FORCAM™ FORCE

Version 5.10

SSO - IIS

Handbuch

Dokument:	**Handbuch - SSO - IIS**
Erstellt:	**20.02.17**
Letzte Änderung:	**30.09.19**
Autor:	**AEgilmez**

Inhaltsverzeichnis

1 Konzept 3
1.1 Allgemein 3
1.2 Lösung in FORCAM FORCE™ 4
2 IIS 6
2.1 Überblick 6
2.2 Installation & Konfiguration ISAPI Redirector 6
2.3 Screenshots zur Verdeutlichung der IIS-Konfiguration: 9
3 Internet Explorer 10
4 FFWorkbench-Tomcat 11
5 Lokalisierung des FF 13
6 Anhang 14

1 Konzept

Dieses Dokument beschreibt die notwendige Konfiguration des Internetinformationsdienstes und des Client Browsers Internet Explorer, um damit FORCAM FORCE™ in eine SSO-Umgebung einzubinden. Die beschriebene Konfiguration wurde mit IIS Version 6.0 unter Windows 2003 Server Enterprise Edition getestet.

1.1 Allgemein

Bei dem Single Sign-on-Verfahren (SSO) authentifiziert sich ein Benutzer an einem Netzwerk-PC und kann anschließend auf alle Rechner und Dienste, für die er lokal autorisiert ist, am selben PC zugreifen. Er muss sich dabei nicht mehr jedes Mal neu anmelden. Wechselt der Benutzer den PC, werden Authentifizierung und Autorisierung aufgehoben.

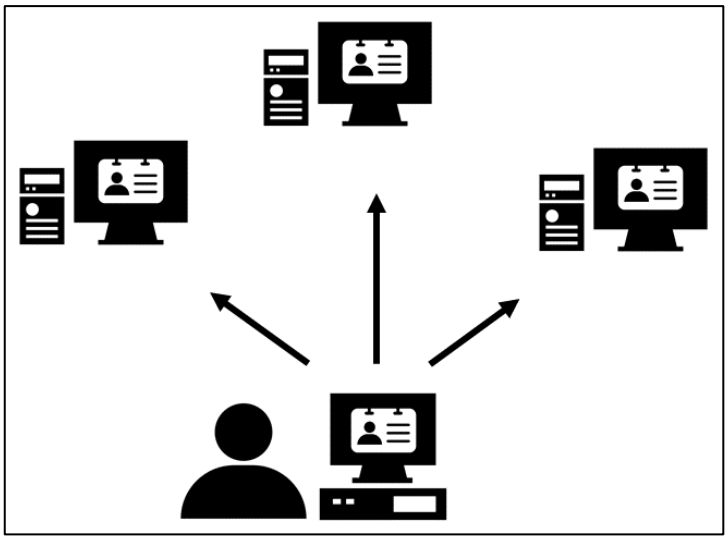


Bild 1: Prinzip des Single Sign-on

- Ticketsystem:
  Austausch von Tickets, die einen Benutzer (und Dienste sowie Rechner) identifizieren
  → Kerberos (auch in MS AD genutzt)
- Portal:
  Durch Portal wird dem Benutzer ein Merkmal vergeben, das ihn gegenüber den Diensten im Portal ausweist.

Die Authentifizierung erfolgt immer durch die Infrastruktur.

1.2 Lösung in FORCAM FORCE™

Die Architektur von SSO ist folgendermaßen aufgebaut:

