Liferay®

Identity Management and Governance

Manage users while ensuring data compliance and the security of your digital environment

Liferay DXP is built with security in mind. This includes mitigation of common security vulnerabilities and exploits. Robust identity management and security tools ensure that users get access to the content and services they need, organizations adhere to data privacy regulations, and sites are protected from potential security threats.

Benefits

Secure web services with 4 security layers that cover IP permission, server access policies, and user authentication and permissions.

Easily control what content users see or the functions they have access to at the account, user, or role level, using detailed permissions settings.

Securely manage identity with authentication widgets or other configurable options, such as multi-factor authentication and SSO.

Core Features

Users, Organization, and Account Management

Every person who accesses a Liferay site is considered a user. With Liferay DXP, you have a default Admin user who has complete control of and access to the system, that enables you to manage and configure what users are able to do on a site, based on different levels of access:

- Administrators have full system access and control of the site.
- Guests have view access to public pages and sites, but cannot create or add content unless permitted.
- Users have the same access as guests but are also able to create content.

As an administrator, you can add, edit, and delete users. Administrators also have access to user views to help diagnose permission issue. You also have the ability to manage your users' metadata (like name or department), permissions, and the status of activation in the Control Panel or through the API.

To help you organize and administer your users, you can use Liferay's Organizations entity. This allows users in a group to be in a distributed hierarchy and enables large organizations to empower and delegate users to administer their organizations.

Personal Data Management

Liferay's User Associated Data (UAD) framework helps your organization meet two of the General Data Protection Regulation's (GDPR) technically challenging requirements:

- The right to data portability. Users have the right to receive their personal data in a machine-readable format.
- The right to be forgotten. Organizations can remove the ability (even for administrators) to glean information that could lead to knowing the identity of the user whose personal data was erased or anonymized. This mainly consists of deleting the identity information from the system and erasing or anonymizing content the user has interacted with, so it cannot be tracked to a real person.

Management and Authentication

There are several aspects of securing a Liferay installation including, but not limited to, following the best security practices for your hosting environment, database, search provider, application server, and Liferay DXP itself. 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

For permissions, Liferay has a Robust Role-Based Access Control (RBAC) system, where users assigned to roles are scoped to apply only in a specific context such as a site, organization, or globally.

Securing Web Services

Service Access Policies define what services or service methods can be invoked remotely. Liferay Web Services have a multi-layered and configurable approach to security and authorization:

- IP Permission Layer controls access to the portal from previously white-listed addresses.
- Service Access Policies provide access to remote APIs.
- Authentication Verifiers verify provided credentials and check permissions of users when invoking a web service.
- Cross-Origin Resource Sharing configuration enables retrieving resources from trusted sources only.