About these Instructions

<table>
<thead>
<tr>
<th>Document number and language version</th>
<th>000000-2240-366-AddGA03-GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>4.2</td>
</tr>
<tr>
<td>Date</td>
<td>101117</td>
</tr>
</tbody>
</table>

Scope

These Instructions for Use apply to FORUM Hospital IT Integration Module, version 2.0, and to the 4.2 version of FORUM.

Information about the manufacturer

Carl Zeiss Meditec AG
Goeschwitzer Str. 51-52
07745 Jena
Germany

E-mail: info.meditec@zeiss.com
Internet: www.zeiss.com/med

Subject to changes in design and the scope of delivery, as well as further technical developments. Printed in Germany.

© Carl Zeiss Meditec AG 2017
Chapter overview

Introduction 3
Single Sign On - Active Directory / Kerberos 5 4
Configuring LDAP and LDAPS 12
Introduction

This document covers the implementation of Windows Kerberos v5 based Single Sign On and the usage of an LDAP server as the authentication server for FORUM users.

The two methods are based upon fundamentally different principles and are not interdependent in any manner. While the LDAP implementation is connecting to the LDAP/AD server to query for user, groups and authentication, the SSO implementation never directly communicates with the LDAP/AD server. It is important to understand this to begin with.
In a Microsoft Active Directory environment, Kerberos is already used for many scenarios where authentication is required without the end user noticing it. For example, the end user can access shared folders and files without the need to enter credentials again after initially logging in to the Windows session. Here is a basic explanation of this concept.

- The user enters their username and password to login to Windows. Windows automatically requests a TGT (tickets granting ticket) from the AS (authentication service) which is part of the AD controller. Along with the TGT, the user receives an encrypted “session” key which can be decrypted by the user and the TGS (ticket granting service) which is also part of the AD controller. The TGT is only valid for a defined amount of time (e.g. 8 hours). The Ticket Granting Ticket is cached locally in the user profile and can be inspected by issuing the klist command in the command prompt.

- The user starts the FORUM Viewer which contacts the FORUM Server and is forced to authenticate using Kerberos. The FORUM Viewer uses the Windows SSP Interface to request an HTTP “service” ticket authenticating with the users TGT. The TGS issues a service ticket which can be decrypted with the key of the FORUM server and sends it back to the user. In Microsoft’s Kerberos implementation, the service ticket also contains the information of all group memberships of a user in the PAC (Privilege Account Certificate).

- The FORUM Viewer sends the service ticket to the FORUM server which can decrypt it and read the PAC content. Based on the PAC content and the role mapping in the configuration file of the FORUM server, access is either denied or granted by performing a string comparison. The group membership with the highest privileges is applied if the string comparison finds multiple matches.
Licensing

Prerequisite ✓ The SSO authentication is a licensed feature and requires a license to function.

Actions • To verify if this feature is licensed, open the FORUM Viewer and check the <Help><About> dialog:

```
FORUM_GLACOMA_WORKPLACE_USER 3.0 (1)
FORUM_BETTA_WORKPLACE_USER 1.0 (1)
VNA 1.0 (UNCOUNTED)
STANDARD_HIG_REPORT 1.0 (1)
FORUM_CATARACT_WORKPLACE_ZOCALC 1.0 (1)
SSD 1.0 (UNCOUNTED)
FORUM_CATARACT_WORKPLACE_USER 1.0 (1)
FORUM_CATARACT_WORKPLACE_BASIC 1.0 (1)
F IV BASIC 1.0 (1)
GAA_INTERACTIVE_DASHBOARDS 1.0 (1)

JRI Architecture (Viewer): 64 Bit
Plugins:
FORUM Language Pack (English, United Kingdom)
```
Configuring SSO

There are two things which need to be done by the Active Directory team first: Number one is to add the HTTP service principal to the computer object where FORUM Archive is installed (see “Creating the HTTP Service Principal” on Page 6). The second step is to create four groups (security, not distribution) which will represent the four user levels from FORUM (see “Creating AD Groups” on Page 8).

