

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:

- 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.

npus						
_DAP Conf	iguration ☆			User Managemen	t > Settings > I	LDAP Configu
+ New	Save 😣 Delete					
LDAP Server Con Connection Status	figuration Name	Server URL				
Error	Test LDAP					
Disabled	mgtest					
Disabled	mgtest					
Disabled	mgtest					
Disabled	mgtest					
Disabled	mgtest					
Disabled Configuration Det	ail		_			
Disabled Configuration Det *LDAP Name:	ati mgtest					
Disabled Configuration Det *LDAP Name: Configuration Det	ail mgtest DAP Configuration.	 _	_			
Configuration Det *LDAP Name: Configuration Det	ail mgtest DAP Configuration.					
Configuration Det "LDAP Name: Enable this LI LDAP Server Pool: "Server 1 Host	afi mgtest DAP Configuration.	*Port 636				
Configuration Det *LDAP Name: Enable this LI LDAP Server Pool: *Server 1 Host: Server 2 Host:	ail mgtest DAP Configuration.	*Port: 636 Port:				
Configuration Det "LDAP Name: Enable this LI LDAP Server Pool: "Server 1 Host: Server 2 Host: Server 3 Host:	ail mgtest DAP Configuration.	*Port: 636 Port: Port:				

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

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 assigned to them.
District System	Each district using LDAP should create a system administrator user that is allowed to authenticate against the Campus database.
Administrator Accounts	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.

onnection Status	Name	Server LIPI	
onnection Status	Wallie	JEIVEI ORL	
Configuration Det	ail		
comgaration bet			
*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	gly Recommended.)		
A desistentes.			
*Bind User DN:			
*Bind User Passwor	d:		
User Search Configu	uration:		
*User Search Base:	=infinitecampus,dc=	com	
*User Search Filter:	(sAMAccountName={0})		
Search entire su	ubtree 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 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.
Rind Usor	The administrative password for the directory server
Password	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.



Field	Description	Description and Details				
User Search Filter	Filters the us others. The following • (sAMAcc • (UserPri • (&(objec • Can the The following	er search to are some ex countName= ncipalName= ctClass=user mpus will rep se filters are table descri	allow certain entries in the subtree while excluding xamples: {0}) ={0}) :)(sAMAccountName={0})) place the {0} with the username of the user when e executed upon login. ibes some common filter operands:			
	Operator	Character	Use			
	Equals	=	Creates a filter which requires a field to have a given value.			
	Any	*	A wildcard represents 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 in the series must be true.			
	Or	or Joins filters together. At least one condition in series must be true.				
	Not	!	Excludes all objects that match the filter.			
Search entire subtree of the user search base	When marked specified in t results or the best results a	d, Infinite Ca he User Sear search reac and use of it	mpus will search the LDAP server from the level The Base field downwards until the server restricts the Thes the bottom of the tree. This option provides the 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.

	Save 🔇 Delete	 New
Server URL	figuration Name	LDAP Server Con Connection Statu
1025:3268	test 2	Successful
10. 25:3268	1025 (converted)	Successful
10. 25:3268	10	Successful

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.

🕂 New 🕒	Save 🙁 Delete	
LDAP Server Conf	figuration	
Connection Status	Name	Server URL
Successful	google Idap test 2	Idap.google.com:636
Successful	Primary LDAP	.com:636
Disabled	01mgtest	ldap.google.com:636
Configuration Det	ail	
*LDAP Name:	google Idap test 2	
Enable this LD	AP Configuration.	
LDAP Server Pool:		
*Server 1 Host:	Idap.google.com	*Port: 636
Server 2 Host		Port
Conver 2 Heat:		Dot:
Server 5 host.		
Server 4 Host:		Port:
Use SSL (Strong	gly Recommended.) 🗲 🗕 🚽	
Administrator:		
	L <u></u>	
Simple SASI		
Bind User DN:		
Bind User DN: Bind User Password	d: Change Password	
Bind User DN: Bind User Password	1: Change Password	
User Search Config *User Search Base:	d: Change Password uration: dc=gedu,dc=demo,dc=infinitecampustes	st,dc=com
User Search Config *User Search Base:	d: Change Password uration: dc=gedu,dc=demo,dc=infinitecampustes (&(objectClass=person)(cn={0}))	st,dc=com
User Search Config *User Search Config *User Search Base: *User Search Filter: Search entire su	d: Change Password uration: dc=gedu,dc=demo,dc=infinitecampustes (&(objectClass=person)(cn={0})) ubtree of the user search base.	st,dc=com
User Search Config *User Search Config *User Search Base: *User Search Filter: Search entire su Validation:	d: Change Password uration: dc=gedu,dc=demo,dc=infinitecampustes (&(objectClass=person)(cn={0})) ubtree of the user search base.	st,dc=com
User Search Config *User Search Config *User Search Base: *User Search Filter: Search entire su Validation: Test Username:	d: Change Password uration: dc=gedu,dc=demo,dc=infinitecampustes (&(objectClass=person)(cn={0}))) ubtree of the user search base. Test Co	st,dc=com
User Search Config "User Search Config "User Search Base: "User Search Filter: Search entire su Validation: Test Username: Server	d: Change Password uration: dc=gedu,dc=demo,dc=infinitecampustes (&(objectClass=person)(cn={0}))) ubtree of the user search base. Test Co Status Message	st,dc=com
Validation: Test Username: Server SIS-129170B App	d: Change Password uration: dc=gedu,dc=demo,dc=infinitecampustes (&(objectClass=person)(cn={0}))) ubtree of the user search base. Status Message Success	onfiguration Last Updated Last Success 02/18/2020 15:44:39 02/18/2020 15:44:39

- 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.

