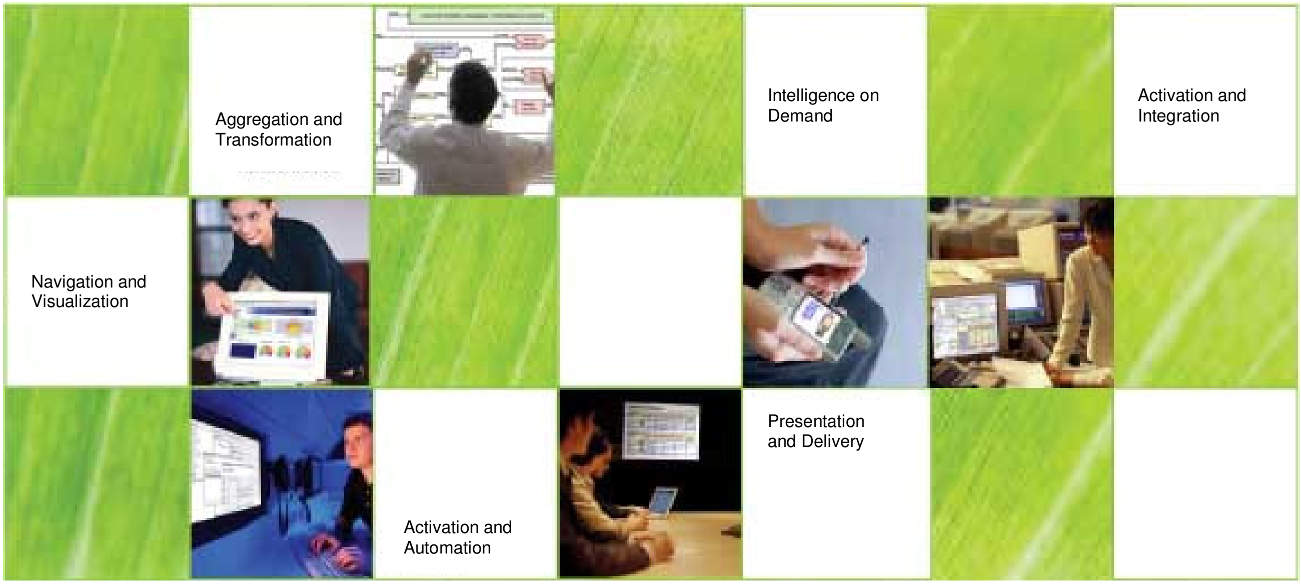

Aggregation and Transformation
Intelligence on Demand
Activation and Integration
Navigation and Visualization
Activation and Automation
Presentation and Delivery

Elixir Repertoire Server

Reference guide for logging on to Repertoire Server with LDAP Secondary Authentication

Table of Contents

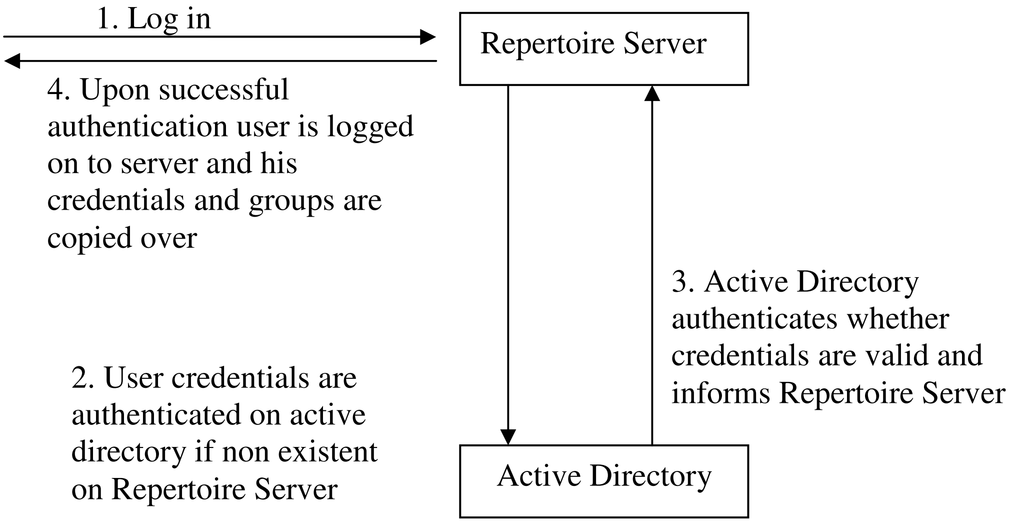
1. Introduction

This document serves as a reference guide to assist users in integrating the Repertoire Server with Active Directory as secondary authentication. The example in this exercise will cover integrating the Repertoire Server with a Microsoft active directory.

