LDAP

Liferay DXP fully supports LDAP as a user store. Use the LDAP tab in Instance Settings's Authentication page to connect Liferay DXP to an LDAP directory. Users can be imported into Liferay DXP from LDAP or exported to LDAP from Liferay DXP. If your organization already stores user information on an LDAP server, it's convenient for both users and administrators to simply have the LDAP user information imported into Liferay DXP. Importing LDAP user information to Liferay DXP means that users don't have to remember an extra set of credentials for Liferay DXP. Importing LDAP user information to Liferay DXP also means that administrators don't have to create a whole new set of user accounts for Liferay DXP. In this article, you'll learn how to connect Liferay DXP to an LDAP server and how to configure import settings, export settings, and related LDAP configuration settings.

Configuring Liferay DXP's LDAP Settings

To access Liferay DXP's LDAP configuration settings, navigate to *Control Panel* → *Configuration* → *Instance Settings*, then scroll down and expand the form's *Authentication* section. Go to the *LDAP* tab. Use this form to connect Liferay DXP to an LDAP directory.

You configure the global values from the LDAP tab of the Authentication page.

Enabled: Check this box to enable LDAP Authentication.

Required: Check this box if LDAP authentication is required. Liferay DXP then won't allow a user to log in unless he or she can successfully bind to the LDAP directory first. Uncheck this box if users with Liferay DXP accounts but no LDAP accounts can log in to Liferay DXP.

LDAP Servers: Liferay DXP supports connections to multiple LDAP servers. Use the Add button beneath this heading to add LDAP servers. Each LDAP server has the following configuration options:

Import/Export: You can import and export user data from LDAP directories using the following options:

- *Enable Import:* Checking this box to cause Liferay DXP to do a mass import from your LDAP directories. Leave this unchecked to keep the default behavior, which synchronizes users only when they log in.

- *Enable Export:* Check this box to enable Liferay DXP to export user accounts from its database to LDAP. Liferay DXP uses a listener to track any changes made to the `User` object. Liferay DXP pushes updates out to the LDAP server whenever a `User` object is modified. Note that by default on every login, fields such as `lastLoginDate` are updated. When export is enabled, this has the effect of causing a user export every time the user logs in. You can prevent updates to users' `lastLoginDate` fields from triggering LDAP user exports by setting the following property in your `portal-ext.properties` file:

```
users.update.last.login=false
```

- *Enable Import on Startup:* Checking this box instructs Liferay DXP to run the LDAP user import when it starts up. Note: This box only appears if you check the *Enable Import* box described above.

Use LDAP Password Policy: Liferay DXP uses its own password policy by default. This can be configured on the Control Panel's Password Policies page. Check the *Use LDAP Password Policy* box if you want to use the password policies defined by your LDAP directory. Once this is enabled, the Password Policies tab states that you are not using a local password policy. You must now use your LDAP directory's mechanism for setting password policies. Liferay DXP cannot enforce these policies; the best it can do is pass through the messages returned by your LDAP server. It does this by parsing the messages in the LDAP controls the server returns. By default, Liferay DXP is configured to parse the messages returned by the Fedora Directory Server. If you use a different LDAP server, you must customize the messages in *System Settings* → *Foundation* → *System LDAP Configuration*.

Once you've finished configuring LDAP, click the *Save* button.

LDAP OPTIONS AVAILABLE IN SYSTEM SETTINGS

Although most LDAP configuration can be done from Instance Settings, there are several configuration parameters that are only available in System Settings. In previous versions of Liferay DXP, system scoped settings for LDAP were set in the `portal.properties` file and modified using a `portal-ext.properties` file. Those settings must now be made via System Settings.

If you need to change any of these options, navigate to *Control Panel* → *Configuration* → *System Settings*. Go to the *Foundation* section and find the entries with LDAP in the title.

Note: To use `config` files for LDAP server configuration, you must specify the Virtual Instance ID (in the source, the variable name is `companyId`) in the exported configuration file, because servers are defined at the instance scope, not the system scope. To do this, specify the virtual instance ID somewhere in the file like this:

```
companyId=1234
```

- On the *LDAP Auth* page, you can set the authentication method and the password encryption algorithm. The Bind authentication method is preferred by most vendors so you don't have to worry about encryption strategies. Password compare does exactly what it sounds like: it reads the user's password out of LDAP, decrypts it and compares it with the user's password in Liferay DXP, syncing the two. If you use password compare, you can also choose the encryption algorithm to use for the comparison.

- On the *LDAP Import* page, you can configure import settings from LDAP. One example is the import methods. If you set this to User, Liferay DXP imports all users from the specified portion of the LDAP tree. If you set this to Group, Liferay DXP searches all the groups and imports the users in each group. If you have users who do not belong to any groups, they are not imported.

- Use the *System LDAP Configuration* entry to manage error properties like *Error password age keywords* which lets you set a list of phrases from error messages which can possibly be returned by the LDAP server. When a user binds to LDAP, the server returns *controls* with its response of success or failure. These controls contain a message describing the error or the information that is returned with the response. Though the controls are the same across LDAP servers, the messages can be different. The properties described here contain snippets of words from those messages and work with Red Hat's Fedora Directory Server. If you are not using that server, the word snippets may not work with your LDAP server. If they don't, you can replace the values of these properties with phrases from your server's error messages. This enables Liferay DXP to recognize them.

