Lightweight Directory Access Protocol (LDAP)

Schoolwires® Centricity2™

schoolwires®
come together

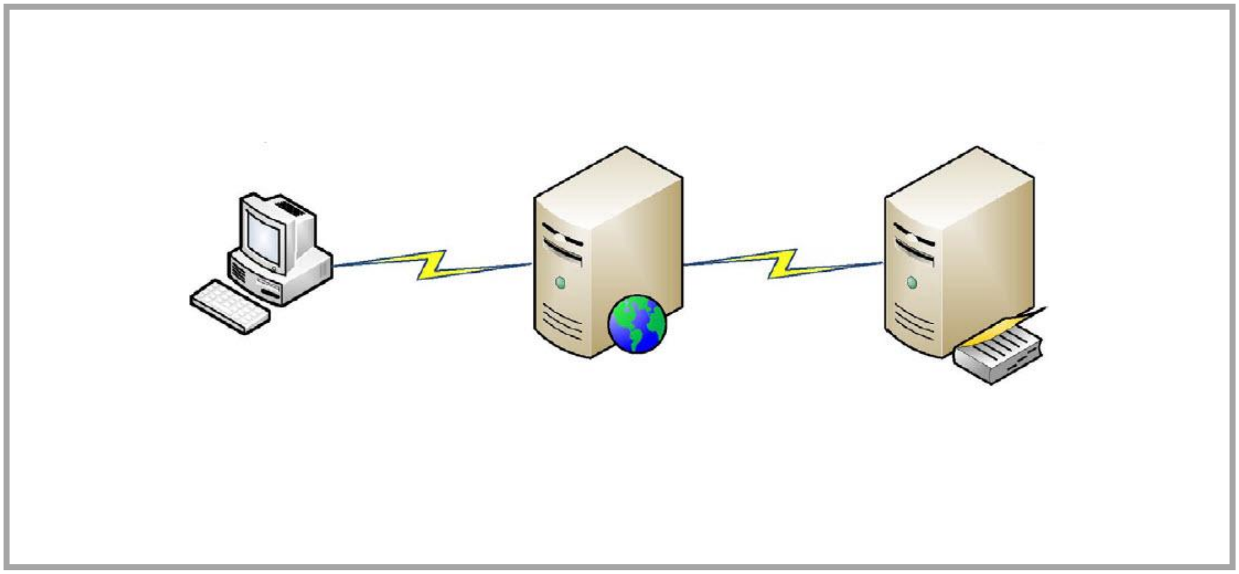
Table of Contents

Introduction

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

Here is what you will do to set up LDAP Authentication for your Centricity2 website.

1. Prepare your LDAP Server for LDAP connectivity.
2. Set up Centricity2.
   - Create a passport with the extended privilege *Allow users to sign in using LDAP.*
   - Create categories.
   - Create groups.
3. Create a non-LDAP Site Director user account with a passport having all extended privileges except *Allow users to sign in using LDAP*.
4. Complete the *Getting Started with LDAP* form.
5. Plan your Centricity2 group to LDAP group cross-references.



About LDAP

LDAP provides for a single sign in where one user name and password for a user is shared between many services.

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.

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.

Primary Benefit of LDAP Authentication

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

Here are the LDAP Directory Servers that your Centricity2 website supports.

