Unified Access for Enterprise Users

Informational webinar

Chinmay Meghani
Liferay Portal Specialist
Fulcrum Worldwide, Inc.

Mehria Askaryar
Business Development Manager
Fulcrum Worldwide, Inc.
Agenda

Introduction to Liferay

- Liferay capabilities & Various integration features

What is CAS?

- Overview and History
- Current Deployments

Why CAS?

- Benefits of using CAS as an SSO implementation

Easy integration of Liferay with LDAP and CAS

Liferay LDAP Integration features Liferay CAS integration features

Demo

Q&A
Introduction to Liferay

Liferay is an enterprise portal which has shown one of the fastest adoptions in the marketplace in recent times. Why?

1. Liferay is open source
2. Liferay is adaptable
3. Liferay is scalable
4. Liferay runs on all major application servers, operating systems and databases
5. Liferay easily integrates with third party applications

Let us concentrate on the fifth bullet above.

“Liferay easily integrates with third party applications”

Easy integration - What is it?

Easy integration means the ability to integrate with minimal configuration with the existing applications that an enterprise uses
Introduction to Liferay

Examples of Liferay’s seamless integration features with respect to authentication:

- LDAP
- Open SSO
- OpenID
- CAS
- Facebook

and the best part about Liferay’s integration features:

- They’re out of the box - which means they ship with Liferay
- Users can choose from over 60 portlets and 20 themes
Introduction to Liferay

Liferay integration points:

**Authentication**

Liferay supports authentication using Database, LDAP, CAS and OpenID by default. For custom implementation of authentication mechanism, a flexible set of hooks (Authentication and auto login pipelines) are available.

**Filters**

- Filters intercept client requests before they access backend services.
- One of the most widely used filters by Liferay is the Auto login filter.
- This is an authentication filter.
Introduction to Liferay

**Authentication**: How does Liferay authentication work?
Introduction to Liferay

**Filters**: How do Liferay filters work?
What is CAS and How does it work?

**CAS** – Central Authentication Service

- A single sign on protocol for web
- Provides enterprise single sign on service
- CAS permits a user to access multiple applications while providing their credentials (such as user id and password) once
Why CAS?

- **Easy Integration**: Integrates easily with and is supported by Liferay portal
- **Open Source**: An open-source Java server component
- **Libraries**: A library of clients for Java, .NET, PHP, Perl, Apache, uPortal, and others
- **Support**: Community documentation and implementation support
- **Security**: CAS reduces the proliferation of user login experiences
- **User Convenience**: CAS centralizes the authentication user experience so that users need to only log in once in a browser session and not present their credentials again to authenticate to additional participating web applications
Integration of Liferay with CAS

The following steps explain in detail how easy it is to integrate Liferay with CAS.

Added bonus! We will be using LDAP integration with Liferay which helps in easy user maintenance.

1. To integrate Liferay with CAS, you need CAS which can be downloaded from [http://www.jasig.org/cas/download](http://www.jasig.org/cas/download).

2. Once CAS has been downloaded, there are two options to set it up.

   **First option** is to download an application server of choice and deploy the CAS WAR. This means that CAS will be running on a stand-alone server.

   **Second option** is to deploy CAS on the same application server on which the Liferay portal is running.

   - Once CAS has been deployed, create a trusted certificate.
   - CAS works on the concept of trusted certificates over secured channel (HTTPS).
   - CAS uses LDAP extensively and integrates with LDAP easily. Therefore it is advisable to have an LDAP integration enabled for Liferay.
   - LDAP integration can be enabled by navigating to the portal settings>authentication in Liferay’s Control Panel.
Liferay CAS Integration Features

- CAS has been set up on a stand-alone server.
- Setting up CAS on a stand-alone server (Tomcat in this case) is as simple as it can get.
- Download the CAS WAR file from http://www.jasig.org/cas/download/cas-server-335-final
- As mentioned earlier, CAS uses tickets or certificates added to trusted stores. Therefore, before proceeding further, generate the certificate Keytool.
- Keytool is a key and certificate management utility.
- A certificate is a digitally signed statement from one entity (person, company, etc.), saying that the public key (and some other information) of some other entity has a particular value.
- A trusted key store such as CACERTS can be used to store the generated certificate.

