

DJIGZO EMAIL ENCRYPTION

Djigzo Gateway Web LDAP Authentication Guide



Author: Martijn BRINKERS

June 25, 2010, Rev: 4253



1 Introduction

By default, Djigzo web authenticates the administrators against a list of registered users stored in the Djigzo database. Administrators, passwords and roles can be managed with the Djigzo web administration page. Sometimes however, it is required to authenticate administrators against an external LDAP. This guide explains how to setup Djigzo to authenticate and authorize administrators against an external LDAP.

Enabling LDAP authentication require the following steps:

1. Create an LDAP configuration file.
2. Add users and roles to the LDAP.
3. Configure Tomcat.

2 Create an LDAP configuration file

Djigzo uses Spring security for authentication and authorization. To enable LDAP support for the Djigzo web application, a Spring xml configuration file is required.

Create the file *djigzo-ldap.xml* in directory */usr/share/djigzo-web*¹ with the following content:

```
<beans xmlns="http://www.springframework.org/schema/beans"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:security="http://www.springframework.org/schema/security"
  xsi:schemaLocation=
    "http://www.springframework.org/schema/beans
    http://www.springframework.org/schema/beans/spring-beans-2.5.xsd
    http://www.springframework.org/schema/security
    http://www.springframework.org/schema/security/spring-security-2.0.xsd">

  <security:ldap-server url="ldap://192.168.178.22:389/dc=djigzo,dc=com" />

  <security:ldap-authentication-provider
    user-dn-pattern="uid={0},ou=users"
    group-search-base="ou=groups"/>
</beans>
```

The URL for the LDAP server should be changed to match the URL of the actual LDAP server. The root DIT should also be changed from *dc=djigzo,dc=com* to the root DIT where the Djigzo administrators and groups are stored.

¹The file can be differently named and stored on another location. The only requirement is that the file is readable by Tomcat.

Note: Additional LDAP servers can be specified. Additional LDAP servers should be space separated (example: "ldap://1.2.3.4 ldap://5.6.7.8"). When logging in, the LDAP servers are tried in succession until a successful login.

user-dn-pattern pattern: The *user-dn-pattern* pattern is used to build the DN to bind to using the password entered by the user. {0} in the pattern is replaced with the username.

Example: When the user john tries to login, an attempt is made to bind to *uid=john,ou=users,dc=djigzo,dc=com* using the password entered by john.

group-search-base pattern The *group-search-base* pattern is used to locate the roles for the user. This is the part of the directory tree under which group searches are performed. By default, records of class *groupOfUniqueNames* are searched with a *uniqueMember* attribute equal to the DN of the user. The returned role is the value of the *cn* attribute(s). The role name is converted to uppercase and prefixed with `ROLE_`².

Example: When the user john successfully logs into Djigzo, a search is done for a record with class *groupOfUniqueNames* under *ou=groups,dc=djigzo,dc=com* containing the attribute *uniqueMember* with the value *uid=john,ou=users,dc=djigzo,dc=com*. If the *cn* attribute has value `login` the returned role is `ROLE_LOGIN`.

For more information on *user-dn-pattern* and *group-search-base* see <http://static.springsource.org/spring-security/site/docs/2.0.x/reference/ldap.html>.

3 Add users and roles to the LDAP

The required users and roles should be added to the LDAP server. The actual commands required for adding users and roles depends on the LDAP implementation. The following example shows how to add users and roles to OpenLDAP.

The following LDAP Data Interchange Format (LDIF) example is used to add two users, john and jane. John has password "password" and Jane has a hashed password "test". John will have the following roles: *login* and *admin*. Jane will have the following roles: *login* and *queue_manager*.

