Secure Your Liferay DXP Platform

Lecture Script

# Introduction

Slide 1:

(Read out Slide Numbers)

Hello, my name is [your name]. In this module, I’ll be showing you how to Secure Your Platform in Liferay DXP 7.4 [seven dot four].

Slide 2:

Our key takeaways for this module are:

Multi-Factor authentication, SSO, and other User authentication methods can be configured for Users to sign into Liferay DXP.

To secure web service, Liferay DXP provides four security layers: IP permission, service access policy, authentication/verification, and User permission.

Files, documents, and media can be secured by enabling an antivirus scanner.

Slide 3:

Before we begin, make sure you have a Java JDK installed to run Liferay DXP. This can be done 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.

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. The Mondego Group has customer, partner, and employee portals, each with their own unique security concerns and priorities. The group needs robust security measures on its banking and investment Sites to protect its customers and their finances, and it also needs to ensure that company information and assets are protected. To establish strong security on its platform, Mondego wants to:

Enable Multi-Factor Authentication.

Define permissions and policies for passwords and remote services.

Ensure file, document, and media security.

Slide 5:

The relevant Key Performance Indicators for the Mondego Group will be as follows:

Increase account security by configuring multi-factor authentication

Increase platform and document security by enabling antivirus and utilizing other security tools

Reduce the risk of unauthorized access to documents and services

*(End of Video 1)*

# Securing Liferay with User Authentication

Slide 6:

In this section, we’ll discuss how to secure your platform with a variety of user authentication methods available in Liferay DXP 7.4.

Slide 7:

In Liferay DXP, the Sign In widget is the default tool for authenticating users. The Sign In widget uses the instance database to authenticate users. Users can log in using one of the following authentication types: Screen Name, Email Address, and User ID.

Screen Name is a username established at account creation. It can be changed by the User as needed. Email Address, which is the default authentication type used by the sign in widget, is also established at account creation and can be changed later. User ID is an automatically generated ID number associated with the account at creation and cannot be changed.

Only one of these authentication types can be used at a time to authenticate Users when they sign in.

By default, Guests can create an account at the sign in page. Certain pages and functions may be hidden unless an account is created. When a guest creates an account, they will need to fill out their information, including providing an email address and screen name, agree to any Terms and Conditions, and provide a security question or reminder query to be used when recovering passwords. These can be managed in the Control Panel. If guests should not be able to create accounts, you can disable this feature in the Control Panel.

The Mondego Group, our use case, wants Guests to create accounts since many of its features require an account. Mondego can also change the authentication type from Email Address to Screen Name.

Liferay takes a “Secure by Default” approach, so the default security settings for user authentication are enabled with that in mind.

Slide 8:

General Users Authentication settings include enabling or disabling automatic login, password reset, new account creation, and email verification. Note, that in our exercises for this and other modules we disable “require email verification” since we will not have a mail server set up. In an active instance, requiring email verification adds some extra security.

In addition to these general settings, there are two additional tabs in User Authentication settings for managing Reminder Queries and Reserved Credentials. Reminder Queries, which are enabled by default, allow you to set password reminders and custom questions. This adds another layer of security if Users need to recover their passwords. The Reserved Credentials tab allows you to reserve certain screen names or email addresses so that Users are unable to use those when creating their accounts.

In addition to maintaining the default settings of allowing strangers to create accounts but requiring them to verify their email addresses, Mondego requires Reminder Queries for all new accounts. This adds a layer of security, especially should Users need to recover their account passwords. Mondego can also reserve specific Screen Names for administrative use only.

Slide 9:

CAPTCHA and reCAPTCHA can be configured to prevent bots from creating and accessing accounts. By default, Create Account CAPTCHA and Send Password CAPTCHA are enabled in Liferay DXP, both using Simple CAPTCHA which uses a text verification. This means that Users have to complete a CAPTCHA when they create a new account and if they need to request a new password. You can also enable Simple CAPTCHA for Message Boards and Forms.

You can also use Google’s reCAPTCHA, which provides more accessible CAPTCHA options, such as audible CAPTCHA, but also requires an external service to be configured separately. CAPTCHA settings are managed in the Control Panel under System Settings.