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

LDAP Authentication Scenarios

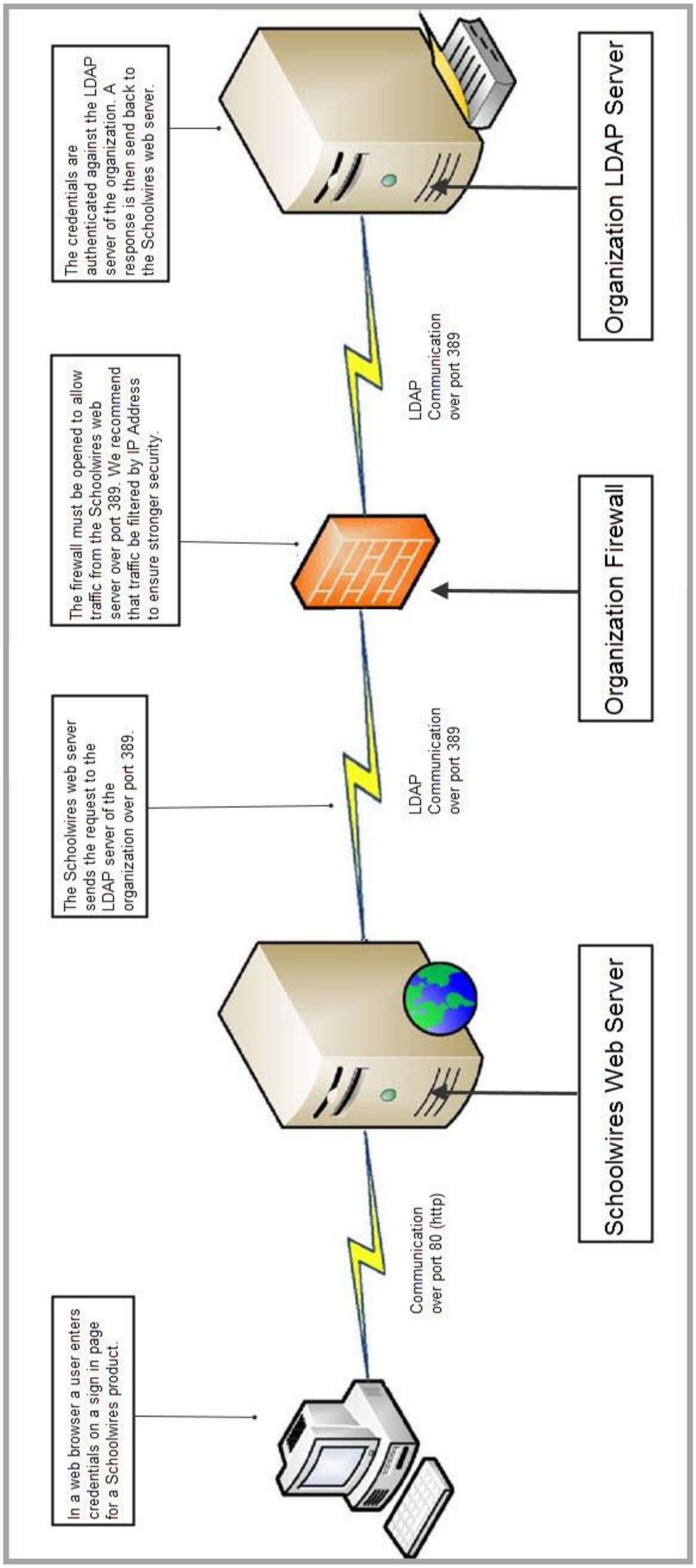
Schoolwires LDAP integration can be tailored to fit your network and security needs. We use one of two possible scenarios.

Here are the LDAP Authentication scenarios.

- Standard LDAP Implementation
- LDAP over SSL Implementation

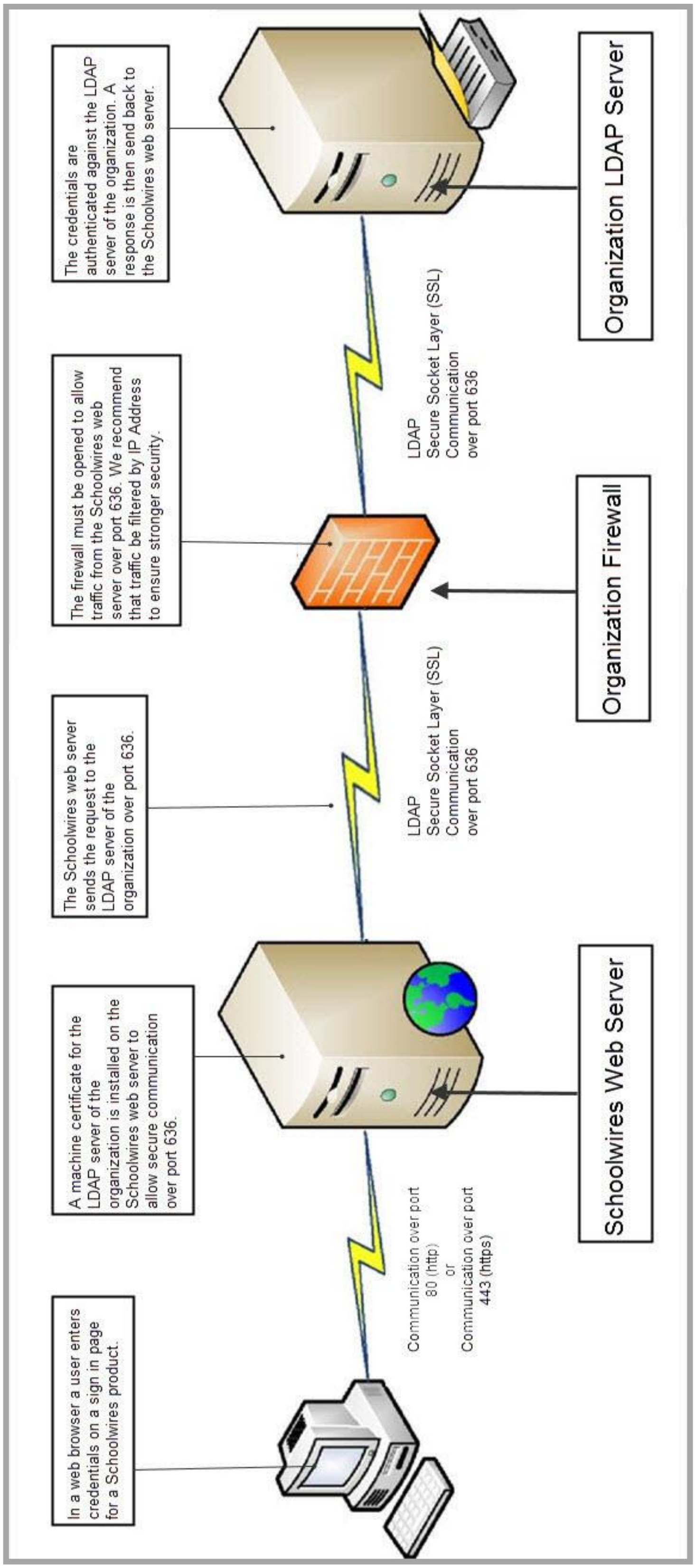
Standard Implementation

Here is the Standard LDAP implementation scenario.


