LDAP Configuration

Last Modified on 12/16/2024 9:54 am CST

Tool Search: LDAP Configuration

In a district that requires a user management system, Campus LDAP (Lightweight Directory Access Protocol) tools allow Campus users to be linked to LDAP user accounts. LDAP tools allow secure systems management and compress the amount of time a system administrator must spend managing user-security tasks.

This article includes the following topics:

Users of both small and large districts can be authenticated through LDAP, even when an existing LDAP structure is already being used. LDAP supports multiple domains/ directory trees and sub-second login capabilities. Users can exist virtually anywhere within tiers of multiple organizational units because they are bound to LDAP on an individual basis.

Using Active Directory/LDAP functionality is not required. A district may still authenticate against the Campus database, if desired.

Enabling LDAP Authentication does not mean ALL accounts must be verified via LDAP. Campus accounts can be configured to LDAP while existing within the same environment.

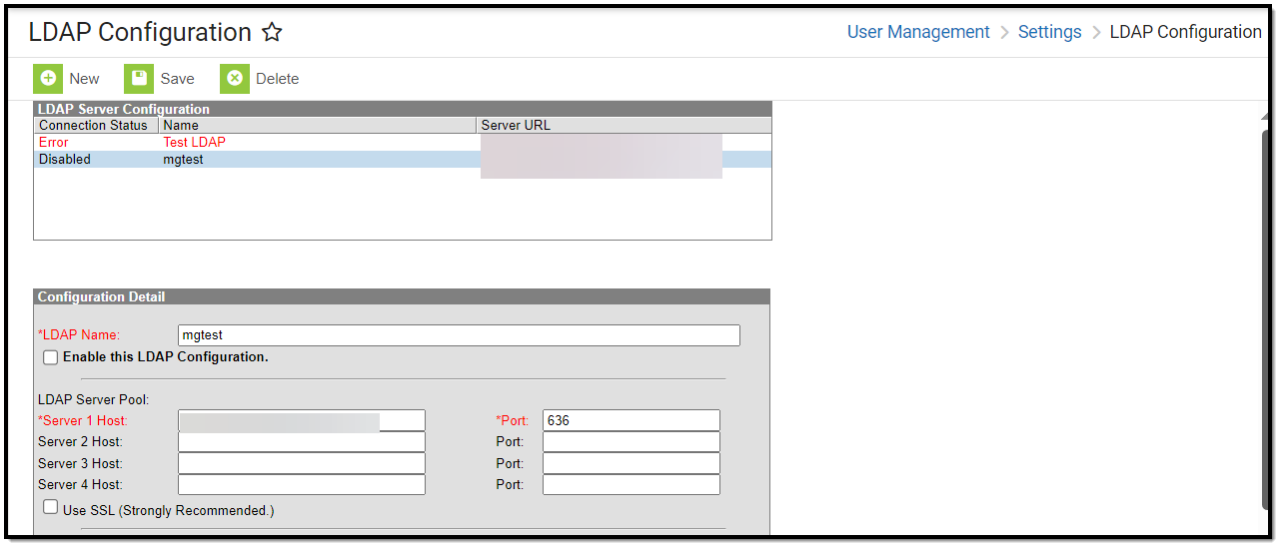


Image 1: LDAP Authentication Tool

Only users assigned a Product Security Role of **Student Information System (SIS)** are allowed to use this tool.

LDAP Technical Components

The Lightweight Directory Access Protocol (LDAP) is a standardized application protocol that allows access to information directories for querying and modification. LDAP allows access to credentials information. It supports TCP/IP communication and allows most applications across platforms the ability to obtain directory information.

The LDAP directory tree reflects directory boundaries. A directory tree has many entries, or objects with similar attributes organized in a logical and hierarchical manner.

Each entry has attributes, attribute names, and attribute values as defined in the Campus schema. Each entry also has a unique identifier, known as a Distinguished Name.

Campus Schema Details

While LDAP is an open standard, it is similar to XML in that it does not define a schema.

In Campus, the Distinguished Name (DN) from the instance of the applicable directory will be stored at the user account level. The DN value will have no functional purpose outside of reporting or reference.

If a district wants to use a different LDAP implementation, it will need to add UUID/GUIDs to its

user account objects.

Interface Configuration of LDAP/Active Directory

While some setup may be necessary within the LDAP service, many LDAP settings are configured directly within the Campus user interface.

Initial Considerations

Please consider the following before configuring LDAP authentication.

Firewall Adjustments	If there is a firewall between Campus application servers and the Active Directory servers, it should be configured to allow LDAP requests from the Campus servers to the Active Directory servers.
Active Directory	Active Directory uses Relative Distinguished Names for authentication. This type of authentication process only requires a username to be unique to the organizational unit in which it is directly contained. Campus setup is more restrictive, requiring that the Active Directory attribute used as a login name be unique. All Campus users MUST have unique login names in the Active Directory domain assigned to them.
District System Administrator Accounts	Each district using LDAP should create a system administrator user that is allowed to authenticate against the Campus database. The district system administrator account SHOULD NOT be linked to LDAP. He/she should have two accounts: the normal administrator account linked to the Active Directory and a backup account set to authenticate against Campus in the event that the LDAP service is unavailable.
Allow List Campus IPs	In order to properly connect to third-party servers, firewalls and other network systems must allow list Campus IPs.

Configuring Campus for LDAP Authentication

The main interface configuration of LDAP occurs on the LDAP Authentication tab.

Enabling LDAP Authentication does not mean ALL accounts must be verified via LDAP. Campus accounts can be linked or unlinked to LDAP while existing within the same environment.

When two or more servers are configured, Campus will balance LDAP authentications between available servers using internal load balancing technology.

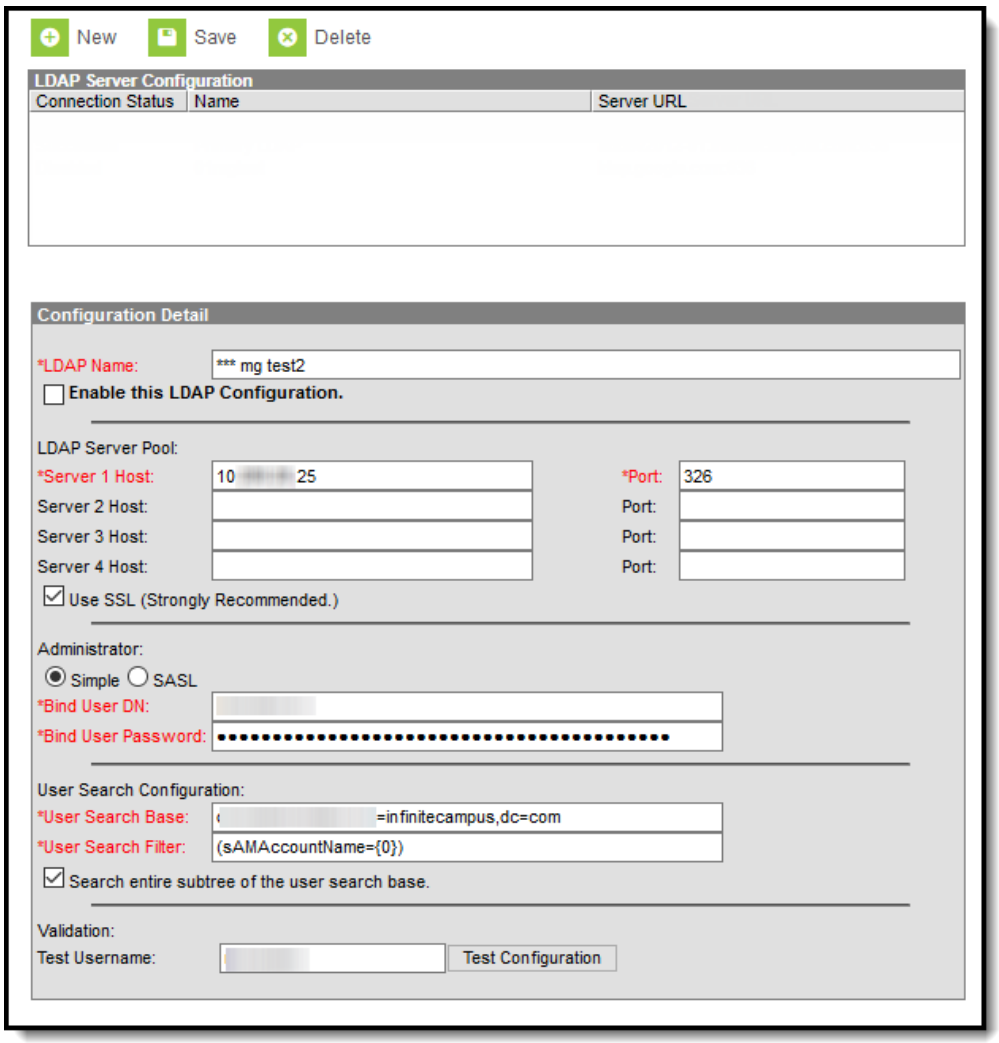


Image 3: LDAP Configuration Editor

1. Click the **New** icon.
2. Determine if you plan to utilize SSL:

    - If Yes - Upload an LDAPS certificate via the LDAPS Certificates tool and then continue the steps listed below.

        Users configuring LDAP for SASL must use SSL.

- If No - Move on to Step 2 below.

