

#### **LDAP** Authentication

Last Modified on 10/22/2022 10:10 am CDT

#### Classic View: System Administration > User Security > LDAP Authentication

#### Search Term: LDAP Authentication

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:

- Tool Rights
- LDAP Technical Components
- Interface Configuration of LDAP/Active Directory
   Initial Considerations
- Configuring Campus for LDAP Authentication
- Configuring LDAP for Multi-Forest Support
- Configuring LDAP for SASL
- Converting Existing Campus User Accounts to LDAP Authentication
- User Authentication
- LDAP Authentication Methods
- Converting LDAP Accounts Back to Campus-Authenticated Accounts
- Generating a List of LDAP Enabled Students/Staff
- Configuring Google Suite to Work with Campus LDAP

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 subsecond 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.

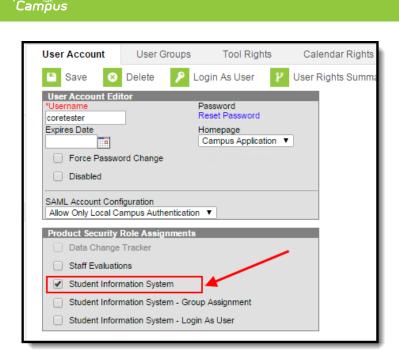
Infini	te 🔿	(	
Ca	mï	ວົບຣ	

DAP Configu	uration ☆ Settings > LDAP Configuratio				
ser Management 🦻 🤉	Settings > LDAP Configuration	on			
🕂 New 🕒 Sa	ave 🙁 Delete				
LDAP Server Configu					
Connection Status Na Successful m	ame otest4		Server UF	Com:636	
	gtest4 rimary LDAP			COIII.030	npus.com:636
	1mgtest			n:636	1940.0011.000
	-				
Configuration Detail					
Configuration Detail					
*LDAP Name:	Primary LDAP				
Enable this LDAP					
<u> </u>					
LDAP Server Pool:					
*Server 1 Host:	campus.	com	*Port:	636	
Server 2 Host:			Port		
Server 3 Host:			Port		
Server 4 Host:			Port	<u> </u>	
			Fun.		
Use SSL (Strongly	Recommended.)				
Administrator:					
Simple      SASL					
*Bind User DN:	deva				
*Bind User Password:	Change Password				
Dinu User Password.	Change Password				
User Search Configurat	tion:				
*User Search Base:		ampus,dc=com			
*User Search Filter:		countName={0}))			
	ree of the user search base.				
	ee of the user search base.				
Validation:					
Test Username:	Administrator Tes	t Configuration			
Server	Status Message		Last Upda		Last Success
SIS-129170B App	Success			15:13:24	
SIS-129170A App	Success		02/17/2020	15:13:38	02/17/2020 15:13:38

Image 1: LDAP Authentication Tool

## **Tool Rights**

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



Infinite 🔶 🗐

Image 2: Student Information System (SIS) Product Security Role

# **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
- Configuring Campus for LDAP Authentication

#### **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 to which they are assigned.
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 back-up account set to authenticate against Campus in the event that the LDAP service is unavailable.

## **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.

DAP Server Config onnection Status		Server UF	31
Johnection Status	Name	Server OF	(L
Configuration Deta	ail		
*LDAP Name:	*** mg test2		
Enable this LD	AP Configuration.		
LDAP Server Pool:			
*Server 1 Host:	10 25	*Port:	326
Server 2 Host:		Port:	
Server 3 Host:		Port:	
Server 4 Host:		Port:	
Use SSL (Strong	by Recommended )		
	hy recommended.y		
Administrator:			
● Simple ○ SASI			
*Bind User DN:			
*Bind User Passwor	d:	•••••	
User Search Configu	uration:		
*User Search Base:		:com	
*User Search Filter:			
	btree of the user search base.		
	buce of the user search base.		
Validation:			

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 onto 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.
- 7. Enter the **Port** numbers of the LDAP server(s) entered in Step 3.
- 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 easily identify the correct server.
Enable LDAP Authentication	If marked, this indicates Campus users can be authenticated using this LDAP Configuration.
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.