Note: The entries will be added under the *dc=djigzo,dc=com* tree.

```
dn: ou=users,dc=djigzo,dc=com
objectClass: organizationalUnit
ou: users
```

²Make sure the roles stored in LDAP are not pre-fixed with `ROLE_`.

```
dn: ou=groups,dc=djigzo,dc=com
objectClass: organizationalUnit
ou: groups
```

```
dn: uid=john,ou=users,dc=djigzo,dc=com
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: john
userPassword: password
sn: Doe
givenName: John
cn: John Doe
```

```
dn: uid=jane,ou=users,dc=djigzo,dc=com
objectClass: inetOrgPerson
objectClass: shadowAccount
uid: jane
userPassword: {SHA}qUqP5cyxm6YcTAhz05Hph5gvu9M=
sn: Doe
givenName: Jane
cn: Jane Doe
```

```
dn: cn=admin,ou=groups,dc=djigzo,dc=com
objectClass: groupOfUniqueNames
cn: login
uniqueMember: uid=john,ou=users,dc=djigzo,dc=com
```

```
dn: cn=queue_manager,ou=groups,dc=djigzo,dc=com
objectClass: groupOfUniqueNames
cn: login
uniqueMember: uid=jane,ou=users,dc=djigzo,dc=com
```

The LDIF should be stored in a file (djigzo.ldif) and imported into OpenLDAP using the following command:

```
$ ldapadd -x -D cn=admin,dc=djigzo,dc=com -W -f djigzo.ldif
```

Note: change dc=djigzo,dc=com to match the actual sub tree.

Supported roles The following roles are supported:

1. login
2. admin
3. domain_manager
4. global_manager

5. log_manager
6. pki_manager
7. queue_manager
8. sms_manager
9. template_manager
10. user_manager

Note: Every user should at least have the login role. The admin role is a combination of all other roles. See the administration guide for more info on the roles.

4 Configure Tomcat

Djigzo web application should be configured to use the new authenticator. The Java system property *djigzo-web.spring.authenticator.config* determines which authenticator configuration file is loaded when Djigzo web application is started. The Java property should be set in the Tomcat default properties files which is read by Tomcat when Tomcat starts. The location of the Tomcat defaults file is different for Ubuntu/Debian and RedHat/CentOS.

Ubuntu/Debian

Ubuntu/Debian the default properties file for Tomcat 5.5 is */etc/default/tomcat5.5*. The required property can be directly set using the following command:

```
$ sudo bash -c 'echo "JAVA_OPTS=\"\$JAVA_OPTS \  
-Ddjigzo-web.spring.authenticator.config=  
file:/usr/share/djigzo-web/djigzo-ldap.xml\"" >> /etc/default/tomcat5.5'
```

Tomcat should be now be restarted:

```
$ sudo /etc/init.d/tomcat5.5 restart
```

RedHat/CentOS

RedHat/CentOS the default properties file for Tomcat 5.5 is */etc/sysconfig/tomcat5*. The required property can be directly set using the following command:

```
$ sudo bash -c 'echo "JAVA_OPTS=\"\$JAVA_OPTS \  
-Ddjigzo-web.spring.authenticator.config=  
file:/usr/share/djigzo-web/djigzo-ldap.xml\"" >> /etc/sysconfig/tomcat5'
```

Tomcat should be now be restarted:

```
$ /sbin/service tomcat5 restart
```

Login When a user logs into Djigzo, details of the login attempt are written to the Djigzo MPA log. The user and the roles assigned to the user are logged.

Example successful login:³

```
[21 Aug 2009 11:15:39 11650554@qtp-24482011-5] INFO
Authentication success...
Username: jane; Password: [PROTECTED]; Enabled: true;
AccountNonExpired: true; credentialsNonExpired: true;
AccountNonLocked: true;
Granted Authorities: ROLE_LOGIN, ROLE_QUEUE_MANAGER
```

Example login failure:

```
[21 Aug 2009 11:20:31 31737213@qtp-24482011-4] WARN
Authentication failure...
Principal: d; Password: [PROTECTED];
Authenticated: false; RemoteIpAddress: 192.168.178.20;
SessionId: 1ejsszduvhtn;
Not granted any authorities
```

³Some log information is removed to make the example fit the page.