In a web browser a user enters credentials on a sign in page for a Schoolwires product.
Communication over port 80 (http)
Schoolwires Web Server
The Schoolwires web server sends the request to the LDAP server of the organization over port 389.
LDAP Communication over port 389
Organization Firewall
The firewall must be opened to allow traffic from the Schoolwires web server over port 389. We recommend that traffic be filtered by IP Address to ensure stronger security.
LDAP Communication over port 389
Organization LDAP Server
The credentials are authenticated against the LDAP server of the organization. A response is then send back to the Schoolwires web server.

LDAP over SSL Implementation

Here is the LDAP over Secure Socket Layer (SSL) implementation scenario.



In a web browser a user enters credentials on a sign in page for a Schoolwires product.

A machine certificate for the LDAP server of the organization is installed on the Schoolwires web server to allow secure communication over port 636.

The Schoolwires web server sends the request to the LDAP server of the organization over port 636.

The firewall must be opened to allow traffic from the Schoolwires web server over port 636. We recommend that traffic be filtered by IP Address to ensure stronger security.

The credentials are authenticated against the LDAP server of the organization. A response is then send back to the Schoolwires web server.

Communication over port 80 (http) or Communication over port 443 (https)
Schoolwires Web Server
LDAP Secure Socket Layer (SSL) Communication over port 636
Organization Firewall
LDAP Secure Socket Layer (SSL) Communication over port 636
Organization LDAP Server

Implementation of LDAP Authentication

You may choose to set up LDAP Authentication on your own or choose to work with us to accomplish this task.

Initial Implementation

If we host your website on one of our servers, you need to open your firewall and allow the specific IP Address and port we provide to you in order to access the LDAP Directory server. Once opened, we will test the connectivity between the servers.

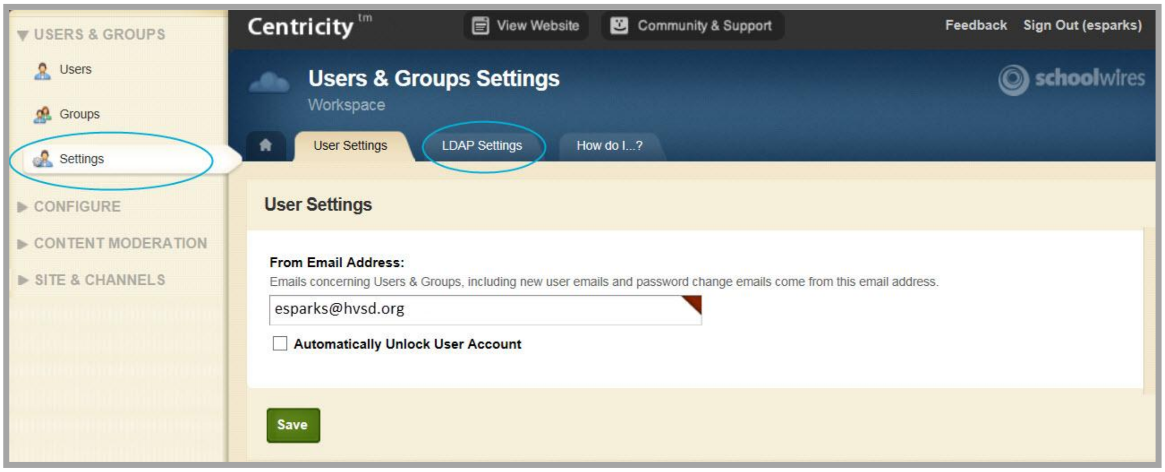
Here is a list of additional information necessary to populate LDAP settings in your Centricity2 website and create group cross-references between your Centricity2 website and designated LDAP Directory or Directories.

- LDAP server or servers
- Domain Name or IP Address for your LDAP Directory server or servers
- SSL
  If your website is hosted by Schoolwires and you use SSL, you must create a certificate on your server that we will install on the server hosting your Centricity2 website.
- Distinguished Name (DN). The DN indicates the unique starting point within your LDAP Directory or Directories where user credentials are located.
- The user name and password Centricity2 should use when it accesses your LDAP Directory or Directories.
- User Name Format. Is the user name format used in Centricity2 the same format used for user names in your LDAP Directory or Directories? If you have already created user accounts in your Centricity2 website and they are not identical to that of your LDAP Directory or Directories, the authentication process results in the creation of duplicate user accounts within Centricity2. If not the same, we can run a correction script that changes the format of your Centricity2 user names to that of your LDAP Directory.
- The DN for each LDAP Directory group you wish to associate with a Centricity2 website group and the group to which it will be associated.

