Oracle® Fusion Middleware

WebCenter Forms Recognition ALE Learnset Manager Installation Guide

14c (14.1.1.0.0)

F76454-01

August 2023

Describes how to install and upgrade ALE Learnset Manager

ORACLE®

Oracle Fusion Middleware Oracle WebCenter Forms Recognition ALE Learnset Manager Installation Guide, 14c (14.1.1.0.0)

F76454-01

Table of Contents

About ALE Learnset Manager

The ALE Learnset Manager or ALM is a web-based administration client that enables you to create, modify, and delete projects and classes which will be used by the Automated Learning Engine (ALE) to learn how to classify or extract data from documents. You can also edit classes by adding and removing training documents to improve the performance of each learnset.

Prerequisites

Before you start installing ALM, you need to ensure that the following applications are installed:

- Java Runtime Environment 8. Please make sure to use a version that is appropriate for your operating system (64 bit). For information related to download, visit https://www.oracle.com/java/technologies/javase/javase8u211-later-archive-downloads.html
- Apache Tomcat 8.5 or 9. For information related to download, visit https://tomcat.apache.org/index.html
- Microsoft SQL Server (versions 2012, 2014, 2016, or 2017) Or Oracle (versions 12c, 12c R2 or 19c)
- Word position files

  Note: All training and test documents must be uploaded with word position files. For more information, refer to the *ALE Learnset Manager Admin Guide*.
- ImageMagick 6, or 7.0.9. For information related to download, visit https://imagemagick.org/script/download.php#windows

  Notes:

  - ImageMagick is recommended for best performance in image conversion. If ImageMagick is not installed, an internal converter is used.
  - Make sure the option *Install legacy utilities (e.g. convert)* is selected during installation.
- Microsoft Visual C++ 2015 Redistributables (x64). For information related to download, visit https://www.microsoft.com/en-us/download/details.aspx?id=48145

You can install ALE Learnset Manager on the following operating systems:

Note: Only 64-bit operating systems are supported

- Windows 10
- Windows Server 2019
- Windows Server 2016

When working with Microsoft SQL Server, verify the following settings are in place.

- Go to **SQL Server Configuration Manager > SQL Server Network Configuration** and enable TCP/IP connections.
- Go to **TCP/IP > Properties > IPAll** and enter the desired port for your SQL server instance. The value is usually 1433.
- Activate SQL Server authentication.
- Prepare a database account that ALM can use.

Create a database user for Oracle Environment

To create a database user in an Oracle environment, complete the following steps:

1. Create a user account that is identified or authenticated by a specific password using the system or a predefined administrative account that gets generated during Oracle installation.

   Note: A default tablespace and a temporary tablespace are required to create the ALM user and the schema.

2. Assign **DBA** role to the user account created in Step 1.

For more information on creating users and tablespace, refer to Oracle documentation.

Create a database user for SQL Environment

For SQL environment, before installing ALM, it is recommended that you create new database user credentials in order to prevent ALM from creating tables under the master database.

To create a database user in an SQL environment, complete the following steps:

1. Create a new empty database.
2. Create a new user credential for logging on to the database server. The default database of the newly created user credentials must be mapped with the database created in Step 1.

   Note: Under **User Mapping**, assign **DB Owner** role to the database user account.

Installation Process

This section describes the installation and configuration procedure for ALE Learnset Manager.

ALM is installed with the **ALMSetup.exe** installer.

- For a Windows installation without an active user account control, double-click **ALMSetup.exe**.
- For a Windows installation with an active user account control, right-click **ALMSetup.exe** and click **Run as administrator**.

A sequence of panels is displayed. You need to enter the configuration details on each panel and click > to proceed to the next panel. In case of an error, you need to review the log messages that are displayed simultaneously during the installation process and fix the issue before you proceed. The following high-level steps need to be performed.

- Configure Target Directories
- Configure Database
- Configure User Authentication

Configure Target Directories

The REST services and the web client are deployed as a web application to an Apache Tomcat installation. Some native libraries are installed to a directory outside of Tomcat’s directory structure. That directory is also used as the data directory for local files.

To configure the target directories, complete the following steps.

1. In the **Installation Directories** dialog box, enter the details, as required. For more information on specific fields, refer to the following table.

Field	Description
Directory	Enter the name of the directory for native libraries and local data.
Tomcat Directory	Enter the name of the directory where Tomcat is installed. **Note**: Setup will try to resolve this directory automatically and set the correct value as the default value.
Name of Web Application	Enter the name of the web application, under which the application will be deployed. This name becomes part of the URL.
Tomcat URL	Enter the base URL of your Tomcat installation. **Note**: The full URL of the web application will be the Tomcat base URL and the name of the web application (for example: `http://servername:8080/ALM`). This URL is case-sensitive.

