Liferay DXP Application Security Features for Banking

Table of Contents

Executive Summary 1
- Transport Security 1
- Encryption 1
- Web Service Security Layers 2
- Password Policies 3
- Single Sign On (SSO) 4
- Entitlement Management 5
  - Roles and Permissions 5
  - Defining Permissions on a Role 6
    - Control Panel 6
    - Site Administration 7
    - My Account 7
  - Permission for Delegating Administration 7
- OAuth 8
- Audit Application 8

Conclusion 8

Moving Forward 9
- Schedule a Free Demo 9
- Liferay Global Services 9

Executive Summary

Liferay Digital Experience Platform (DXP) is a highly secure platform that combines best-of-class portal and CMS technology with important business benefits, including integration, security, flexibility, cost effectiveness, scalability and 24x7 support. Liferay technology is a trusted choice for small and medium-sized enterprises and global financial and insurance companies. Liferay DXP enables enterprises to manage users and site access on a certified platform that is flexible enough to meet changing compliance standards.

Security is paramount in banking. Along with support for rigorous identity management and mobile security, Liferay DXP includes a new web service access layer that prevents invocation requests from unsafe or non white-listed IP addresses. Liferay complies to financial security regulations worldwide, including but not limited to SOX and PCI DSS and regularly exceeds the standards listed in FIPS 140-2.

Managing a secure website involves more than protecting against external threats. Security flaws can appear in internal processes and user management, such as when an inexperienced user is given full access to a website's controls, or when password functionalities don't support custom password requirements, regular password expiration or other widely-accepted best practices. Liferay DXP addresses these areas on an application level and is highly customizable. This ensures that the processes put into effect are suitable for financial business needs and will operate in a way that makes sense for your workforce.

This document provides an overview of application-level security features in Liferay DXP. These features give Liferay's customers confidence in the security and ongoing reliability of Liferay DXP.

Transport Security

Liferay DXP supports HTTPS for all communication between browser and mobile clients and Liferay DXP servers. All responses from Liferay DXP contain appropriate secure headers and cookie flags to avoid user session leaks.

Encryption

Liferay DXP utilizes strong encryption algorithms for a variety of features, including passwords. Customers using Liferay DXP's out-of-the-box authentication will benefit from user passwords encrypted using cryptographic key stretching algorithms. By default, Liferay DXP uses the PBKDF2WithHmacSHA1/160/128000

encryption algorithm, which generates 160 bit hashes using 128,000 rounds to apply very good security with medium performance trade off. The length of hashes and number of rounds can be increased to further increase cryptographic strength. In addition, customers may choose alternative encryption algorithms as needed.

Liferay DXP supports data encryption at rest for its binary asset store and database storage. Customers leveraging on-premise deployments may deploy third-party technologies at the database and file system levels to encrypt the data prior to storing physical media. Those looking to utilize Cloud Infrastructure as a Service (IaaS) providers like Amazon Web Services (AWS) can leverage similar features in S3 and RDS that protect data at rest.

Web Service Security Layers

Liferay DXP adds a new service access policy layer to Liferay's web service security. Service access policies define services or service methods that can be invoked remotely, and apply only to remote services, not to local services. Service access policies are especially useful when remote applications such as mobile devices or Liferay Sync instances need to access Liferay Portal's web services. Your portal administrators can use service access policies to ensure that these devices can only invoke remote services from approved lists that can be modified at runtime.

To help you understand how service access policies fit into the big picture, here's a summary of Liferay DXP's web service security layers:

IP permission layer: The IP address from which a web service invocation request originates must be white-listed in the Liferay DXP server's portal properties file. Any attempted web service invocation coming from a non-whitelisted IP address automatically fails.

Service access policy layer: The method corresponding to a web service invocation request must be whitelisted by each service access policy that's in effect. Wildcards can be used to reduce the number of service classes and methods that must be explicitly whitelisted.

Authentication/verification layer (browser-only): If a web service invocation request comes from a browser, the request must include an authentication token. This authentication token is the value of the `p_auth` URL parameter. The value of the authentication token is generated by Liferay DXP and is associated with your browser session. The `p_auth` parameter is automatically supplied when you

invoke a Liferay Portal web service via the JSON web services API page or via JavaScript using `Liferay.Service(...)`. If Liferay DXP cannot associate the caller's authentication token with a portal user, the web service invocation request fails.

User permission layer: Properly implemented web services have permission checks. The user invoking a web service must have the appropriate Liferay DXP permissions to invoke the service.

Note that service access policies respect Liferay DXP's permissions system. Even if a service access policy grants a user access to a remote service, the user must still have the appropriate permissions to invoke that service.