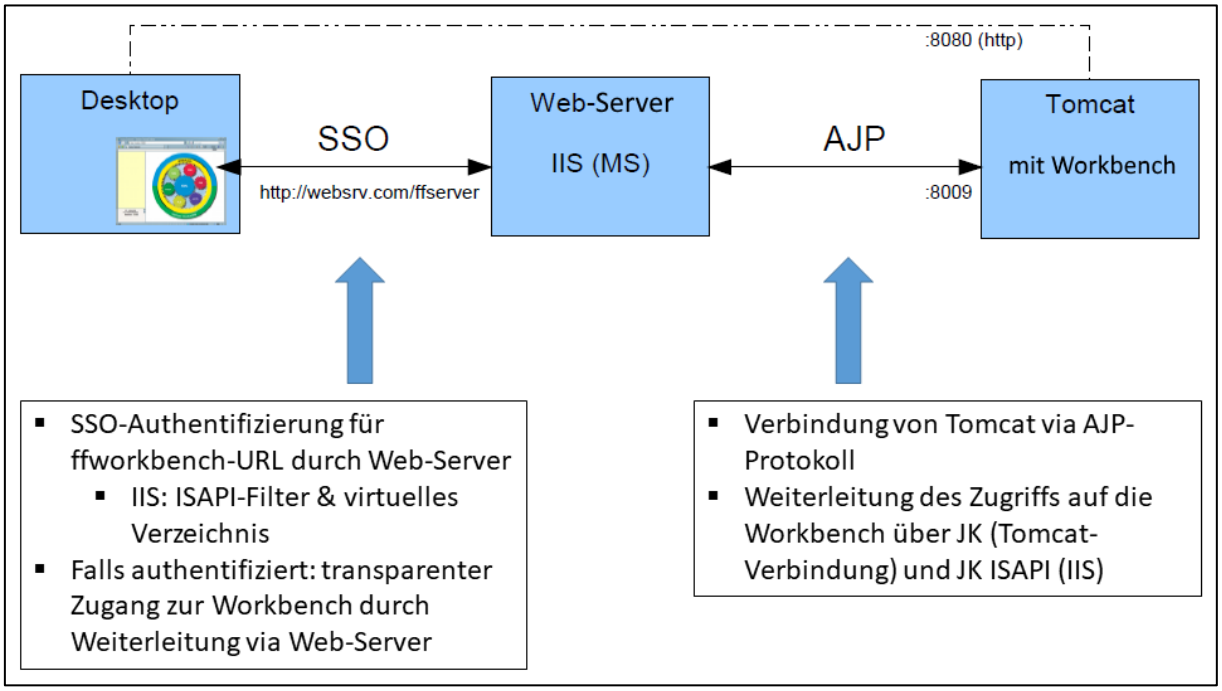


Bild 2: Überblick der SSO-Architektur

SSO und ffworkbench:

- AD & IIS
  - IIS ist integriert in AD. AD stellt nötige Dienste zur Verfügung (Kerberos etc.).
  - Aufgrund von Domainzugehörigkeit bzw. gültigem AD-Login ist ein Desktop-Client automatisch in der Lage, die SSO-Funktionalität zu nutzen → IWA.
  - IIS dient als Authentifikator und setzt die SSO-Kommunikation durch IWA um (ffworkbench ist daran nicht beteiligt).
  - Bei erfolgreicher Authentifizierung dient IIS als Weiterleitung zu Tomcat, auf dem ffworkbench läuft.
- REMOTE_USER
  - Hier ist kein IIS notwendig. Ein spezifischer HTTP-Header wird von einer Portalumgebung eingesteuert (z.B. Sideminder). Darin ist üblicherweise ein Benutzername hinterlegt, der bereits authentifiziert ist.
    Diese Information wird von der Workbench genutzt, um den Login zu überspringen. Der entsprechende Benutzer muss dazu in der lokalen Benutzerverwaltung vorhanden sein.