By default, any new Users must complete a CAPTCHA when they create a Mondego account. Mondego can manage what kind of CAPTCHA is offered, including switching to use a reCAPTCHA, which includes more accessible options for Users.

Slide 10:

Password Policies add additional security to an instance of Liferay DXP by configuring certain password properties, including: Password Changes, Password Syntax Checking, Password History, Password Expiration, and Lockout.

Password Changes allows or prevents a user from changing a password and sets a time limit for a password reset link.

Password Syntax Checking requires passwords to meet a certain syntax, checking for length and words. You can specify whether dictionary words are permitted, set a minimum number of characters, upper and lower case letters, symbols, numbers, and overall length.

Password History lets you set how many passwords to keep in history to prevent old passwords from being reused.

Password Expiration determines whether passwords expire. If enabled, you can set the length of time passwords are valid, when and whether a warning is sent, and whether there is a grace limit before a password change is forced.

Lockout allows you to set the maximum number of fail attempts before an account is locked, how long lockout lasts, and how long the record of failed attempts is stored.

Liferay DXP ships with a default password policy that can be modified as needed. All new Users are automatically assigned the default policy.

Additional Password Policies can be created as needed, and Users are then assigned as members of the new policy in order for it to apply to them. Users can be assigned individually or as an Organization. New Password Policies can also be added to the portal-ext.properties file

Since the Mondego Group handles sensitive information, the company highly recommends strong passwords for all its Users, both internal and external. Users are also expected to regularly change their passwords for added security. To ensure that Users follow these recommendations, Mondego creates a new Password Policy that requires a password change every six months, disallows the use of passwords that have been used in the past two years, and requires that the password consist of at least 10 characters including one symbol, one upper case letter, one lower case letter, and one number.

Slide 11:

Additional authentication methods can be configured in Liferay DXP depending on the specific instance needs. The methods available for configuring authentication of users and applications include:

**LDAP** [el-dap], which integrates with an existing LDAP server and authenticates users against those in the directory.

**SAML** [sam-el], which provides SSO and SLO by using Identity Providers and Service Providers.

**Kerberos**, which authenticates Microsoft Windows accounts with Liferay DXP

**OpenID Connect**, an authentication layer built on OAuth 2.0, which enables user authentication using accounts from other systems.

**OpenAM** (v13 only), which is an SSO solution that integrates Liferay DXP into an infrastructure containing several authentication schemes.

**Token-Based Solutions**, which standardize support for Shibboleth, SiteMinder, Oracle OAM, and any SSO that propagates a token via HTTP request parameter, HTTP request header, HTTP cookie, Session Attribute. Tokens contain the User’s screen name, email address, or User ID.

**OAuth 2.0**, which is an industry-standard authorization protocol that shares select credentials with various clients, authorizing password-less access to portions of user-owned resources.

And, **Multi-Factor Authentication**, which requires Users to prove identity in multiple ways, such as a username and password AND a One Time Password.

To better manage the security of the instance, Mondego can configure one of these method for User authentication. For instance, they already have an LDAP server storing existing Users. They can integrate with the server and authenticate Users against the directory. Alternatively, Mondego might consider using Multi-Factor Authentication, which we’ll look at more closely now.

Slide 12:

Configuring Multi-Factor Authentication provides more robust security by requiring Users to prove their identity in multiple ways, including One Time Password, Configurable IP Address, Time-Based OTP, and FIDO2 [fido-two] Compliant Devices. To use MFA, one-factor forms of authentication, such as Basic Auth, Digest Auth, or WebDAV, should be disabled.

One Time Password is the default factor and requires a working mail configuration to send the OTP to users via email. Enabling MFA without a working mail server will lock everyone out of the system.

In Liferay DXP 7.4, two additional factors are shipped, though disabled by default: the IP Address checker and the Time-Based OTP.

The IP Address MFA Checker checks Users’ IP addresses with allowed IP address masks to verify identity.

The Time-Based OTP MFA Checker is based on the Google App Authenticator. This adds a profile option where Users can generate a code that provides an additional, time-restricted factor.

The last MFA method that can be configured in Liferay DXP is FIDO2, or Fast IDentity Online 2. This allows Users to authenticate without a password by using biometrics (such as fingerprint readers), mobile devices, or other security keys. Once FIDO2 is enabled for the platform, Users can register and use their FIDO2 compliant devices to sign in.