Note: When you make a change in System Settings, it takes effect for the virtual instance you're in. If after changing a setting you create a new virtual instance, that virtual instance inherits the settings of the one it was created from as defaults. For example, say you have virtual instances named A, B, and C. From A, you modify *Error password history keywords*. This change appears only in A, not in B or C. Then from A, you create virtual instance D. The change to *Error password history keywords* appears in D (not B or C), since D defaults to A's settings because you created it from A.

In summary, if there's a configuration you need to set up Liferay DXP with LDAP, and you don't find it in Instance Settings, look in the LDAP System Settings entries.

ADDING LDAP SERVERS

Click on the *Add* button beneath the LDAP Servers heading to add an LDAP server connection. If you have more than one LDAP server, you can arrange the servers by order of preference using the up/down arrows. When you add an LDAP Server, you must provide several pieces of data so Liferay DXP can bind to that LDAP server and search it for user records. Regardless of how many LDAP servers you add, each server has the same configuration options.

Server Name: Enter a name for your LDAP server.

Connection: These settings cover the basic connection to LDAP.

- *Base Provider URL:* The link to the LDAP server. Make sure the Liferay DXP server can communicate with the LDAP server. If there is a firewall between the two systems, check to make sure the appropriate ports are opened.

- *Base DN:* The Base Distinguished Name for your LDAP directory. It is usually modeled after your organization. For a commercial organization, it may look similar to this: `dc=companynamehere,dc=com`.

- *Principal:* By default, the LDAP administrator user ID is populated here. If you have removed the default LDAP administrator, you will need to use the fully qualified name of the administrative credential that you use instead. You need an administrative credential because Liferay DXP uses this ID to synchronize user accounts to and from LDAP.

- *Credentials:* This is the password for the LDAP administrative user.

This is all you need to make a regular connection to an LDAP directory. The rest of the configuration is optional. The default attribute mappings usually provide enough data to synchronize back to the Liferay DXP database when a user attempts to log in. To test the connection to your LDAP server, click the *Test LDAP Connection* button.

Checkpoint

Before proceeding to fine tune Liferay DXP's LDAP connections, ensure the following steps have been taken:

1. The LDAP connection has been enabled in the *Control Panel*. Depending on your needs, LDAP authentication may be required so that only users who have been bound may log in.

2. *Export/Import*: for users in a clustered environment, this should be disabled so that there are no massive imports on every node upon start up.

3. When adding the LDAP server, the *Server Name*, *Default Values*, *Connection* values are correct. It is always a good idea to click the *Test LDAP Connection* before saving.

SECURITY

If you are running your LDAP directory in SSL mode to prevent credential information from passing through the network unencrypted, you must perform extra steps to share the encryption key and certificate between the two systems.

Click *Start* → *Administrative Tools* → *Certificate Authority*. Highlight the machine that is the certificate authority, right-click on it, and click *Properties*. From the General menu, click *View Certificate*. Select the Details view, and click *Copy To File*. Use the resulting wizard to save the certificate as a file. You will also need to import the certificate into the *cacerts keystore*. The import is handled by a command like the following:

```
keytool –import –trustcacerts –keystore /some/path/jdk1.5.0_11/jre/lib/security/cacert
```

The *keytool* utility ships as part of the Java SDK.

Once this is done, go back to the LDAP page in the Control Panel. Modify the LDAP URL in the Base DN field to the secure version by changing the protocol to `ldaps` and the port to `636` like this:

```
ldaps://myLdapServerHostname:636
```

Save the changes. Your Liferay DXP now encrypts its authentication to LDAP.

Managing LDAP Server

Users: This section contains settings for finding users in your LDAP directory.

- *Authentication Search Filter:* The search filter box can be used to determine the search criteria for user logins. By default, Liferay DXP uses users' email addresses for their login names. If you have changed this setting, you must modify the search filter here, which has been configured to use the email address attribute from LDAP as a search criterion. For example, if you changed Liferay DXP's authentication method to use screen names instead of the email addresses, you would modify the search filter so it can match the entered log in name:

    ```
    (cn=@screen_name@)
    ```

- *Import Search Filter:* Depending on the **LDAP** server, there are different ways to identify the user. The default setting is usually fine:

    ```
    (objectClass=inetOrgPerson)
    ```

- *User Mapping:* The next series of fields allows you to define mappings from LDAP attributes to Liferay DXP fields. Though your LDAP user attributes may be different from LDAP server to LDAP server, there are five fields Liferay DXP requires to be mapped for the user to be recognized:
    - *Screen Name* (e.g., *uid*)
    - *Password* (e.g., *userPassword*)
    - *Email Address* (e.g., *mail* or *email*)
    - *First Name* (e.g., *name* or *givenName*)
    - *Last Name* (e.g., *sn*)

Note: If you intend to create or import users with no email addresses, then you must set `users.email.address.required=false` in your `portal-ext.properties`. With this set, Liferay auto-generates an email address combining the user ID plus the suffix defined in the property `users.email.address.auto.suffix=`. Finally, make sure to set Liferay and LDAP authentication to something other than email address.

```
If you want to import LDAP groups as Liferay DXP user groups, make sure to
define a mapping for the Liferay DXP group field so that membership information
is preserved:

+   *Group* (e.g., *member*)

The other LDAP user mapping fields are optional.
```

The Control Panel provides default mappings for commonly used LDAP attributes. You can also add your own mappings.

