Liferay DXP Application Security Features

Executive Summary

Liferay Digital Experience Platform (DXP) is a complete platform that was built with security in mind. For over two decades, security, compliance, and data protection have been at the core of our product, offerings, and operations at Liferay. Because of our expertise and emphasis on security, we've been able to provide trusted solutions to industries where security is paramount, like finance, government, and healthcare.

Liferay DXP enables enterprises to manage users and site access on a certified platform that is flexible enough to meet changing compliance standards. 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 your unique 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.

Certifications

Liferay takes threats to the availability, integrity, and confidentiality of our clients' information seriously. As such, Liferay is an ISO/IEC 27001:2013 certified provider whose Information Security Management System (ISMS) has received third-party accreditation from the International Standards Organization.

Compliance with this internationally recognized standard confirms that Liferay's security management program is comprehensive and follows leading practices. The scope of our ISO/IEC 27001:2013 certification addresses the development, operations, maintenance and delivery of services for all of our products, including Liferay DXP.

For more information, read the Trust Center pages.

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.

Liferay DXP also supports encrypted connections to integrated systems such as LDAP and databases, where supported.

Encryption

Liferay DXP utilizes encryption and hashing for a variety of features. 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 PBKDF2WithHmacSHA1/160/1300000 encryption algorithm, which generates 160 bit hashes using 128,000 rounds to apply very good security with medium performance trade off. The number of rounds can be increased to further increase cryptographic strength. In addition, customers may choose alternative encryption algorithms as needed.

Symmetric encryption is configured to use Advanced Encryption Standard (AES) with 128b keys; both encryption algorithm and key size can be configured to pass any compliance requirements. Asymmetric encryption used in the SAML application relies on user-provided X.509 certificates or self-generated pair or RSA 2048b keys.

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 it to 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.

Data Privacy

In Liferay DXP, access to personal data is controlled by the permission framework. No unauthorized user has access to Personally Identifiable Information (PII).

To support **General Data Protection Regulation (GDPR)** and **California Consumer Privacy Act (CCPA)**, Liferay DXP includes features to anonymize user personal data and export of the user data. Liferay Portal supports deletion or retention (deactivation) of personal accounts and data out-of-the-box.

Web Service Security Layers

Liferay DXP relies on several layers of security measures to protect Liferay's web services, including customer deployed web services and/or REST applications.

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 configuration. Any attempted web service invocation coming from a non-whitelisted IP address will automatically fail.

Authentication Verification Layer: The authentication verification layer serves to validate provided credentials and to create portal authorization contexts for Service Access Policies, OAuth 2.0 Resource Server access checks and user permissions layer.

The layer contains various implementations to support different clients and their authorization technologies. Portal provides out-of-the-box solution for Single Page Application and JavaScript clients relying on active portal session and protects them against CSRF attacks, legacy web service API clients using HTTP Basic and Digest schemes, remote applications using new OAuth 2.0

Bearer tokens or any other custom developed client and authorization credentials through AuthVerifier extension points.

Service Access Policy Layer: Service access policies allow the portal administrator to whitelist web service endpoints available to remote clients. They allow public services to require no authentication as well as restrict endpoints available to clients relying on user password, OAuth 2.0 and other supported credentials.

Service access policies are especially useful when remote applications such as mobile devices or Liferay Sync instances need to access Liferay Portal's JSON Web Services. 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, wildcards can be used to reduce the number of service classes and methods that must be explicitly whitelisted.

User Permission Layer: Properly implemented web services have data permission checks. The user invoking a web service must have the appropriate Liferay DXP permissions to manipulate with the respective entities and data.

OAuth 2.0 Resource Server Authorization Layer: This layer, similar to Service Access Policies, restricts access to JSON WS and REST resources for clients relying on OAuth 2.0 authorization credentials. The access is restricted based on OAuth 2.0 scopes that were granted during authorization phase by user and must match the scopes required by the respective JSONWS or REST application endpoints.

The portal administrator can modify the available JSON WS and REST resource scopes and their names, it is possible to redefine the scope checks for a particular service, application or whole portal. API extension points also allow developers to modify the process using custom code.

CORS Support: Cross-origin resource sharing (CORS) is a standard allowing users to request resources stored on another origin, or web server at a different domain. Users can leverage CORS on Liferay in order to enable JavaScript clients or Single Page Applications to use Liferay Portal web services as a headless server.

Password Policies

Customers leveraging Liferay DXP's out-of-the-box authentication can apply 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. Learn more about the fields available in the Password Policy settings here.

Authentication and User Management

Authentication in Liferay is flexible; you can just use the Sign In widget to log in, and guests can use the same widget to create accounts with default permissions. Nearly every element of the default authentication experience can be changed by an administrator, including:

- Multi-factor authentication
- Single Sign-On (SSO)
- Lightweight Directory Access Protocol (LDAP) for user validation
- Account Restrictions

Multi-factor authentication

Multi-Factor Authentication (MFA) provides better security by requiring users to prove their identity in multiple ways, or factors. The basic user name/password combination is augmented with one or more further, configurable factors. These include the default One Time Password (OTP) and configurable IP address, time-based OTP, FIDO2-compliant devices, and because the system is extensible, any factor you wish to write.