2. Click **>** to proceed.
3. If there is an existing installation, you will be prompted if the existing files should be overwritten. You can do any of the following:

- Click **Yes** to replace the files with the latest version

Or,

- Click **No** to update the configuration.

The necessary files are copied to the target locations, and the system's PATH environment variable is updated. If updating the PATH fails for some reason you will see an error message displayed in the log window. In that case, you need to edit the PATH manually and add the values that are displayed in the error message.

Configure Database

ALE Learnset Manager stores its configuration and the training sets in a database.

To configure access to the prepared database, complete the following steps.

1. In the **Database** dialog box, enter the details, as required. For more information on specific fields, refer to the following table.

Field	Description
Database Type	Select the type of the database – either Oracle or Microsoft SQL Server.
Host	Enter the name or IP address of the host on which Oracle SQL Server are running.
Port	Enter the port for TCP/IP connections - this is usually 1521 for Oracle and 1433 for SQL Server.
Oracle SID	When connecting to an Oracle database, enter the SID.
Username	Enter the username that is used to connect to the database.
Password	Enter the password that is used to connect to the database.

2. Click **>** to proceed.

The installer connects to the database and prepares the configuration repository. If there is a problem, the log message displays an error message.

Configure User Authentication

ALE Learnset Manager supports two kinds of authentication:

- An LDAP server can be used to authenticate users
- An internal user account can be used

Note: Password complexity is not enforced with internal users.

Both approaches can be combined with support for Single Sign-On (SSO). When configuring SSO, it is expected that the SSO provider protects the access to the web application and puts the name of the authenticated user into an **HTTP header** field.

To support user authentication via an SSO provider, complete these steps:

1. In the **SSO Header** field, enter the name of the HTTP header field that the SSO provider uses to submit the name of the authenticated user.
2. Configure your SSO provider so that the following paths within the web application are protected:

   /packages/framework-core/sso

   /service/session/
3. Click **>** to proceed, setting up details for the selected authentication type.

LDAP Authentication

There are two options for configuring LDAP authentication:

- All users are stored within a single node of the directory. In this case, only the server URL and a pattern is required that defines how the distinguished name (DN) of a user is constructed.
- The users are stored in a tree structure. In this case, additional information is required including a user account that can log into the LDAP server and perform a search operation for a given username.

To configure LDAP authentication with all users in a single node, complete the following steps.

1. In the **LDAP Authentication** dialog box, enter the details, as required. For more information on specific fields, refer to the following table.

Field	Description
Users are	In the **Users are** list, click **In a single node**.
Server URL	Enter the LDAP URL of the server. **Note**: URLs should start with ldap or ldaps and contain the name or IP address of the server and the port. Optionally, the URL can also include a root path within the directory. Example: ldap://ad.mycompany.com:389/DC=ad,DC= DC=mycompany,DC=com
User DN Template	Enter a template for distinguished names for user. Use `{user}` as a placeholder for the username. Example: uid={user},ou=employee,o=mycompany
User	Enter a user account that will be used to test the configuration. **Note**: This is an optional step.
Password	Enter the password for the user account that will be used to test the configuration. **Note**: This is an optional step.

2. Click **>** to proceed.

To configure LDAP authentication with users in a directory structure, complete the following steps.

1. In the **LDAP Authentication** dialog box, enter the details, as required. For more information on specific fields, refer to the following table.

Field	Description
Users are	In the **Users are** list, click **In a tree structure**.
Server URL	Enter the LDAP URL of the server. **Note**: URLs should start with ldap or ldaps and contain the name or IP address of the server and the port. Optionally, the URL can also include a root path within the directory. Example: ldap://ad.mycompany.com:389/DC=ad,DC= DC=mycompany,DC=com
User DN	Enter the distinguished name of a user account. This account will be used to connect to the LDAP server and perform search operations.
Password	Enter the password associated with the DN user account.
Search Filter	Enter a pattern for the filter that is used for searching the user whose authentication is to be checked. Use `{user}` as a placeholder for the username. When connecting to Active Directory, use the following pattern: `sAMAccountName={user}`.
Search Paths	Enter one or more paths that contain the users. **Note**: This is an optional step. Only valid LDAP paths are accepted (for example: ou=users). Multiple paths can be separated by semicolons. If no path is provided at all, the entire directory is searched.
User	Enter a user account that will be used to test the configuration. **Note**: This is an optional step.
Password	Enter the password for the user account that will be used to test the configuration. **Note**: This is an optional step.