3. Enter an **LDAP Name** for the LDAP server. Entering a recognizable name is important so that users assigning an LDAP server to a user account are able to easily identify the correct server.
4. Mark the **Enable LDAP Authentication** checkbox to enable LDAP authentication for Campus log-ins.
5. Mark the **Use this configuration to enable Portal login for SSO users** checkbox to enable the ability for portal users with SSO credentials to log into Campus when using a mobile device.
6. Enter the Server Host name(s) of the LDAP Servers.

   - NOTE: Your third-party SFTP server must allow list Campus IPs so traffic can pass. For more information, see this article.

     If Server Host 1 fails to connect, the system will try the next host entered (Server Host 2) and continue down the Server Host list until it makes a successful connection.

7. Enter the **Port** numbers of the LDAP server(s) entered in Step 6.
8. Mark the **Use SSL (Strongly Recommended)** checkbox to use SSL for all connections.

   This SSL option is only applicable when using LDAPS ports. Users configuring LDAP for SASL must use SSL.

   In order to utilize SSL, you must upload an LDAPS certificate via the LDAPS Certificates tool.

9. Determine if you are enabling a **Simple** or **SASL** connection:
   1. **Simple** - The most common way to configure an LDAP connection. This requires the Bind User DN and Bind User Password.
   2. **SASL** - This is for authenticating via an LDAP SASL such as Google Suite. For more information on configuring Google Suite to work with Campus, see the Configuring Google Suite to Work with Campus LDAP section.
10. If Simple is selected, specify the **Bind User DN** and **Binder User Password** (Note: there is a 20-character limit).
11. Indicate a **User Search Base** level at which LDAP will start searching for users.
12. Enter the **User Search Filter**. See the table below for more information about using this field.
13. Mark the **Search entire subtree of the user search base checkbox** . This ensures all subtrees in the search base are searched when locating LDAP accounts for authentication with Campus.

    Campus highly recommends marking this checkbox.

14. Enter a Test Username and click the **Test Configuration** button. This will allow you to test and ensure the configuration values entered above are correct. Test results will appear below this field.

USERS ARE HIGHLY ADVISED TO TEST ANY CONFIGURATION PRIOR TO SAVING.

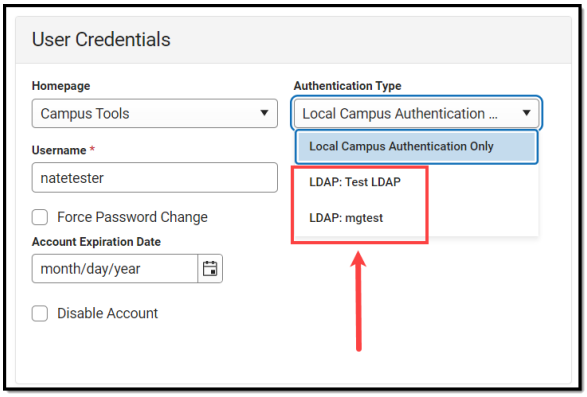
FAILURE TO ENTER CORRECT LDAP AUTHENTICATION CONFIGURATION INFORMATION WILL RESULT IN AN INABILITY TO LOG INTO CAMPUS USING LDAP FOR ANY USER IN THAT SERVER.

15. If successful, select the **Save** icon. The LDAP server is now configured and saved within Campus.

If additional servers need to be added (such as a multi-forest environment), Click the **New** button and repeat Steps 1 through 12.

Now that LDAP is enabled, you may want to convert all user accounts from using local Campus authentication to LDAP authentication. See the Converting Existing Campus User Accounts to LDAP Authentication section for more information.

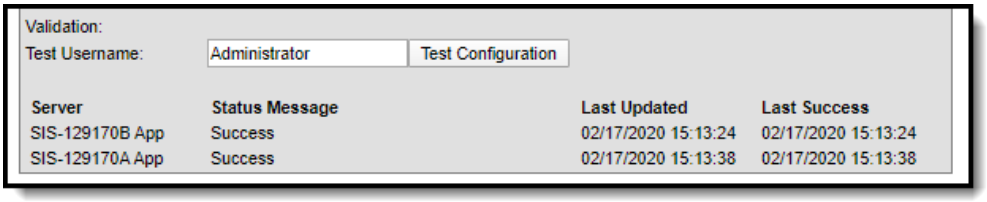
LDAP Configuration Field Definitions

Field	Description and Details
LDAP Name	The name of the LDAP server being configured. Entering a recognizable name is important so that users assigning an LDAP server to a user account are able to identify the correct server easily. 
Enable LDAP Authentication	If marked, this indicates Campus users can be authenticated using this LDAP Configuration.

Field	Description and Details
Use this configuration to enable Portal login for SSO users.	If marked, Portal users with SSO credentials are able to log into Campus when using a mobile device.
Server (1, 2, 3, 4) Host	Server 1 Hostname is required for LDAP. This should be the name of the Active Directory server. Up to three additional servers may be specified. When two or more servers are configured, Campus will balance data between available servers using internal load balancing technology.
Port	LDAP is firewall-sensitive. When LDAPS ports are used, the Use SSL checkbox should be marked. Ports specified for LDAP servers are generally one of the following: • **Single domain searches** - 389 LDAP or 636 LDAPS • **Global catalog searches (multi-domain)** - 3268 LDAP or 3269 LDAPS
Use SSL	The Use SSL checkbox should only be marked when LDAPS ports are used. Users configuring LDAP for SASL must use SSL. Using SSL/LDAPS is strongly recommended. Regular LDAP bind operations send passwords in plain text. The use of SSL is all/nothing; it cannot be configured per connection. **In order to utilize SSL, you must upload an LDAPS certificate via the LDAPS Certificates tool.**
Simple	The most common way to configure an LDAP connection. This requires the Bind User DN and Bind User Password.
SASL	This is for authenticating via an LDAP SASL such as Google Suite. For more information on configuring Google Suite to work with Campus, see the Configuring Google Suite to Work with Campus LDAP section.

Field	Description and Details
Bind User DN	The bind user is the administrative username for the directory server. It is needed in order for Campus to run LDAP queries to find and update user accounts. This field is used to bind a read rights user to the LDAP server. To LDAP, the bind user is the same type of user account as a user trying to authenticate his/herself into the system. Campus recommends using your SAMAccountName and if the test fails, use your LDAP distinguished name. This is encouraged because if the bind user gets moved within the active directory, an update to this reference won't be needed. Although Microsoft Active Directory will accept a sAMAccountName or domain\username format, it is recommended that the actual Distinguished Name format be used (i.e., CN=John Doe,OU=Employee,DC=example,DC=com) so that there will be no mistaking the user providing the access to the instance of Active Directory, OpenLDAP, etc.
Bind User Password	The administrative password for the directory server. 20-character limit.
User Search Base	The search base is the highest level of the LDAP tree at which LDAP should begin searching for users. This value used in conjunction with the **Search entire subtree of the user search base** checkbox can apply the largest scope to a simple filter for the best results.

<table>
<tr><th>Field</th><th>Description and Details</th></tr>
<tr><td>User Search Filter</td><td>Filters the user search to allow certain entries in the subtree while excluding others.
The following are some examples:
(sAMAccountName={0})
(UserPrincipalName={0})
(&(objectClass=user)(sAMAccountName={0}))
Campus will replace the {0} with the username of the user when these filters are executed upon login.
The following table describes some common filter operands:<table><tr><th>Operator</th><th>Character</th><th>Use</th></tr><tr><td>Equals</td><td>=</td><td>Creates a filter which requires a field to have a given value.</td></tr><tr><td>Any</td><td>*</td><td>A wildcard represents that a field can equal anything other than null.</td></tr><tr><td>Parenthesis</td><td>( )</td><td>Separates filters to allow other logical operators to function.</td></tr><tr><td>And</td><td>&</td><td>Joins filters together. At least one condition in the series must be true.</td></tr><tr><td>Or</td><td>or</td><td>Joins filters together. At least one condition in the series must be true.</td></tr><tr><td>Not</td><td>!</td><td>Excludes all objects that match the filter.</td></tr></table></td></tr>
<tr><td>Search entire subtree of the user search base</td><td>When marked, Infinite Campus will search the LDAP server from the level specified in the User Search Base field downwards until the server restricts the results or the search reaches the bottom of the tree. This option provides the best results and use of it is highly encouraged.</td></tr>
</table>

Field	Description and Details
Test Username	This field allows you to test and ensure the configuration values entered are correct. Once selected, test results will appear below, indicating whether or not the test was a success.  **USERS ARE HIGHLY ADVISED TO TEST ANY CONFIGURATION PRIOR TO SAVING.** **FAILURE TO ENTER CORRECT LDAP AUTHENTICATION CONFIGURATION INFORMATION WILL RESULT IN AN INABILITY TO LOG INTO CAMPUS USING LDAP FOR ANY USER IN THAT SERVER.**

Configuring LDAP for Multi-Forest Support

The LDAP Authentication tool allows you to configure and validate against multiple domains within a different LDAP repository. Each LDAP configuration created will appear within the LDAP Server Configuration window with an indication of whether or not each is enabled (or disabled) and their Server URL (Image 4).

To add an LDAP configuration, select the **New** button.