If multiple factors are enabled, the MFA Checkers must be given a numeric order to determine which executes first, with the highest number running first.

For extra security, Mondego enables Multi-Factor Authentication, using an OTP in addition to the standard username/password login. Users log in by entering their credentials and then retrieving the OTP from their email.

Slide 13:

Let’s review how the Mondego Group can authenticate users.   
As a financial services company, Mondego prioritizes security of its Users’ accounts. Mondego Users should be confident that their accounts are properly protected but also be able to retrieve their accounts if necessary. To accomplish this, Mondego has a variety of options, such as:

Requesting email verification, CAPTCHA, and Reminder Queries from Users upon account creation

Enabling Multi-Factor Authentication and requiring Users to authenticate with an OTP or other MFA checker when they log in

Slide 14:

Now, we’ve reached our Knowledge Check for this section.

For basic but secure User authentication, Mondego can use the *Blank* with *Blank* enabled to allow secure password recovery.

To prevent bots from creating scam accounts, Mondego requires Users to complete a *Blank* when they create an account.

Mondego can also use a variety of methods to authenticate Users, including:

* + *Blank*
  + *Blank*
  + *Blank*

*(End of Video 2)*

# Securing Web Services

Slide 20:

In this section, we’ll discuss securing web services in Liferay DXP 7.4.

Slide 21:

Liferay DXP provides four security layers for web services.

In the IP Permission Layer any web service invocation coming from a non-approved IP address automatically fails.

In the Service Access Policy Layer, methods corresponding to a web service invocation request must be approved by service access policies.

In the Authentication//Verification Layer, which is browser-only, web service invocation requests coming from a browser must include authentication tokens.

In the User Permission Layer, the User invoking a web service must have appropriate permissions.

Slide 22:

Liferay DXP provides several adjustable authorization layers:

Remote IP and HTTPS transport check limits access to Liferay DXP’s Java servlets

Extensible Access Control Policies layer performs portal service-related authorization checks

Extensible Role-based Permission Framework for Liferay assets

Portlet container security checks control portlet access

Remote IP check for remote API authentication methods

Service Access Policies to control access to remote APIs

Authentication Verifiers that verify provided credentials

Cross-Origin Resource Sharing configuration to enable retrieving resources from trusted sources only

Slide 23:

Let’s look at some of these security and authorization layers.

Liferay DXP uses the Role-Based Permissions Framework to manage User access to assets and resources on the platform. Roles are created with the principle of least permissions in mind. To reduce unnecessary or unauthorized access, Users are granted Roles with only the fewest required permissions. By default, new Users are given the “User” Role. In most cases, this grants the Users permission to view a Site, Pages, and the User’s individual account. Other Roles with more tailored permissions must be assigned to a User by the Administrator.

Permissions and Roles are covered in greater detail in the module, “Add Users and Manage Permissions with Liferay DXP.”

The Mondego Group, our use case, will use Role-Based permissions to manage User access to their Sites. Creating distinct Roles and applying them to individuals, organizations, user groups, or segments allows the group to make sure that people can access only the assets, resources, and Sites that they need to in order to manage their accounts or complete their work.

Slide 24:

Service Access Policies define what services or service methods can be invoked remotely. Service Access Policies respect the permissions system.

Keep in mind, Service Access Policy:

Names must be unique per portal instance.

Names can only include certain characters.

Titles, but not names, can be localized.

Service signatures are entered one per line.

By default, twelve Service Access Policies are enabled, including five related to the system:

Asset Entry Default updates the view counter for an asset when the asset is retrieved

Authorized OAUTH2 SAP allows all REST requests authorized by OAuth 2

Calendar Default makes it possible to search public events in the calendar

System Default allows access to country/region services by JavaScript calls so Users can switch languages

System User Password allows any method to be invoked (so long as the User has the required permission)

The other seven policies relate to OAuth and JSON web services.

Slide 25:

Authentication Verifiers authenticate remote invocations of Liferay Portal’s API in a centralized and extensible way. Authentication Verifiers have two main responsibilities:

Verify provided credentials using registered AuthVerifier instances.

