Add Users and Manage Permissions with Liferay DXP

Lecture Script

# Introduction

Slide 1: [Read out Slide Number]

Hello, my name is [your name]. In this module, we’ll discuss how to Add Users and Manage Permissions in Liferay DXP 7.4 *[seven dot four].*

Slide 2:

The Key Takeaways for this module are:

Users can be created or imported from existing databases.

Users can be organized into hierarchical structures and individual groups.

Permissions are actions on resources and can be assigned to Users through Roles.

And, roles exist in three scopes: Regular, Organization, and Site.

Slide 3:

There are a few exercise prerequisites for this module. Make sure you have a Java JDK installed to run Liferay DXP. That can be found using the link on the screen, which will direct you to download Java JDK 8. Note that using more recent versions of Java JDK may result in errors.

Also, be sure that you have unzipped the module exercise files in the appropriate folder structure for your OS. For Windows, we recommend the C:\Liferay path. For Unix systems, we recommend the [user-home]/liferay path.

Slide 4:

Our use case for this module is the Mondego Group, an international financial services organization that is using Liferay DXP to create its customer service portal and its employee portal. The Mondego Group needs to create User structures that represent its Subsidiaries, Department Structures, and Customer and Investor Groups. Intro to Use Case: The Mondego Group

Slide 5:

Mondego also needs to control User access for actions on the platform, including the Organization of User Accounts into Organizations and User Groups, the Creation of Mondego Sites, and Platform Configuration.

Slide 6:

Mondego will use the following Key Performance Indicators to determine the success of its portals. The company is looking to:

Increase the number of Users on the platform.

Improve the organizational structures of platform Users.

Improve User autonomy through the assignment of Roles.

Reduce User permissions to only include those relevant to the User’s position.

*(End Video One)*

# Adding Users to Liferay DXP

Slide 7:

In this section, we’ll learn how to Add Users to Liferay DXP.

Slide 8:

There are several ways to add Users to the platform in Liferay DXP.

New Users can be created from the Administrator account, using either the Control Panel or a REST API. We’ll demonstrate how to add Users from the Control Panel in our exercise “Create New Users.”

Users can also register themselves. By default, Guests, or unauthenticated users, can create authenticated Users accounts. You can manage account registration and authentication methods in Instance Settings under User Authentication.

And, finally, Users can be synced from an LDAP *[el-dap]* server. For Organizations that manage Users with LDAP, Users can be imported into and exported from Liferay DXP.

We’ll discuss importing and authenticating Users on the next slides.

For our Use Case, the Mondego group can use all three methods to add Users. Mondego has an LDAP server of existing Users that can be imported to Liferay DXP. The platform Administrator creates accounts for employees on the employee portal. And customers can register for their own accounts on the customer portal.

Slide 9:

In Liferay, there are two primary methods for importing and authenticating outside Users:

Importing Users from an LDAP server, which we just mentioned.

And, using Single-sign on, OAuth 2, and SAML authentication options.

Again, if your organization already uses an LDAP server, Users can be imported and authenticated by syncing the LDAP server with Liferay.

Since most businesses will have a variety of users on their platforms—including Employees, Customers, Business Partners, and Contractors—other authentication options may be useful.

In addition to importing users from the LDAP server, the Mondego Group also plans to set up another authentication method, such as Single-Sign On, for registering and authenticating new customer accounts.

Slide 10:

Liferay integrates with LDAP and allows administrators to keep the systems in sync by determining what data needs to be imported from the LDAP server and determining what data needs to be exported back to the LDAP server.

LDAP Mapping in Liferay includes options to: enable import from LDAP, import or auto-generate passwords, import users as individuals or groups, create a Role per group on import, enable export and group export from Liferay DXP back to the authentication system, and use the LDAP password policy in Liferay.

Slide 11:

General Liferay DXP authentication settings can be configured to control User authentication protocols, User password protocols, and Account creation/verification protocols.

These authentication settings are configured in the Control Panel under Configuration > Instance Settings > User Authentication. The general section, picture here, includes configurable settings for: how users authenticate, how to manage user passwords, who can create accounts, and how accounts are verified.

For example, we disable the email verification requirement in our exercises since we won’t set up a mail server.

Depending on the Site, Mondego may choose to disallow strangers to create accounts. Additionally, for internal or partner Sites, Mondego requires that a User register with a company email address, whereas the public facing Sites simply require a valid email address for account creation.

Slide 12:

By default, Liferay uses the Sign In widget to authenticate Users. However, this is not the only authentication method available. Other forms of authentication within Liferay DXP include: OAuth 2.0 *[O Auth two point oh]*, SSO configuration, and Multi-Factor Configuration.

OAuth 2.0 authorizes users to access certain data by enabling an application to access another application’s data without revealing a user’s credentials. For example, when someone signs into a website using Facebook, Google, or another account.