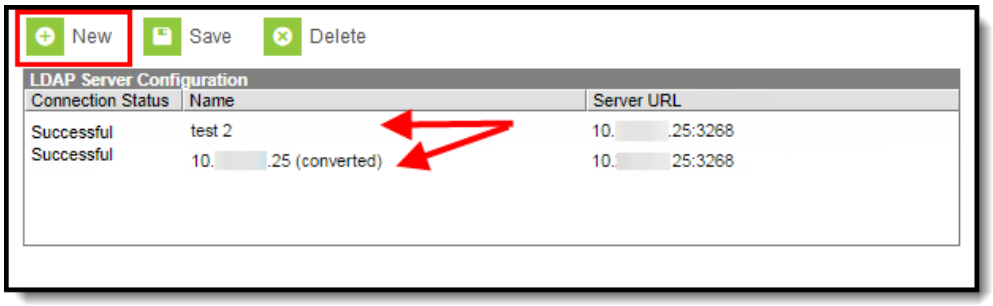
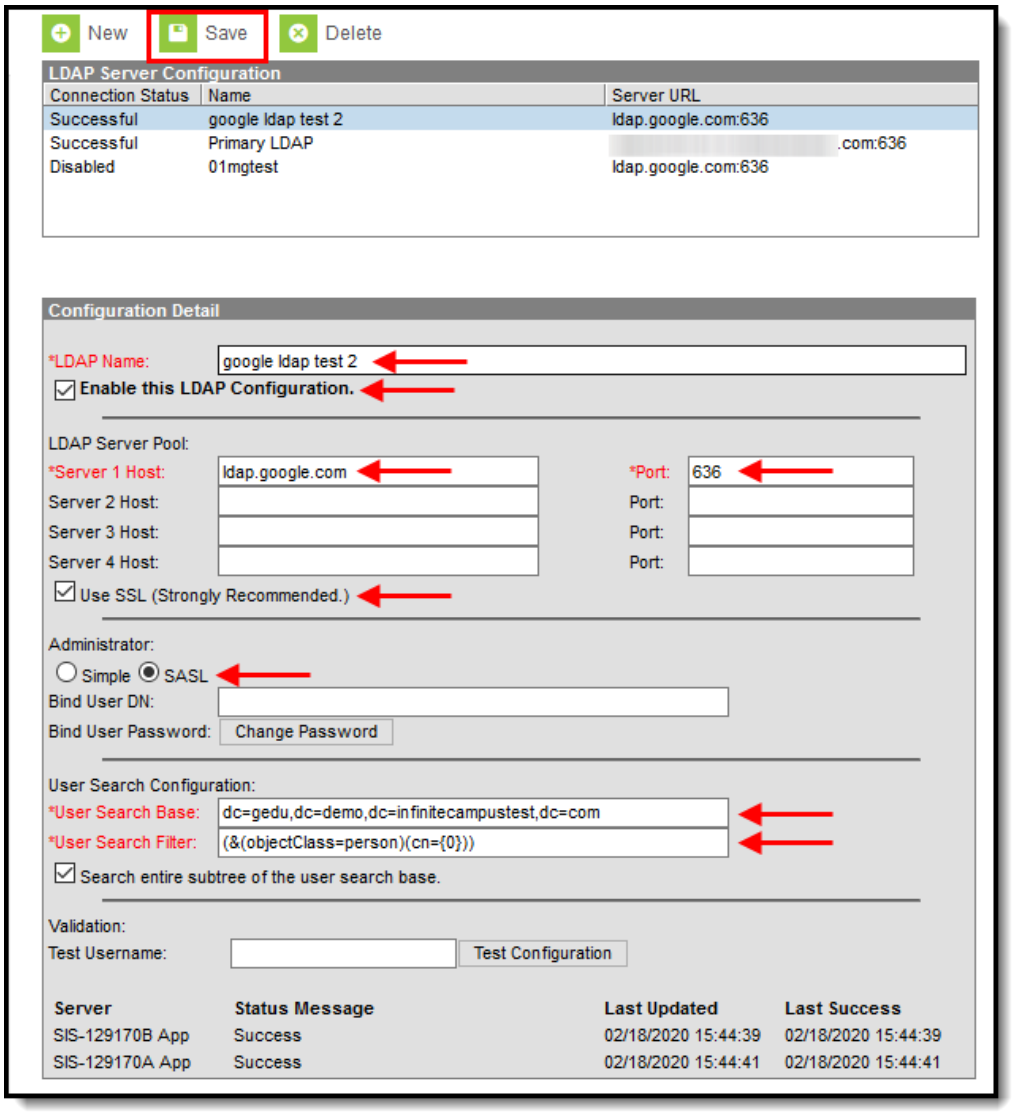


Image 4: Example of a Multi-Forest LDAP Configuration

Configuring LDAP for SASL

This section will walk you through the steps needed to configure LDAP for SASL.

For a step-by-step guide on how to configure Campus to work with Google Suite, see the Configuring Google Suite to Work with Campus LDAP section.



1. Select the **New** icon. The Configuration Detail editor will appear at the bottom of the screen.
2. Enter the **LDAP Name**. Campus recommends naming it something you can easily identify.
3. Mark the **Enable this LDAP Configuration** checkbox.
4. Enter the **Server 1 Host**. This should be the name of the SASL server. Up to three additional servers may be specified.
5. Enter the **Port**.
6. Mark the **Use SSL** checkbox. This is required in order to configure a SASL connection.
7. Click the **SASL** radio button.
8. Indicate a **User Search Base** level at which LDAP will start searching for users. See the table in the section above for more information about using this field.
9. Enter the **User Search Filter**. See the table in the section above for more information about using this field.
10. Mark the **Search entire subtree of the user search base** checkbox.

11. Click **Save**.
12. Navigate to the LDAPS Certificates tool and upload your Certificate and Key files. See the LDAPS Certificates article for more information about this process.
13. Once Cert and Key files have been uploaded into Campus, return to the LDAP Authentication tool, enter a **Test Username** (test email address) and click **Test Configuration**. The tool will indicate if the test was a success or failure. If successful, LDAP is now properly configured in Campus.

> Now that LDAP is enabled, you may want to convert all user accounts from using local Campus authentication to LDAP authentication. See the Converting Existing Campus User Accounts to LDAP Authentication section for more information.

Converting Existing Campus User Accounts to LDAP Authentication

Tool Search: User Account Type Wizard

Existing Campus accounts can be converted individually or en masse to LDAP authentication by using the User Account Type Wizard.

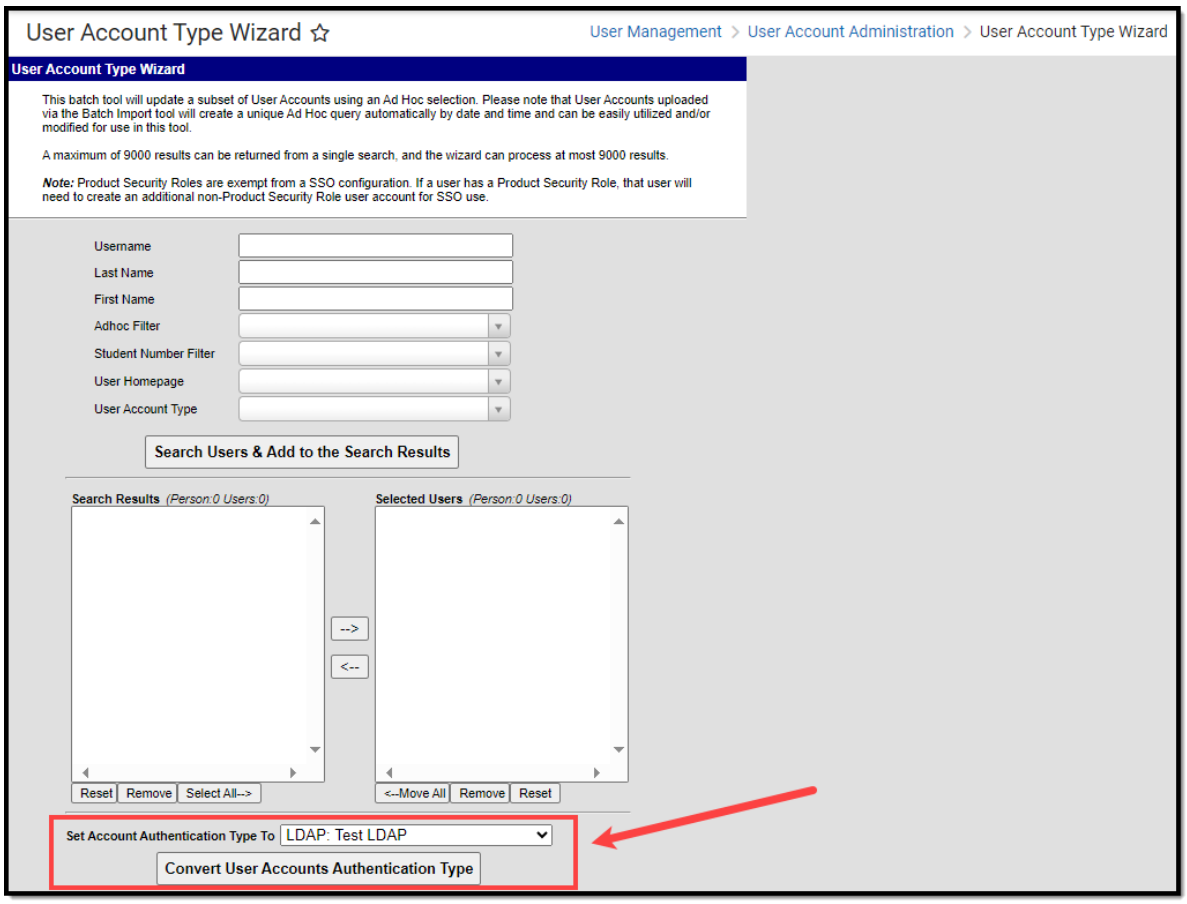


Image 5: Converting Campus Accounts to LDAP

Enabling LDAP Authentication does not mean ALL accounts must be verified via LDAP. Campus accounts can be linked or unlinked to LDAP while existing within the same environment.