Creating the HTTP Service Principal

This can either be done by going to the Attribute Editor or via command line.

Via Attribute Editor

Here is how this is achieved using the <Attribute Editor> to add the HTTP service principal using the fully qualified domain name and the host name of the server that runs FORUM Archive:

**Actions**

- Open the Active Directory Users and Computers management console as a Domain Administrator and select <View> from the menu then enable “Advanced Features”.

- Browse to the computer object where FORUM Archive is installed, open the properties of the object and select the <Attribute Editor> (only available when <Advanced Features> is enabled).
• Scroll down to the servicePrincipalName Attribute and select it, click <View> to open the Attribute properties.

• Add the HTTP service principal twice, using the hostname for the first and the fully qualified domain name (FQDN) for the second one.
Example of a service principal using the FQDN:
http/forumservername.mydomain.org
Example of a service principal using the hostname:
http/forumservername

Via Command Line
This can also be done via command line.

Actions
• Issue the setspn command with the –a parameter:
  setspn -a http/forumservername.mydomain.org forumservername
  Registering ServicePrincipalNames for CN=forumservername,
  CN=Computers,DC=mydomain,DC=org
  http/forumservername.mydomain.org
  Updated object
• Do the same using the hostname this time:
  setspn -a http/forumservername forumservername
• You can now verify the result by issuing the setspn -l forumservername
  command (list).

Creating AD Groups
The matrix below shows all of the available user groups in FORUM and the
rights associated with it. There are no requirements for the group names
which allows the groups to use the name conventions of the individual
institution.

FORUM can use up to seven groups. Four groups which represent different
sets of user rights (roles) in FORUM and an additional three groups which can
be used optionally to control access to the clinical workplaces such as the
Retina and Glaucoma workplace. Alternatively, workplace access can also be
managed by any of the users that are part of the administrators group.
The following table lists the different rights:

- ■ = available
- □ = available on a limited basis
- □ = not available

<table>
<thead>
<tr>
<th>Menu item</th>
<th>Administrator</th>
<th>Editor</th>
<th>Reader</th>
<th>EMR reader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>□</td>
</tr>
<tr>
<td>Patient Directory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document Display</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>□</td>
</tr>
<tr>
<td>Worklist</td>
<td>■</td>
<td>■</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>Patient Administration</td>
<td>■</td>
<td>■</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>DICOM Import</td>
<td>■</td>
<td>■</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>System</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Messages</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forward Documents</td>
<td>■</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>Storage Locations</td>
<td>■</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>AET Administration</td>
<td>■</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>User Administration</td>
<td>■</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>Procedure Codes</td>
<td>■</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>Configuration Administration</td>
<td>■</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>Show icons (e.g. OCT scans)</td>
<td>■</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>Workplace Administration</td>
<td>■</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
<tr>
<td>Help</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Info</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User manual</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Online help</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Logging</td>
<td>■</td>
<td>■</td>
<td>■</td>
<td>■</td>
</tr>
<tr>
<td>Upload License File</td>
<td>■</td>
<td>□</td>
<td>□</td>
<td>□</td>
</tr>
</tbody>
</table>

a) Not possible: create / delete new patient, edit patient data
b) Only viewing and editing user’s own data. No change for access to the optional “Glaucoma Workplace” software module.
c) Only available if an optional FORUM Workplace Plugin is installed.
Enabling Single Sign On

The configuration is done within the
CZM\FORUM\settings\application-sam.properties file. It is available as
application-sam.properties.template by default and needs to be renamed
once configured.

To enable Single Sign On, the authentication filter needs to be set to
"negotiate" as the first value followed by Oauth,
ForumLocalWindowsAuthentication and ForumLocalInstallation.