**Commands to generate, export, and add the certificate to CACERT:**

**Command to generate the key:**
- keytool -genkey -alias tomcat -keypass changeit -keyalg RSA

**Command to export the generated key to a certificate**
- keytool -export -alias tomcat -keypass changeit -file %FILE_NAME%
- Here file name is to be replaced by your custom certificate name eg: "server.cer"

**Command to import the certificate to a trusted store (cacerts in this case)**
- keytool -import -alias tomcat -file %FILE_NAME% -keypass changeit -keystore %JAVA_HOME%/jre/lib/security/cacerts

**Command to verify if the certificate was successfully added to the trusted store**
- keytool -list -alias tomcat -keystore cacerts
  (Present working directory :%JAVA_HOME%/jre/lib/security)

**Next step is to deploy the CAS WAR file and access it via HTTPS port**
Liferay CAS Integration Features

Accessing CAS via HTTPS port:
Liferay CAS Integration Features

Accessing CAS via HTTPS port:
Liferay CAS Integration Features

Configuring CAS-Liferay integration:

Copyright 2013 Fulcrum Worldwide Inc.
Liferay CAS Integration Features

Configuring CAS-Liferay integration:
Liferay CAS Integration Features

That’s it! Liferay-LDAP-CAS integration is over. Next time the user tries to log in, he/she will be taken to the SSO page. After keying in the credentials, the user is taken back to the portal and is not required to log in anymore for any application implementing SSO.
Liferay CAS Integration Features

User then gets redirected to the SSO login page:
After keying in the credentials the user is logged in to the portal:
Liferay LDAP Integration Features

LDAP Settings
Liferay LDAP Integration Features

LDAP Settings

Copyright 2013 Fulcrum Worldwide Inc.
Liferay LDAP Integration Features

LDAP Settings

Liferay has successfully connected to the LDAP server.
Liferay LDAP Integration Features

LDAP Settings

Copyright 2013 Fulcrum Worldwide Inc.
Liferay LDAP Integration Features
Social Media Integration with Twitter

Liferay supports easy integration with Twitter

- Twitter integration can be enabled using a simple Twitter portlet from Liferay’s marketplace.

- Once the portlet has been dropped on the desired page, navigate to Liferay’s control panel and go to user’s settings page.

- On the settings page, select Social Network and key in the Twitter ID.

- That is it! Any Tweets made from that account will periodically appear on the Twitter portlet.
Points to Remember

✓ Groups created in the LDAP server must be group-of-unique-names else Liferay will not import that group.

✓ Liferay uses the LDAP bind method by default for authentication. This means that even though the LDAP password is imported into Liferay, it does not use that password while authenticating.

✓ We can even use multiple LDAP servers and set the priority dynamically at runtime.

✓ The server certificate must contain the name of the server in which CAS server exists.

✓ When testing locally, if Liferay and CAS use different JVMs, then the certificate needs to be imported in both JVMs.

✓ CAS uses ticketing mechanism during authentication. Once CAS passes on the authentication ticket with a “granted” status, Liferay trusts CAS to do the job for it and grants permission to the user.

✓ Examples of certification authorities are VeriSign, Digicert etc.
ABOUT FULCRUM

- Fulcrum Worldwide started in 1999 – privately owned
- Global Headquarters in New Jersey, with Global Delivery Centers in Reading UK, Mumbai & Pune (India)
- CMMi Appraised – Level 3; Practicing Level 5
- IBM Advanced Level, Microsoft Gold Certified, Liferay Silver Services Partner
- 2000 seater- State of the Art Knowledge Campus