User Authentication

Successful User Login

When the user attempts to log into Campus with his/her LDAP credentials for the first time, the system will query the directory using the filter in the applicable LDAP configuration.

If a user is able to log into Campus, the LDAP account has been successfully found and the authentication process is complete. Additionally, the directory Distinguished Name (DN) will be stored as a complementary reference to the user account.

If the LDAP user attempting authentication has already been successfully authenticated, or if an account with the same name already exists, the existing account will be updated with the new DN and the user will login without issues.

Unsuccessful User Login

If a user is unable to log into Campus, the authentication process failed.

Failure to logon using the LDAP account to the Campus user-entered credentials will occur if the user's LDAP account has been disabled, locked out or the wrong credentials were entered.

LDAP Authentication Methods

The following describes possible LDAP authentication methods/scenarios:

- Standard Logins
- Logins after User Changes in Active Directory

When attempting to log a user into Campus, the system reacts to accounts in the following ways:

- LDAP accounts are distinguished from normal Campus accounts because the ldapConfigurationID is not null.
- User accounts with null ldapConfigurationID field is authenticated as normal Campus accounts.

Standard Logins

In a normal, successful login scenario, the user is authenticated as follows:

1. The user enters his/her LDAP username and password.

2. The UserAccount object is located in the Campus database. The LDAP server info is retrieved using the ldapConfigurationID field of the UserAccount.
3. The user's distinguished name (DN) is retrieved by searching the username within the LDAP directory using the bind admin user from the LDAP configuration.
4. Binding a LDAP user with the user's DN and password succeeds and does not produce authentication errors.
5. The user is successfully logged in/authenticated.

Logins after User Changes in Active Directory

If a user's Organizational Unit or Distinguished Name changes in the Active Directory the user will be able to log in and the system will update cached information automatically.

Campus will attempt a search against the Active Directory tree as the user account assigned LDAP configuration dictates (please see "Search Filter" above). If the search is successful, the Active Directory will return the user's new Distinguished Name and update the Campus database. Since the search filter is executed upon every logon attempt, organization changes in Active Directory should not factor unless the search base is restricted and/or the subtree checkbox is not checked or the search filter is restrictive.

The process works as follows:

1. The user types in his or her LDAP username and password.
2. The UserAccount object is located in the Campus database. The LDAPDN field is null or populated from a previous successful authentication.
3. Binding an LDAP user with the user's username and password succeeds and does not produce authentication errors.
4. The user is successfully logged in/authenticated.

Converting LDAP Accounts Back to Campus-Authenticated Accounts

Tool Search: User Account Type Wizard

You can convert LDAP accounts back to using Campus authentication by using the **User Account Type Wizard**.

> Enabling LDAP Authentication does not mean ALL accounts must be verified via LDAP. Campus accounts can be configured to or removed from LDAP while existing within the same environment.

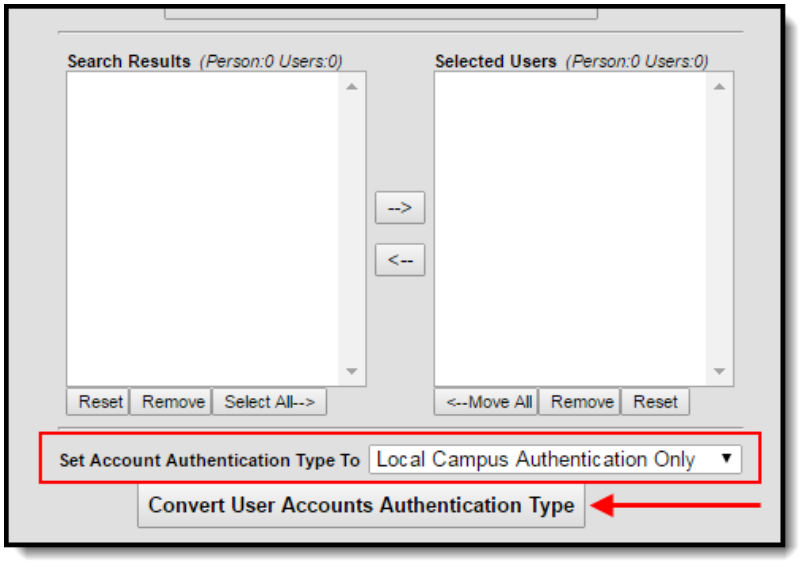


Image 6: Converting LDAP Accounts to Campus-Authenticated Accounts

Generating a List of LDAP Enabled Students/Staff

Tool Search: Filter Designer

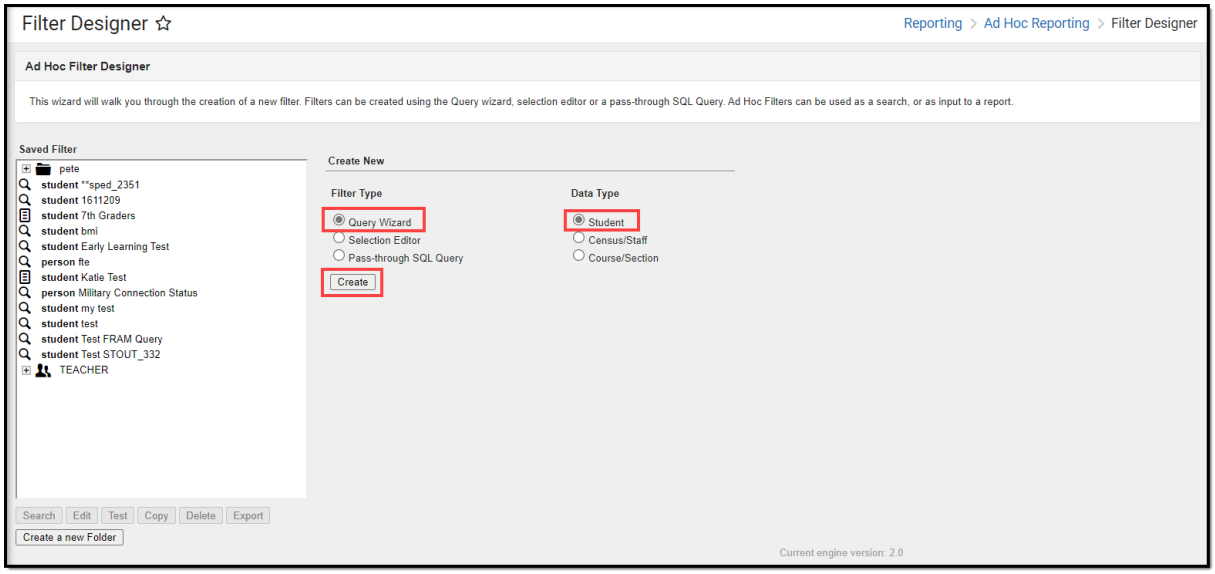
Using the Filter Designer, you can build filters that indicate which students and staff members have LDAP enabled for their account.