Logon-Szenarien ffoffice:

Tabelle 1: Logon-Szenarien für ffoffice

Mit SSO	
Gegen lokale Benutzerverwaltung	– Externe Benutzerauthentifizierung – keine Logon-Maske, kein Passwort lokal gepflegt – Benutzer muss parallel in lokaler Benutzerverwaltung gepflegt sein – Autorisierung (Rechte & Rollen) standardmäßig – Kein Logoff vorhanden
Gegen externes Verzeichnis (AD oder LDAP)	– Externe Benutzerauthentifizierung – keine Logon-Maske, kein Passwort lokal gepflegt – Benutzer ist in lokaler Benutzerverwaltung nicht vorhanden – Autorisierung (Rollen) via kundenspezifischer Zuordnung Externe Gruppen – Interne Rollen – Kein Logoff vorhanden
Ohne SSO	
Gegen lokale Benutzerverwaltung (Standard)	– Lokale Benutzerauthentifizierung – Logon-Maske, Passwort lokal gepflegt – Benutzer in lokaler Benutzerverwaltung gepflegt – Autorisierung (Rechte & Rollen) standardmäßig
Gegen externes Verzeichnis (AD oder LDAP)	– Externe Benutzerauthentifizierung – Logon-Maske, kein Passwort lokal gepflegt – Benutzer ist in lokaler Benutzerverwaltung nicht vorhanden – Autorisierung (Rollen) via kundenspezifischer Zuordnung Externe Gruppen – Interne Rollen

2 IIS

2.1 Überblick

- IIS ist in ein AD integriert. Das AD stellt die notwendigen Dienste für SSO zur Verfügung. Aufgrund der AD Domänenmitgliedschaft bzw. gültiger AD Logindaten und entsprechender IE-Konfiguration können Client-PCs automatisch die SSO Funktionalität nutzen → IWA (Integrierte Windows-Authentifizierung).
- IIS dient als Authentikator, der die gesamte SSO-Kommunikation aufgrund entsprechender Konfiguration mithilfe von IWA abwickelt (siehe Architekturskizze). Dieser Vorgang findet ausschließlich zwischen dem Client (IE) und dem IIS statt.
- Ist ein Client für die betreffende Website bzw. das virtuelle Verzeichnis (FF-URL) erfolgreich authentifiziert, wirkt IIS mithilfe einer Webdiensterweiterung als Redirektor für die dahinterliegende Webanwendung FF unter einem Tomcat Servlet-Container.

Voraussetzungen IIS

- IIS benötigt die Webdiensterweiterung (Plug-in) ISAPI-Redirector (die IIS Notation lautet ISAPI-Filter).
- Virtuelles Verzeichnis in IIS für die entsprechende FF-URL (zum Redirect). Parametrierung desselben mit dem ISAPI-Filter, sowie mit Verzeichnissicherheit IWA
- Ankopplung des Tomcat via AJP-Protokoll erfolgt durch einen entsprechend parametrierten Worker(-Prozess)

2.2 Installation & Konfiguration ISAPI Redirector

1. Einspielen der notwendigen Dateien in ein passendes Verzeichnis, auf das IIS Zugriff hat, beispielsweise nach *C:\Inetpub\ff_redirect*. Ein entsprechendes ZIP mit den Dateien steht zur Verfügung. Die Dateien sind im Einzelnen:
   - isapi_redirect.dll
   - isapi_redirect.properties
   - uriworkermap.properties
   - workers.properties.
2. Gegebenenfalls Anpassen der Konfigurationsdateien ***.properties** an örtliche Gegebenheiten. Die üblicherweise anzupassenden Attribute sind gelb hinterlegt. Alle Weiteren können, dem Beispiel gemäß, in der Regel so belassen werden.