SSO Configuration options include SAML *[sam-el]*, Facebook Connect, OpenID Connect, OpenSSO, Token Based SSO, and others. In Liferay, Single Sign-On must be enabled before it can be used.

Multi-factor Authentication requires that users prove their identity in multiple ways (or factors), which may be a priority when it comes to sensitive information or content on a Site.

Our use case example, the Mondego Group, opts to use Multi-factor authentication on its banking and investments Sites as an added safety measure. Other Sites on the Mondego Platform may opt for another authentication method, such as one of the SSO options.

Keep in mind that Liferay DXP takes a “secure by default” philosophy. Take caution when modifying security-specific defaults to avoid misconfiguration or an insecure deployment. For more information on User authentication and security, see the “Secure Your Liferay DXP Platform” module or the Securing Liferay documentation.

Slide 13:

Let’s revisit our Use Case for this module. The Mondego Group can add Users to its platform in a variety of ways, including:

Importing Users from its existing LDAP server and maintaining the data on that server as needed.

Creating new Users from the Administrator account whenever new employees or partners are added to the platform.

Allowing Users to register and create their own accounts on the Mondego banking and investment Sites.

Mondego also has several options for authenticating users, including SSO, SAML, and Multifactor Authentication.

Slide 14:

We’ve now reached our knowledge check for this section.

The Mondego Group needs its platform to include several kinds of users, including employees, partners, and customers. It can do this by:

Importing existing users from an (blank)

Creating new Users using the (blank) account

Enabling Open (blank) and setting (blank) options

Authentication options available to Mondego with Liferay DXP include (blank), (blank), and (blank).

Mondego Administrators can keep Liferay and their LDAP in sync by establishing what data needs to be (blank) and (blank).

Take a moment to pause the video and fill in the blanks yourself.

[Pause for 10 seconds before continuing.]

*(End Video Two)*

# Manage and Organize Users

Slide 21:

In this section, we’ll discuss how you can Manage and Organize Users in Liferay DXP.

Slide 22:

Organizations give you the ability to organize Users hierarchically according to the structure of real-world groups and companies. Organization Administrators can manage all the Users in their organization as well as all of its Sub-Organizations.

The defining feature of Organizations is that they are purely about organizing Users in a hierarchy. This is a distinct concept from Sites and Site hierarchies, which will be discussed in another module.

Users can belong to multiple Organizations as needed.

The Mondego Group, for example, uses Organizations to organize its subsidiaries, branches, departments, and even customers. The subsidiary, Mondego Investments, can organize its departments and regional offices using the Organizations feature. The Departments organization has its own sub-organizations for Human Resources and Marketing, and the Regional Offices has Toronto and London sub-organizations. And, both organizations still fall under the Mondego Investments head organization.

Slide 23:

Organization Sites are Sites that can be created in conjunction with an Organization. This means that Organization Administrators become the Site administrator and members of the Organization become members of the Site.

Organization Sites are not required for an Organization to exist in Liferay DXP. Depending on the nature of the Organization, some may not need a distinct Organization Site.

So, with our use case example, because each subsidiary within the Mondego Group has its own internal structure and departments, Organization Sites allow the subsidiaries to organize content specific to each Organization and Sub-Organization. Mondego Investments, for example, can create distinct Sites for each Department or Regional Team.

Slide 24:

Another way to organize Users in Liferay is through User Groups. User Groups are logical groupings of Users that traverse the Organizational structure. Users Groups are created for a specific purpose and are not bound by the hierarchy of Organizations.

Some common use cases for User groups include: managing Site membership by assigning membership to an entire User Group, managing the personal pages of Users in the group, and collecting permissions and assigning Roles to an entire group rather than individuals.

There are two primary ways to create User Groups on the platform: User Groups are created by default when an LDAP group is imported, or User Groups can be manually created to intentionally create new groupings for a specific purpose.

So, for our use case, Mondego Banking may choose to create User Groups for various reward levels for credit cards offered by the bank. Rather than managing permissions and access to pages reserved for different rewards levels on an individual basis, Mondego Bank can organize Users into the appropriate User Group for their rewards level and grant permissions to the entire group. These permissions will not be limited by the individual’s position in the platform hierarchy.

Slide 25:

By default, all Users have a Profile and Dashboard. A User Group Site is a template of pages that is added to the Profile or Dashboard of every User Group member.

Unlike Organization Sites which can be created in conjunction with the Organization, User Group Sites don’t appear as a separate Site that Users access but rather as Pages on individual Users’ Dashboards.

These pages are dynamic and show with any other pages a User has on their personal Site. Users cannot modify Pages inherited from the User Group.

So, for Mondego Banking’s credit card rewards system, a Silver card holder who has been assigned to the Silver User Group will have pages relevant to that group show up on their personal Site or User Dashboard.