- Students with LDAP Enabled
- Staff with LDAP Enabled

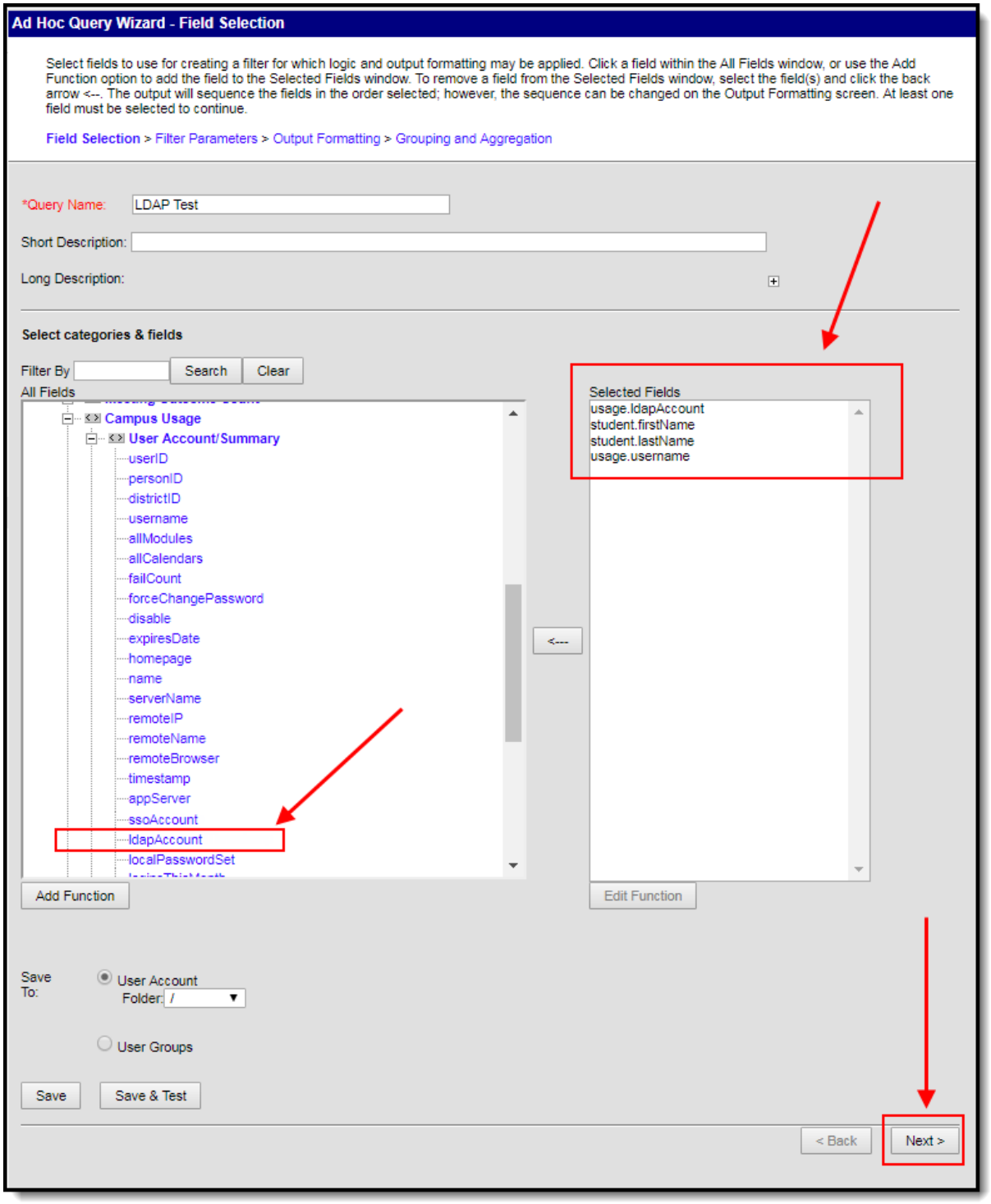
Students with LDAP Enabled

To generate a list of students who have LDAP enabled:

1. Select a Filter Type of **Query Wizard** and Data Type of **Student**.
2. Select the **Create** button.

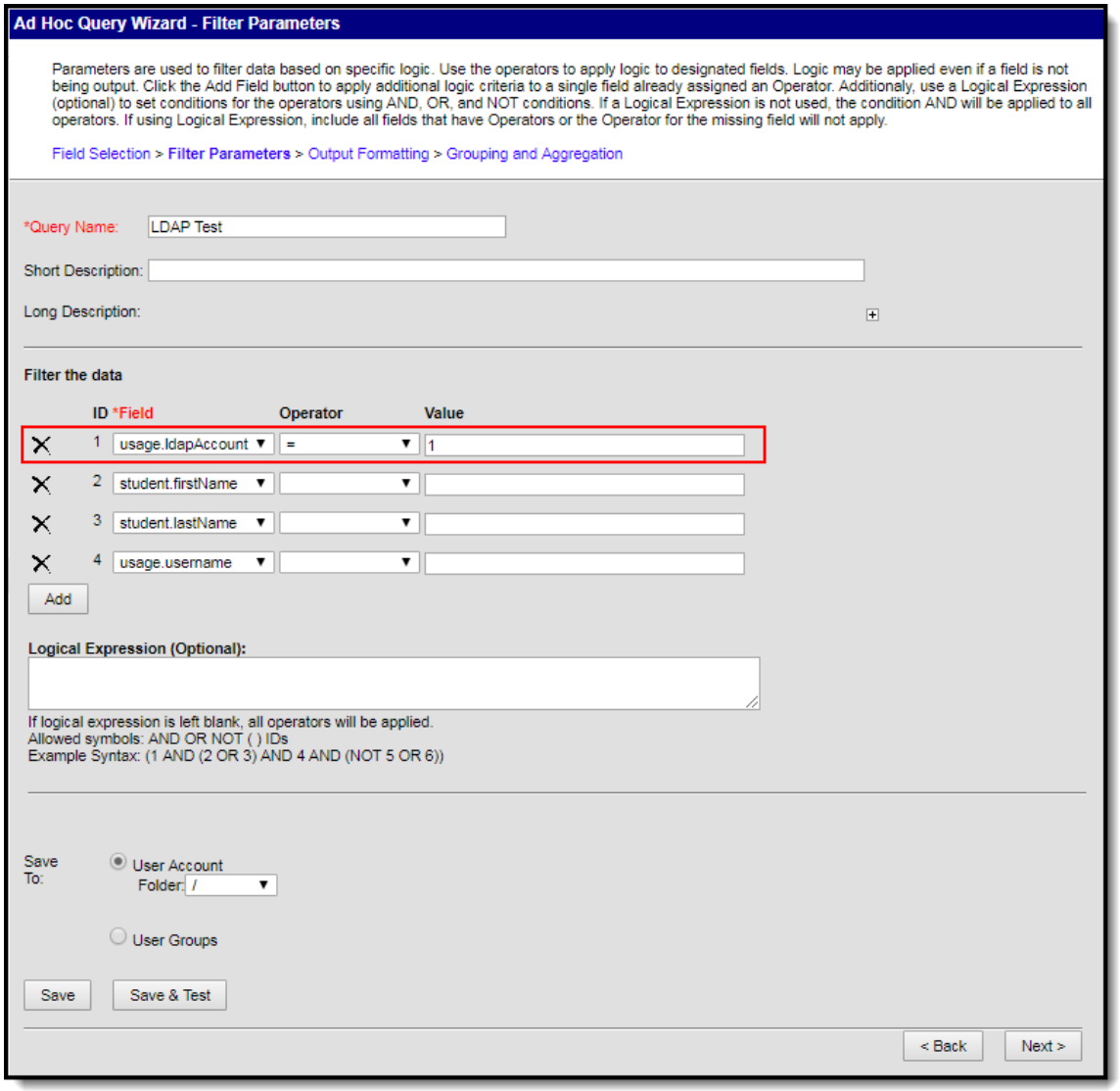


3. Enter a **Query Name**.
4. Go to Campus Usage > User Account/Summary and select **ldapAccount**. The usage.ldapAccount field will appear in the Selected Fields window.



5. Add additional fields to the filter, preferably identifiers such as first name, last name, username, etc to help in identifying and differentiating between filter results. Below are a few examples:
    - student.firstName
    - student.lastName
    - usage.username
6. Click the **Next** button. You will be redirected to the Filter Parameters editor.
7. Give the usage.ldapAccount the following values:
    - An **Operator** of **=**
    - A **Value** of **1** (see image below).

This ensures the field only reports users who have LDAP enabled (indicated by a value of 1). To do the reverse and identify users who do not have LDAP enabled, give this field a value of 0).



8. Click the **Save & Test** button. The filter will be saved and a separate window will appear, displaying filter report results. For example:

LDAP Test New Total Records: 656

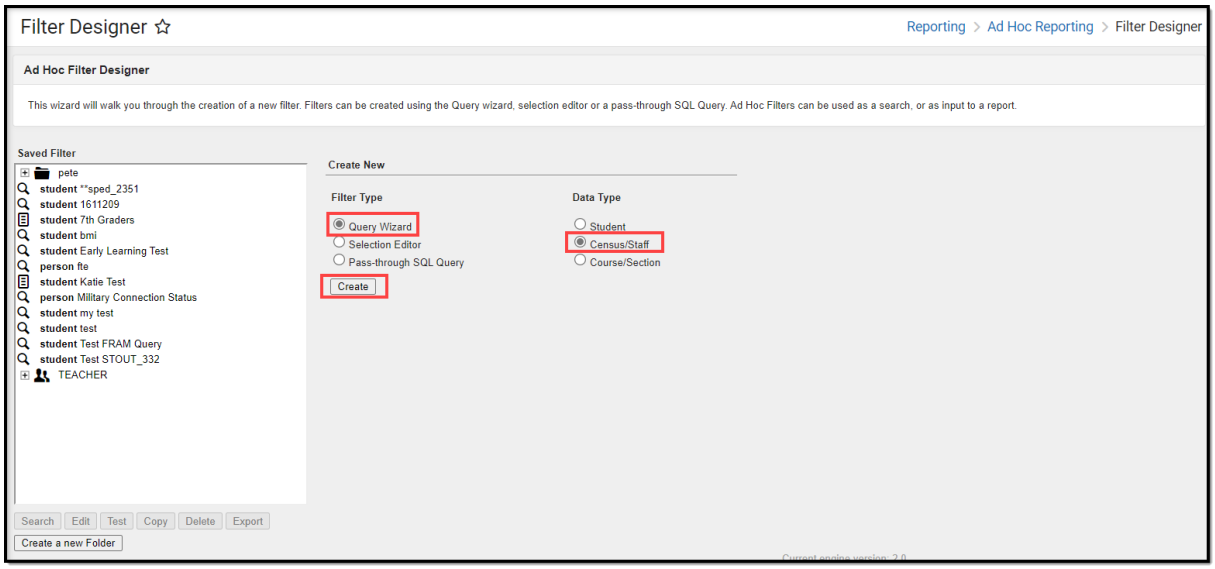
All Records

usage.ldapAccount	student.firstName	student.lastName	usage.username
1	Britney		91060134
1	Jacqueline		91059782
1	Mark		91131131
1	Miguel		91086522
1	Javier		91072678
1	Fransisca		91064289
1	ReAnne		91061968