And, Create portal authorization contexts based on verification results.

Authentication Verifiers that ship with Liferay DXP include Basic Auth Header, Digest Authentication, HTTP Tunnel Extender, Image Request, Portal Sessions, Request Parameter, Tunnel Auth.

Authentication verifiers focus on verifying authentication not providing credentials. It does not issue tokens or credentials or display the Sign In widget. Essentially, the authentication verification layer is a border between authentication and authorization.

Slide 26:

Cross-Origin Resource Sharing (CORS) can be configured to enable resource retrieval from trusted sources only.

An Origin is a web server at a different domain. A Resource is an asset stored on the server. A Cross-Origin Request refers to when you request resources stored on another origin.

If the Mondego Group has an external server that stores assets or resources that they want to be able to call to use or access from their main Site, they can configure CORS to allow access to certain origins.

Slide 27:

Let’s go over our use case. The Mondego Group needs to secure web services, managing who is allowed to access certain content and what services can be accessed remotely.

Mondego HR personnel need to be able to access employee documents and company policies. To keep non-HR personnel from accessing this content, the system administrators can use Roles and Permissions to limit or extend User access to certain documents and Sites.

To customize what services and service methods can be invoked remotely, Mondego creates a custom Service Access Policy which establishes a list of approved web services.

One of the Web Teams at Mondego uses an external server to host a collection of resources. By setting up Cross-Origin Resource Sharing, Mondego enables that team to retrieve only those approved resources.

Slide 28:

We’ve reached our Knowledge Check for this section.

Mondego needs robust security for its system, and Liferay DXP has four security layers for web services:

* *Blank*
* *Blank*
* *Blank*
* *Blank*

The Role-based Permissions Framework to prevent users from accessing unauthorized content on Mondego’s Sites. To allow users to access resources hosted on another web server, Mondego can configure *Blank*.

*(End of Video 3)*

# Securing Content and Fine-Tuning Security

Slide 34:

In this section, we’ll take a look at securing content on your Liferay platform and fine-tuning security settings.

Slide 35:

Portal Properties are used to fine-tune security features in Liferay DXP. Features that can be configured include:

Liferay Portal’s HTTPS web server address.

The list of allowed servers to which Users can be redirected.

The list of portlets that can be accessed from any page.

The file types allowed to be uploaded and downloaded.

As it starts creating its platform with Liferay, Mondego has a checklist of features and elements that need robust security. The security team can fine-tune additional security features as needed to ensure that the platform remains safe, no insecure or malicious content is uploaded, and everything deploys successfully.

Liferay DXP allows a great deal of flexibility when it comes to fine-tuning or disabling security features. However, it is important to exercise caution when configuring or altering default security settings to avoid an insecure system. Additional information on security can be found in the Liferay Security Statement, and additional security plugins can be found on the Liferay Marketplace

Slide 36:

In Liferay DXP, the AntiSamy module protects against user-entered malicious code on blogs, message boards, and other applications that allow users to post content. AntiSamy works by adding package paths to the appropriate list (sanitized or not sanitized). The module then filters HTML/CSS fragments and removes suspect JavaScript.

The AntiSamy Sanitizer is used to define entities that should be sanitized or not sanitized. The “Blacklist” filters out the designated content type while the “Whitelist” prevents the content type from being filtered. Wildcards can also be used to configure AntiSamy to sanitize only one part of Liferay DXP, such as only message boards. For example, by setting the whitelist to an asterisk and the blacklist to com.liferay.message.boards.asterisk, the AntiSamy Sanitizer will only sanitize the message boards.

AntiSamy Sanitizer by Class Name is another way for developers to configure AntiSamy. Developers specify an AntiSamy configuration XML file for each model class name.

The Mondego Group hosts a blog on one of its Sites. In order to ensure that guests leaving comments do not upload any malicious code, Mondego can configure AntiSamy to sanitize the blog comments.

