

Lightweight Directory Access Protocol (LDAP)

Blackboard Web Community Manager

Blackboard®

Trademark Notice

Blackboard, the Blackboard logos, and the unique trade dress of Blackboard are the trademarks, service marks, trade dress and logos of Blackboard, Inc. All other trademarks, service marks, trade dress and logos used in Blackboard and the Website are the trademarks, service marks, trade dress and logos of their respective owners.

Copyright Notice

© 2016 Blackboard Inc. All rights reserved.

This guide covers all available features and functionality. Features included in your contract may vary.

Table of Contents

Introduction 1

About LDAP 2

 Primary Benefit of LDAP Authentication..... 2

 LDAP Servers Supported by Web Community Manager 2

 LDAP Authentication Scenario 2

 LDAP over SSL/TLS Implementation..... 3

Implementation of LDAP Authentication..... 4

 Initial Implementation 4

 Creating Domains..... 5

 Test Sign In 6

 Creating Cross-References 7

 Groups..... 7

 Passports..... 8

 LDAP Directory and Website Group Cross-References 10

The Effects of LDAP on the Use of Web Community Manager 11

 The Authentication Process 11

 Effects of LDAP on Users of Web Community Manager 12

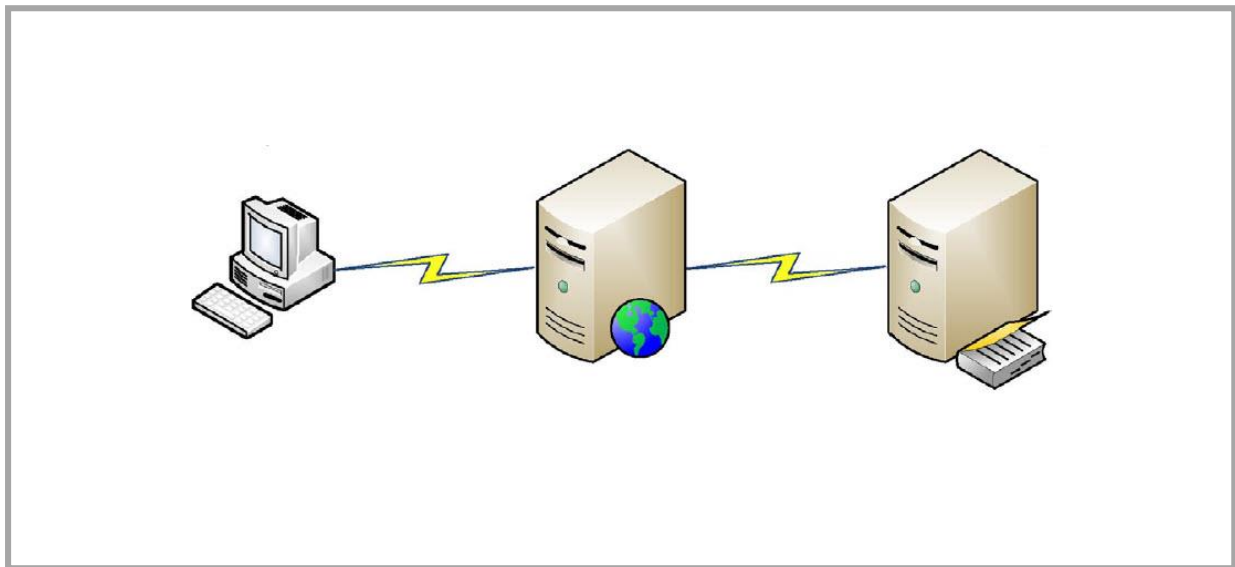
Post Implementation 13

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 Web Community Manager User Management Systems.

Here is what you will do to set up LDAP Authentication for your Web Community Manager website.

1. Prepare your LDAP Server for LDAP connectivity.
2. Set up Web Community Manager.
 - 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 Web Community Manager 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 Web Community Manager website. If your LDAP administrator changes the password for a user within your LDAP Directory, that user's password is automatically updated in your Web Community Manager website.