Slide 26:

Let’s review our use case. Mondego Investments needs to organize its Users, so it creates Organizations to reflect the departments, including Advisors, Marketing, and Human Resources.

Suborganizations, including Sales and Events, are then created under the Marketing Organization. A Marketing Organization Site is also created to allow Users to view content specific to that Organization.

To organize Users for one of the rewards programs, Mondego can create User Groups for the different reward levels. A User Group for Platinum Card holders can also have a User Group Site, which adds a template of pages unique to the Platinum rewards level to each User’s Dashboard.

Slide 27:

And now we’re at our knowledge check.

To reflect the hierarchical structure of its company and its subsidiaries, Mondego can use (blank).

Mondego’s Human Resources department can create an (blank) to manage relevant content.

(Blank) can be created to manage Mondego Users that share a similar purpose but belong to different subsidiaries or departments.

To make sure these Users can find relevant pages on their Profile or Dashboard, a (blank) can be added.

Take a moment to pause the video and fill in the blanks.

[Pause for 10 seconds before continuing.]

*(End Video Three)*

# Roles and Permissions

Slide 37:

In this section, we’ll discuss Roles and Permissions and how to assign them to Users in Liferay.

Slide 38:

Administrators will need to control the following: Platform access, Site access, Page access, and Asset access.

As you may recall, the Administrator account is created by default in any new installation of Liferay DXP. The Administrator has full permissions to modify every facet of the instance.

As the default Administrator, you can create a new admin account by either creating a new User or assigning an existing User to the Administrator Role under Regular Roles. We’ll discuss Regular Roles in a minute. It is highly recommended that you add another Administrator account after you start your Liferay instance.

Mondego’s main platform Administrator will need to create or assign additional Administrators once the instance is up and running to distribute the workload. Since different Sites and Organizations may have different work plans, an Admin for each level is essential.

Slide 39:

The administrator manages access through permissions. Permissions are actions that can be taken on platform resources, including things like: adding content, editing content, viewing content, uploading images, and creating pages.

Permissions can also be scoped. Application Scoped Permissions are permissions granted on each widget or administrative application. Asset Scoped Permissions are permissions for individual assets, for instance a blog post or document folder.

Permissions are important for ensuring that Users on the Mondego platform can access everything they need without unwittingly changing something important. Mondego Customers, for instance, need to be able to manage their account information but they should not be able to change the integral components of the customer portal.

Slide 40:

We apply permissions using Role. Roles are collections of permissions that can be granted to Users. Roles are scoped to the following contexts.

Regular Roles are scoped to the entire platform. Assigning a Regular Role to a User means they’ll have the permissions defined in that role across the entire platform. For example, our Platform Administrator is a Regular Role. Mondego, our use case, could add several Regular Roles to manage the platform.

Organization Roles are scoped to the Organization level. This means the permissions defined for those Roles only apply to members of the Organization or Sub-Organization and on the Organization Sites. Mondego’s Marketing department, for example, can use Organization Roles to assign permissions to its members.

Site Roles are scoped to the Site level. This means that permissions apply to a specific Site (or Sites). A User with a Site Role only has those permissions in the appropriate Site. So, a Site Administrator for Mondego Banking does not have those administrator permissions on the Mondego Investments Site.

Two additional scopes new in Liferay DXP 7.3 and 7.4 include Asset Library Roles and Account Roles. Asset Library Roles are limited to Asset Libraries. A Content Creator in an Asset Library can only create content in that library. Account Roles relate to the new Accounts feature, so those roles apply permissions specific to Account management, including Account Users and Account Groups.

In order to save time, Roles can be applied to several Users at once rather than one at time. Roles can also be applied to Sites, Organizations, User Groups, and User Segments.

Slide 41:

Administrators can create and assign custom Roles. When creating Roles, they should consider the following:

What actions and resources are required for the Role?

What Scope will this Role primarily function in?

Keep in mind that Roles should be created using the principle of least permissions. This is to make sure that people only have the permissions they need to do their job and nothing more, so it's a good principle to follow when creating custom Roles.

The Mondego Group needs several of its managers to be able to access multiple Sites on the Platform. Though at first glance it may be tempting to issue them Regular Roles, the principle of least permissions reminds us that the fewest number of permissions should be granted. In this case, assigning multiple Site Roles would allow the Users to manage their necessary Sites without granting them too much access.

Slide 42:

Roles can also be integrated with Workflows. Workflows can be created with actions assigned to specific Roles. If a Role is assigned in a Workflow Definition but does not already exist, the Role will be auto-generated.

We’ll talk more about Workflows in a separate Module, so for now the main thing to know is that Workflow is a process to review a resource, like making sure content is copy-edited before it's published. Users with a workflow-designated Role can: receive notifications when a workflow process begins, assign a workflow task to themselves, and provide feedback in the workflow processes (e.g., approving or rejecting).