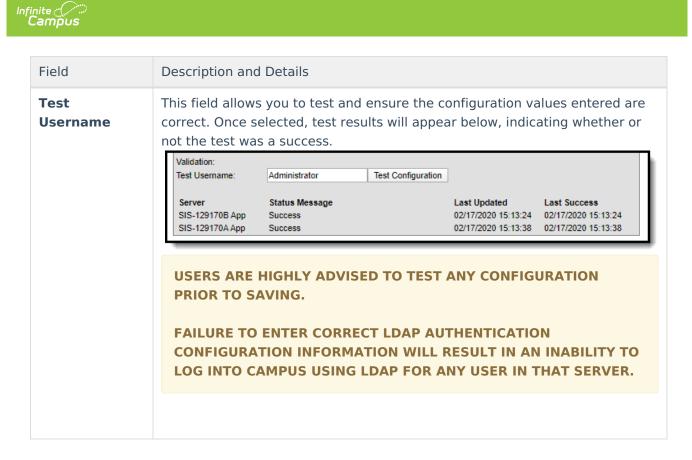


Field	Description and Details
Server (1, 2, 3, 4) Host	Server 1 Host name is required for LDAP. This should be the name of the Active Directory server. Up to three additional servers may be specified.
	When two or more servers are configured, Campus will balance data between available servers using internal load balancing technology.
Port	LDAP is firewall-sensitive. When LDAPS ports are used, the Use SSL checkbox should be marked.
	<ul> <li>Ports specified for LDAP servers are generally one of the following:</li> <li>Single domain searches - 389 LDAP or 636 LDAPS</li> <li>Global catalog searches (multi-domain) - 3268 LDAP or 3269 LDAPS</li> </ul>
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
Simple	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.
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 <b>Search entire subtree of the</b> <b>user search base</b> checkbox can apply the largest scope to a simple filter for the best results.

Field	Description ar	d Details		
User Search Filter	others. The following (sAMAcco (UserPrin (&(object ° Cam thes	are some exa ountName={0 cipalName={ Class=user)(s pus will repla e filters are e	)})	
	Operator	Character	Use	
	Equals	=	Creates a filter which requires a field to have a given value.	
	Any	*	A wildcard to represent that a field can equal anything other than null.	
	Parenthesis	( )	Separates filters to allow other logical operators to function.	
	And & Joins filters together. At least one condition the series must be true.			
	Or	or	Joins filters together. At least one condition in the series must be true.	
	Not	!	Excludes all objects that match the filter.	
Search entire subtree of the user search base	specified in th the results or	e User Search the search rea	pus will search the LDAP server from the level Base field downwards until the server restricts aches the bottom of the tree. This option provides It is highly encouraged.	



## **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.

DAP Server Co Connection State		Server URL	_
Successful	test 2	1025:3268	
Successful	1025 (converted)	10.: 25:3268	

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.