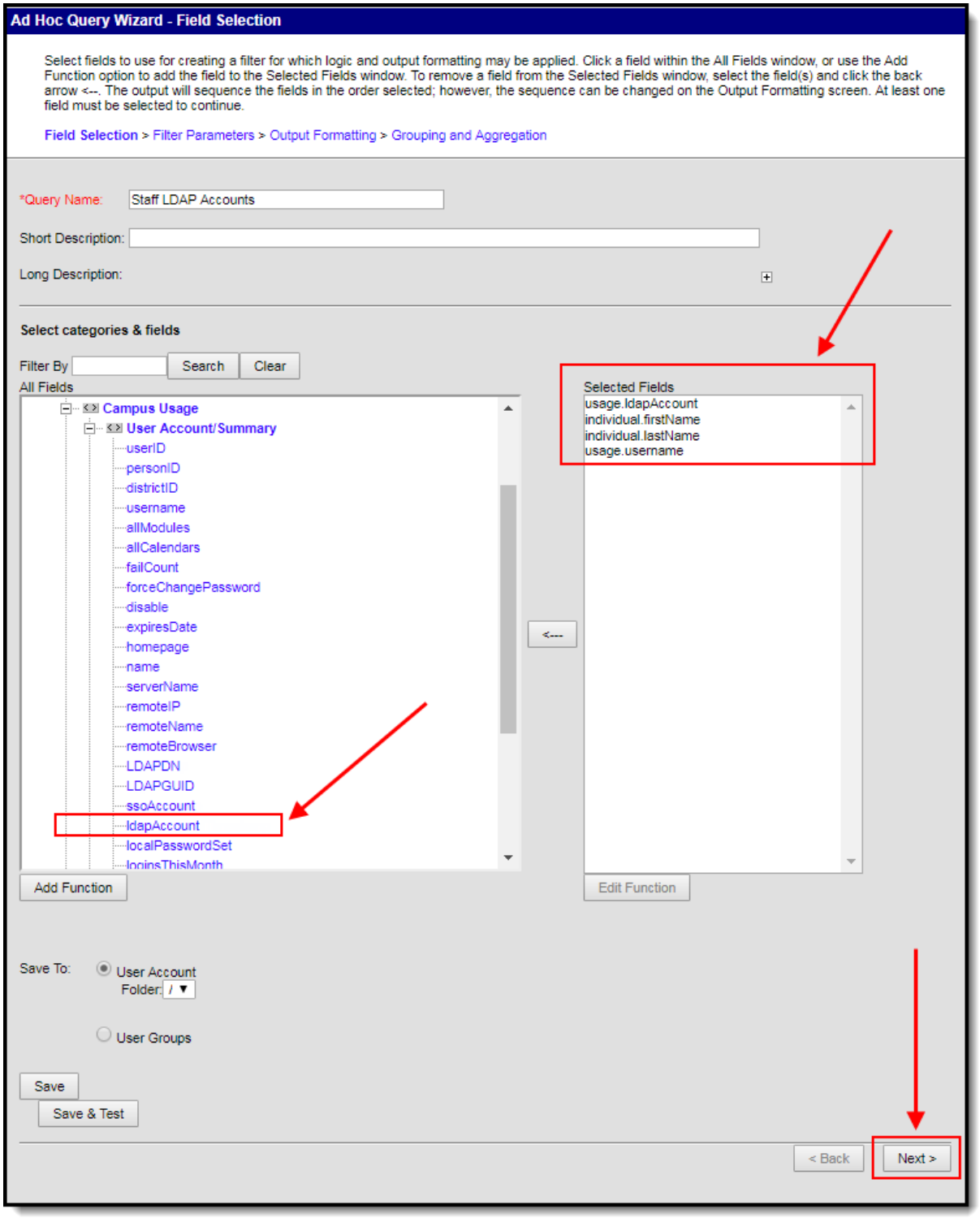
Staff with LDAP Enabled

To generate a list of staff who have LDAP enabled:

1. Navigate to the Filter Designer tool.
2. Select a Filter Type of **Query Wizard** and Data Type of **Staff**.
3. Select the **Create** button.



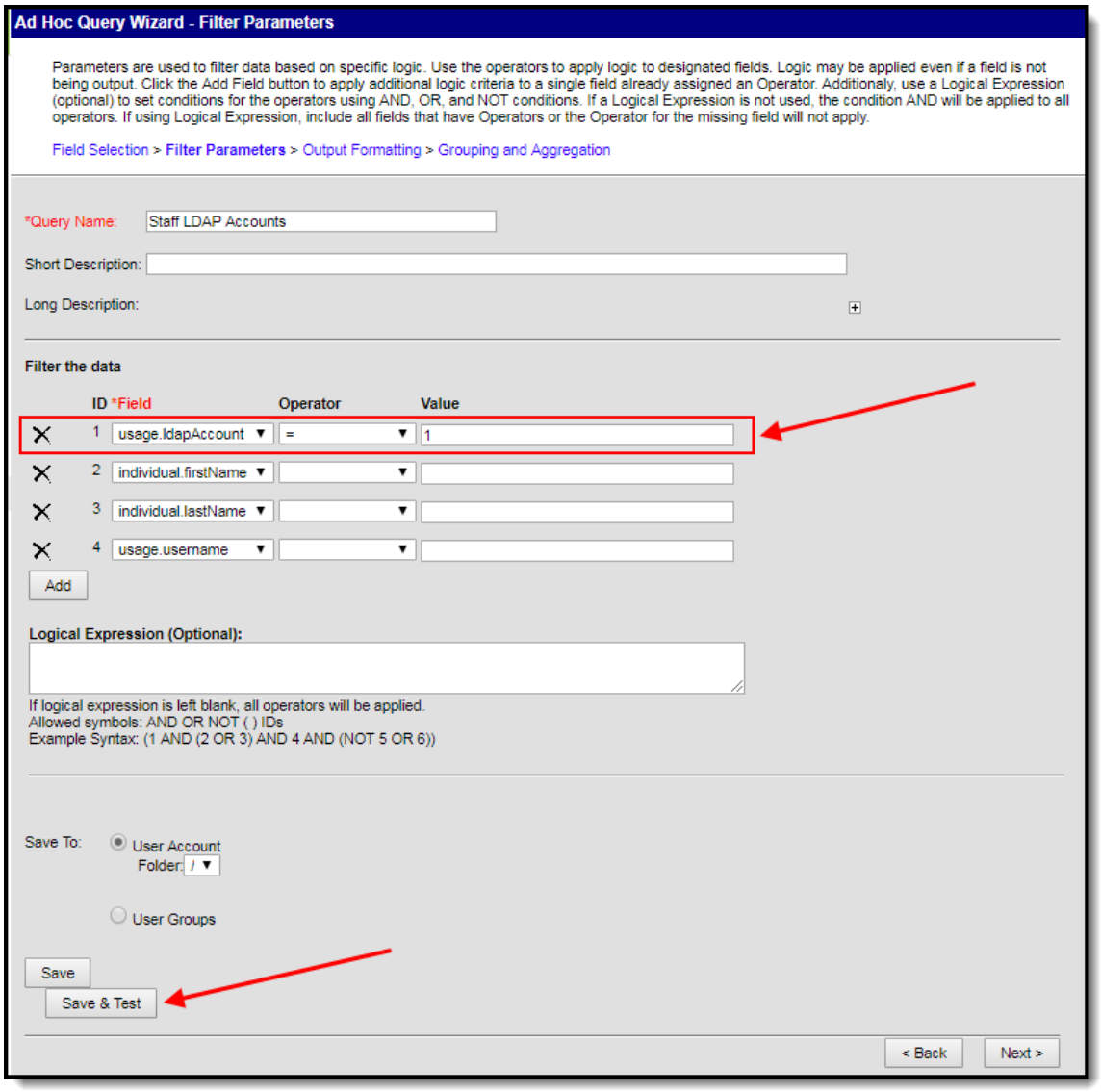
4. Go to Campus Usage > User Account/Summary and select **ldapAccount**. The usage.ldapAccount field will appear in the Selected Fields window.



5. Add additional fields to the filter, preferably identifiers such as first name, last name, username, etc to help in identifying and differentiating between filter results. Below are a few examples:
    - individual.firstName
    - individual.lastName
    - usage.username
6. Click the **Next** button. You will be redirected to the Filter Parameters editor.
7. Give the usage.ldapAccount the following values:
    - An **Operator** of **=**

- A **Value** of **1** (see image below).

> This ensures the field only reports users who have LDAP enabled (indicated by a value of 1). To do the reverse and identify users who do not have LDAP enabled, give this field a value of 0).