For this document it is assumed that the active directory has already been set up and that users are looking into the integration of the two.

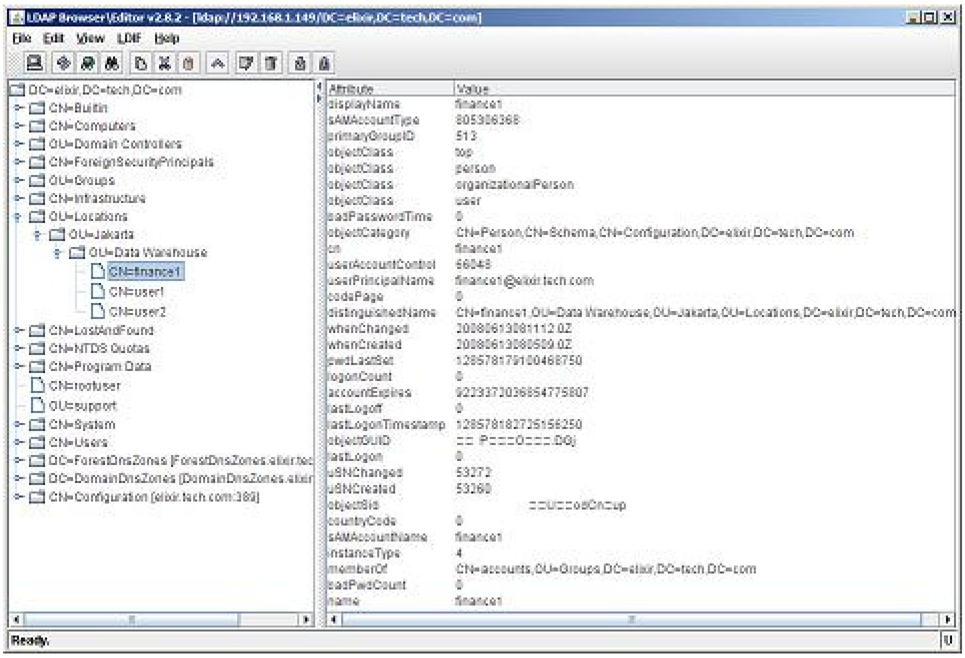
2. Objectives

The example used in this document is a general active directory architecture to enable users to understand the basic configuration and set up.


1. Log in
Repertoire Server
4. Upon successful authentication user is logged on to server and his credentials and groups are copied over
3. Active Directory authenticates whether credentials are valid and informs Repertoire Server
2. User credentials are authenticated on active directory if non existent on Repertoire Server
Active Directory

3. Understanding the Active Directory Structure

Before integration, users should understand the architecture of their active directory. One recommendation is to use an LDAP browser to view the architecture and bindings of the active directory:


LDAP Browser\Editor v2.8.2 - [ldap://192.168.1.149/DC=elixir,DC=tech,DC=com]
File
Edit
View
LDIF
Help
Ready.

```
DC=elixir,DC=tech,DC=com
  CN=Builtin
  CN=Computers
  OU=Domain Controllers
  CN=ForeignSecurityPrincipals
  OU=Groups
  CN=Infrastructure
  OU=Locations
    OU=Jakarta
      OU=Data Warehouse
        CN=finance1
        CN=user1
        CN=user2
  CN=LostAndFound
  CN=NTDS Quotas
  CN=Program Data
  CN=rootuser
  OU=support
  CN=System
  CN=Users
  DC=ForestDnsZones [ForestDnsZones.elixir.tec
  DC=DomainDnsZones [DomainDnsZones.elixir
  CN=Configuration [elixir.tech.com:389]
```