# use this file to override the default security settings
# to activate rename to application-sam.properties

# HTTP authentication configuration
authentication.filters.enabled=Negotiate,Oauth,
ForumLocalWindowsAuthentication,ForumLocalInstallation

The following is the definition of the values:

Negotiate = Force Kerberos authentication
Oauth = Use Oauth authentication for Workplace Services (GW, RW, etc…)
ForumLocalWindowsAuthentication = FORUM Viewer authentication running
on the FORUM server
ForumLocalInstallation = Authentication method used Service Tool on the
FORUM server
Role Mapping - SSO

Once the groups are created in Active Directory, they need to be mapped to
the user roles in FORUM. Role mapping is the configuration part where you
can assign the Active Directory groups to the FORUM roles.

In the example configuration below, the domain administrator of the
mydomain.org created four groups representing the roles in FORUM.
The groups are called AD_FORUM_ADMINS, AD_FORUM_EDITORS,
AD_FORUM_READONLY and AD_FORUM_EMRREADERS. The AD groups
need to get the "ROLE_DOMAINNAME\" prefix to match the entries in the
Kerberos ticket. To enable local administrators to be able to log in to FORUM
using the FORUM Viewer directly on the server, local user groups should be
used. The group of local Administrators has been added to the FORUM Admin-
istrators group.

# Role mapping
authentication.forum.ADMINGROUP.roles=
ROLE_MYDOMAIN\AD_FORUM_ADMINS,Administrators
authentication.forum.USERGROUP.roles=ROLE_MYDOMAIN\AD_FORUM_EDITORS
authentication.forum.RESTRICTEDUSERGROUP.roles=
ROLE_MYDOMAIN\AD_FORUM_READONLY
authentication.forum.EMRRESTRICTEDUSERGROUP.roles=
ROLE_MYDOMAIN\AD_FORUM_EMRREADERS

The customer can decide if a Glaucoma, Retina, Cataract Workplace access
should be controlled by the members of the FORUM Administrators group or
if that should be also controlled by the domain administrators. In the event
that the clinical workplace access is managed by the domain admin, an
additional three groups need to be created in Active directory.

In the example below, the domain admin created three groups called
AD_FORUM_RW, AD_FORUM_GW and AD_FORUM_CW which now are
mapped to the their equivalent roles in FORUM.

# Workplace Roles
authentication.forum.RETINAWORKPLACEGROUP.roles=
ROLE_MYDOMAIN\AD_FORUM_RW
authentication.forum.GLAUCOMAWORKPLACEGROUP.roles=
ROLE_MYDOMAIN\AD_FORUM_GW
authentication.forum.CATARACTWORKPLACEGROUP.roles=
ROLE_MYDOMAIN\AD_FORUM_CW
Configuring LDAP and LDAPS

Licensing

Prerequisite ✓ LDAP authentication is a licensed feature and requires a license to function.

Actions • To verify if this feature is licensed, open the FORUM Viewer and check the <Help><About> dialog:

<table>
<thead>
<tr>
<th>Plugin Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>FORUM_CATALOG, WORKPLACE_2G4C4.1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>FORUM_CATALOG, WORKPLACE_USER_1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>FORUM_CATALOG, WORKPLACE_BASIC_1.0</td>
<td>1.0</td>
</tr>
<tr>
<td>PRINT_BASIC_1.0</td>
<td></td>
</tr>
<tr>
<td>LCDP_1.0 (LCAPLEXE10)</td>
<td></td>
</tr>
<tr>
<td>JAVA_INTERACTIVE_DASHBOARD_0.0</td>
<td></td>
</tr>
<tr>
<td>JRE Architecture (Viewer): 64 Bit</td>
<td></td>
</tr>
<tr>
<td>Plug-ins</td>
<td></td>
</tr>
<tr>
<td>FORUM Language Fragment (English, United Kingdom)</td>
<td>4.0.4</td>
</tr>
<tr>
<td>MetaData_en_GB_language_fragment</td>
<td></td>
</tr>
<tr>
<td>Product Version: 4.0.4</td>
<td></td>
</tr>
<tr>
<td>FORUM Language Fragment (English)</td>
<td></td>
</tr>
<tr>
<td>MetaData_en_language_fragment</td>
<td></td>
</tr>
</tbody>
</table>

LDAP Configuration

Unlike the Single Sign On in the previous chapter, the LDAP authentication is actively communicating with the Active Directory server.