8. Click the **Save & Test** button. The filter will be saved and a separate window will appear, displaying filter report results. For example:

Staff LDAP Accounts Total Records: 161267

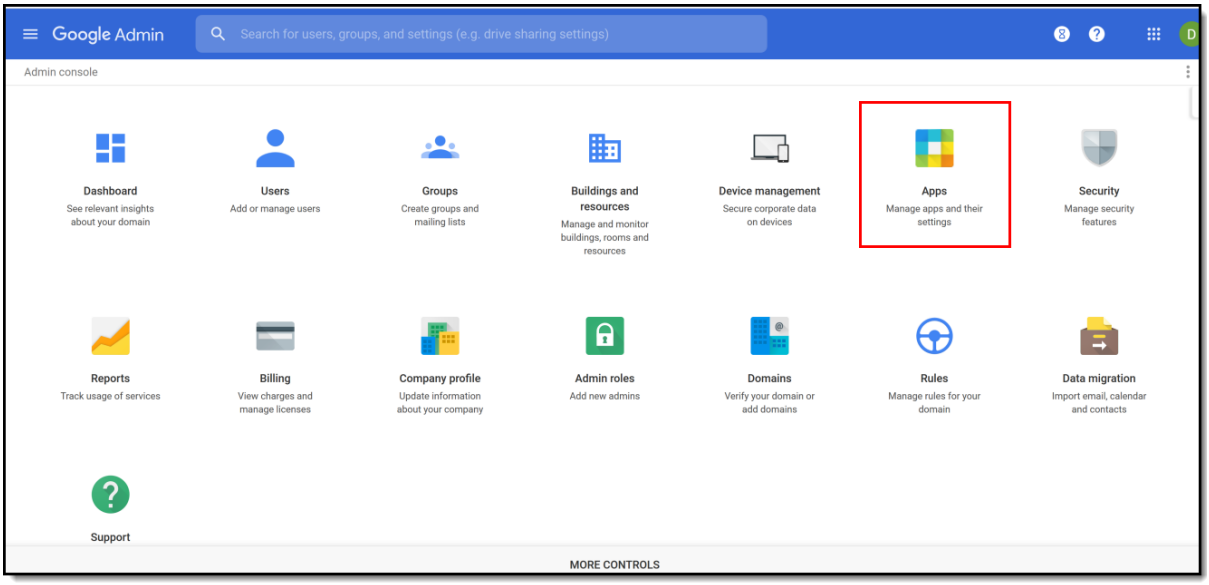
All Records

usage.ldapAccount	individual.firstName	individual.lastName	usage.username
1	Edwina	[redacted]	00170588
1	Lavonndia	[redacted]	00076443
1	Arlene	[redacted]	00223292
1	Mayra	[redacted]	00139842
1	Catalina	[redacted]	00217070

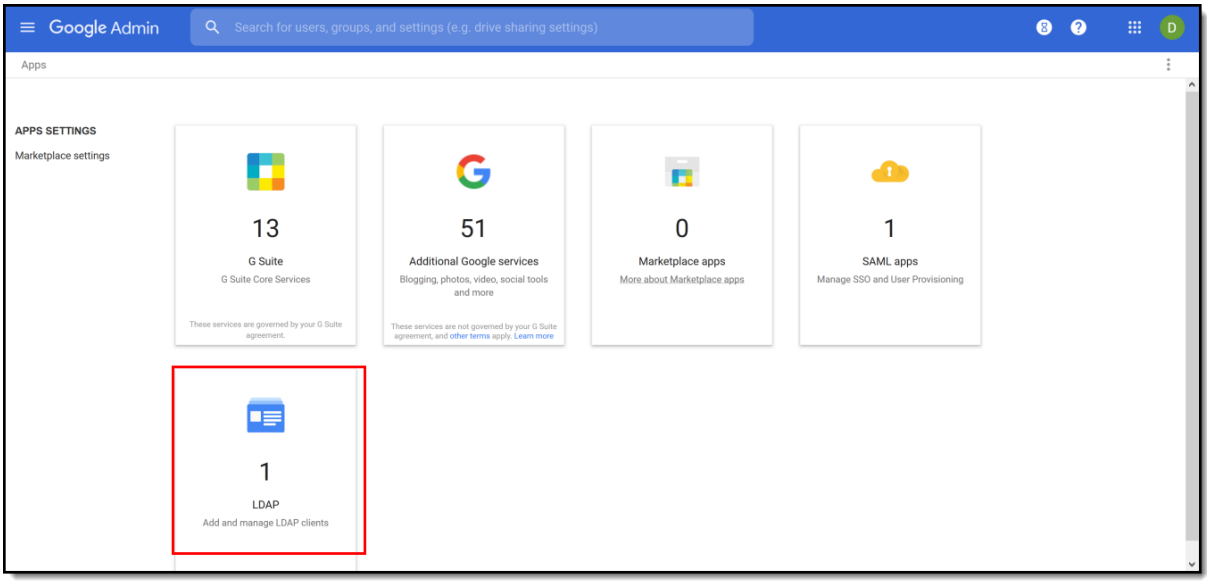
Configuring Google Suite to Work with Campus LDAP

This section will walk you through the process of configuring Google and Campus to set up an LDAP SASL connection.

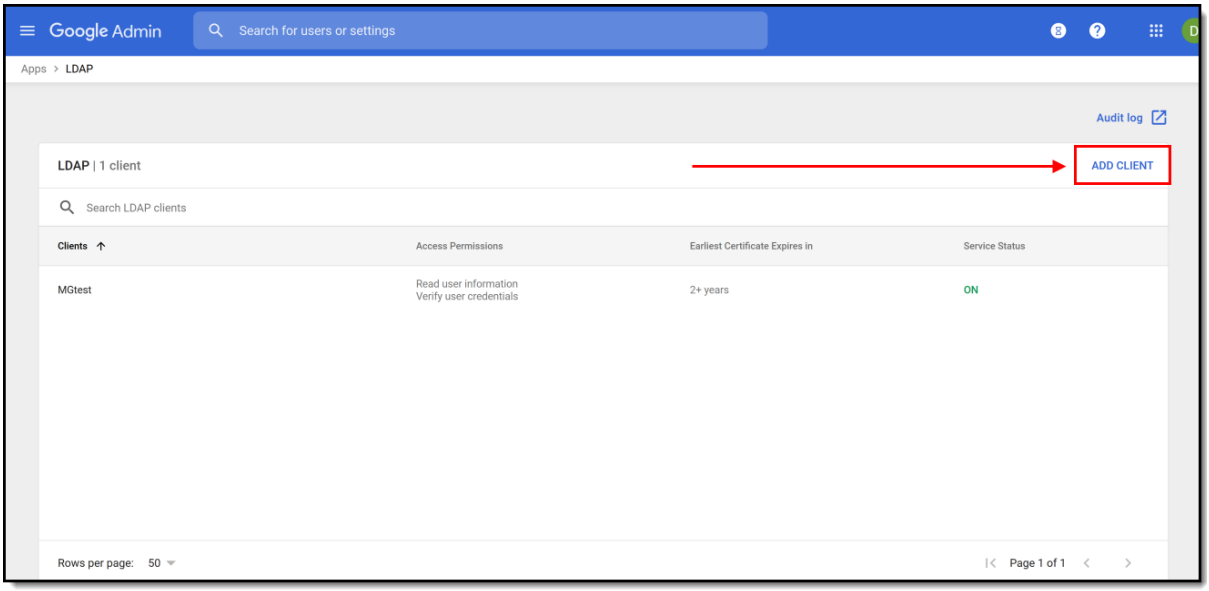
1. Log into your Google Admin console.
2. Select **Apps**.



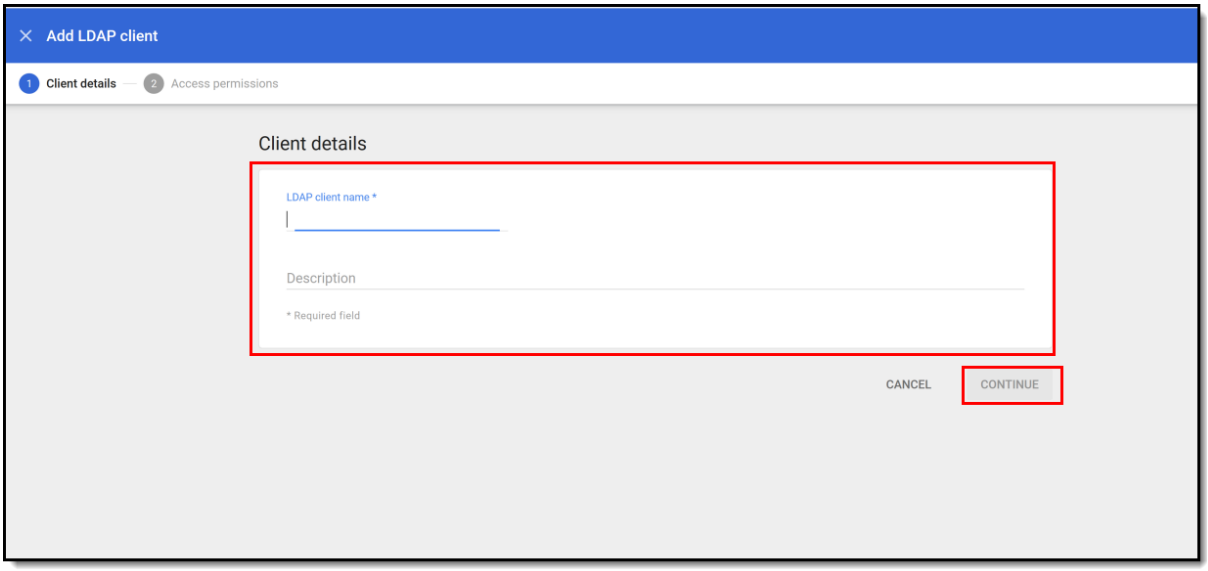
3. Select **LDAP**.