Attribute	Value
displayName	finance1
sAMAccountType	805306368
primaryGroupID	513
objectClass	top
objectClass	person
objectClass	organizationalPerson
objectClass	user
badPasswordTime	0
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=elixir,DC=tech,DC=com
cn	finance1
userAccountControl	66048
userPrincipalName	finance1@elixir.tech.com
codePage	0
distinguishedName	CN=finance1,OU=Data Warehouse,OU=Jakarta,OU=Locations,DC=elixir,DC=tech,DC=com
whenChanged	20080613081112.0Z
whenCreated	20080613080509.0Z
pwdLastSet	128578179100468750
logonCount	0
accountExpires	9223372036854775807
lastLogoff	0
lastLogonTimestamp	128578182725156250
objectGUID	□□ P□□□O□□□.DGj
lastLogon	0
uSNChanged	53272
uSNCreated	53260
objectSid	□□U□□o8Cn□up
countryCode	0
sAMAccountName	finance1
instanceType	4
memberOf	CN=accounts,OU=Groups,DC=elixir,DC=tech,DC=com
badPwdCount	0
name	finance1

Users can obtain an open source version of the LDAP Browser from this link: http://www.mcs.anl.gov/~gawor/ldap/

4. Configuring the Repertoire Server

To use Active Directory as secondary authentication with Repertoire Server edit the following in ERS2.xml found in the /config directory of the server installation. Below is an example configuration which was carried out for a Microsoft active directory server.

```
<ers:mbean name="ERS2:name=LDAPUserRoleAuthentication"
                              class="com.elixirtech.ers2.security.ldap.LDAPUserRoleAuthentication">
<ers:property name="Enabled">true</ers:property>
<ers:property name="LDAPServerURL">ldap://192.168.1.149:389</ers:property>
<ers:property name="AuthenticationType"></ers:property>
<ers:property name="Realm"></ers:property>
<ers:property name="UsersDN">OU=CLAS,OU=App,dc=elixir,dc=tech,dc=com</ers:property>
<ers:property name="UserAttributeKey">sAMAccountName</ers:property>
<ers:property name="GroupsDN">OU=CLAS,OU=App,dc=elixir,dc=tech,dc=com</ers:property>
<ers:property name="GroupMatchKey">member</ers:property>
<ers:property name="GroupReturningAttribute">cn</ers:property>

<!-- Setting Principal and Credentials will use the "Search and Bind" two-step approach to
authentication, rather than direct authentication. Active Directory requires Search and Bind.
You can leave these blank if users themselves have search permissions (most implementations) -->
<ers:property name="Principal">rootuser@elixir.tech.com</ers:property>
<ers:property name="Credentials">elixir</ers:property>
</ers:mbean>
```

Property Name	Description
Enabled	Set to “true” to enable
LDAPServerURL	Set the URL of the LDAP
AuthenticationType	Set the LDAP authentication type
Realm	Repository where the server stores user and group information
UsersDN	Find user from a directory path
UserAttributeKey	Name attribute e.g. cn, sAMAccountName
GroupsDN	Find groups from a directory path
GroupMatchKey	Find groups user belongs to
GroupReturningAttribute	Returning name of each group found

From version 7.3 onwards, additional properties have been included to facilitate a "search and bind" in situations where the Active Directory and the Repertoire Server reside on separate servers running different operating systems.

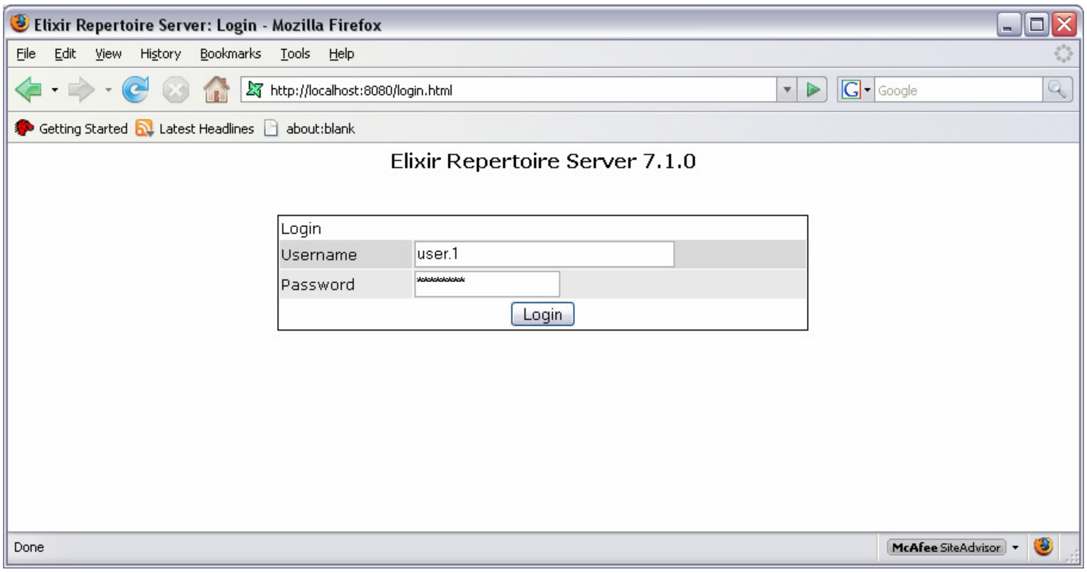
Property Name	**Description**
Principal	Administrator ID
Credentials	Password