- *Test LDAP Users:* Once you have your attribute mappings set up (see above), click the *Test LDAP Users* button and Liferay DXP will attempt to pull LDAP users and match them with their mappings as a preview.



Figure 1: Testing LDAP Users

Groups: This section contains settings for mapping LDAP groups to Liferay DXP user groups.

- *Import Search Filter:* This is the filter for finding the LDAP groups that you want to map to Liferay DXP user groups. E.g.,

  ```
  (objectClass=groupOfNames)
  ```

  Enter the LDAP group attributes you want retrieved for this mapping. The following attributes can be mapped. The *Group Name* and *User* fields are required, the *Description* is optional.

  - *Group Name* (e.g., *cn* or *o*)
  - *Description* (e.g., *description*)
  - *User* (e.g., *member*)

- *Test LDAP Groups:* Click the *Test LDAP Groups* button to display a list of the groups returned by your search filter.

Export: This section contains settings for exporting user data from LDAP.

- *Users DN:* Enter the location in your LDAP tree where the users will be stored. When Liferay DXP does an export, it will export the users to this location.
- *User Default Object Classes:* When a user is exported, the user is created with the listed default object classes. To find out what your default object classes are, use an LDAP browser tool such as JXplorer to locate a user and view the Object Class attributes stored in LDAP for that user.

- *Group Default Object Classes:* When a group is exported, the group is created with the listed default object classes. To find out what your default object classes are, use an LDAP browser tool such as *Jxplorer* to locate a group and view the Object Class attributes stored in LDAP for that group.

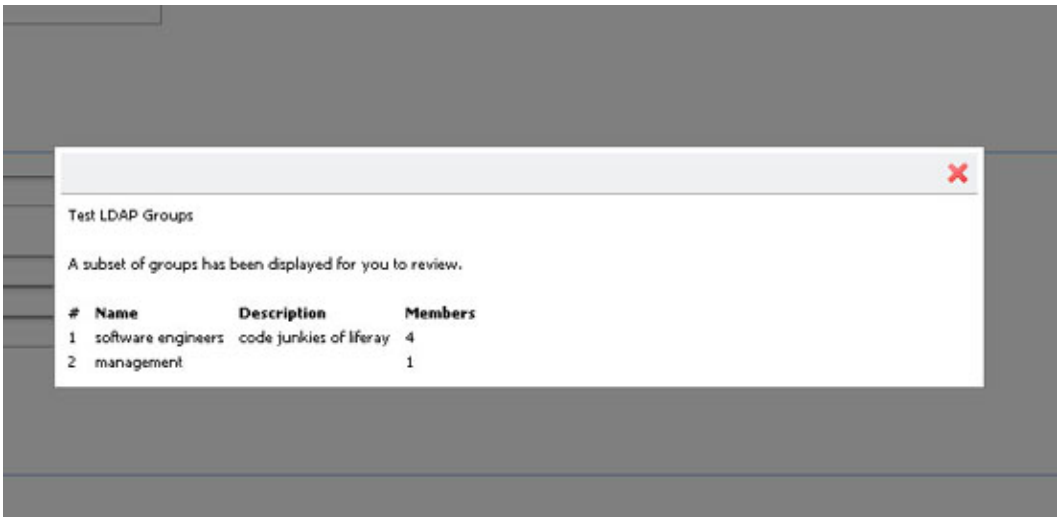


Figure 2: Mapping LDAP Groups

Once you set all your options and tested your connection, click *Save*. From here, you can add another LDAP server or set just a few more options that apply to all of your LDAP server connections.

Note: If a user changes a value like a password in Liferay DXP, that change is passed to the LDAP server, provided Liferay DXP has enough schema access to make the change.

Now you know how to connect an LDAP server to Liferay DXP and how to configure user import behavior, export behavior, and other LDAP settings.

Related Topics

Liferay DXP Security Overview Logging into Liferay DXP

« Authentication Verifiers Token-based Single Sign On Authentication »

¿Fue útil este artículo?

Sí No

¿Necesitas más ayuda?

Abre un ticket

Contacta con nosotros

Pregunta en la Comunidad

Liferay University
Forma a tu equipo en los puntos esenciales del uso de Liferay con videos detallados y ejercicios prácticos diseñados para simular una formación presencial

Liferay Global Services
Aumenta tu conocimiento sobre el producto y el desarrollo gracias a expertos que te ayudarán a maximizar tu ROI

© 2023 LIFERAY INC. ALL RIGHTS RESERVED