LDAP can automatically create user accounts in your Web Community Manager website for any users entered in your LDAP Directory. When users first sign in to an LDAP enabled Web Community Manager 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 Web Community Manager 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 Web Community Manager website and groups that exist in your LDAP Directory. Users assigned to groups in your LDAP Directory are assigned to the cross-referenced Web Community Manager groups each time the LDAP authenticated users sign in to Web Community Manager. LDAP authenticated users are added or removed from Web Community Manager groups as determined by the LDAP to Web Community Manager 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 Web Community Manager

Here are the LDAP Directory Servers that your Web Community Manager website supports.

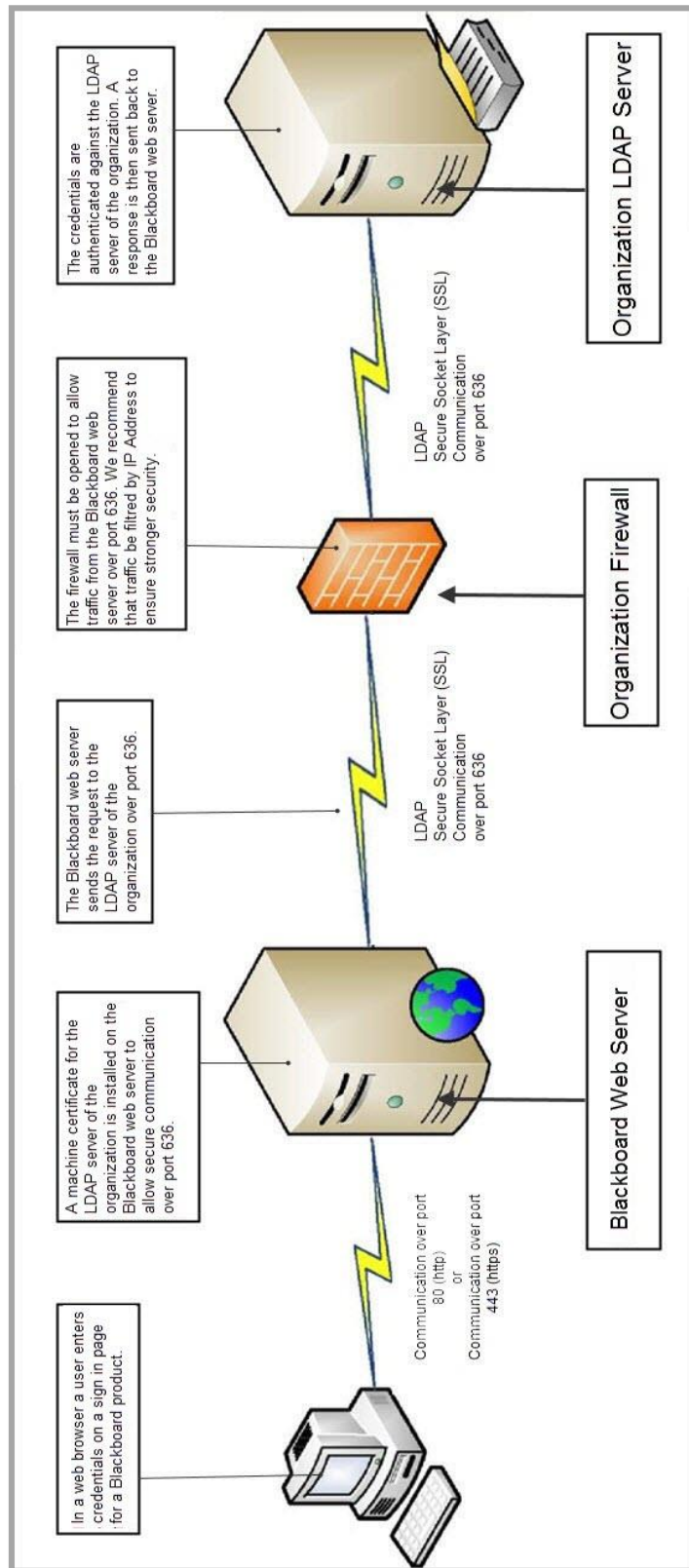
- Novell® eDirectory™
- Microsoft® Active directory®
- OpenLDAP™ (an open source directory)

LDAP Authentication Scenario

Web Community Manager LDAP integration is tailored to fit your network and security needs. We use Secure LDAP which is also known as LDAP over Secure Socket Layer (SSL)/Transport Layer Security (TLS) in order to assure that communication is protected at the highest industry standard.