User Account Type Wizard ☆	User Management $>$ User Account Administration $>$ User Account Type Wizard
User Account Type Wizard	
This batch tool will update a subset of User Accounts using an Ad Hoc selection. Please note that U via the Batch Import tool will create a unique Ad Hoc query automatically by date and time and can modified for use in this tool.	Iser Accounts uploaded be easily utilized and/or
A maximum of 9000 results can be returned from a single search, and the wizard can process at m	ost 9000 results.
Note: Product Security Roles are exempt from a SSO configuration. If a user has a Product Securi need to create an additional non-Product Security Role user account for SSO use.	y Role, that user will
Usemame	
Last Name	
First Name	
Adhoc Filter	
Student Number Filter	
User Homepage	
User Account Type	
Search Users & Add to the Search Results	
Search Results (Person:0 Users:0) Selected Users (Person:0 Users:0)	
A	
<	
•	*
Reset Remove Select All> 	
Set Account Authentication Type To LDAP: Test LDAP	
Convert User Accounts Authentication Type	

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

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.

Search	Results (Person	1.0 Users.0)		Selected Use	is (Person.o c	▲
			> <			
	Damara Cal	-		- Marca All	Damage D	Ŧ

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.

Filter Designer &		Reporting > Ad Hoc Reporting > F
Ad Hoc Filter Designer		
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.
Saved Filter	Create New Filter Type @ Query Wizard O Salection Editor Pass-through SQL Query Create	Data Type Student Census/Staff Course/Section

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

Select fields	o use for creating a filter for which logic and	l output formatting may be applied. C	lick a field within the All Fields wi	ndow, or use the Add
arrow < Th	on to add the field to the Selected Fields win e output will sequence the fields in the order	r selected; however, the sequence ca	in be changed on the Output Forr	matting screen. At least on
field must be	selected to continue.			
Field Select	on > Filter Parameters > Output Formatting	> Grouping and Aggregation		
*Query Name:	LDAP Test			1
Short Description				
Short Bosonprior				
Long Description			+	
				-/
Select categorie	s & fields			- F
Filter By	Search Clear			
All Fields		<u>s</u>	elected Fields	
÷ K≥ Ca	npus Usage	▲ U	sage.ldapAccount	A
K	User Account/Summary	s	tudent.lastName	
	userID	u	sage.username	
	personID			
	districtID			
	username			
	allModules			
	failCount			
	fore-ChangeBergword			
	disable			
	expiresDate			
	homepage			
	name			
	serverName			
	remoteIP			
	-remoteName			
	remoteBrowser			
	-timestamp			
	-appServer			
	ssoAccount			
	-IdapAccount			
	localPasswordSet	-		+
Add Eunction	1		Edit Euroction	
	J	L	Carranon	
Save 💿	ser Account			
To:	Folder: /			
0	ser Groups			
0	ser oroups			
Save	ave & Test			•
				< Back Nevt S
				< DOCK NOAL >

- 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).

Ad Hoc Query Wizard - Filter Parameters	
Parameters are used to filter data based on specific logic. Use the operators to apply logic to designated fi being output. Click the Add Field button to apply additional logic criteria to a single field already assigned a (optional) to set conditions for the operators using AND, OR, and NOT conditions. If a Logical Expression i operators. If using Logical Expression, include all fields that have Operators or the Operator for the missing	elds. Logic may be applied even if a field is not in Operator. Additionaly, use a Logical Expression s not used, the condition AND will be applied to all g field will not apply.
Field Selection > Filter Parameters > Output Formatting > Grouping and Aggregation	
*Query Name: LDAP Test	
Short Description:	
Long Department	
Long Description.	±
Filter the data	
ID *Field Operator Value	
ID Field Operation V 1 usage IdapAccount V	1
	J
X ³ student.lastName V V	
X 4 usage.username V V	
Add	
Logical Expression (Ontional)	
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 Ouser Account	
Folder, / V	
O User Groups	
Save & Test	
	< Back Next >
	S DOON NOAL >

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

Filter Designer 🏠		Reporting > /	Ad Hoc Reporting > Filter Designer
Ad Hoc Filter Designer			
This wizard will walk you through the creation of a new filter.	Filters can be created using the Query wizard, sele	ction editor or a pass-through SQL Query. Ad Hoc Filters can be used as a search, or as input to a r	eport.
Saved Filter Saved Filter Student "sped 2351 Student to 161209 Student Th Graders student Early Learning Test person file student Kais Test person Millary Connection Status student try test student try test student test FAM Ouery student Test FFAM Ouery student Test STOUT_332 TEACHER	Create New Filter Type Cuery Wizard Selection Editor Pass-through SQL Query Create	Data Type Student Course/Section	
Search Edit Test Copy Delete Export Create a new Folder			
		Current engine version: 2.0	

