

LDAP Preferences

Preferences

- [Patrons](#)
- [Items](#)
- [Circulation](#)
- [Codes](#)
- [Circulation Groups](#)
- [Z39.50](#)
- [Sounds](#)
- [Setup](#)
- [Services](#)
- [SIS Integration](#)
- [Advanced Bookings](#)

How helpful was this page?



Unknown macro: 'rate'

Tell us what we can improve.

Related Blog Posts

Blog Posts

- [Blog: Winter storms—recompute due dates](#) created by [Bethany Brown](#)
Jan 23, 2024
[Alexandria](#)
- [Blog: Cleaning up the grade table—Authority Control](#) created by [Bethany Brown](#)
Apr 26, 2023
[Alexandria](#)
- [Blog: Make a calendar just for the senior class!](#) created by [Bethany Brown](#)
Aug 02, 2022
[Alexandria](#)
- [Blog: When does an overdue item become lost?](#) created by [Bethany Brown](#)
Mar 15, 2022
[Alexandria](#)
- [Blog: Setting rules—Patron Policy Preferences](#) created by [Bethany Brown](#)
Mar 08, 2022
[Alexandria](#)
- [Blog: Seeing double \(barcodes\) on patrons and items?](#) created by [Bethany Brown](#)
Feb 23, 2022
[Alexandria](#)
- [Blog: Automatic email notices... What are you waiting for?](#) created by [Bethany Brown](#)
Nov 17, 2021
[Alexandria](#)
- [Blog: Winter \(break\) is coming! Are your period due dates set?](#) created by [Bethany Brown](#)
Oct 20, 2021
[Alexandria](#)

- Blog: [Unused Barcodes: Reporting for Duty](#) created by [Bethany Brown](#) Sep 15, 2021 [Alexandria](#)
- Blog: [Introducing... FAQs!](#) created by [Morgan](#) Jul 07, 2021 [Alexandria](#)

[Save as PDF](#)

LDAP

SYSTEM-A/TT



LDAP Preferences



This page has been moved to <https://support.goalexandria.com/ldap-preferences/>

LDAP supports user-authentication for open or active directories.

Lightweight Directory Access Protocol (LDAP) is an application protocol for querying and modifying directory services running over TCP/IP. Alexandria supports user-authentication using existing log-on credentials maintained on a separate directory server. With LDAP enabled, administrators can now choose to manage these credentials on a central LDAP server as these credentials may change frequently and often need to be standardized across many different systems. A permanent record **must** exist locally in the Alexandria database for all patrons and operators that use the system however their log-on credentials can be managed outside of Alexandria on your LDAP server directly.

Note that LDAP is an add-on that requires registration.



Operator usernames and barcodes must be unique. Please make sure your Alexandria patrons do not have the same barcode as an operator.

How Does it Work?

When a user enters credentials in any login dialog, COMPAnion software will first check if they are Alexandria credentials and try to find a match. If no match is found, the credentials will be sent to the specified LDAP server in the form of a BIND. If the BIND is successful, the software will locate the user's record within the local database by searching the information returned in the specified Local ID field from the LDAP server. Either way, once the record is found, the user will be logged in.

Last Updated: \$

Still getting used to it? Switch to the old view.

SYST

LDAP

Off

These settings configure the LDAP application protocol for querying and modifying directory services running on TCP/IP. Alexandria supports querying an LDAP server for the purpose of authenticating operator and patron accounts.

You are **not registered** for this add-on.

LDAP Domain

LDAP Server

Port

389

Allow non-SSL connections

LDAP Server Type

Windows Active Directory Macintosh Open Directory

Base DN for all LDAP users

User ID

cn

Local ID

Settings

If you are a Centralized Catalog these settings will apply to **all sites** within your controller.

Enable LDAP

Click this toggle.

LDAP Domain

Enter the name of your LDAP domain, such as *yourdomain.com*. The domain name is used in conjunction with sAMAccountName to produce a complete userPrincipalName.

LDAP Server

Enter the full name of the LDAP server, such as *yourdomain.com*. This is the host address of the LDAP server for network communication.

Allow Non-Secure Connections (optional)

Check this box if you would like Alexandria to use non-TLS connections when it cannot make an TLS connection.

We highly recommend that you secure communications with the LDAP server by requiring TLS. TLS configuration is performed at the system level. When these settings are correctly configured for secure communications with your LDAP server, Alexandria will be able to communicate with the LDAP server securely.

LDAP Server Type

Select Microsoft Active Directory or macOS Open Directory.

Base DN for all LDAP Users

Enter a DN that matches all the users, i.e. *cn=users,dc=ldap,dc=yourdomain,dc=com*.

Multiple Base DNs can be specified if separated by semicolons, i.e. *cn=staff,ou=COMPanion,dc=demo,dc=goalexandria,dc=com;cn=student,ou=COMPanion,dc=demo,dc=goalexandria,dc=com*.

User ID

Select the **User ID** from the dropdown menu. This is the LDAP login name; for an *Open Directory*, this is typically uid (i.e. "uid=yourlogin"). For an *Active Directory* this is typically sAMAccountName or userPrincipalName.

Local ID

Enter the LDAP database username that contains the patron username or patron barcode in Alexandria in the **Local ID** field. This **must** be one of the users' LDAP attributes; common attribute names include uid, uidNumber, givenName, cn, and others.

Test Login

Enter a username and password to test your settings. Since the test password is not encrypted, we suggest using a non-administrative login for this test. Unlike other logins, it can be used and configured only on the LDAP server; no actual operator-level login is required.

Click **Test** to continue. It will attempt to log into the LDAP server using the settings and credentials you've entered. LDAP cannot be enabled until the test is successful. If any of your settings are invalid, the test may stall for several minutes before it fails. Check your settings and test login, then try again.

Once the test is successful, click **Save** in the upper right corner of the window to save your settings.

More LDAP Testing

If configured correctly, your users should be able to log into Alexandria using the same login credentials as configured on the directory server for their account. However, sometimes difficulty arises. In these cases, verify your preferences settings and test whether the Base DN and other information you have specified is accurate to your configuration.

We have found that Active Directory configurations seem to prefer binds using the user's CN while OSx's Open Directory prefers the uid (i.e. user identification). The use of [ldapsearch tool](#) is suggested. For example:

```
ldapsearch -x -v -H ldap://LDAP.yourdomain.com -b"cn=users, dc=LDAP, dc=yourdomain, dc=com" -D"cn=testing user id,  
cn=users, dc=LDAP, dc=yourdomain, dc=com" -w the users password -ZZ
```



Non Secure Connection Testing

The -ZZ parameter requires successful connection utilizing StartTLS over port 389. If you have selected to Allow Non-Secure Connections, omit this in your testing with ldapsearch as well.

Alternately, [ldp.exe](#) can be utilized for testing in a Windows environment.