LDAP over SSL/TLS Implementation

Here is the LDAP over SSL/TLS implementation scenario.



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.

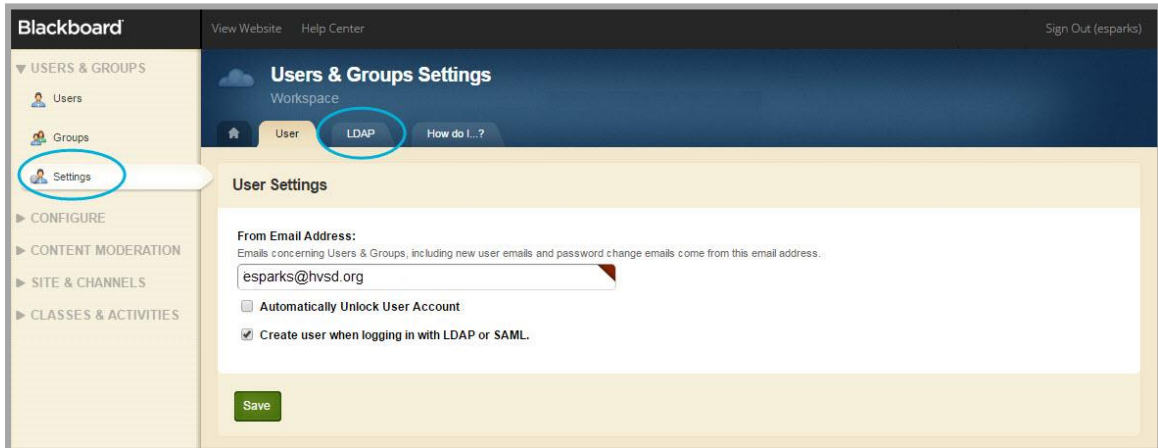
Here is a list of additional information necessary to populate LDAP settings in your Web Community Manager website and create group cross-references between your Web Community Manager website and designated LDAP Directory or Directories.

- LDAP server or servers
- Domain Name or IP Address for your LDAP Directory server or servers
- Secure LDAP over SSL/TLS
 - When your directory server is set up for secure LDAP, a certificate was installed on it. For our servers to accept that certificate as legitimate, they need to trust the issuer of that certificate.
 - If the issuer is a public authority (like *verisign*) then we likely have trust established.
 - If the issuer is a Certificate Authority (CA) within your network (the most common scenario), then we need a copy of the CA's own certificate so we can add it to our servers' list of trusted root authorities.
 - If the issuer is the same server as the Active Directory (a *self-signed* certificate) then we simply need a copy of that certificate to trust.
- 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 Web Community Manager should use when it accesses your LDAP Directory or Directories.
- User Name Format
 - Is the user name format used in Web Community Manager the same format used for user names in your LDAP Directory or Directories? If you have already created user accounts in your Web Community Manager 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 Web Community Manager. If not the same, we can run a correction script that changes the format of your Web Community Manager user names to that of your LDAP Directory.
- The DN for each LDAP Directory group you wish to associate with a Web Community Manager website group and the group to which it will be associated.

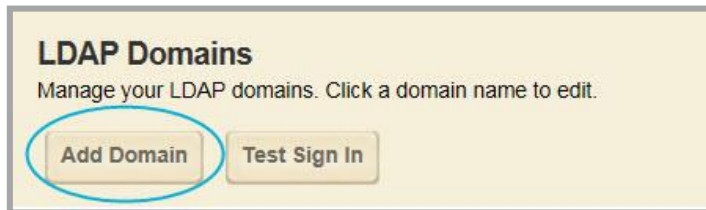
Creating Domains

Here's how you create a Domain.