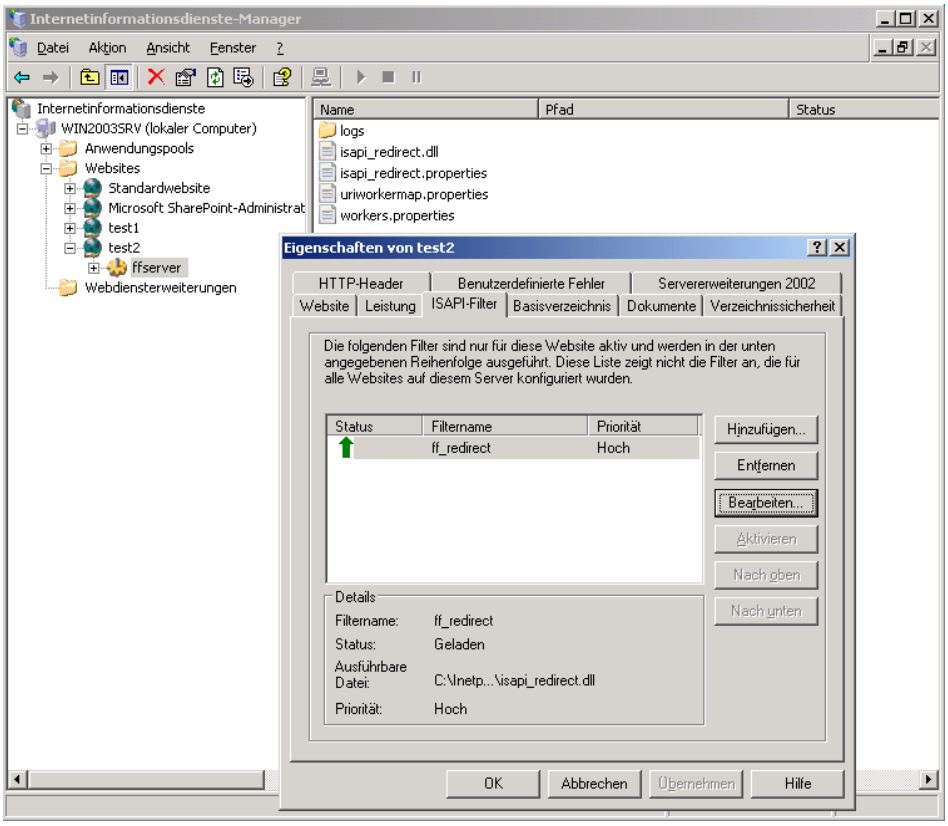
Die Attribute der einzelnen Dateien lauten wie folgt:

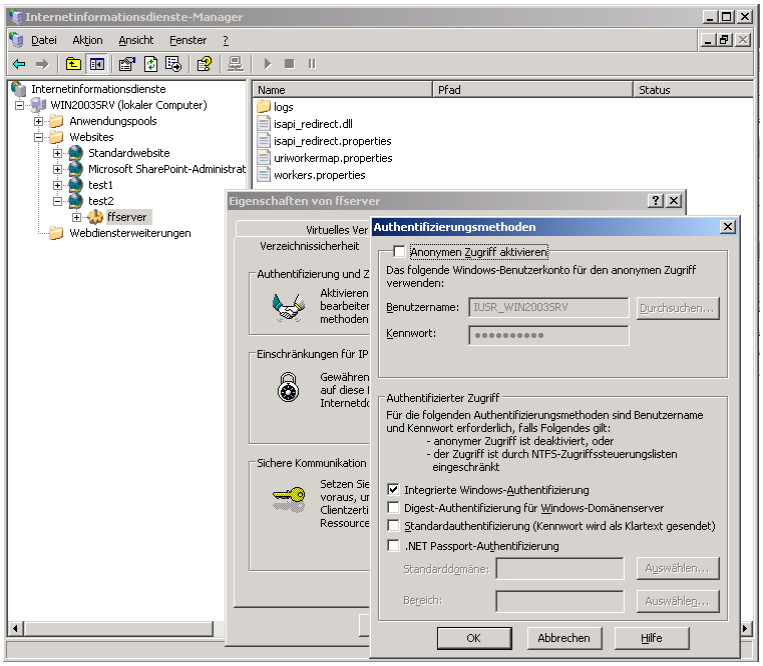
Datei isapi_redirect.properties
extension_uri=/ffserver/isapi_redirect.dll Die Teil-Pfadangabe *ffserver* muss exakt dem Namen des virtuellen IIS-Verzeichnisses entsprechen.
log_file=c:\inetpub\ff_redirect\logs\ff_redirect.log Angabe eines beliebigen Pfades für die Logdatei
log_level=info ⚠ Höhere Loglevel verursachen u.U. riesige Logdateien und beeinflussen die Performance negativ. Im Produktivbetrieb daher **warn** oder **info** einstellen.
worker_file=c:\inetpub\ff_redirect\workers.properties Entsprechenden Pfad angeben
worker_mount_file=c:\inetpub\ff_redirect\uriworkermap.properties Entsprechenden Pfad angeben
Datei uriworkermap.properties
/ffserver/*=ajp13 Zuweisung der FF-URL auf den Tomcat-Worker, also den Prozess, der das Redirect vornimmt. ⚠ Die weiterzuleitende URL muss dem virtuellen Verzeichnisnamen in IIS entsprechen.
Datei workers.properties ⓘ Die Angaben zum Tomcat-Worker müssen denen des AJP-Connectors in der Datei *server.xml* des Tomcat entsprechen.
worker.list=ajp13 Angabe des Tomcat-Workers
worker.ajp13.port=8009 Port des Tomcat mit FF. 8009 ist Standard.
worker.ajp13.host=claudius_2.ibb.local Hostadresse des Tomcat mit FF. Der FQDN muss entsprechend angegeben werden.
worker.ajp13.type=ajp13 Angabe des Protokolls