LUAP Server Col	nfiguration	
Connection Status		Server URL
Successful	google Idap test 2	ldap.google.com:636
Successful	Primary LDAP	.com:636
Disabled	01mgtest	ldap.google.com:636
Configuration De LDAP Name:	google Idap test 2	
DAP Server Pool:	- •	
Server 1 Host:	ldap.google.com	*Port: 636
Server 2 Host:		
		Port:
Server 3 Host:		Port:
Server 4 Host:		Port:
Use SSL (Stro	ngly Recommended.)	
	ngly Recommended.)	
Administrator:		
Administrator: O Simple  SA Bind User DN:	SL	
Administrator: O Simple O SA Bind User DN: Bind User Passwo User Search Confi	SL	
Administrator: O Simple O SA Bind User DN: Bind User Passwo User Search Confi	SL	ustest,dc=com
Administrator:	SL Change Password iguration: e: dc=gedu,dc=demo,dc=infinitecamp	pustest,dc=com
Administrator: Simple SA Bind User DN: Bind User Passwo User Search Confi *User Search Base *User Search Filter	SL Change Password iguration: e: dc=gedu,dc=demo,dc=infinitecamp	pustest,dc=com
Administrator: Simple SA Bind User DN: Bind User Passwo User Search Confi *User Search Base *User Search Filter	SL ord: Change Password iguration: e: dc=gedu,dc=demo,dc=infinitecamp r: (&(objectClass=person)(cn={0}))	pustest,dc=com
Administrator: Simple SA Bind User DN: Bind User Passwo User Search Confi *User Search Base *User Search Filter Search entire	SL ord: Change Password iguration: e: dc=gedu,dc=demo,dc=infinitecamp r: (&(objectClass=person)(cn={0})) subtree of the user search base.	pustest,dc=com
Administrator: Simple SA Bind User DN: Bind User Passwo User Search Confi *User Search Base *User Search Filter Search entire : Validation:	SL ord: Change Password iguration: e: dc=gedu,dc=demo,dc=infinitecamp r: (&(objectClass=person)(cn={0})) subtree of the user search base.	Test Configuration
Administrator: Simple SA Bind User DN: Bind User Passwo User Search Confi "User Search Filter User Search Filter Search entire : Validation: Test Username:	SL Change Password iguration: e: dc=gedu,dc=demo,dc=infinitecamp r: (&(objectClass=person)(cn={0})) subtree of the user search base. The status Message	Test Configuration

- 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**

**PATH:** System Administration > User Security > Batch and Import Wizards > User Account Type Wizard

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

Index	Search <	User Account Type Wizard
► Messen ► PLP	ger	This batch tool will update a subset of User Accounts using an Ad Hoc selection. Please note that User Accounts uploaded via the Batch Import tool will create a unique Ad Hoc query automatically by date and time and can be easily utilized and/or modified for use in this tool.
► Portal		Note: Product Security Roles are exempt from a SSO configuration. If a user has a Product Security Role, that user will need to create an additional non-Product Security Role user account for SSO use.
Preferei	nces	
► Resour	ces	Username
▶ Respon	se to Intervention	Last Name
► Roster		First Name
► School	Choice	Adhoc Filter
► Special	Ed	Student Number Filter Verschaft Student Number Filter
► Student		User Account Type
	pp Settings	Search Users & Add to the Search Results
▶ Student		
Surveys		Search Results (Person: 0 Users: 0) Selected Users (Person: 0 Users: 0)
▶ Transpo	ortation	
▼ User Se	curity	
User	rs	
User	r Groups	
Stud	ent Accounts	<
▼ Ba	atch and Import Wizards	
	Account Letter Designer	
	Account Letter Builder	· · · · ·
	User Account Batch Import Tool	Reset Remove Select All> <move all="" remove="" reset<="" th=""></move>
	User Account Messenger	Set Account Authentication Type To LDAP: 10. 20.25 (converted)
	User Account Type Wizard	Convert User Accounts Authentication Type
► LC	OAP Management	
► O/	Auth Management	

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 IdapConfigurationID is not null.
- User accounts with null IdapConfigurationID 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 IdapConfigurationID 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**

## **PATH:** System Administration > User Security > Batch and Import Wizards > 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.

finite Campus	
Search F	Results (Person:0 Users:0) Selected Users (Person:0 Users:0)
	->
Reset	Remove     Select All> <move all<="" td="">     Remove</move>
Set Accor	unt Authentication Type To       Local Campus Authentication Only         Convert User Accounts Authentication Type