Creating Domains

Here’s how you create a Domain.

1. In *Site Manager*, expand USERS & GROUPS in the Content Browser.
2. Click **Settings**. The Users & Groups Settings Workspace displays.

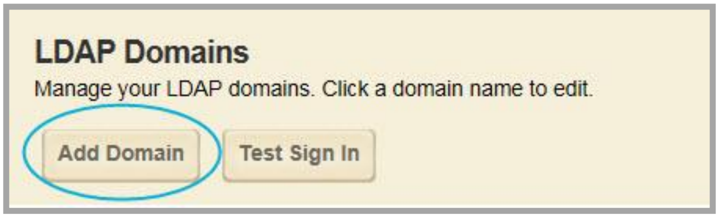


User Settings

From Email Address:
Emails concerning Users & Groups, including new user emails and password change emails come from this email address.
esparks@hvsd.org

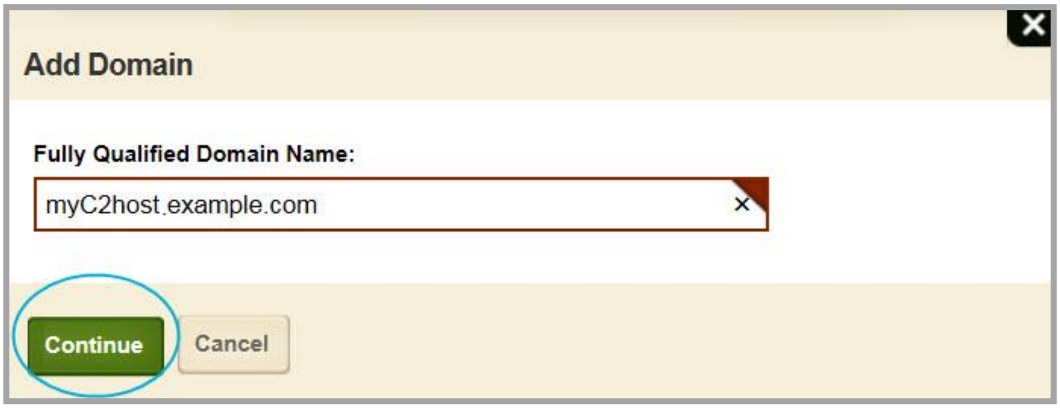
□ Automatically Unlock User Account

3. Click the **LDAP Settings** tab. LDAP Domains displays.
4. Click **Add Domain**. The Add Domain dialog displays.


LDAP Domains

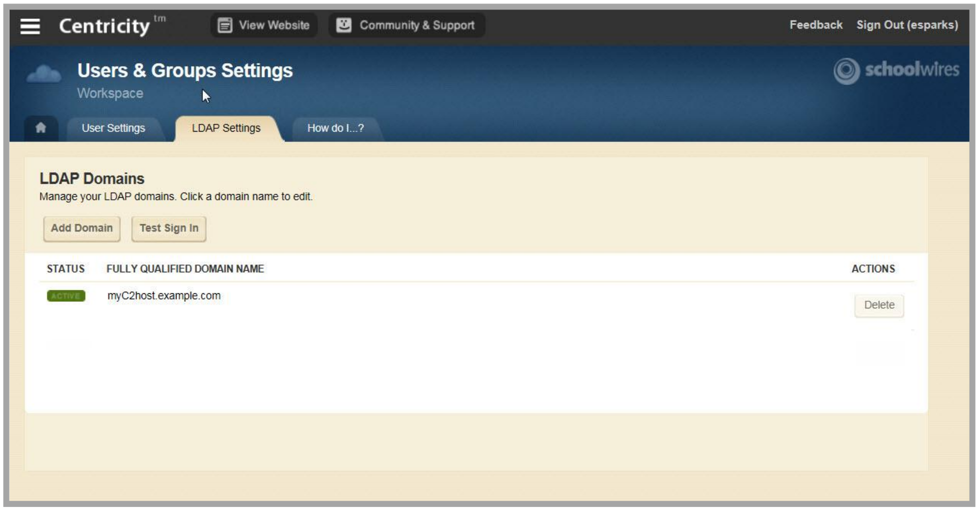
Manage your LDAP domains. Click a domain name to edit.

5. Enter a Fully Qualified Domain Name.


Add Domain

Fully Qualified Domain Name:
myC2host.example.com

6. Click **Continue**. LDAP Domains displays.



LDAP Domains

Manage your LDAP domains. Click a domain name to edit.