For a large number of users, this can cause a lot of communication between the FORUM Archive and the active directory or other LDAP server. The server is capable of caching credentials in the memory (not on disk) for performance reasons.

The example configuration below assumes the following environment:

AD/LDAP server: myldapserver
AD/LDAP global catalog port: 3268
Domain: mydomain.org

The configuration is done in the CZM\FORUM\settings\application-sam.properties the same way as the SSO configuration from the previous chapter.
To enable LDAP authentication, the authentication filter needs to be set to "Basic" as the first value followed by Oauth, ForumLocalWindowsAuthentication and ForumLocalInstallation.

The following is the definition of the values:

**Basic** = FORUM internal security realm which uses LDAP authentication if LDAP authentication is enabled.

**Oauth** = Use Oauth authentication for Workplace Services (GW, RW, etc…)

**ForumLocalWindowsAuthentication** = FORUM Viewer authentication running on the FORUM server

**ForumLocalInstallation** = Authentication method used Service Tool on the FORUM server

```java
# use this file to override the default security settings
# to activate rename to application-sam.properties

# HTTP authentication configuration
authentication.filters.enabled=Basic,OAuth,ForumLocalInstallation, ForumLocalWindowsAuthentication

# LDAP authentication settings
ldap.authentication.enabled=true

For performance reasons it is recommended to enable the authentication cache as authentication is required for every HTTP request. The authentication.cache.interval defines how long (seconds) credentials can stay cached. A higher interval is recommended for environments with a large amount of users. The example below has the credential cache enabled and keeps credentials in memory for four hours.

```java
authentication.cache.enabled=true
authentication.cache.interval=14400
```

An LDAP manager user is required to be able to communicate on behalf of FORUM Archive. Only an active directory user can query the LDAP interface. This user should not be an administrator but should have a password that does not expire.

```java
ldap.manager.user=mydomain\aduser (in LDAP notation:
ldap.manager.user=uid=rod,ou=people,dc=springframework,dc=org)
ldap.manager.password=adusers-password
```

AD/LDAP server URL including protocol (ldap), servername and LDAP port (default Active Directory: 389). In some cases, the LDAP Global Catalog port may be required instead (default Active Directory: 3286)

```java
# ldap.url=ldap://myldapserver:3268
ldap.url=ldap://myldapserver:389
```
The domain root is set as the search base for users. The search filter has to be set to uid and sAMAccountName.

```
ldap.userSearchBase=DC=mydomain,DC=org
ldap.userSearchFilter=(uid={0})
ldap.userSearchFilter=(sAMAccountName={0})
```

The domain root is set as the search base for groups.

```
ldap.groupSearchBase=DC=mydomain,DC=org (in LDAP notation: ldap.userSearchBase=ou=people)
ldap.groupSearchFilter=(member={0})
```

### Role Mapping - LDAP

Just as with the SSO configuration, the LDAP configuration requires role mapping and, therefore, it requires as many user groups in Active Directory as the number of roles intended to be used by the institution. If it is intended that all four roles available roles in FORUM are to be used, then four groups are required. The SSO chapter contains a matrix describing the roles in detail.

FORUM can use up to seven groups in total. The four group which represents different sets of user rights (roles) in FORUM and the additional three group which can (optionally) be used to control access to the clinical workplaces such as the Retina and Glaucoma workplace. Alternatively, workplace access can also be managed by any of the users that are part of the administrators group.

Once the groups are created in Active Directory, they need to be mapped to the user roles in FORUM. Role mapping is the configuration part where you can assign the Active Directory groups to the FORUM roles.

In the example configuration below, the domain administrator of the mydomain.org created four groups representing the roles in FORUM. The groups are called AD_FORUM_ADMINS, AD_FORUM_EDITORS, AD_FORUM_READONLY and AD_FORUM_EMREADERS. Unlike with the SSO configuration, AD groups don’t any prefixes in the configuration.