Image 6: Converting LDAP Accounts to Campus-Authenticated Accounts

## Generating a List of LDAP Enabled Students/Staff

**PATH:** *Ad Hoc Reporting > Filter Designer* 

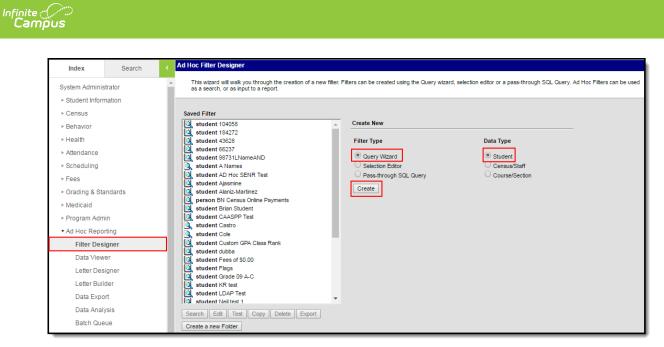
Using the Filter Designer, you can build filters which indicate which students and staff members have LDAP enabled for their account.

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

Beech fields to use for reating a file for which logic and output formating may be applied. Click a field within the All Fields window. The read window of the read window. The read within the All Fields window. The read window of the read window of the read window of the read window. The read window of the read window. The read window of the read		izard - Field Selection	Cicles Estimative the All Fields window serves the Add
Reid must be selected to continue.         Field Selection > Filter Parameters > Output Formatting > Grouping and Aggregation         *Ouery Name       DAP Test         Short Description:	Function optio	n to add the field to the Selected Fields window. To remove a field from the Selected	lected Fields window, select the field(s) and click the back
"Ouery Name:       DAP Test         Short Description:	field must be s	elected to continue.	an be changed on the Oulput Formatung screen. At least o
Shot Description: Long Description: Select categories & fields Filter By Search Clear All Fields Select categories & Stard Select categories & Stard	Field Selectio	n > Filter Parameters > Output Formatting > Grouping and Aggregation	
Shot Description: Long Description: Select categories & fields Filter By Search Clear All Fields Select categories & Stard Select categories & Stard			
Short Description: Long Description: Select categories & fields Filter By Search Clear All Fields Select all Select All Fields Usage dipAccount student firstName student firstName serverName remotelParter remotelParter student firstName student firstName serverName remotelParter serverName remotelParter student stud	Ouenr Neme:	L DAD Toot	
Long Description:  Select categories & fields  Filter By Search Clear  All Fields  Filter By Search Clear  Selected Tields  S	Query Name.	LDAP ICSI	/
Select categories & fields  Filter By Search Clear  All Fields  Select dat User Account Summary  Select dat Fields  Select dat  Select dat Select dat  Select dat  Select dat Select dat Select dat  Select dat Select dat Select dat Select dat Select dat Se	hort Description:		
Filter By   all Fields     Selected Fields   User Account/Summary   User Modules   ellCatendars   ellCatendars   ellCatendars   ellCatendars   ellCatendars   endlCatendars   endledars	ong Description:		
Filter By   all Fields     Selected Fields   User Account/Summary   User Modules   ellCatendars   ellCatendars   ellCatendars   ellCatendars   ellCatendars   endlCatendars   endledars			
All Fields  Selected Fields  User Account Save  Vertage  Selected Fields	elect categories	& fields	4
All Fields  Selected Fields  User Account Save  Vertage  Selected Fields			
Best Campus Usage       usege IdapAccount         - useriD       - useriD         - districtID       - usermame         - districtID       - usermame         - allModules       - allCalendars         - failCount       - forceChangePassword         - dissible       - expiresDate         - homepage       - name         - serverName       - remoteName         - remoteName       - remoteName         - dimestramp       - spSeAver         - spSeAver       - sobacount         - didapAccount       - didapAccount         - didapAccount<			Selected Fields
Image: Sel User Account/Summary         useriD         personiD         districtID         useridical         allAdules         allCalendars         fielCount         forceChangePassword         districtID         user Account         forceChangePassword         districtID         user Account         forceChangePassword         districtID         user Account         remotelP         remotelP         remotelP         remotelPasswordSet         dotation         dd Function			usage.ldapAccount
Save       • User Account         To:       • User Account         Folder.//       • User Groups			
Add Function         Save         • User Account         Folder[		-	
Save          • User Account         Folder[ ]         • Juser Strues         • Juser Strue			
all/Calendars		districtID	
Add Function Save Output Outpu		username	
Save     Ouser Account     Folder /			
Save     Image: Save To:     Image: Save To: <td></td> <td>allCalendars</td> <td></td>		allCalendars	
disable         expiresDate         homepage         name         serverName         remoteIP         remoteBrowser         uimestamp         appServer         ssoAccount         UiserAccount         CocalPasswordSet         Interference         Edit Function		failCount	
expiresDate		forceChangePassword	
Add Function Save Save User Account Folder: To: User Groups			
Add Function Save Output Outpu			
Add Function  Save Output Outp	1 1 1		
remotelP      remoteBrowser      timestamp      appServer      ssoAccount      IdapAccount      IdapAsswordSet      IocalPasswordSet      IocalPasswordSet <td< td=""><td></td><td></td><td></td></td<>			
Add Function Save Output Outpu			
Add Function Save Output Outpu			
Add Function  Save Ouser Account Folder:  User Groups			
Add Function  Save Ouser Account Folder:  User Account Ouser Groups			
Add Function  Save Ouser Account Folder:  User Groups			
Image: IndepAccount       Image: IndepAccount       Image: IndepAccount       Add Function       Save       Image: IndepAccount       Folder: IndepAccount       Folder: IndepAccount       Image: IndepAccount			
Add Function  Save Outer Account Folder: Outer Groups			
Add Function Edit Function Save Ouser Account Folder:			
Save Ouser Account To: Folder:			
To: Folder: / T	Add Function		Edit Function
To: Folder: / T			
To: Folder: / To: Vuer Groups			
To: Folder: / T			
User Groups			
	0. F	older: / 🔻	
	O Us	ser Groups	
Save & Test			
	Saus Co-	no 8 Test	
	Save Sa		
< Back N			< Back Next