3. In der IIS Mgmt Konsole ein virtuelles Verzeichnis zum Redirect an FF einrichten. Es wird empfohlen, für den Redirect an FF eine separate Website einzurichten (im Beispiel *test2*). Genauso gut kann das virtuelle Verzeichnis aber auch in einer bestehenden Website angelegt werden.
   Als Aliasname beispielsweise *ffserver* angeben (muss der `extension_uri` aus *isapi_redirect.properties* entsprechen). Der Pfad zeigt auf das Verzeichnis von 1., also auf *C:\Inetpub\ff_redirect*. Als Zugriffsrechte **Lesen**, **Skripts ausführen** und **Ausführen** vergeben.
4. In der IIS Mgmt Konsole die *isapi_redirect.dll* aus 1. als ISAPI-Filter für die Website *test2* anlegen. Als Filtername beispielsweise **ff_redirect** vergeben. Die ausführbare Datei zeigt auf *isapi_redirect.dll* aus 1.

5. In der IIS Mgmt Konsole den ISAPI-Filter als neue Webdiensterweiterung anlegen. Als Erweiterungsname beispielsweise **ff_redirec** vergeben. Als erforderliche Datei *isapi_redirect.dll* aus 1. angeben. Erweiterungsstatus auf **Zugelassen** setzen.
6. Sicherstellen, dass die Host-Adresse des Tomcat mit FF durch IIS erreichbar ist (DNS Auflösung etc.). Ist dies nicht der Fall, kann der ISAPI-Filter nicht korrekt gestartet werden. Die Logdatei gibt entsprechende Hinweise.
   IIS Service neu starten. Der ISAPI-Filter der entsprechen Website muss als Status einen grünen Pfeil aufweisen.
7. Die grundsätzliche Funktion der Weiterleitung durch IIS an den Tomcat mit FF kann nun, zunächst noch ohne SSO, getestet werden. Hierzu im Browser die entsprechende URL eingeben, im Beispiel also *<DN_IIS>:<Port_IIS_Website>/ffworkbench*. Die FF Loginseite erscheint.
8. SSO-Funktionalität für die FF Weiterleitung einrichten. In der IIS Mgmt Konsole in den Eigenschaften des virtuellen Verzeichnisses unter dem Reiter **Verzeichnissicherheit** den **Anonymen Zugriff** deselektieren. Dafür den **Authentifizierten Zugriff IWA** einstellen.
   Den Client-Browser für SSO einrichten, siehe Kapitel Internet Explorer. Bei Zugriff wird der Benutzer nun via SSO implizit authentifiziert. Die Startseite des FF erscheint.