2. Click **>** to proceed. The installer connects to the LDAP server to verify the configuration and performs an authentication with the test account, if applicable.

Internal Authentication

Internal authentication is designed to be used for very simple use cases that do not require any real user management at all, or as a fallback authentication type in combination with SSO.

To use internal authentication, in the **User** and **Password** fields, enter an appropriate username and the password associated with the username, respectively.

Authorized Users

When working with LDAP authentication or internal authentication with SSO, you can configure a list of users to use the application. Other users can log in but will not be able to access any functionality.

To set up a list of authenticated users, enter one username per line.

Apache Tomcat Troubleshooting and KB Topics

Configure Tomcat URL Character Restrictions

In the more recent versions of Apache Tomcat, such as 9.0.8, 8.5.31 and above, the characters that can be present in a URL has been restricted. For ALM to work correctly, this restriction must be relaxed. To configure your Apache installation, complete the following steps.

1. Modify the server.xml file in the Apache Tomcat Conf directory.
2. Find the Connector element that defines the port on which Tomcat receives requests. Typically, it is port 8080 but this could have been modified at your site.

```
<Connector port="8080" protocol="HTTP/1.1"
       xpoweredby="false" server="Web"
       connectionTimeout="20000"
       redirectPort="8443"
  />
```

3. Add the underlined lines and restart Tomcat.

```
<Connector port="8080"
       protocol="HTTP/1.1"
       xpoweredby="false" server="Web"
       connectionTimeout="20000"
       redirectPort="8443"
       relaxedPathChars='[]|'
       relaxedQueryChars='[]|{}^&#x5c;&#x60;&quot;&lt;&gt;'
/>
```

Note: You must apply this configuration to all Tomcat servers which have the ALE Learnset Manager web application installed.

Configure Tomcat X-Frame-Options Header

Injecting HTTP Response with the secure header can mitigate most of the web security vulnerabilities.

To enable secure HTTP header in Apache Tomcat, configuring ‘X-Frame-Options Header’ is very essential to prevent ‘clickjacking attack’.

To configure X-Frame-Options Header, complete the following steps.

1. Modify the web.xml file in the Apache Tomcat Conf directory.
2. In the **Built In Filter Definitions** section in web.xml, add or uncomment the following filter configuration, in case it does not exist already.

```
<filter>
      <filter-name>httpHeaderSecurity</filter-name>
     <filter-
class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
```

```
        <async-supported>true</async-supported>
</filter>
```

3. In the **Built In Filter Mappings** section in web.xml, add the following configuration, in case it does not exist already.

```
<filter-mapping>
    <filter-name>httpHeaderSecurity</filter-name>
    <url-pattern>/*</url-pattern>
</filter-mapping>
```

4. Save the file and restart Tomcat.

Note: You must apply this configuration to all Tomcat servers which have the ALE Learnset Manager web application installed.

Restart Apache Tomcat

Sometimes when you start and stop ALM with the Tomcat Web Application Manager, Tomcat displays the message, “Application at context path/ALM could not be started”. To prevent this issue from occurring you can either restart or update the Apache Tomcat configuration.

To restart Apache Tomcat via the services management console, complete the following steps:

1. Open the services management console.
2. Right click on the Apache Tomcat service and select **Restart** or use the **Stop / Start** options as required.

   Note: The risk with this is that the Apache Tomcat Web Application Manager could still be used to stop and start ALM and result in failures using ALM.
3. Update the Apache Tomcat configuration so that it doesn't attempt to reload the Java Native Interface every time the web application is started.

   Note: You must perform the steps above to every Tomcat web server that is running ALE Learnset Manager.

Update the Apache Tomcat configuration

To update the Apache Tomcat configuration, complete the following steps.

Note: Before proceeding with the steps below, ensure that a backup is taken of the Tomcat installation area.

1. Ensure that all dependent systems are not being used. If required, stop the relevant services and/or websites.
2. Stop the Apache Tomcat service.
3. Create a new folder called shared under the **lib** folder within the Tomcat installation area.
4. Browse to the Apache Tomcat folder where ALE Learnset Manager is installed "...\WEB-INF\lib\".
5. Move the **columbusJNI.jar** file from the location in step 4 to the new folder created in step 3.

6. Browse to the conf folder within the Tomcat installation area and open the catalina.properties files in a text editor.
7. Search for the `shared.loader` entry and update this as follows:

   ```
   shared.loader="${catalina.base}/lib/shared","${catalina.base}/lib/shared/
   *.jar","${catalina.home}/lib/shared","${catalina.home}/lib/shared/*.jar"
   ```

8. Restart the Apache Tomcat service.
9. Restart any services or websites stopped in step 1.