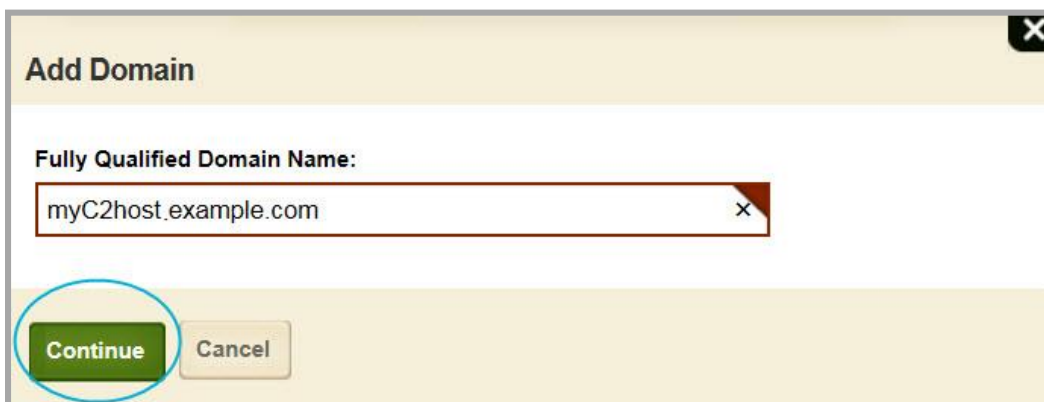
1. In *Site Manager*, expand **USERS & GROUPS** in the Content Browser.
2. Click **Settings**. The Users & Groups Settings Workspace displays.



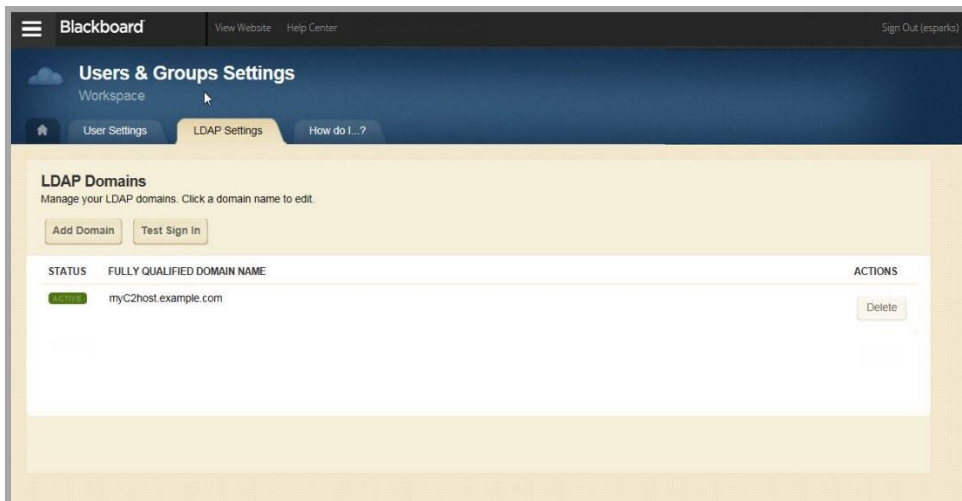
3. Click the **LDAP Settings** tab. LDAP Domains displays.
4. Click **Add Domain**. The Add Domain dialog displays.



5. Enter a Fully Qualified Domain Name.



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



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**.



The Test Sign In dialog displays.