- 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 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).

Ad Hoc Query Wizard - Filter Parameters	
Parameters are used to filter data based on specific logic. Use the operators to apply logic to designated fields. Logic may be being output. Click the Add Field button to apply additional logic criteria to a single field already assigned an Operator. Additi (optional) to set conditions for the operators using AND, OR, and NOT conditions. If a Logical Expression is not used, the co operators. If using Logical Expression, include all fields that have Operators or the Operator for the missing field will not appl Field Selection > Filter Parameters > Output Formatting > Grouping and Aggregation	onaly, use a Logical Expression ndition AND will be applied to all
Field Selection > Filter Parameters > Output Formatting > Grouping and Aggregation	
*Query Name: LDAP Test	
Short Description:	
Long Description:	
Filter the data	
ID *Field Operator Value	
X 1 usage.ldapAccount V = V 1	
X 2 student.firstName V V	
X 3 student.lastName V V	
X 4 usage.username V V	
Add	
Logical Expression (Optional):	
/i	
If logical expression is left blank, all operators will be applied. Allowed symbols: AND OR NOT () IDs Example Syntax: (1 AND (2 OR 3) AND 4 AND (NOT 5 OR 6))	
Save (● User Account To: Folder: / ▼	
O User Groups	
Save Save & Test	
	< Back Next >

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



LDAP Test New Tot	al 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. Select a Filter Type of Query Wizard and Data Type of Staff.
- 2. Select the **Create** button.