For the Mondego Group, workflows are a vital part of daily operations. A review workflow could be as simple as sending a document from a creator to a reviewer before publication. For Mondego’s more formal publications, they implement a multistage review process. Articles are drafted, sent to copy editors, revised, sent to the legal team for approval, and revised further before anything is published.

Slide 43:

Let’s consider how the Mondego Group is using Roles and Permissions.

The Mondego Investments Site can manage which Users can view, edit, and add content using Liferay’s fine-grained permissions and by creating Roles.

To ensure that Users only have the permissions necessary for their job function, Mondego primarily assigns Roles at the Organization or Site level.

Users with Roles in the Mondego Marketing Organization cannot make changes to the main Site and the Banking Site Administrator cannot change the Investments Site.

The Mondego Investments team creates a workflow and assigns a task to the Copyeditor Role. Since this is not an existing Site Role, it will be auto-generated.

Slide 44:

Now, we’ve reached our Knowledge Check.

To make sure Mondego Users do not perform unapproved (blank) on (blank), the Administrator can manage and assign Permissions.

Permissions are collected and granted to Mondego Users as (blank), which are scoped at three different levels:

(Blank)

(Blank)

(Blank)

(Blank)

(Blank)

Mondego workflows (blank) if they are assigned but don’t already exist.

Go ahead and pause the video and fill in the blanks.

[Pause for 10 seconds before continuing.]

*(End of Video Four)*

# Controlling Specific Permissions on Sites

Slide 55:

In this section, we’ll talk about Controlling Specific Permissions on Sites.

Slide 56:

Each resource on a Site has an Options menu that includes a Permissions menu. As you can see in the picture, clicking the three dots beside each item gives you an options menu. And if you select Permissions it opens a grid where you can customize Permissions according to Role.

For Sites or Pages made from Templates and with Inherit Changes switched on, Permissions need to be managed from the Template. For example, widgets on a page created from a template will only show the Export/Import option unless Inherited Changes is switched off.

On the Mondego Investment Site, there are certain resources that are reserved for Site Members. The Site Administrator can remove permissions for Guest Users to view an Offers Page, requiring Users to sign in to access it.

Slide 57:

Site Teams are groups of Site Members that can be given additional permissions on specific resources on a Site.

Site teams are the preferred method for assigning permissions in a single Site.

Since Site Administrators can’t create Roles, Site Teams allow the Administrator to grant Users permissions on the Site regardless of the Users’ existing Roles.

Site Teams are created and managed from the Site Menu > People >Teams.

The Mondego Group can use Site Teams for editing and managing the various blog posts and articles published on one of their regional Sites. Since the publications are infrequent, creating an ad hoc group using Site Teams rather than creating a distinct Site Role adheres to the rule of least possible permissions and allows the Site Admin to make changes to Team membership without needing more permissions.

Slide 58:

Let’s review the Use Case.The Mondego Investments Site Administrator can use Site Teams to assign tasks and roles to Users without creating official Site Roles.

The Publications Site Team manages the collecting, writing, reviewing, and publishing of articles on the Site.

Since some of these articles are reserved for members and don’t need to be viewed by Guest Users who are simply interested in learning about Mondego Investments, the Site Administrator can use the Permissions Menu to set certain articles and resources to be viewable only by Users or Members, not Guests.

Slide 59:

Let’s go over our Knowledge Check.

Mondego’s Regular, Site, and Organization Administrators can grant or remove a User Role’s permissions on a Site resource in the (blank).

The Mondego Investments Site Administrator can assign permissions to Users to manage certain resources on the Site using (blank).

Pause the video and take a moment to fill in the blanks.

[Pause for 10 seconds before continuing.]

*(End Video Five)*

# Summary

Slide 65:

We’ve now reached the end of the module, so let’s review:

Liferay DXP allows platform administrators to create new Users or import existing ones from an LDAP server.

The primary methods of authenticating Users are Single-Sign On, OAuth2, and SAML. Multi-factor authentication can also be configured.

Organizations allow you to organize Users hierarchically and can be associated with Organization Sites.

User Groups are logical groupings of Users that go outside the Organizational structure.

Slide 66:

Permissions are actions on resources on the platform.

Roles are collections of permissions that can be assigned to Users.

Roles come in three scopes: Regular (entire platform), Organization (within the context of an organization), and Site (within the context of a Site).

Each resource on the Site has an associated Permissions menu.

Site Teams are groups of Site Members that can be given additional permissions on specific resources on a Site.

Slide 67:

For more information regarding this module’s topic, you can consult the documentation on Users and Permissions at the link on the screen:

[https://learn.liferay.com/dxp/latest/en/users-and-permissions.html]

For general questions about using Liferay’s products, visit learn-dot-Liferay-dot-com.

[https://learn.liferay.com/]

*(End Video Six)*