The above two parameters are also required for setups whereby the requirement is to log onto the Repertoire Server using the sAMAccountName attribute from the active directory as a log in is required to carry out a search and bind of the users credentials.

Users are required to restart the Repertoire Server (if currently running) once changes have been made to the ERS2.xml configuration file.

5. Elixir Repertoire Server with Secondary Active Directory Authentication

Once the configuration file has been modified, restart the Repertoire Server and attempt to login using the Active Directory user's account credentials.

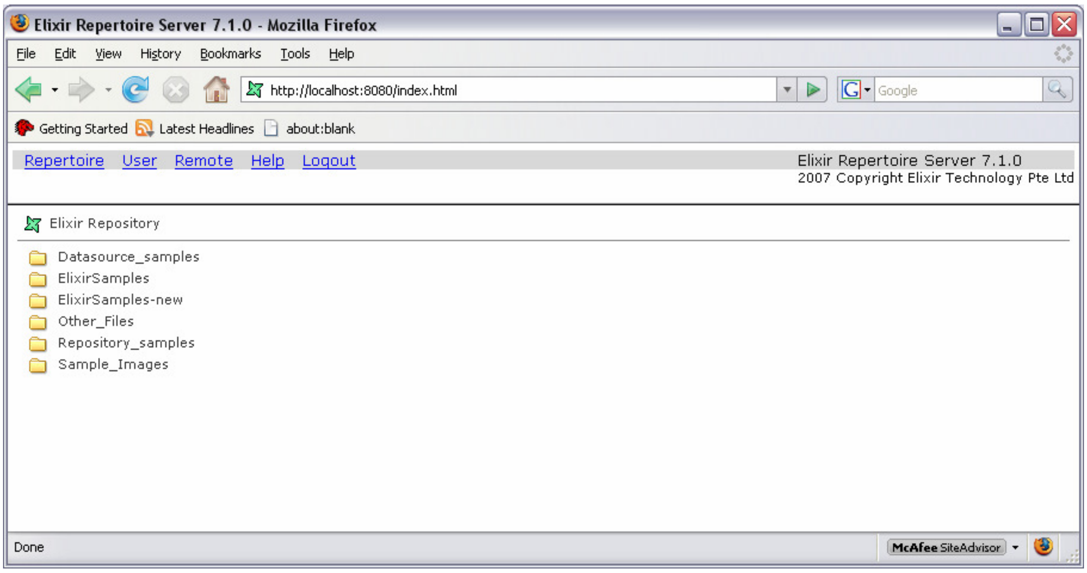

Elixir Repertoire Server: Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:8080/login.html
Google
Getting Started Latest Headlines about:blank
Done
McAfee SiteAdvisor

Elixir Repertoire Server 7.1.0

Login

Username	user.1
Password	********

Enter an active directory username and password to login. If configured correctly, the user would be logged into the server and is able to access the page shown below.