Password Policies

Customers leveraging Liferay DXP's out-of-the-box authentication can use password policies to further enhance the security of the platform. Administrators can set requirements on password strength, frequency of password expiration, user lockout and more. Additionally, administrators can apply different password policies to different sets of users. The administrator can define custom password policies or delegate user authentication to an LDAP server.

The Password Policy settings form contains the following fields, which enable specific settings via check box prompts:

- **Name** requires the administrator to enter a name for the password policy.
- **Description** allows the administrator to describe the password policy.
- **Changeable** determines whether or not a user can change his or her password.
- **Change Required** determines whether a user must change his or her password after logging into the portal for the first time.
- **Minimum Age** lets the administrator choose how long a password must remain in effect before it can be changed.
- **Reset Ticket Max Age** determines how long a password-reset link remains valid.
- **Password Syntax Checking** allows the administrator to:
    - Set a minimum password length;
    - Determine if dictionary words can be in passwords; and
    - Detail requirements such as minimum numbers of alphanumeric characters, lower case letters, upper case letters, numbers or symbols.
- **Password History** lets the administrator:
    - Keep a history (with a defined length) of passwords; and
    - Prevent users from changing their passwords to one that was previously used.

- **Password Expiration** lets the administrator:
  - Choose how long passwords remain active before they expire; and
  - Select the age, the warning time and a grace limit.
- **Lockout** allows the administrator to:
  - Set a number of failed log-in attempts that triggers a user's account to lock; and
  - Choose whether an administrator needs to unlock the account; or
  - Determine if a password becomes unlocked after a specific duration.

From the list of password policies, the administrator can perform other actions:

- **Edit** allows the administrator to modify the password policy.
- **Permissions** allows the administrator to define which users, user groups or roles have permission to edit the password policy.
- **Assign Members** allows the administrator to search and select users assigned to this password policy.
- **Delete** shows up for any password policies added beyond the default policy.

Single Sign On (SSO)

Liferay DXP provides many options for those looking to implement SSO. Liferay DXP has integration with any SAML 2.0 compliant Identity Providers by serving as a SAML 2.0 Service Provider via its SAML app. This includes popular third-party Cloud based Identity Providers (IdP) like Ping Federate and Okta.

For deploying Liferay DXP on premise or in a private cloud, DXP supports SSO with Active Directory Federated Services (ADFS), Oracle Access Manager, CA Siteminder, Tivoli Access Manager, Apache Shibboleth, OpenAM, Novell Identity Manager and CAS. Liferay DXP's ability to serve as a SAML 2.0 Service Provider enables easy integration with other on-premise SAML 2.0 based Identity Providers.

Customers that do not have a dedicated Identity Provider may still benefit from Liferay DXP's SSO capabilities. DXP has built-in LDAP integration, with support for Microsoft Active Directory (AD), Oracle LDAP, Novell Directory and other LDAP providers. For customers relying upon Internet Explorer as their primary browser, Liferay DXP provides integration with NTLM.

For customers looking to define an identity management strategy, Liferay DXP can serve as a SAML 2.0 Identity Provider. This provides added flexibility for customers looking to federate their Liferay DXP-based solution with applications like Salesforce and Workday.

Entitlement Management

Roles and Permissions

Liferay provides a central platform for determining enterprise content policy, including who can edit and publish content, files, communities and applications. Liferay uses a fine-grained "Roles-Based-Access-Control" system which combines the use of both roles and permission.

Permissions define the access and ability given to a certain entity (users, user groups, organizations, etc.). A role is a collection of permissions that defines a function.

Roles are very powerful and allow site administrators to define various permissions in whatever combinations they like. This gives the administrator as much flexibility as possible to build the site with the hierarchy needed to maintain proper security. Roles can be assigned at various granularities to an entity and are the primary means for granting or restricting access to content. When a role is assigned to a user, the user is granted the permissions that have been defined for the role. Therefore, Liferay allows multiple user types to access a single URL and access a unique page view depending on the user's role, group, organization or personal preferences.

In addition to regular roles, site roles and organization roles, Liferay also uses the concept of teams. Site administrators within a specific site can create teams. The permissions granted to a team are defined and applied only within the team's site. The permissions defined by regular, site and organization roles, by contrast, are defined at the portal level, although they are applied to different scopes. The differences between the four types of roles can be described as follows:

- Regular role: Permissions are defined at the portal level and are applied at the *portal* level.
- Site role: Permissions are defined at the portal level and are applied to one specific *site*.
- Organization role: Permissions are defined at the portal level and are applied to one specific *organization.*
- Team: Permissions are defined within a specific site and are assigned within that specific *site*.