2.3 Screenshots zur Verdeutlichung der IIS-Konfiguration:





3 Internet Explorer

Der IE muss für die gewünschte URL (FF Redirect-URL) zum Verwenden von SSO parametriert werden. Für die so vergebene URL wird die Authentifizierung beim Aufruf implizit ausgehandelt.

ⓘ Fehlt die entsprechende Parametrierung, wird unter Windows üblicherweise auf ein niederwertigeres Verfahren zurückgegriffen (NTLM).

Aktivieren der IWA (SSO):

1. Unter Internetoptionen>Erweitert>Sicherheit **Integrierte Windows Authentifizierung aktivieren** auswählen.
2. Unter Internetoptionen>Sicherheit (Lokales Intranet)>Sites>Erweitert die FF-URL (über Webserver) zur Zone hinzufügen.

4 FFWorkbench-Tomcat

Damit SSO mit dem FFWorkbench-Tomcat funktioniert, müssen folgende Punkte beachtet werden:

1. Die JAR-Datei **common-modules.jndi-X.X.X*.jar** von „ffworkbench-tomcat\webapps\ffworkbench\WEB-INF\lib“ nach „ffworkbench-tomcat\lib“ verschieben.

   ⚠ Die Datei darf nicht mehr unter „ffworkbench-tomcat\webapps\ffworkbench\WEB-INF\lib“ vorhanden sein. Andernfalls erfolgen Fehler beim SSO.
2. **Context.xml** um folgenden Eintrag erweitern:
   <ResourceLink global="forcam/ffoffice/auth" name="forcam/ffoffice/auth"
   type="com.forcam.na.common.jndi.JNDIMap"/>
3. **Server.xml** um folgenden Eintrag innerhalb von **GlobalNamingResources** erweitern (Beschreibung der Attribute in Tabelle 2):
   <Resource description="user authentification"
   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" />

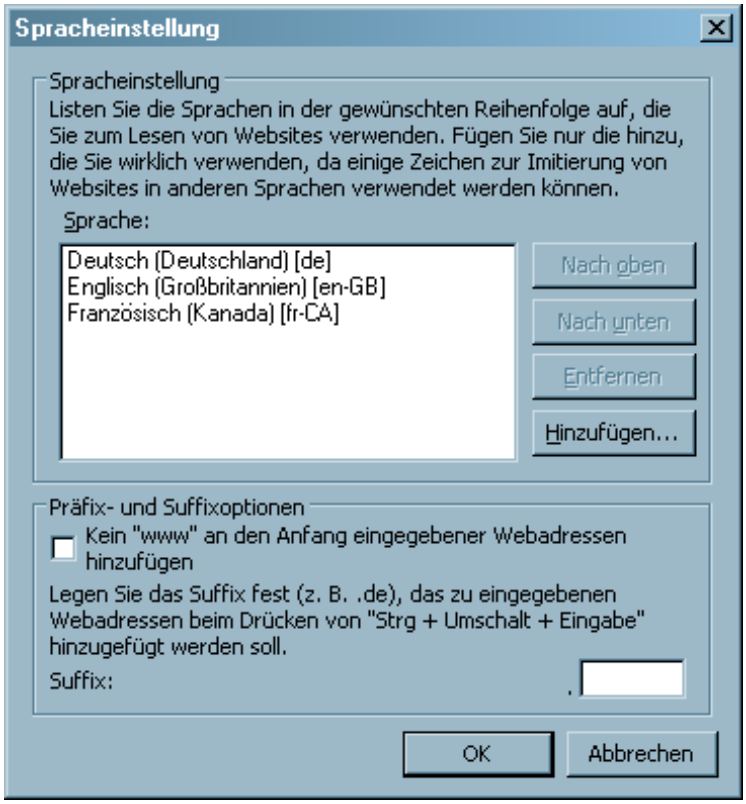
   Bei der Variante **REMOTE_USER** sind die beiden letzten Blöcke nicht notwendig (provider_url_1 bis query_user_pwd_2). Bei dieser Variante muss folgender Modus definiert werden: mode="AUTH_LOCAL_ONLY"
4. Folgendes Statement in FO_MD_PARAMETERS eintragen:
   INSERT INTO FO_MD_PARAMETERS (TERMINAL, PARAGRAPH, PARAMETER, IDX, DATA)
   VALUES('SYSTEM', 'FDM', 'ASGMTS_HIERARCHY_ID', 0, **HIBERNATE-ID**);
   Die Hibernate-ID muss dabei durch die Hibernate-ID der Hierarchie ersetzt werden, die verwendet werden soll (muss aus FF_MD_WORKPLACE_HIERARCHY ermittelt werden).