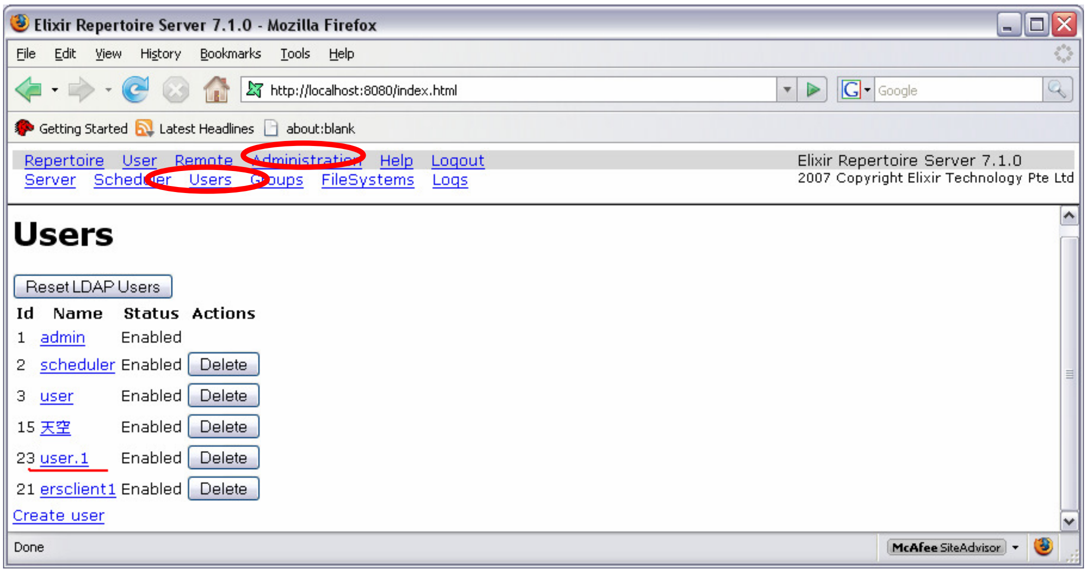

Elixir Repertoire Server 7.1.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:8080/index.html
Google
Getting Started Latest Headlines about:blank
Repertoire User Remote Help Logout
Done
McAfee SiteAdvisor

Elixir Repertoire Server 7.1.0
2007 Copyright Elixir Technology Pte Ltd

Elixir Repository

- Datasource_samples
- ElixirSamples
- ElixirSamples-new
- Other_Files
- Repository_samples
- Sample_Images

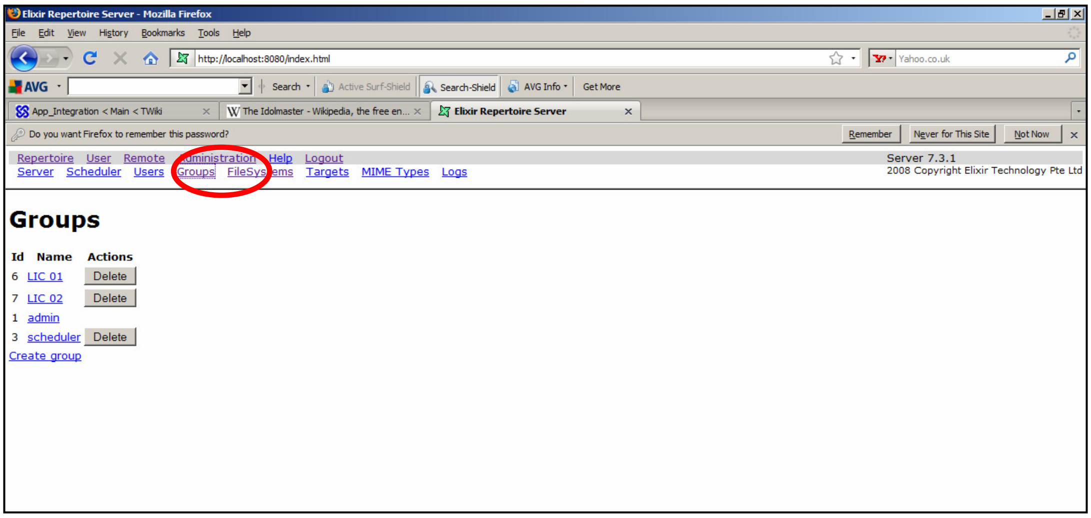
Upon successfully login, the active directory user information would be added to the Elixir Repertoire Server database successfully. This can be verified by selecting "Administration" followed by "Users".


Elixir Repertoire Server 7.1.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:8080/index.html
Google
Getting Started Latest Headlines about:blank
Repertoire User Remote Administration Help Logout
Server Scheduler Users Groups FileSystems Logs
Elixir Repertoire Server 7.1.0
2007 Copyright Elixir Technology Pte Ltd
Reset LDAP Users
Create user
Done
McAfee SiteAdvisor

Users

Id	Name	Status	Actions
1	admin	Enabled	
2	scheduler	Enabled	Delete
3	user	Enabled	Delete
15	天空	Enabled	Delete
23	user.1	Enabled	Delete
21	erclient1	Enabled	Delete

In addition, if users belong to groups on the active directory their respective groups will also be created dynamically on the Repertoire Server. This can be verified by selecting "Administration" followed by "Groups".