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

Creating Cross-References

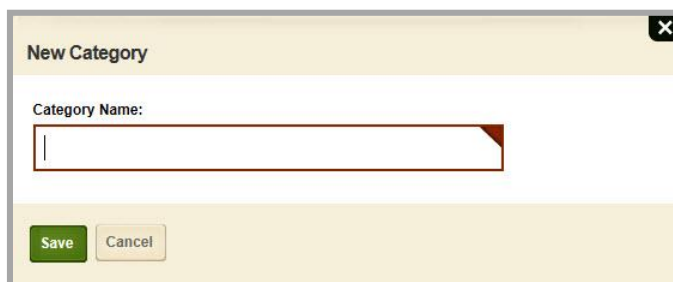
Before you can add your Web Community Manager website and LDAP Directory group cross-references, you create your categories and groups for your Web Community Manager website. You also need to create a passport with the extended privilege that enables LDAP Authentication.

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 Web Community Manager. This passport assignment from the group cross-reference occurs once—when a LDAP Authenticated users sign in to Web Community Manager 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**.

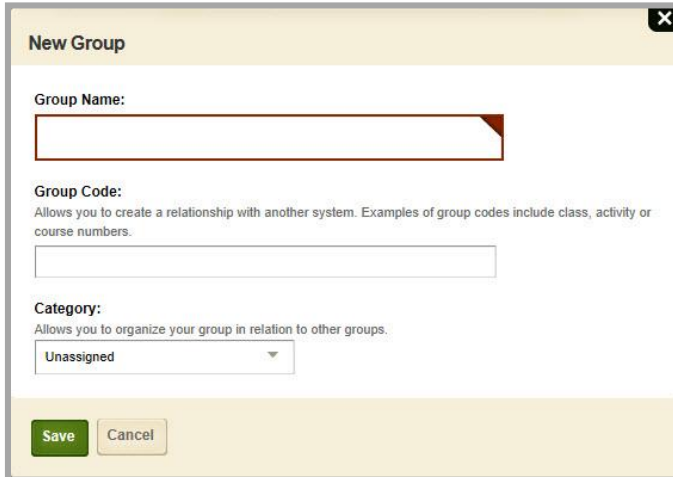
Groups

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 Web Community Manager 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.



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**.

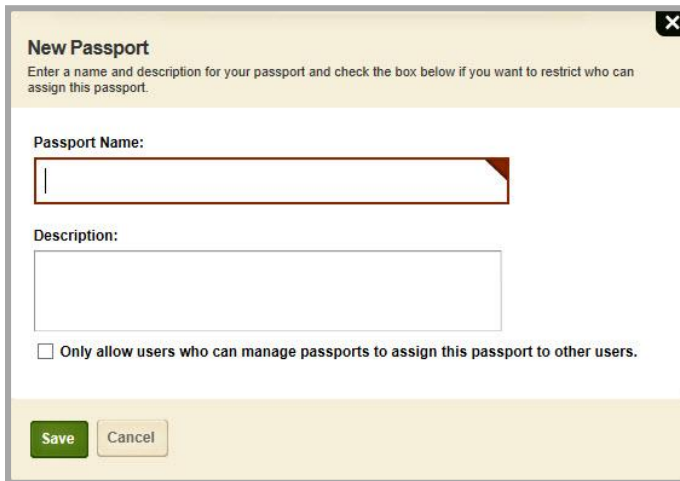
Passports

You use a passport to assign administrative privileges to user accounts in your Web Community Manager 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 Web Community Manager 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.

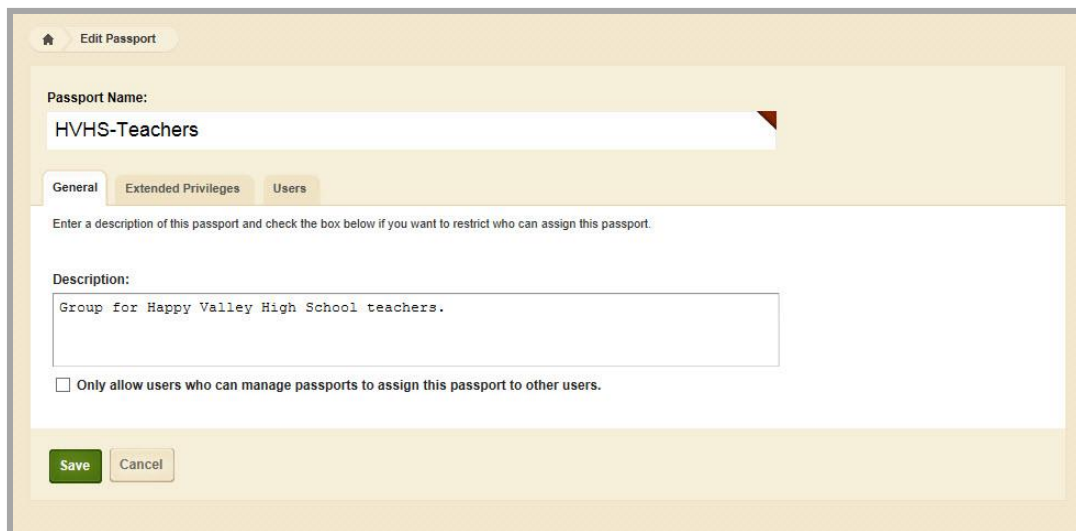
4. Click **New Passport**. The New Passport window displays.