Slide 37:

Another layer for securing Files in Liferay DXP is the antivirus scanner. Enabling the antivirus scanner checks all files uploaded to Liferay for viruses, automatically rejecting them if one is detected. Liferay integrates with the ClamAC Daemon [day-mon] (Clamd), which is configured and (for optimal performance) run on a separate server

To enable the antivirus scanner, first configure and start Clamd on a separate server from your Liferay instance. Then, enable antivirus for your File Store by setting a portal property or Docker environment variable. Next, start the Liferay server. Finally, under Control Panel > System Settings > Antivirus locate the Antivirus Clamd Scanner and add the hostname or IP address, port, and connection timeout time.

Mondego requires its Users to submit a variety of documents to verify their accounts or account information. To ensure that these files are secure and will not damage the Mondego system, Mondego can enable the Clamd scanner to check every document or file users upload to the platform.

Slide 38:

The default search engine in Liferay DXP is Elasticsearch. After installing and connecting Elasticsearch, the search engine is secured by:

Enabling X-Pack Security and setting up X-Pack Users

Enabling Transport Layer Security (TLS) by generating and applying node certificates and keys

Once everything is set up, security can be configured in Liferay DXP by entering property values or using a configuration file.

As with several of the other security features on Liferay DXP, Elasticsearch is run from a separate server. To run Liferay securely, you must install the Basic level of Elasticsearch at a minimum. To configure search security in Liferay DXP, go to Control Panel > System Settings > Platform > Search. Select Elasticsearch 7 for 7.3+. The steps for earlier versions of Liferay differ, but information can be found on the Documentation site.

With any software, security is vital to prevent a server or data breach. Because Mondego needs a search function on its Sites, securing Elasticsearch is another important step to protect sensitive data.

Slide 39:

The Audit section provides a log of actions taken on the system, allowing the system administrators to determine what instance and request an event belongs to. Each item listed on the Audit page can be selected for additional details about the event.

Audit features and settings are managed under System Settings on the Control Panel. There, you can configure settings for Audit, CSV Log Message, Logging Message Audit Message Processor, Persistent Message Audit Message Processor, and Audit Log Context.

The Audit tool allows Mondego Administrators to monitor activity and events on the system. In the case of any problems or security issues, this can help the Administrator determine the origin of an issue.

Slide 40:

Let’s review how the Mondego Group can secure content on its Sites.

The Mondego Group has several Sites that feature blogs, message boards, forums, submissions forms, and other places where Users can post content or upload files. To prevent any security breaches Mondego can:

Configure AntiSamy to sanitize blogs and message boards

Enable Antivirus scanning to check all uploaded files for viruses

If the Mondego system administrators encounter any unusual activity, they can determine the source using Audit.

Slide 41:

We’ve reached our Knowledge Check for this section.

The *Blank* module is enabled on Mondego Sites to sanitize message boards and blogs in case Users post content with *Blank code*.

New Mondego customers fill out a form that includes a field for file upload. To ensure that no dangerous files are uploaded, the *Blank* must be enabled.

The Mondego system administrator can check the system logs under *Blank* to verify activity on the system.

Mondego can also fine-tune security using *Blank* and by properly configuring and securing applications, like the *Blank* search engine.

*(End of Video 4)*

# Summary

Slide 49:

Let’s review what we’ve discussed in this module.

Liferay DXP provides several options for Authenticating Users, including the Sign In Widget, importing Users from an LDAP server, and configuring Single Sign On or Multi-Factor Authentication methods.

For additional security, Liferay DXP includes email verification and reminder query settings. CAPTCHA and reCAPTCHA can be enabled to deter bots.

Password Policies require that User passwords meet the established rules for syntax, changes, and expiration.

Slide 50:

Liferay DXP provides four security layers for web services: IP Permission layer, Service Access layer, Authentication/Verification layer, and User Permission layer.

The Role-based Permission Framework, Authentication Verifiers, Service Access Policies, and Cross-Origin Resource Sharing are used to manage access in the system and from the system to external sources.

Slide 51:

AntiSamy adds additional security by protecting the Liferay platform from user-entered malicious doe on blogs, message boards, and other applications that accept user-posted content.

Enabling the ClamAV Daemon antivirus scanner protects the system by rejecting any file uploads that contain viruses.

Securing Elasticsearch, fine-tuning security settings, and monitoring the Audit system logs also helps to reduce security breaches and risks.

Slide 52:

For more information on securing your Liferay DXP platform, consult the documentation listed on the screen.

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

*(End of Video 5)*