LDAP Connector FAQ's:

What is the LDAP Connector?

Lightweight Directory Access Protocol (LDAP) Authentication allows user information to be maintained in **one centralized location**. User credentials can be shared between the LDAP Directory and the Centricity2 website User Management Systems.

LDAP authenticates user names and passwords using your LDAP Directory rather than your Centricity2 website. If your LDAP administrator changes the password for a user within your LDAP Directory, that user's password is **automatically updated** in your Centricity2 website.

LDAP can **automatically create user accounts** in your Centricty2 website for any users entered in your LDAP Directory. When users first sign in to an LDAP enabled Centricity2 website with a user name and password combination that the website does not recognize, LDAP allows the website to attempt to authenticate with user credentials in your LDAP Directory. If that authentication is successful, your Centricity2 website creates a user account for the user, allowing that user access to the site as a registered user.

Return to top

LDAP allows you to create **cross-references** between groups that you have created in your Cenricity2 website and groups that exist in your LDAP Directory. Users assigned to groups in your LDAP Directory are assigned to the cross-referenced Centricity2 groups each time the LDAP authenticated users sign in to Centricity2. LDAP authenticated users are added or removed from Centricity2 groups as determined by the LDAP to Centricity2 group cross references.

The primary benefit of LDAP Authentication is to have a **single source repository of user information**, your LDAP Directory, for all of your LDAP enabled applications. You maintain user information for all of your LDAP enabled applications at one location, your LDAP Directory. All LDAP enabled applications use the same user name and password.

LDAP Servers Supported by Centricity2

- **Novell® eDirectory™**
- **Microsoft® Active directory®**
- **OpenLDAP™ (an open source directory)**

When my staff signs in to their computer will that automatically sign them into the website?

No, the LDAP connector does not provide single sign in access. See **“What is the LDAP Connector?”** for more details.

Do all my staff/students have to authenticate through the LDAP connector?

No. Permission to authenticate through the LDAP connector is granted through privileges assigned in a Passport. Users that shouldn’t authenticate through the connector would not be assigned the passport with that privilege.

Can I map to nested groups?

No

What type of encrypted SSL certificate do I need?

40 Bit or Wildcard

What format does the self signed certificate need to be in?

The self signed certificate should be in .PFX format.

Why do I need to provide an encrypted SSL certificate and a self signed SSL certificate?

The self signed SSL certificate is for the connection between Active Directory and the web servers.

The encrypted SSL certificate allows us to activate secure login (https) for the website.

Return to top

What fields are passed from the Active Directory to Centricity 2 upon login?

- First Name
- Last Name
- Email address
- Sign In Name
- Groups

My usernames don't match. Can I fix that with imports or is the process manual?

This problem can be fixed easily by running 2 import files. Each excel file contains 2 columns and should be saved in .csv format.

File 1

UserCode	UserName
UserCode = LDAP Username	UserName = C2 Username

File 2

UserCode	UserName
UserCode = LDAP Username	UserName = LDAP Username

If Active Directory (AD) goes down, can my users still login?

No, credentials are not cached on the server. The LDAP connector would need to be disabled until the AD is back online.

What would my user's passwords be if AD went down and the connector was disabled?

Users would login with the password they used prior to the LDAP Connector being implemented on your website. If users don't know their password they would request a new one by clicking on the **Forgot My Password button** on the login screen.

Once the Active Directory is back online and the LDAP Connector is reactivated users would resume logging in with their AD credentials.

Can I set up multiple connections, each to a different domain controller? More specifically, can connections be set-up to 2 Active Directory controllers in the SAME domain so that if one goes down the other can be reached for authentication - with NO INTERVENTION needed within Centricity?

No, this is not possible.

Will the connector remove users from groups?

Yes, it will remove and add to groups.

Return to top

How do my site directors keep the LDAP site director passport if they are in other groups that are cross referenced to a different passport?

Passport is not updated when users login. The assignment of a passport upon login only occurs on the initial creation of a user account.

I have separate passports for students and staff. Can I set-up passports for the LDAP connector in the same respect or can I only have one passport that is applied to all new accounts?

LDAP passports can be set-up in the same respect. Every group cross reference that is created has one passport assigned to it. The appropriate passport would be assigned to the appropriate group cross reference.

Do I have to map all of my Centricity 2 groups to active directory groups? Not all of my groups make sense to have in AD.

No, but keep in mind that the un-mapped groups have to be manually updated.

If a user types in their password and gets it wrong too many times does their account lock like it does under normal (non ldap) circumstances?

An LDAP-enabled account will lock after five failed attempts the same as a non-LDAP account.

What kind of maintenance does the LDAP Connector require?

Post Implementation: Once LDAP Authentication is set up and running, there are a few reasons for you to make changes to the LDAP settings for your C2 website. Here are instances when you might need to make changes:

- You add groups to your C2 website.
- You move your LDAP Directory to a different server.
- You make system software updates to your LDAP Directory.
- You opt to use or discontinue use of SSL.
- You make system software updates of SSL.
- You make changes to your server certificate.
- You make updates to your firewall.
- You make IP address changes.

Contact the Webs that Work team before making changes to the LDAP settings of your C2 website!