Index	Search	Ad Hoc Filter Designer
System Admini		This wizard will walk you through the creation of a new filter. Filters can be created using the Query wizard, selection editor or a pass-through SQL Query. Ad Hoc Filters can be used as a search, or as input to a report.
Student Information	mation	
▶ Census		Saved Filter
Behavior		Create New Create New
▶ Health		student 14058     Create New       student 14272     Filter Type       student 43628     Filter Type       student 65237     Ouery Wizard
Attendance		addent 60237
Scheduling		student A Names     Selection Editor     Census/Staff     Census/Staff     Course/Section
► Fees		student AD Hoc SENR Test     O Pass-through SQL Query     Course/Section     student Alasmine
Grading & St	andards	Create Create
Medicaid		student Al bho: SENR Test     Pass-through SQL Query     Course/Section       student Alani:-Martinez     Create       person BN Census Online Payments     student CAASPP Test
Program Adr	nin	Student CAASP Test
▼ Ad Hoc Repo	orting	Student Castro
	-	student Cole     student Custom GPA Class Rank
Filter Des	signer	student dubba
Data Viev	ver	It student Fees of \$0.00
Letter De	signer	G student Flags
Letter Bui	lder	Student Grade 09 A-C
Data Exp	ort	Restudent LDAP Test
Data Ana		I student Nei test 1
	-	Search Edit Test Copy Delete Export
Batch Qu	eue	Create a new Folder
_		

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

Ad Hoc Query Wizard - Field Selection	
Select fields to use for creating a filter for which logic and output formatting may be app Function option to add the field to the Selected Fields window. To remove a field from th arrow < The output will sequence the fields in the order selected; however, the seque field must be selected to continue. Field Selection > Filter Parameters > Output Formatting > Grouping and Aggregation	he Selected Fields window, select the field(s) and click the back
The selection of their transfers of output formatting of obliging and Aggregation	
Cuery Name: Staff LDAP Accounts  Short Description: Long Description:	
Select categories & fields	
Filter By Search Clear	Selected Fields
Campus Usage	
Save To: User Account Folder: / V O User Groups	
Save & Test	<b>↓</b>
	< Back Next >

- 4. 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
- 5. Click the **Next** button. You be redirected to the Filter Parameters editor.
- 6. 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).

Ad Hoc Query Wizard - Filter Parameters	
Parameters are used to filter data based on specific logic. Use the operators to apply logic to designated fields. Logic may be a being output. Click the Add Field button to apply additional logic criteria to a single field already assigned an Operator. Addition (optional) to set conditions for the operators using AND, OR, and NOT conditions. If a Logical Expression is not used, the cond operators. If using Logical Expression, include all fields that have Operators or the Operator for the missing field will not apply.	aly, use a Logical Expression
Field Selection > Filter Parameters > Output Formatting > Grouping and Aggregation	
*Query Name: Staff LDAP Accounts	
Short Description:	
Long Description:   •	
Filter the data	
ID *Field Operator Value	
X 1 usage.ldapAccount V = V 1	
X 2 individual.firstName V	
X <sup>3</sup> individual lastName V	
X 4 usage.usemame V V	
Add	
Logical Expression (Optional):	
If logical expression is left blank, all operators will be applied. Allowed symbols: AND OR NOT ( ) IDs Example Syntax: (1 AND (2 OR 3) AND 4 AND (NOT 5 OR 6))	
Save To: ● User Account Folder / ▼ ○ User Groups	
Save & Test	
	< Back Next >

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

Staff LDAP Account	ts Total Records: 161267		
usage.ldapAccount	individual.firstName	individual.lastName	usage.username
1	Edwina		00170588
1	Lavonndia		00076443
1	Arlene		00223292
1	Mayra	1111 January	00139842
1	Catalina		00217070



## **Configuring Google Suite to Work** with Campus LDAP

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

1. Select Apps.

≡ Google Admin	Q Search for users, gro	ups, and settings (e.g. drive s	haring settings)			8 ?
Admin console						
Dashboard See relevant insights about your domain	Users Add or manage users	Groups Create groups and mailing lists	Buildings and resources Manage and monitor buildings, rooms and resources	Device management Secure corporate data on devices	Apps Apps and their settings	Security Manage security features
Reports Track usage of services	Billing View charges and manage licenses	Company profile Update information about your company	Add new admins	Domains Verify your domain or add domains	Rules Manage rules for your domain	Data migration Import email, calendar and contacts
Support			MORE CONTROLS			