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

Ad Hoc Query	Wizard - Field Selection			
Select fields Function opt arrow < Th field must be	to use for creating a filter for which logic and output formattin tion to add the field to the Selected Fields window. To remove he output will sequence the fields in the order selected; however e selected to continue.	g may be applie a field from the ver, the sequenc	d. Click a field within the All Field Selected Fields window, select th e can be changed on the Output	is window, or use the Add te field(s) and click the back Formatting screen. At least one
Field Select	tion > Filter Parameters > Output Formatting > Grouping and	Aggregation		
*Query Name: Short Description Long Description	Staff LDAP Accounts			
Salaat aatagarii	an 9 fialda			_/
Filter By All Fields	Search Clear	[Selected Fields	¥
Add Function	anpus osage	۲ ۲	Individual. firstName individual. lastName usage.username	~
Save To:	User Account Folder: / ▼ User Groups			
Save Save & Tes	st			Ļ
				< 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:
 - 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).

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 app being output. Click the Add Field button to apply additional logic criteria to a single field already assigned an Operator. Additional (optional) to set conditions for the operators using AND, OR, and NOT conditions. If a Logical Expression is not used, the condition operators. If using Logical Expression, include all fields that have Operators or the Operator for the missing field will not apply. Field Selection > Filter Parameters > Output Formatting > Grouping and Aggregation	blied even if a field is not y, use a Logical Expression on AND will be applied to all
*Query Name: Staff LDAP Accounts	
Short Description:	
Long Description:	
Filter the data	
ID *Field Operator Value	
X 1 usage.ldapAccount T = T 1	
X 2 individual.firstName V V	
X 3 individual.lastName V V	
X 4 usage.username 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	
Save & Test	
	< Back Next >

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 Account	ts Total Records: 161267		
All Records			
usage.ldapAccount	individual.firstName	individual.lastName	usage.username
1	Edwina		00170588
1	Lavonndia		00076443
1	Arlene		00223292
1	Mayra	1 The second sec	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 set up an LDAP SASL connection.

- 1. Log into your Google Admin console.
- 2. 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 Manage 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	Admin roles 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			

3. Select LDAP.

≡ Google Admin	Q Search for users, groups	, and settings (e.g. drive sharing setting	gs)		8 ?	# D
Apps						:
APPS SETTINGS						
Marketplace 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					

4. Click Add Client.

ipυ	5						
_							
	≡ Google Admin	Q Search for users or settings			8	?	
	Apps > LDAP						
						Audit log	
	LDAP 1 client					ADD CLIE	NT
	Q Search LDAP clients						
	Clients 1		Access Permissions	Earliest Certificate Expires in	Service Status		
	MGtest		Read user information Verify user credentials	2+ years	ON		
							_
	Rows per page: 50 👻				I< Page 1 of 1	< >	

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.

× Add LDAP client			
1 Client details — 2 Access permis	sions		
	Client details		
	LDAP client name *		
	Description * Required field		
		CANCEL	CONTINUE

- 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.

× Add LDAP client	
Client details — (2) Access permissions	
	Access permissions
	Verify user credentials Byocity client's access level for verifying user credentials. Changes can take up to 24 hours to take effect. Entire domain (gedu.demo.infinitecampustest.com) Selected organizational units No access Red user information Selectify client's access level for reading user information. Some clients need additional information before authenticating users. Entire domain (gedu.demo.infinitecampustest.com) Selectify client's access level for reading user information. Some clients need additional information before authenticating users. Selected organizational units Selected organizational units Selected organizational units Selected organizational units No access No access
	Read group information Client can read group information. Some clients need additional information before authenticating users.

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.

 mgtest2 added Next, connect your client to the LDAP service 1. Download 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_09.18_56400 Egries. August 16, 2022 Download certificate 2. Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials. Learn more
Next, connect your client to the LDAP service Download 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 Explese August 18_2022 ① Download certificate ②. Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials. Learn more
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 Sea	rch for users or settings						8 (0
Apps > LDAP > Settin	gs for mgtest2								
	mgtest2		Service status					OFF V	
	Status		Access permis	sions	Read user information	Read group	information	~	
	FDIT DETAILS		Entire domain	ara	Entire domain	No access	, mornalism		
	MORE		Authentication				/	~	
			Certificates 1 certificate is asso Access credentials 0 access credential	ociated with this LDAP client	client				
=	≡ Google Adm	nin Q Search for users o	or settings						8 0 8
	Apps > LDAP > Setting	gs for mgtest2 > Service Status				/			
		mgtest2		Showing settings for us	sers in all organizational units				
				Service Status					^
				Service status	ON for eve OFF for eve	eryone			
					(i) Changes ma	ay take up to 24 hours to propagate	to all users.		
								1 unsaved change CANCE	SAVE

Infinite Campus

9. 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

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.