```
# Role mapping
authentication.forum.ADMINGROUP.roles=AD_FORUM_ADMINS
authentication.forum.USERGROUP.roles=AD_FORUM_EDITORS
authentication.forum.RESTRICTEDUSERGROUP.roles=AD_FORUM_READONLY
authentication.forum.EMRRESTRICTEDUSERGROUP.roles=AD_FORUM_EMREADERS
```
The customer can decide if a Glaucoma, Retina, Cataract Workplace access should be controlled by the members of the FORUM Administrators group or if that should be also controlled by the domain administrators. In the event that the clinical workplace access is managed by the domain admin, an additional three groups need to be created in Active directory.

In the example below, the domain admin created three additional groups called AD_FORUM_RW, AD_FORUM_GW and AD_FORWARD_CW which now are mapped to the their equivalent roles in FORUM.

```
# Workplace Roles
authentication.forum.RETINAWORKPLACEGROUP.roles=AD_FORUM_RW  
authentication.forum.GLACOMAWORKPLACEGROUP.roles=AD_FORUM_GW  
authentication.forum.CATARACTWORKPLACEGROUP.roles=AD_FORUM_CW
```

**LDAP Configuration**

The difference between LDAP and LDAPS is the fact that the communication to the AD/LDAP server is tunneled using the SSL or TLS protocol. This is a security feature which secures the communication between the two parties throughout the network.

**Root Certificate Import**

**Prerequisite**

- To be able to accept the certificate of the LDAPS server, the FORUM Archive needs to have the root certificate of the Certificate Authority that has issued the certificate.

The application server of FORUM uses a cacerts.jks file (.jks = Java Key Store) to store all trusted Certificate Authorities (CA) root certificates.

Customer CA root can be added using either the java keytool (command line) or by using a graphical user interface based tool such as KeyStore Explorer (open source). In the example below, the KeyStore Explorer is used to demonstrate how this is done.

The cacerts.jks file is located in...

...CZM\FORUM\server\glassfish\domains\archive\config
**Actions**

- Open the cacerts.jks file with the KeyStore Explorer

![KeyStore Explorer](image)

- Enter the password "changeit" when prompted

![Password Entry](image)

- Simply Drag and Drop the root certificate into the KeyStore Explorer window and confirm with the "Import" button.

![Certificate Import](image)

After successfully importing the certificate, you may need to restart the CZM Server Service to ensure the application server is aware of the institution's newly imported root certificate.
Enabling the LDAPS Protocol

Similar to the LDAP configuration, the URL needs to point the AD/LDAP server but using the LDAPS protocol and the LDAPS port. For Active Directory the default 636. In some cases, the LDAPS Global Catalog port may be required instead (default Active Directory: 3286)

ldap.url=ldaps://myldapserver:636
# ldap.url=ldaps://myldapserver:3269

After any change, in the CZM\FORUM\settings\application-sam.properties file, the CZM Server Service needs to be restarted as the configuration is only read once during the startup.

Logging

All authentication related logging is stored in the forum-security.log. As any other forum log, it is located in the CZM\FORUM\FORUM-logs directory. When troubleshooting SSO/LDAP related issues, it is important to enable the TRACE log level for this particular log file.

To enable the TRACE log level, you need to modify the forum-log4j.xml file which is located in the CZM\FORUM\config directory. Find the logger responsible for security and set it to trace as shown below.

<Logger name="de.zeiss.forum.security" level="trace" additivity="false">

When you have finished troubleshooting, return the log level to info to avoid unnecessary workload on the server.