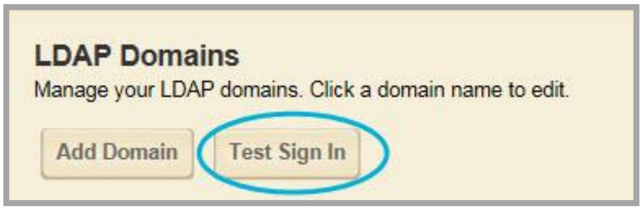
STATUS	FULLY QUALIFIED DOMAIN NAME	ACTIONS
ACTIVE	myC2host.example.com	Delete

Note that you may enter multiple domain names.

Test Sign In

Here's how you test signing into a domain.

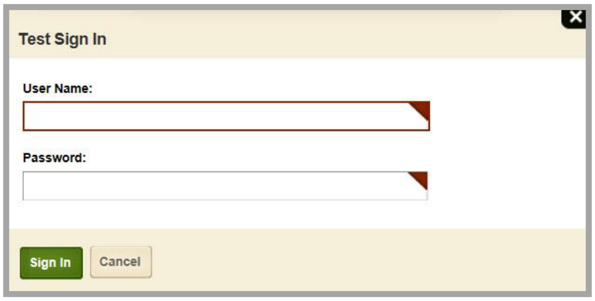
1. In *Site Manager*, expand USERS & GROUPS in the Content Browser.
2. Click **Settings**. The Users & Groups Settings Workspace displays.
3. Click the **LDAP Settings** tab. LDAP Domains displays.
4. Click **Test Sign In**.



LDAP Domains

Manage your LDAP domains. Click a domain name to edit.

The Test Sign In dialog displays.



5. Enter the Test User Name and Password.
6. Click **Sign In**.

Creating Cross-References

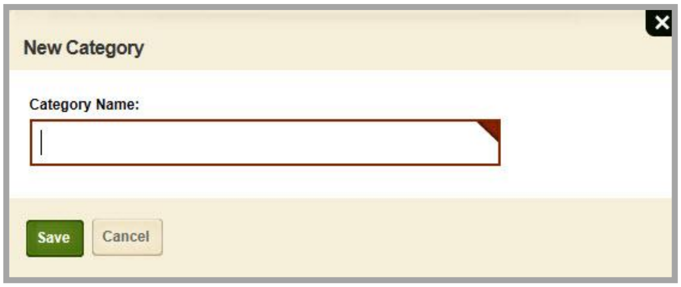
Before you can add your Centricity2 website and LDAP Directory group cross-references, you create your categories and groups for your Centricity2 website. You also need to create a passport with the extended privilege that enables LDAP Authentication.

You must have at least one group cross-reference. A good practice is to create a blanket group mapping for all users and specify the LDAP enabled passport in the cross-reference so that all LDAP Authenticated users are assigned the passport when their account is created in Centricity2. This passport assignment from the group cross-reference occurs once—when a LDAP Authenticated users sign in to Centricity2 for the very first time.

You use categories to create sets of groups. They are used to filter when selecting a group and are typically named by school buildings (e.g., Happy Valley Elementary School, Happy Valley High School, etc.).

Here's how you create a category.

1. In *Site Manager*, expand USERS & GROUPS in the Content Browser.
2. Click **Groups**. The Groups workspace displays.
3. Click the **Categories** tab.
4. Click **New Category**. The New Category window displays.



5. Enter a Category Name.

   It might be wise to develop a consistent naming convention for your categories. For example, categories for schools within the Happy Valley School District might be named HVHS (Happy Valley High School), HVMS (Happy Valley Middle School) and HVES (Happy Valley Elementary School).

6. Click **Save**.

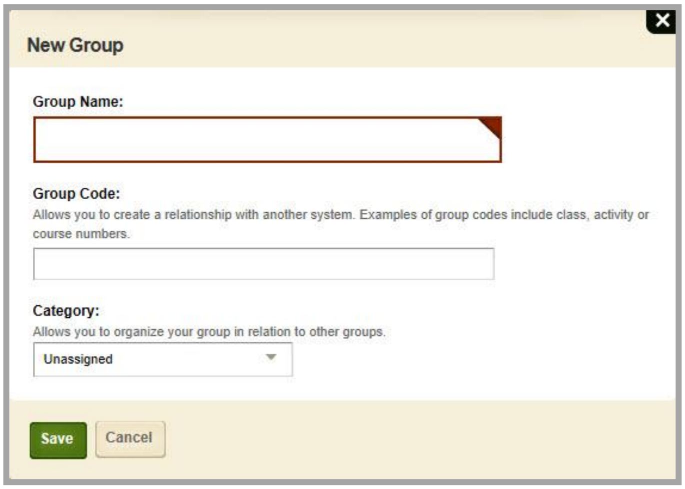
Groups

Groups allow you to create sets of users. You can then assign the group instead of assigning individual users. Here are example instances when you can use groups in your Centricity2 website.

- Setting Viewing Permissions
- Setting Editing Permissions
- Setting Sharing Permissions for Apps and Collections
- Sharing Apps to Display on Other Pages
- Distributing Broadcast E-Alerts
- Setting MyView Configurations
- Allowing access to Passkeys

Here's how you create a group.