Tabelle 2: Beschreibung der Attribute der server.xml

Attribut	Beschreibung
description, type, factory, name	Feste Attribute, die automatisch bezogen werden
mode	Bestimmt den Authentifizierungsmodus. Mögliche Werte sind: – AUTH_LOCAL_ONLY – Default (Auth. gegen FF-eigene Benutzerverwaltung) Möglich ist hier auch SSO. Der Benutzer wurde dann extern authentifiziert, muss aber parallel entsprechend auch in der lokalen Benutzerverwaltung gepflegt sein. Standard ist ohne SSO. – AUTH_EXTERNAL_LDAP – Auth. gegen externen LDAP-Verzeichnisdienst (Benutzer ausschließlich extern gepflegt), mit und ohne SSO – AUTH_EXTERNAL_AD – Auth. gegen externen AD-Verzeichnisdienst (Benutzer ausschließlich extern gepflegt), mit und ohne SSO
provider_url_1	Erster Authentifizierungsserver: vollständige URL des ersten Servers
base_dn_1	Vollständige Base DN Angabe für ersten Authentifizierungsserver
user_suffix_1	Qualifizierung des Benutzernamens (Suffix). Angabe für ersten Authentifizierungsserver
query_user_name_1	Account für reinen Lesezugriff in Verzeichnisdienst. Nur notwendig in SSO-Umgebung. Benutzername des Query-Benutzers
query_user_pwd_1	Account für reinen Lesezugriff in Verzeichnisdienst. Nur notwendig in SSO-Umgebung. Passwort des Query-Benutzers

5 Lokalisierung des FF

Die Sprachwahl des FF für den angemeldeten Benutzer erfolgt automatisch gemäß der im IE als präferiert angegeben Sprache. Die erste zu einer im FF vorhandenen Systemsprache passende Sprachdefinition wird gewählt. Die gewünschten Sprachen müssen unter Extras>Internetoptionen>Allgemein>Sprachen angegeben werden. Standardmäßig ist dort zunächst die lokale Sprache des Betriebssystems eingestellt.
Kann keine passende Sprache gefunden werden, wird die Standardsprache (Deutsch) eingestellt.



6 Anhang

Tabelle 3: Verwendete Abkürzungen

Abkürzung	Erklärung
AJP/JK	Apache JServ Protocol: leitet ankommende Anfragen eines Webservers zu einem dahinterliegenden Applikationsserver weiter
DN	Domain Name
FF	FORCAM FORCE™
IE	Internet Explorer
IIS	Internetinformationsdienst: Satz von internetbasierten Diensten für Server unter Verwendung von Microsoft Windows
ISAPI	Internet Server API: Redirector für IIS
IWA	Integrierte Windows-Authentifizierung: Benutzername und Kennwort werden vor dem Senden über das Netzwerk mit einem Hash versehen.
LDAP	Standard-Protokoll für Verzeichnisdienste
(MS) AD	(Microsoft) Active Directory: Verzeichnisdienst von Microsoft. Ermöglicht es, ein Netzwerk entsprechend der realen Struktur des Unternehmens oder seiner räumlichen Verteilung zu gliedern
NTLM	NT Lan Manager: Suite von Microsoft-Sicherheitsprotokollen
SSO	Single Sign-on: Zugriff auf alle verfügbaren Dienste nach einmaliger Authentifizierung (Rechte vorausgesetzt)