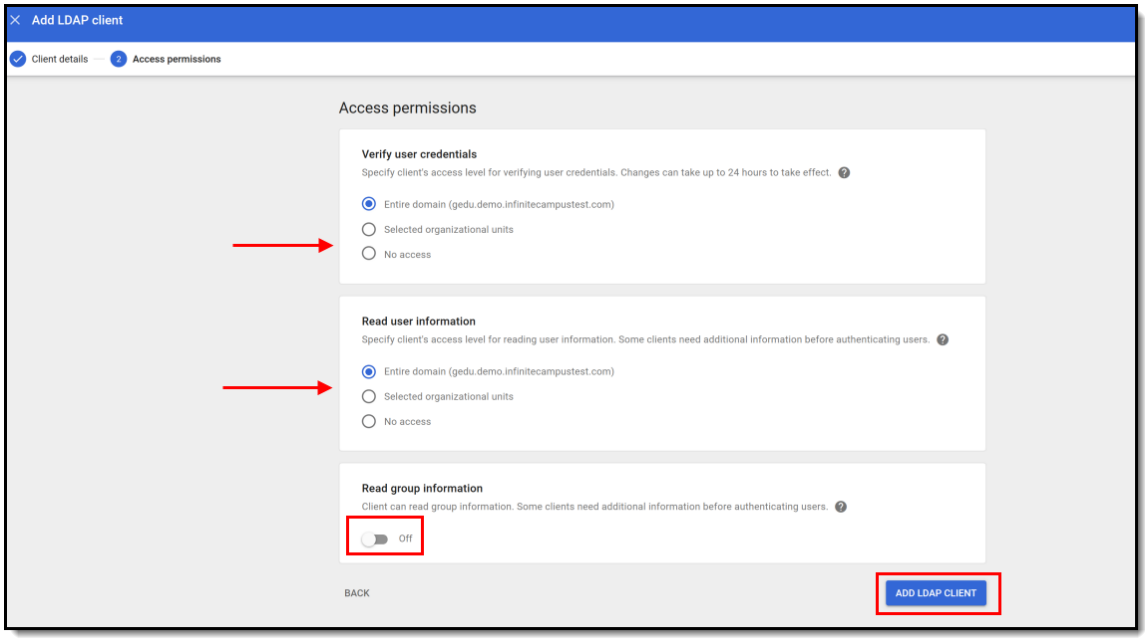
4. Click **Add Client**.



5. Enter the **LDAP Client Name** and **Description**. Campus recommends naming this something that allows you to easily identify it as the LDAP client being used for Campus.

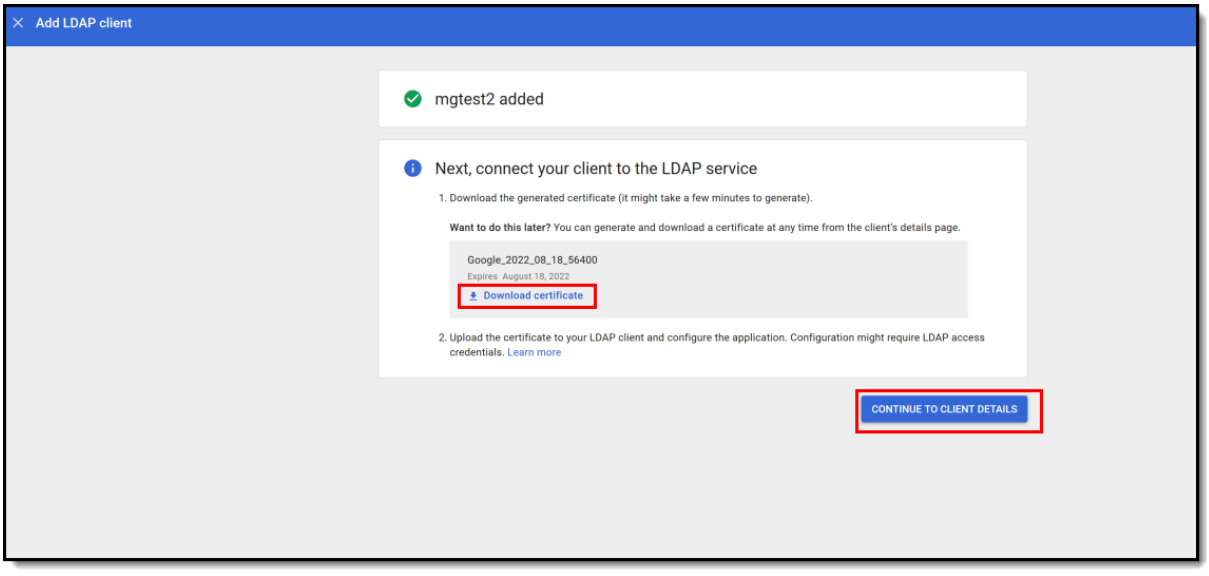


6. Establish access permissions:
   - Set **Verify user credentials** to 'Entire Domain'.
   - Set **Read user information** to 'Entire Domain'
   - Leave the **Read group information** toggle as Off.
   - Select the **Add LDAP Client** button.

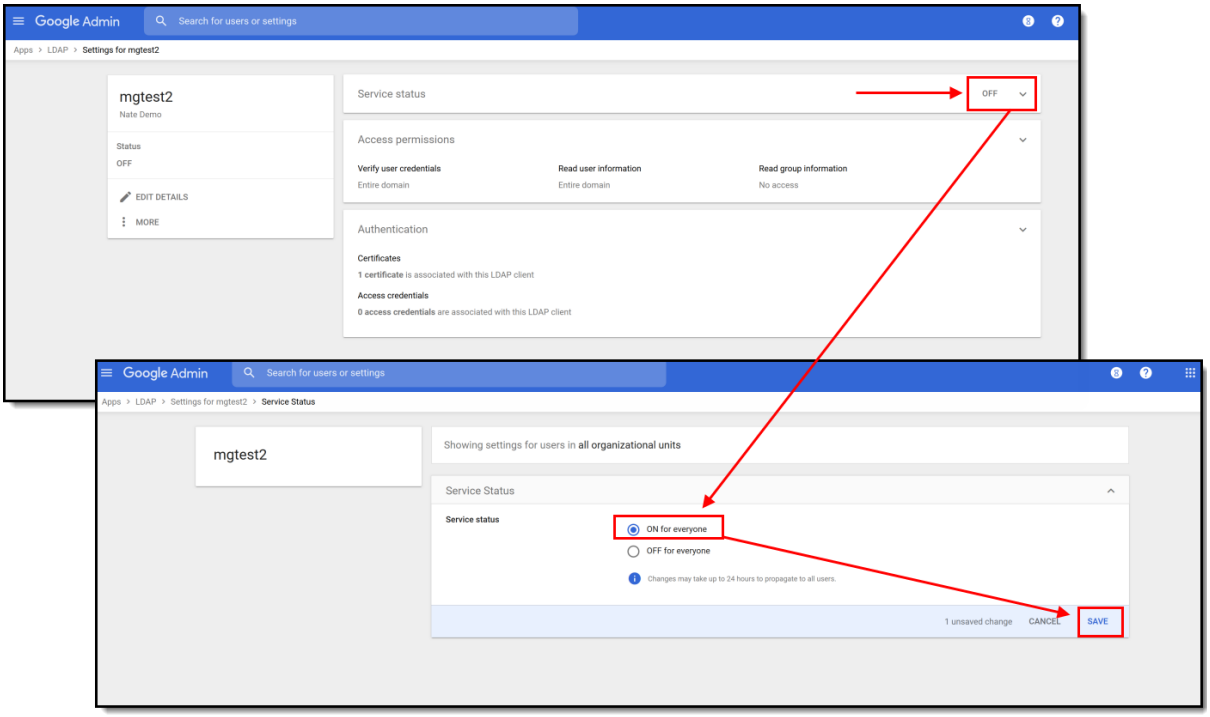


7. Download the LDAP service certificates by clicking the **Download certificate** hyperlink. Once downloaded, click **Continue to Client Details**.

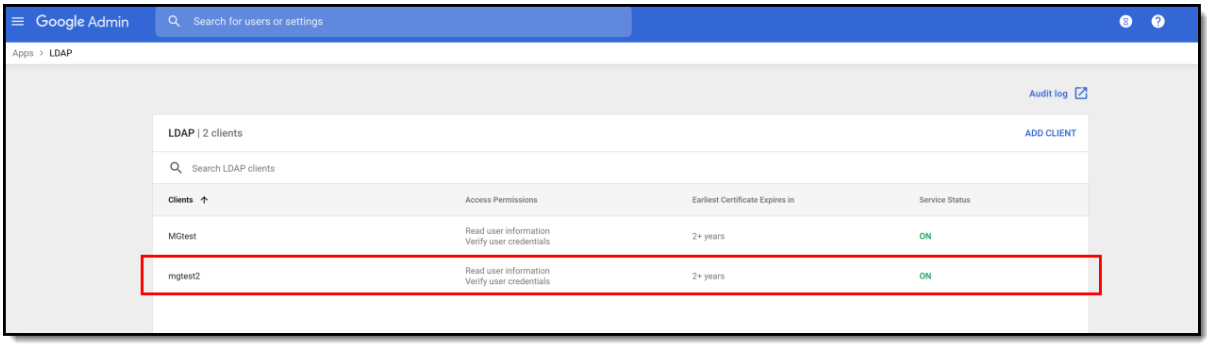
> This file is critical to successfully connecting Campus to Google. Unzip and save these files somewhere where you can easily access them as they will be used later in this process.



8. Click the **OFF** button found in the Service Status area. This will open Service Status options. Select **ON for everyone** and then click **Save**.



9. The service has now been added to your Google Suite and should show a Service Status of ON.



10. Now you need to configure the LDAP connection within Campus. Please follow the steps described in the Configuring LDAP for SASL section to complete the process.