1. In *Site Manager*, expand USERS & GROUPS in the Content Browser.
2. Click **Groups**. The Groups workspace displays.
3. Click **New Group**. The New Group window displays.



New Group

Group Name:

Group Code:
Allows you to create a relationship with another system. Examples of group codes include class, activity or course numbers.

Category:
Allows you to organize your group in relation to other groups.
Unassigned

4. Enter a Group Name.

   It might be wise to develop a consistent naming convention for your groups. For example, groups for the Happy Valley School District might include HVHS-Parents, HVMS-Parents, HVES-Parents and HVHS-Staff.

5. Click the Category drop-down and select a category from the list.
6. Click **Save**.

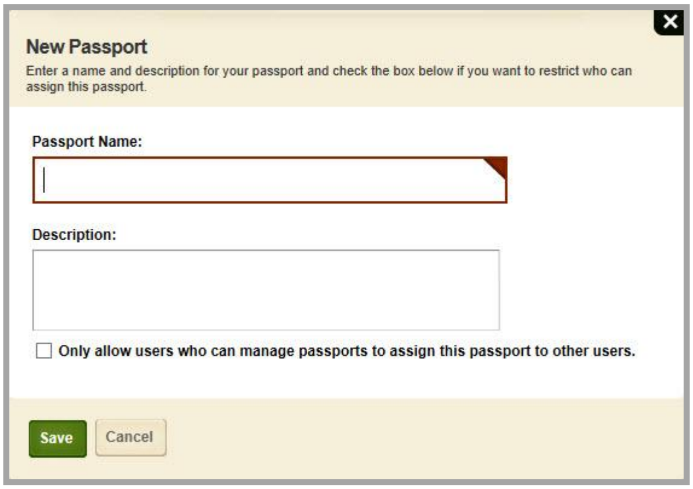
Passports

You use a passport to assign administrative privileges to user accounts in your Centricity2 website. You also can assign the privilege *Allow user to sign in using LDAP.* LDAP Authenticated users need to be assigned a passport with this privilege.

Here's how you create a Centricity2 website passport.

1. In *Site Manager*, expand USERS & GROUPS in the Content Browser.
2. Click *Users*. The Users workspace displays.
3. Click the **Passports** tab.

4. Click **New Passport**. The New Passport window displays.



New Passport

Enter a name and description for your passport and check the box below if you want to restrict who can assign this passport.

Passport Name:

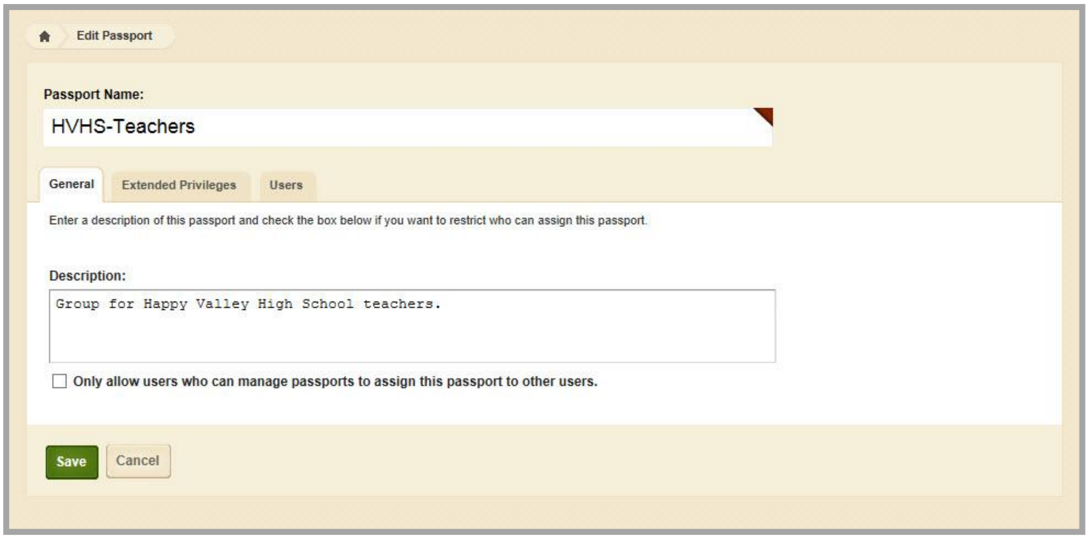
Description:

□ Only allow users who can manage passports to assign this passport to other users.

5. Enter a Passport Name.
6. Enter an optional Description for the passport if you like.
7. Activate the check box if to only allow users who can manage passports assign this passport to other users.
8. Click **Save**.

Here's how you add extended privileges to a passport.

1. In *Site Manager*, navigate to the Users workspace.
2. Click on the name of the passport you wish to edit. The Edit Passport window displays.