Defining Permissions on a Role

Roles serve as repositories of permissions. When a role is assigned to a user, the user receives all the permissions defined by the role. So, to use a role, you need to assign members to it and define the permissions you want to grant to members of the role.

Portal permissions cover portal-wide activities that comprise several categories, such as site, organization, location, password policy and more. This allows the administrator to create a role that, for example, can create new sites within the portal. This would allow the administrator to grant users a particular permission without making them overall portal administrators.

For Liferay, the permissions fall into the following hierarchy of categories:

CONTROL PANEL

- General Permissions
- Users
  - Users and Organizations
  - User Groups
  - Roles
  - Password Policies
  - Monitoring
- Sites
  - Sites
  - Site Templates
  - Page Templates
- Apps
  - Store
  - Purchased
  - App Manager
  - Plugins Configuration
  - License Manager
- Configuration
  - Portal Settings
  - Custom Fields
  - Server Administration
  - Portal Instances

SITE ADMINISTRATION

- Pages
  - Site Pages
- Content
  - Recent Content
  - Web Content
  - Documents and Media
  - Blogs
  - Message Boards
  - Wiki
  - Dynamic Data Lists
  - Bookmarks
  - Polls
  - Software Catalog
  - Tags
  - Categories
  - Recycle Bin
- Users
  - Site Memberships
  - Site Teams
- Configuration
  - Site Settings
  - Site Template Settings
  - Application Display Templates
  - Social Activity
  - Mobile Device Families
  - Applications
  - [too many to list]

MY ACCOUNT

- Account Settings
- My Pages

The three basic categories of permissions are Control Panel, Site Administration and My Account. By default, any user can manage their user account via the permissions belonging to the My Account category. Site administrators can access the site administration tools belonging to the Site Administration category. Portal administrators can access the entire Control Panel. For custom roles, the administrator can mix and match permissions from as many categories as necessary. The administrator can fine-tune which actions are defined for a role within a specific application like the Message Boards.

Permission for Delegating Administration

With permissions, site administrators are also able to delegate responsibility for administrative tasks to other users, such as configuring social activities. Once these permissions have been assigned to the chosen role, any users assigned to the role will be able to manage the site's configuration.

OAuth

OAuth delegates user authentication to the service provider. An OAuth-enabled plugin uses a token ITSto prove it is authorized to access the user's third-party profile data and invoke authorized services. By implementing OAuth in your plugin, you get the best of both worlds—access to an outside service provider, and your users' trust that the plugin won't have access to their protected resources.

In addition, Liferay DXP instances can act as OAuth service providers: you can provide a means for your users to use their portal credentials to access other services that have OAuth configured. We refer to such portals as Liferay Service Portals. The OAuth framework lets Liferay Service Portal administrators specify well-defined service authorizations. Once authorized, the users can invoke the services via OAuth clients.

Audit Application

Liferay's Audit app makes it easy to see a history of what users are doing in applications, in order to pinpoint the cause of events that disrupt security. The app stores audit trails in log files, a database, or advanced log analysis tool like Splunk or Elastic's ELK so that they are searchable. Customer security teams may utilize these logs to identify events and the users triggering those events.

Out of the box, Liferay's Audit app captures events for user login, logout, password changes, entitlement (roles and permission) changes, group membership changes and more.

Conclusion

Today, all businesses run on software, and it is important for financial institutions to question the security features in a product. When purchase decisions are made without attention to secure processes, enterprises can introduce vulnerabilities to their critical data and systems. With its extensive options for implementing secure processes, Liferay Digital Experience Platform is able to ensure enterprise-grade security across all its applications.

Moving Forward

Schedule a Free Demo

A Liferay team member is available to give you an in-depth look into the features and solutions possible with the latest version of Liferay DXP. Hundreds of organizations in financial services, healthcare, government, insurance, retail, manufacturing and other industries use Liferay. Request a free demo by visiting liferay.com/request-a-demo

Liferay Global Services

Learn how Liferay's Global Services team can support your Liferay DXP project with a Go Live consultation. Contact sales@liferay.com for more information.

Liferay makes software that helps companies create digital experiences on web, mobile and connected devices. Our platform is open source, which makes it more reliable, innovative and secure. We try to leave a positive mark on the world through business and technology. Hundreds of organizations in financial services, healthcare, government, insurance, retail, manufacturing and multiple other industries use Liferay. Visit us at liferay.com.

© 2018 Liferay, Inc. All rights reserved.

181022