Elixir Repertoire Server - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:8080/index.html
Yahoo.co.uk
AVG Search Active Surf-Shield Search-Shield AVG Info Get More
App_Integration < Main < TWiki
The Idolmaster - Wikipedia, the free en...
Elixir Repertoire Server
Do you want Firefox to remember this password?
Remember Never for This Site Not Now
Repertoire User Remote Administration Help Logout
Server Scheduler Users Groups FileSystems Targets MIME Types Logs
Server 7.3.1
2008 Copyright Elixir Technology Pte Ltd
Create group

Groups

Id	Name	Actions
6	LIC 01	Delete
7	LIC 02	Delete
1	admin	
3	scheduler	Delete

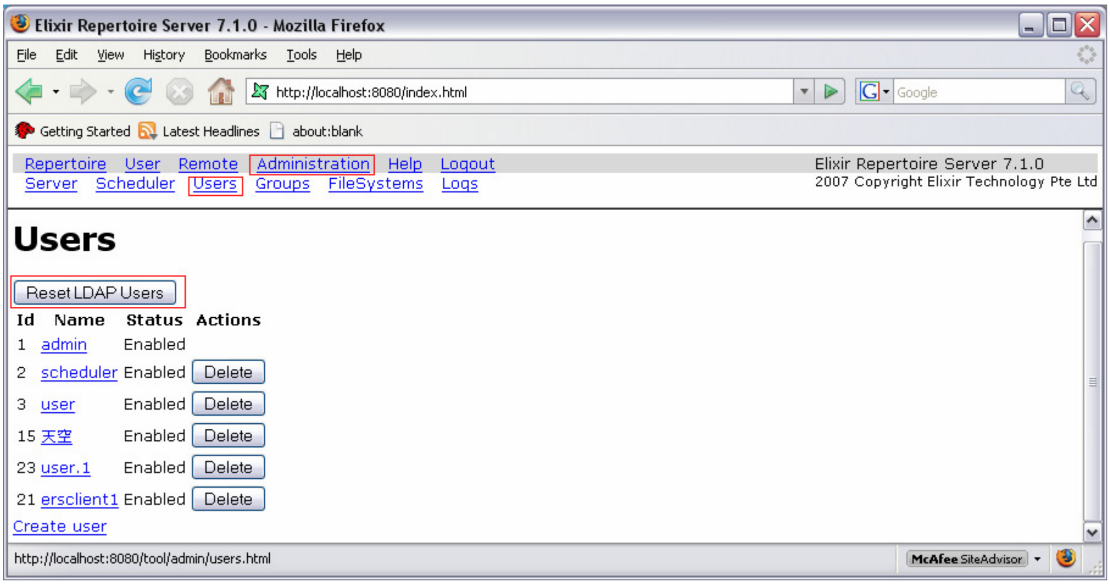
If the groups were not dynamically created on the Repertoire Server double check the following attribute values in the ERS2.xml file.

Property Name	Description
GroupsDN	Find groups from a directory path
GroupMatchKey	Find groups user belongs to
GroupReturningAttribute	Returning name of each group found

5.1. Changing Active Directory user password

LDAP users are only allowed to change their password at the active directory level. Once the user's password has been changed, the administrator is required to reset the password on the Repertoire Server for the changes to take effect.

Go to the **Administration** -> **Users** page and click on the **Reset LDAP Users** button.