Federated Identity Management

Federated Identity Management (FIM) is a common set of policies, practices, and protocols used for end users and devices across groups. Establishing a FIM helps companies safely exchange data and lowers the risk associated with authentication of identity information. Within this greater strategy is Identity

Management (IdM) which includes authentication, authorization, and onboarding and deactivation of user accounts.

Liferay provides customers with a robust Single Sign On (SSO) framework for federated authentication and Role Based Access Control (RBAC) system that allows customers to configure the management of users in Liferay DXP as desired. Users can be onboarded and synchronized using LDAP, SAML 2.0, or OpenID Connect, supported by major players like MS Active Directory, MS Active Directory Federated Services (i.e. Azure), Google Identity Platform, and others.

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.

Federated Authentication (Single Sign On)

Liferay DXP offers a robust suite of Single Sign On (SSO) and federated authentication options to streamline your login experience.

SAML 2.0 Integration: Liferay DXP seamlessly integrates with any SAML 2.0 compliant Identity Provider (IdP), including popular cloud-based options like Azure Active Directory, Okta, and PingFederate. This extends to on-premise and private-cloud solutions like Microsoft Azure AD and Active Directory Federation Services (ADFS) for a truly versatile SSO experience.

OpenID Connect Support: Liferay DXP implements the client-side (Relying Party) of the OpenID Connect protocol. This lightweight layer built on OAuth 2.0 allows you to delegate user authentication to providers like Google, leveraging existing user accounts for a smooth login process. This is ideal for organizations without a dedicated IdP.

Token-Based SSO: Liferay DXP offers standardized token-based SSO support for Shibboleth, SiteMinder, Oracle OAM, and any token-based SSO product. This enables easy integration with existing authentication infrastructures.

OpenAM Integration: For organizations with diverse authentication schemes and identity repositories, Liferay DXP integrates with OpenAM to centralize user management.

Kerberos Authentication: Additionally, Liferay DXP supports Kerberos configuration for seamless authentication of Microsoft Windows™ accounts.

In essence, Liferay DXP caters to a wide range of SSO and federated authentication needs, ensuring a secure and convenient login experience for your users.

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.). Every data related user action is guarded by a permission.

A role is a collection of permissions that defines a function, for example Content Reviewer. Roles are very powerful and allow 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.

For more information on roles and permissioning, read this article.

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, users assigned to the role will be able to manage the site's configuration.

Impersonation

The impersonation feature allows administrators to act on behalf of respective users, drop privileges, and use specific user permissions to troubleshoot a situation or understand permission setup.

OAuth 2.0 Support

OAuth 2.0 is an industry-standard authorization protocol (RFC 6749) where users can grant access for a third-party site to fetch or manipulate user data without user's authentication credentials.

Liferay DXP allows the portal administrator to register trusted third-party sites and configure the scope of accessible web services or REST applications resources. When a portal user visits the third-party site that needs portal data, the site can ask the user to authorize an access to the Liferay DXP resources for the site. The third-party site then accesses the Liferay DXP data and resources on behalf of the user, but only with the user permissions and OAuth 2.0 token, never with the user credentials.

Liferay DXP supports different kinds of applications like standard web sites, mobile native devices applications, Single Page Applications, or server-side-only jobs.

For more information on how OAuth 2.0 works with Liferay, read this article.

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 searchable database or advanced log analysis tool like Splunk or Elastic's ELK. 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, and group membership changes. Custom audit events can also be implemented.

Conclusion

Today, all businesses run on software, and it is important for enterprises to consider the security features in a product. Security must be a priority during procurement processes, otherwise you will waste time with a solution that isn't able to secure or protect your data and even introduce vulnerabilities into your systems.

Liferay has made security a priority of our platform to ensure enterprise-grade security across all our applications, so that you can conduct your business operations with a platform you can trust.

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. See why 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.

Security in the Cloud

Launching your solutions in the cloud can provide additional security benefits. With Liferay SaaS offering, customers do not have to worry about applying security-related updates for the infrastructure or services stack. Liferay is responsible for security updates as well as 24/7 runtime protection of your SaaS deployment, which is built on top of Liferay PaaS.

Customers that need code customizations or more control over their solutions can use Liferay PaaS to deploy and manage their DXP in a certified environment hosted by Liferay and provided by Google Cloud.

Learn how Cloud offerings secure your solution >

Both Liferay SaaS and PaaS are audited annually by external vendors and keep security certifications like SOC 2 Type II, ISO 27001, HIPAA, CSA Star Level 2, etc. For more information please visit Liferay's Trust Center.

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

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.