2. Select LDAP.

≡ Google Admir	n Q Search for users, groups				8 ?	
Apps						:
PPS SETTINGS						
larketplace settings		G		-		
	13	51	0	1		
	G Suite G Suite Core Services	Additional Google services Blogging, photos, video, social tools and more	Marketplace apps More about Marketplace apps	SAML apps Manage SSO and User Provisioning		
	These services are governed by your G Suite agreement.	These services are not governed by your G Suite agreement, and other terms apply. Learn more				
	1					
	LDAP Add and manage LDAP clients					
	ļ					

3. Click Add Client.

Google Admin	Q Search for users or settings			8 ? :
ps > LDAP				
				Audit log
LDAP   1 client				ADD CLIENT
Q Search LDAP clients				
Clients 🛧		Access Permissions	Earliest Certificate Expires in	Service Status
MGtest		Read user information Verify user credentials	2+ years	ON

4. 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.

imes Add LDAP client			
1 Client details — 2 Access permi	ssions		
	Client details		
	LDAP client name *		
	Description * Required field		
		CANCEL CONTINUE	

- 5. 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.

× Add LDAP client	
Client details — 2 Access permissions	
	Access permissions
	Verify user credentials         Specify client's access level for verifying user credentials. Changes can take up to 24 hours to take effect. <ul> <li>Entire domain (gedu demo.infinitecampustest.com)</li> <li>Selected organizational units</li> <li>No access</li> </ul>
-	Read user information         Specify client's access level for reading user information. Some clients need additional information before authenticating users.         Image: Third comparison of the system of the
	Read group information Client can read group information. Some clients need additional information before authenticating users.

6. 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.

mgtest2 added      Next, connect your client to the LDAP service      .ownload the generated certificate (it might take a few minutes to generate).      Want to do this later? You can generate and download a certificate at any time from the client's details page.      Google_2022_08_18_56400     Epires August 18_2022     Download certificate      .upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access     credentials. Learn more      CONTINUE TO CLIENT DETAILS
<ol> <li>Download the generated certificate (it might take a few minutes to generate).</li> <li>Want to do this later? You can generate and download a certificate at any time from the client's details page.</li> <li>Boogle_2022_08_18_56400         <pre>Copies Argent 18_2022         </pre> </li> <li>Download certificate         </li> <li>Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access         credentials. Learn more</li> </ol>
CONTINUE TO CLIENT DETAILS

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

≡ Google Adn	nin Q Search	for users or settings					8 0	
Apps > LDAP > Settin	gs for mgtest2							1
	mgtest2 Nate Demo Status OFF		Service status				OFF 🗸	
			Access permis		Read user information	Read group information	~	
🖋 EDIT DETAILS		Entire domain		Entire domain	No access			
	MORE		Authentication				~	
			Access credentials	oclated with this LDAP client is	client	/		
=	≡ Google Admin	Q Search for users	or settings					8 ? :
/	Apps > LDAP > Settings fo	or mgtest2 > Service Status						
		mgtest2		Showing settings for us	ers in all organizational units			
				Service Status	ON for everyon     OFF for everyon			^
					(i) Changes may tak	e up to 24 hours to propagate to all users.		
							1 unsaved change CANCEL	SAVE

Infinite Campus

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

≡ Google Admin	Q Search for users or settings				
Apps > LDAP					
				Audit log	
	LDAP   2 clients			ADD CLIENT	
	Q Search LDAP clients				
	Clients 1	Access Permissions	Earliest Certificate Expires in	Service Status	
_	MGtest	Read user information Verify user credentials	2+ years	ON	
	mgtest2	Read user information Verify user credentials	2+ years	ON	
[					

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