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.



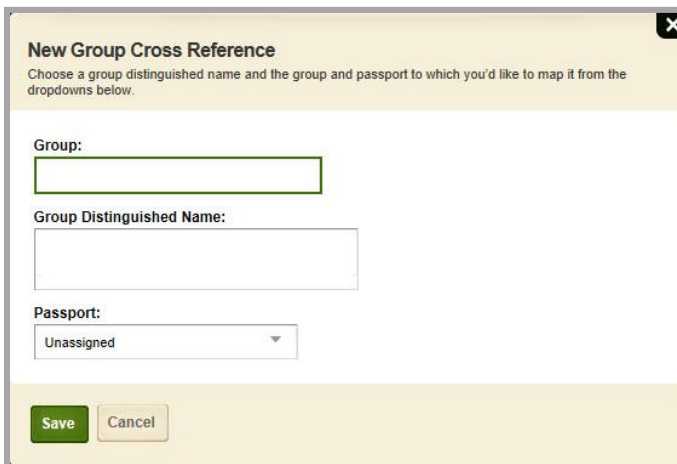
3. Click the **Extended Privileges** tab.
4. Use the drop-down and select an option from the list to filter the Extended Privileges display.
5. In the Status column, click **INACTIVE** to activate a privilege for the passport. Click **ACTIVE** to inactivate a privilege.
6. Click **Save**.

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 Web Community Manager 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 Web Community Manager 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 on the Fully Qualified Domain Name.
8. Click the **Group Cross Reference** tab.
9. 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:

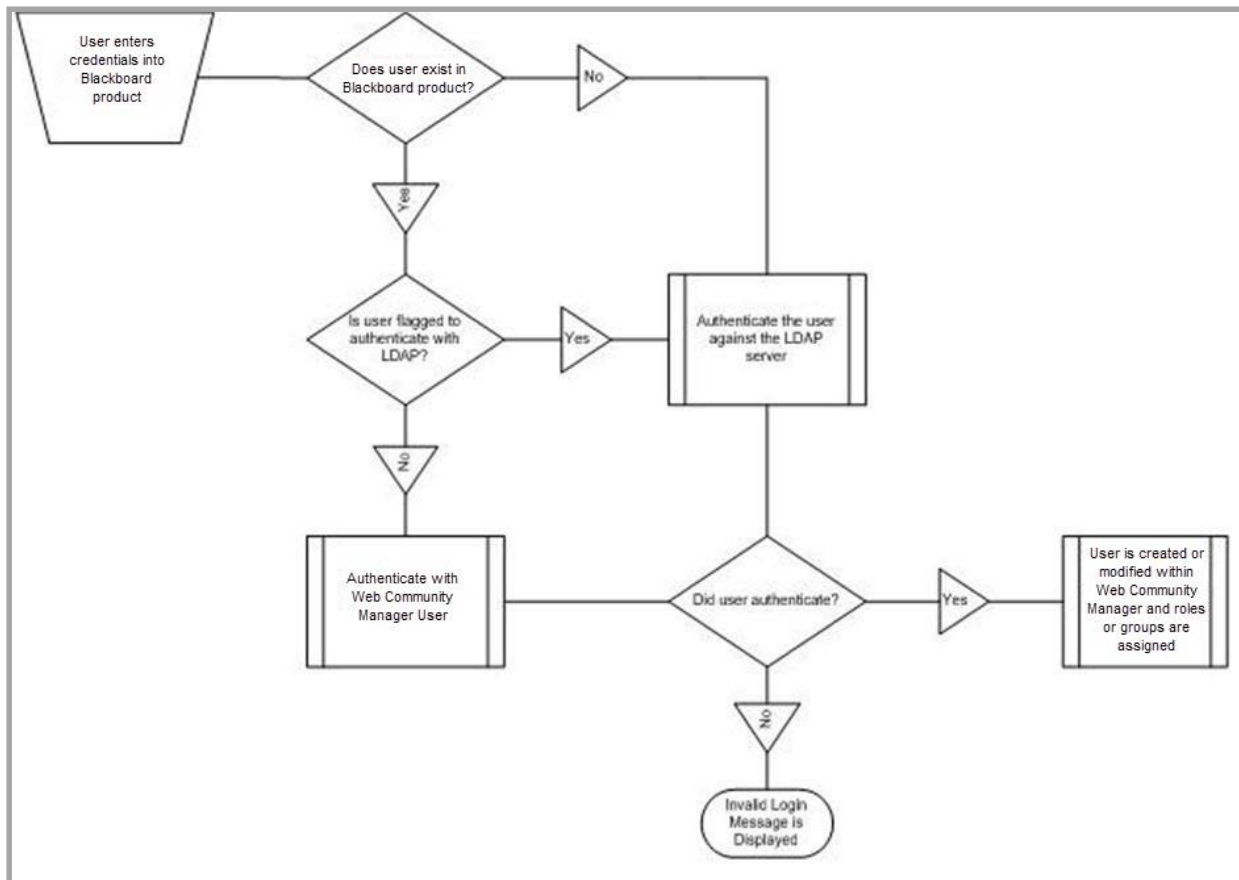
Passport:
Unassigned

Save Cancel

10. From the Group drop-down list, select the Web Community Manager group to which you wish to make the cross-reference.
11. From the **Group Distinguished Name** drop-down-list, select the directory Group Distinguished Name. Members of this group will be assigned to the selected Web Community Manager group.
12. 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 Web Community Manager 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 Web Community Manager for the very first time.
13. Click **Save**.

The Effects of LDAP on the Use of Web Community Manager

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



The Authentication Process

When a user attempts to sign in to Web Community Manager, that user is authenticated.

1. If the user is found in Web Community Manager 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 Web Community Manager website, but is found in your LDAP Directory, the user is added as an LDAP user within your Web Community Manager website. Additional information is passed from the LDAP Directory and saved within in the user's Web Community Manager user account.

Here's the information that is passed to Web Community Manager.

- 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 Web Community Manager 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 Web Community Manager website.

3. If that user is found in your Web Community Manager website and not marked as an LDAP user, the user will be authenticated against the user database in Web Community Manager. If the sign in name and password match, the sign in will be successful.
4. If that user is not found in your Web Community Manager 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 Web Community Manager

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

- The user account created in your Web Community Manager 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 Web Community Manager 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 Web Community Manager website. The authentication will fail and that user will be unable to sign in to the Web Community Manager website. You may want to purge non-functioning user accounts from your Web Community Manager website periodically.
- LDAP users of your Web Community Manager 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 Web Community Manager 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 Web Community Manager website.
- The user accounts for users of your Web Community Manager website who are not LDAP enabled users are maintained within your Web Community Manager 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 Web Community Manager 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 Web Community Manager website. Here are instances when you might need to make changes.

- You add groups to your Web Community Manager website.
- You move your LDAP Directory to a different server.
- You make system software updates to your LDAP Directory.
- You opt to discontinue use of SSL/TLS.
- You make system software updates of SSL/TLS.
- 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 Web Community Manager website.