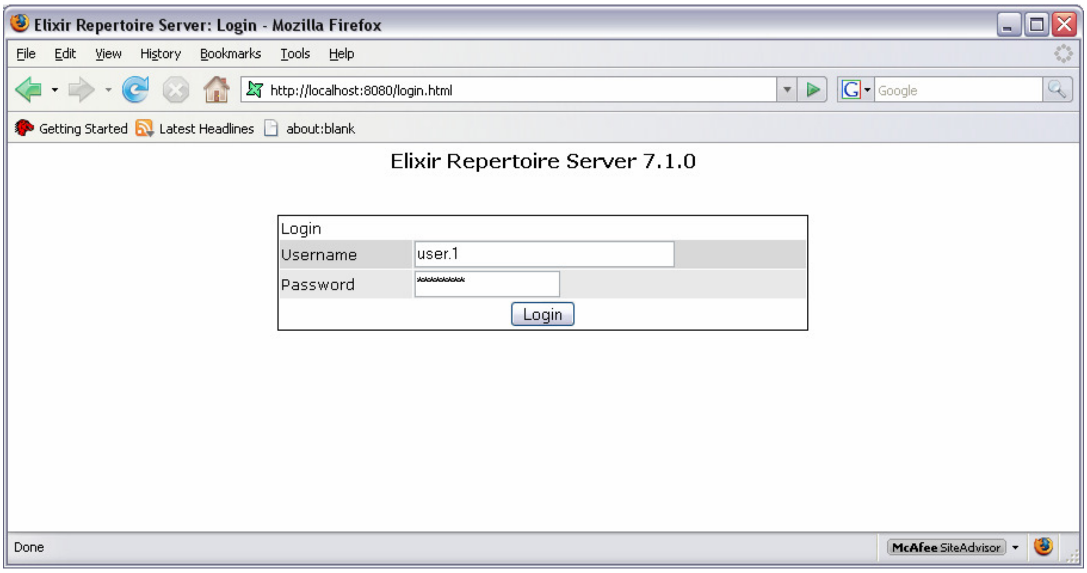

Elixir Repertoire Server 7.1.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:8080/index.html
Google
Getting Started Latest Headlines about:blank
Repertoire User Remote Administration Help Logout
Server Scheduler Users Groups FileSystems Logs
Elixir Repertoire Server 7.1.0
2007 Copyright Elixir Technology Pte Ltd
Reset LDAP Users
Create user
http://localhost:8080/tool/admin/users.html
McAfee SiteAdvisor

Users

Id	Name	Status	Actions
1	admin	Enabled	
2	scheduler	Enabled	Delete
3	user	Enabled	Delete
15	天空	Enabled	Delete
23	user.1	Enabled	Delete
21	ersclient1	Enabled	Delete

Alternatively, the LDAP user's password can be reset using the REST API call:
http://localhost:8080/tool/admin/users.html?action=ResetLDAPUsers

Once the password has been reset, verify that the LDAP user can only login with their new password by attempting to log onto the server using both old and new passwords.


Elixir Repertoire Server: Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:8080/login.html
Google
Getting Started Latest Headlines about:blank
Elixir Repertoire Server 7.1.0
Login
Done
McAfee SiteAdvisor

Username: user.1

Password: ********

If configured correctly, the new changes would have taken place and users can only log in using their new password.

6. Frequently Asked Questions

Q1. What happens when a valid user in active directory attempts to login to Repertoire Server?

The specified user account details such as username, password and group will be copied and stored in the Repertoire Sever databases.

Q2. What happens when a user is deleted from the active directory?

Deleted user will fail to login to the Repertoire Server as authentication checking would be sent in between Repertoire Server and the active directory. So, if the user no longer exists in the active directory, Repertoire Server will deny the access of the user.

Q3. I'm unable to configure the Repertoire Server to dynamically copy over the groups from the active directory / I'm unable to log on to the Repertoire Server using the sAMAccountName attributes

Refer to the server logs for any errors reflected regarding the active directory authentication. An example of an error message would look like this:

```
2008-09-23 11:52:57,301,btpool0-2,INFO , ldap.LDAPUserRoleAuthentication - Login failed for
clas: javax.naming.AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-
0C090334, comment: AcceptSecurityContext error, data 525, vece ]
```

Below is a reference of the three digit error code highlighted in bold:

525 - user not found
52e - invalid credentials
530 - not permitted to logon at this time
532 - password expired
533 - account disabled
701 - account expired
773 - user must reset password

It should be noted for users of versions 7.2 and below that for setup whereby the Repertoire Server and active directory are either on different servers or operating systems or if they are logging onto the Repertoire Server using the sAMAccountName attribute that they are required to upgrade to version 7.3 as the Repertoire Server is required to log onto the active directory with a principal and credential value to do a "search and bind" of the user attributes.

Contact sales@elixirtech.com or support@elixirtech.com for more information on upgrading to the latest version of the Repertoire Server.

Q4. What happens when a user changes his/her password in the active directory?

User will be still be able to login with his/her old password instead of the new password. This is due to the active directory server cache setting. In order to allow the user to login with their new password, users with admin privileges are required to perform the “Reset LDAP Users” action in order for the new password to take effect.

Q4. What if I need to configure the Repertoire Server to read my active directory which has user credentials stored in multiple branches?

A customised code plug in is required to read through the branches depending on your active directory architecture. Contact support@elixirtech.com for more details.