Passport Name: HVHS-Teachers

Enter a description of this passport and check the box below if you want to restrict who can assign this passport.

Description: Group for Happy Valley High School teachers.

□ Only allow users who can manage passports to assign this passport to other users.

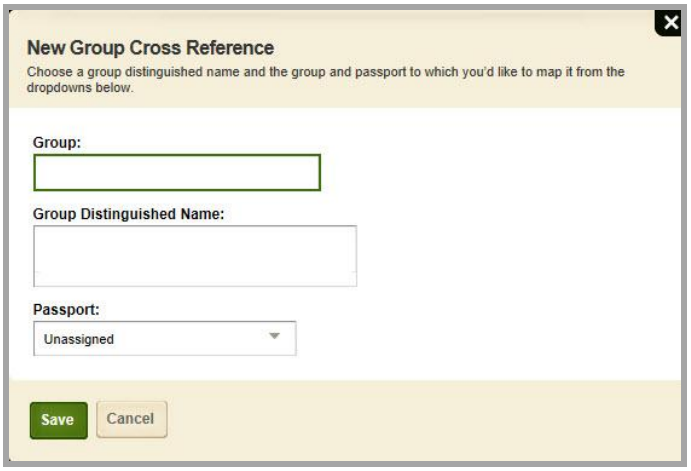
3. Click the **Extended Privileges** tab.
4. Use the drop-down and select an option from the list to filter the Extended Privileges display.
5. In the Status column, click **INACTIVE** to activate a privilege for the passport. Click **ACTIVE** to inactivate a privilege.
6. Click **Save**.

The Passport Extended Privilege *Allow user to sign in using LDAP* must be activated within the passport you intend to assign to your LDAP authenticated user accounts. This is what enables your Centricity2 website to authenticate an existing user account user name and password against your LDAP Directory.

LDAP Directory and Website Group Cross-References

Here's how you create your LDAP Directory and Centricity2 website cross-references.

1. Create categories for each of your schools.
2. Manually create or import groups based on your needs.
3. Create your group cross-references.
4. In *Site Manager*, expand USERS & GROUPS in the Content Browser.
5. Click *Settings*. The Users & Groups Settings workspace displays.
6. Click **LDAP Settings** tab.
7. Click the **Group Cross Reference** tab.
8. Click **New Cross Reference**. The New Group Cross Reference window displays.



New Group Cross Reference

Choose a group distinguished name and the group and passport to which you'd like to map it from the dropdowns below.

Group:

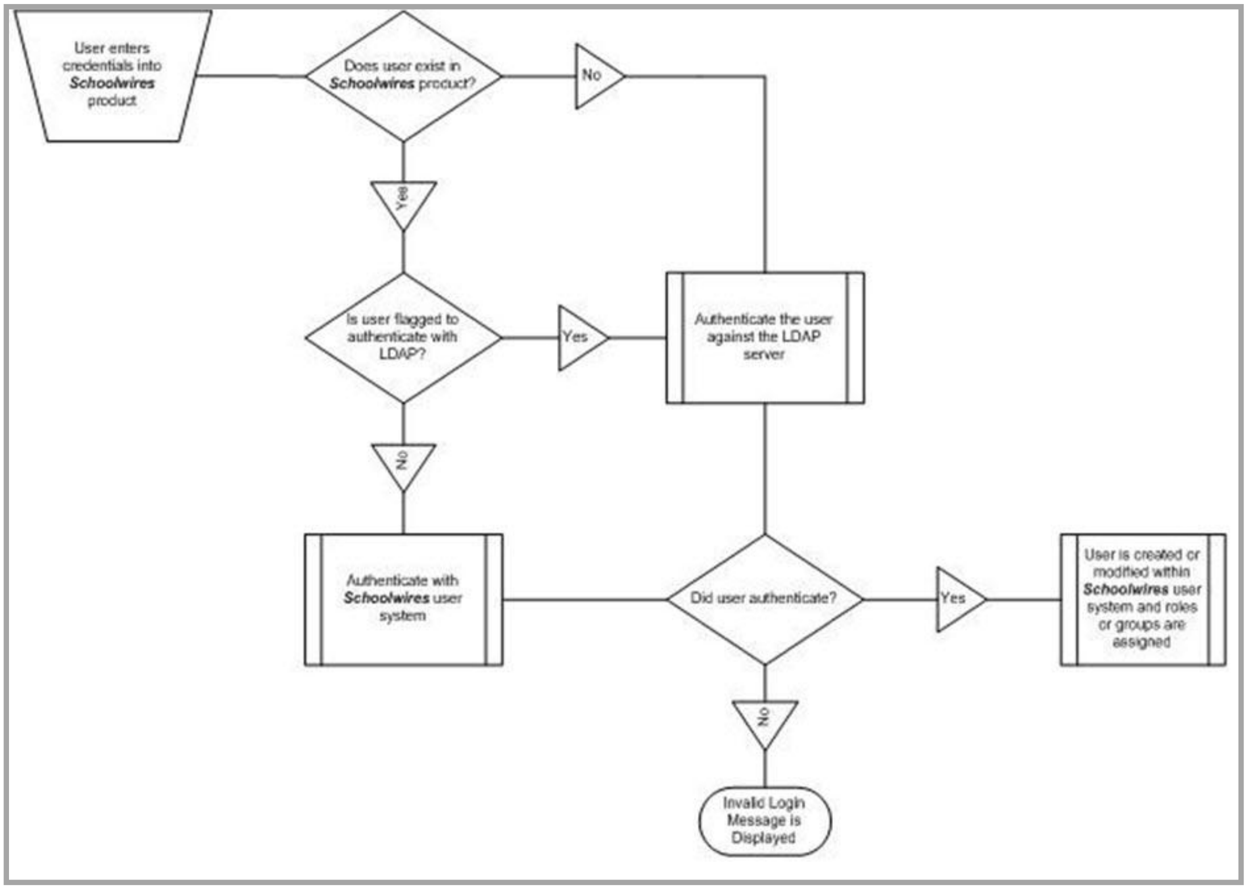
Group Distinguished Name:

Passport: Unassigned

9. From the Group drop-down list, select the Centricity2 group to which you wish to make the cross-reference.
10. From the **Group Distinguished Name** drop-down-list, select the directory Group Distinguished Name. Members of this group will be assigned to the selected Centricity2 group.
11. From the Passport drop-down list, select a passport to associate with the cross-reference. When LDAP Authentication creates a new user account in your Centricity2 website, the passport specified here is assigned to the new user account. This assignment occurs once, on the initial creation of the account—that is, when a LDAP enabled user signs in to Centricity2 for the very first time.
12. Click **Save**.

The Effects of LDAP on the Use of Centricty2

Within your Centricity2 website, you may have a combination of user accounts that authenticate using your LDAP Directory and user accounts that authenticate using Centricity2.


User enters credentials into Schoolwires product
Does user exist in Schoolwires product?
No
Yes
Is user flagged to authenticate with LDAP?
Yes
Authenticate the user against the LDAP server
No
Authenticate with Schoolwires user system
Did user authenticate?
Yes
User is created or modified within Schoolwires user system and roles or groups are assigned
No
Invalid Login Message is Displayed

The Authentication Process

When a user attempts to sign in to Centricity2, that user is authenticated.

1. If the user is found in Centricity2 and flagged as an LDAP user, the user is authenticated against your LDAP Directory.
    - If that user is found on the LDAP Directory and the sign in name and password match, the sign in is successful.
    - If that user is not found in your LDAP Directory server or the sign in name and password do not match, the sign in fails.
2. If that user is not found in your Centricity2 website, but is found in your LDAP Directory, the user is added as an LDAP user within your Centricity2 website. Additional information is passed from the LDAP Directory and saved within in the user’s Centricity2 user account.

Here's the information that is passed to Centricity2.

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

  Note that groups can be created within your LDAP Directory and users assigned to them. During the implementation of LDAP, we set up a table that cross-references these groups within the LDAP directory to groups in your Centricity2 website. If a user is assigned to a group on the LDAP Directory, then the user will be assigned to the associated group in your Centricity2 website.

3. If that user is found in your Centricity2 website and not marked as an LDAP user, the user will be authenticated against the user database in Centricity2. If the sign in name and password match, the sign in will be successful.
4. If that user is not found in your Centricity2 website or your LDAP Director server, or the sign in name and password do not match, the sign in fails.

Effects of LDAP on Users of Centricty2

Once LDAP Authentication is implemented, you will notice these effects.

- The user account created in your Centricity2 website for each LDAP user will be associated with a passport that contains the extended privilege for sign in using LDAP.
- The user account created in your Centricity2 website for each LDAP user will have will have a non-functioning encrypted password.
- If you delete a user from your LDAP Directory, you do not need to delete that user from your Centricity2 website. The authentication will fail and that user will be unable to sign in to the Centricity2 website. You may want to purge non-functioning user accounts from your Centricity2 website periodically.
- LDAP users of your Centricity2 website need to sign in. They will use the same sign in name and password that they use for your network.
- When LDAP users of your Centricity2 website edit their account information using the My Account option in the MyStart bar, they will not see the User Name, Password or Confirm Password fields.
- If you make any changes to a User Account (e.g., add a zip code, unlock a user) for a user in your LDAP Directory, that user will not receive any confirmation from your Centricity2 website.
- The user accounts for users of your Centricity2 website who are not LDAP enabled users are maintained within your Centricity2 website. They will be able to access their own accounts and modify their User Name, Password and Confirm Password fields. They will receive the normal confirmation messages from your Centricity2 website.

Post Implementation

Once LDAP Authentication is set up and running, there are few reasons for you to make changes to the LDAP settings for your Centricity2 website. Here are instances when you might need to make changes.

- You add groups to your Centricity2 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.

We recommend that you contact us before making changes to the LDAP settings of your Centricity2 website.