WEB-INF\lib" to "ffworkbench-tomcat\lib".
 ⚠ The file must not exist anymore in "ffworkbench-tomcat\webapps\ffworkbench\WEB-INF\lib". Otherwise there will be errors with SSO.
2. Extend the **context.xml** file with the following entry:
`<ResourceLink global="forcam/ffoffice/auth" name="forcam/ffoffice/auth" type="com.forcam.na.common.jndi.JNDIMap"/>`
3. Extend the **server.xml** file within **GlobalNamingResources** with the following entry (Attribute Description in Table 2):

```
<Resource description="user authentication"
type="com.forcam.na.common.jndi.JNDIMap"
factory="com.forcam.na.common.jndi.JNDIMapFactory"
name="forcam/ffoffice/auth"
```

```
mode="AUTH_EXTERNAL_AD"
```

```
provider_url_1="ldap://192.168.1.2:389"
base_dn_1="dc=ibb,dc=ad"
user_suffix_1="ibb.ad"
query_user_name_1="query"
query_user_pwd_1="query"
```

```
provider_url_2="ldap://192.168.1.2:389"
base_dn_2="dc=xy,dc=org"
user_suffix_2="ou=users,dc=xy,dc=org"
query_user_name_2="query"
query_user_pwd_2="query" />
```

With the variant **REMOTE_USER**, the last two blocks are not necessary (provider_url_1 to query_user_pwd_2). The following mode must be defined for this variant:

```
mode="AUTH_LOCAL_ONLY"
```

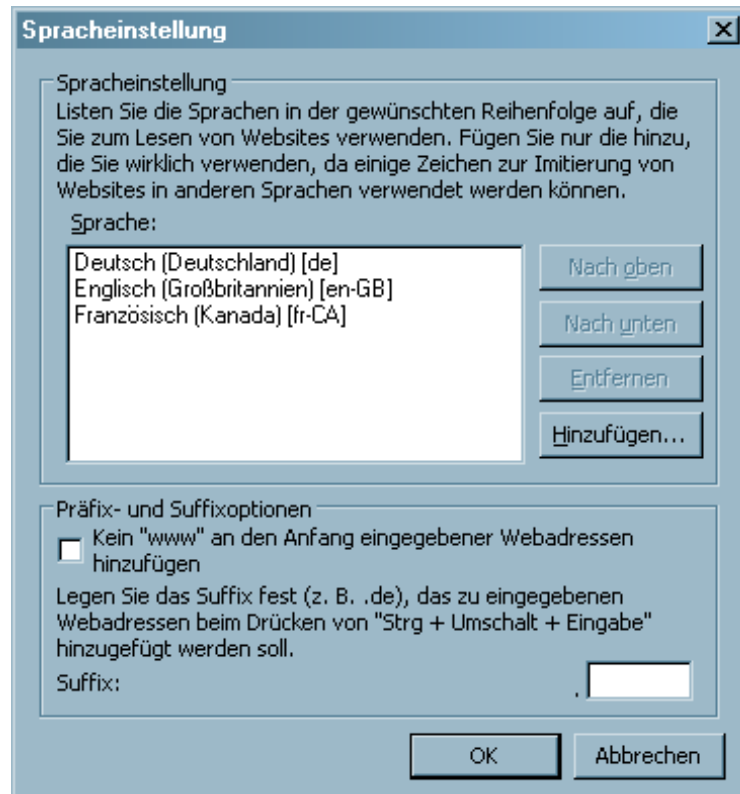
4. Enter the following statement in FO_MD_PARAMETERS:
`INSERT INTO FO_MD_PARAMETERS (TERMINAL, PARAGRAPH, PARAMETER, IDX, DATA) VALUES('SYSTEM', 'FDM', 'ASGMTS_HIERARCHY_ID', 0, HIBERNATE-ID);`
 Replace "HIBERNATE-ID" in this statement by the hibernate ID of the hierarchy to be used (must be determined from FF_MD_WORKPLACE_HIERARCHY).

Table 2: Description of the Attributes of server.xml

Attribute	Description
description, type, factory, name	Fixed attributes that are obtained automatically
mode	<p>Specifies the authentication mode. Possible values are:</p> <ul style="list-style-type: none"> — AUTH_LOCAL_ONLY – Default (auth. against FF-internal user administration) SSO is also possible here. The user was then externally authenticated, but must also be maintained in the local user administration simultaneously. Standard is without SSO. — AUTH_EXTERNAL_LDAP – auth. against external LDAP directory service (user only maintained externally), with and without SSO — AUTH_EXTERNAL_AD – auth. against external AD- directory service (user only maintained externally), with and without SSO
provider_url_1	First authentication server: full URL of the first server
base_dn_1	Complete Base DN specification for first authentication server
user_suffix_1	Qualification of the user name (suffix). Specification for first authentication server
query_user_name_1	Account for read-only access to directory service. Only necessary in SSO environment. User name of the query user
query_user_pwd_1	Account for read-only access to directory service. Only necessary in SSO environment. Password of the query user

5 Localizing the FF

The dialog language in FF for the user logged in is selected automatically according to the language set as the preference in the IE. The first language definition corresponding to a system language available in the FF will be selected. Specify the desired languages in Extras>Internet Options>General>Languages. Initially the local language of the operating system is set there. If a suitable language is not found, the standard language (German) is set.



6 Appendix

Table 3: Abbreviations used

Abbreviation	Description
AJP/JK	Apache JServ Protocol: Forwards incoming requests from a web server to an application server behind it
DN	Domain Name
FF	FORCAM FORCE™
IE	Internet Explorer
IIS	Internet Information Service: Set of Internet-based services for servers using Microsoft Windows
ISAPI	Internet Server API: Redirector for IIS
IWA	Integrated Windows Authentication: With Integrated Windows Authentication the user name and password are hashed before being sent across the network
LDAP	Lightweight Directory Access Protocol: standard protocol for directory services
(MS) AD	(Microsoft) Active Directory: Directory service from Microsoft. Allows you to organize a network according to the real structure of the company or its geographical distribution
NTLM	NT Lan Manager: Suite of Microsoft security protocols
SSO	Single Sign-on: access to all available services after one-time authentication (rights assumed)