LDAPS Certificates

Last Modified on 10/21/2024 8:20 am CDT

Upload a Certificate (LDAPS) | Upload a Certificate (SASL) | Replace a Certificate | Certificate Expiration Warnings

Tool Search: LDAP Certificate Management

The LDAP Certificate Management tool provides district administrators the ability to store and replace their public key certificates used by LDAP for authentication. By storing certificates in this tool, districts can mitigate the issue of having users locked out of Campus when certificates expire.

Existing certificates that were added by Campus are not impacted by this tool however, once your existing certificate expires, you will need to use this tool to upload a new certificate.

Uploading certificates into Campus is only required if your LDAP configuration is set to **Use SSL**.

LDAP Certificate Manag	ement 🏠				User Management > Settings > LDAP Certificate Management
🕒 Upload 🦻 New					
Certificates Subject Name	type	Effective Date	Expiration Date	Expires in	
Certificate Upload					- 1
Certificate File (.cer, .crt)					
Choose File No file chosen					

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

Upload a Certificate (LDAPS)

To upload an LDAP certificate:



- 1. Click the **New** icon. The Certificate Upload editor will appear.
- 2. Select **LDAPS**. If you need to upload SASL certificates, see the Upload a Certificate (SASL) section.
- Click Choose File. You will be prompted to locate the certificate on your local hard drive or network.

You must upload a Cert File (.CER) in Base64 encoded x.509 or DER encoded library x.509 format.

4. Select the certificate and click **Open**.

Upload 💡 New						
Certificates Subject Name	type	Effective Date	Expiration Date	Expires in		
Certificate Upload © LDAPS O SASL Certificate File (.cer, .crt) Browse No file selected.	© Open					×
	$\leftarrow \rightarrow \wedge \uparrow \square \ll$	Desk > LDAPS	Certificate	v Č Sea	arch LDAPS Certifica	tes 1925 🔎
	Organize Vew fo ConeDrive This PC Desktop Documents Downloads Music Pictures Videos	lder	IdapTestin	ng		
	File	e name:		م ا	ustom Files Open	✓ Cancel

Image 3: Adding the LDAP Certificate

Once the certificate has been selected, it will appear in the Certificate Upload editor next to the Choose file button (Image 4). Click the **Upload** button to upload the certificate to Campus.

🕒 Upload 💡 New				
Certificates Subject Name	type	Effective Date	Expiration Date	Expires in
Certificate Upload LDAPS O SASL Certificate File (.cer, .crt) Browse IdapTesting.cer				

Image 4: Uploading the Certificate

Once the certificate is uploaded into Campus, the certificate's Effective Date, Expiration Date, and number of days until expiration will appear in the Certificates window (Image 5).

8 New			
Certificates			
Subject Name	Effective Date	Expiration Date	Expires in
infinitecampus.com,O	Tue Jul 17 19:00:00 CDT 2018	Wed Jul 22 07:00:00 CDT 2020	412 Days
		1	

Image 5: Certificate Information

The final step in this process is to navigate to the LDAP Authentication tool, ensure LDAP is configured properly, and test your LDAP connection by entering a **Test Username** and selecting **Test Configuration**.

If your LDAP configuration and certificate(s) is valid, a message will appear stating 'Test Configuration Success!'. LDAP is now successfully configured in Campus.

Vev Save Delete DDAP Server Configuration Connection Statis Name Error Test LDAP Disabled mglest	
New Save Onnection Status Name Connection Status Name Error Test LDAP Disabled mgtest Configuration Detail *LDAP Name: mgtest *LDAP Name: mgtest *LDAP Server Pool: *Server 1 Host: *Port *Server 2 Host: Port Server 3 Host: Port Outse SSL (Strongly Recommended.) Administrator: Single Sale *Bind User DN: Change Password: Change Password:	
LDAP Server Configuration Connection Status Bisabled mgtest	
Configuration Detail Configuration Detail Configuration Detail LDAP Name: mgtest Enable this LDAP Configuration. DAP Server Pool: Server 1 Host: Server 2 Host: Server 2 Host: Server 4 Host: Port: Server 4 Host: Server 4 Host: Port: Server 4 Host: Port: Server 4 Host: Change Password Change Password	
Disabled mgtest Donfiguration Detail LDAP Name: mgtest DAP Server Pool: Server 1 Host: Port: 636 Port: Port: Port: Port: Output Port:	
Image: mgtest DAP Name: mgtest Enable this LDAP Configuration. DAP Server Pool: Server 1 Host: Port: Gase erver 2 Host: Port:	
onfiguration Detail DAP Name: mglest Enable this LDAP Configuration. DAP Server Pool: Server 1 Host erver 2 Host: Port: Babel Port: Port: </td <td></td>	
onfiguration Detail DAP Name: Instant in the second seco	
onfiguration Detail DAP Name: mgtest Enable this LDAP Configuration. DAP Server Pool: Server 1 Host "Port: erver 2 Host: Port: erver 3 Host: Port: erver 4 Host: Port: Use SSL (Strongly Recommended.) dministrator: © Simple SASL ind User DN: Test2012LDAP1hadministrator ind User Password: Change Password	
DAP Name: mgtest DaP Name: mgtest Enable this LDAP Configuration.	
DAP Name: mgtest Enable this LDAP Configuration. DAP Server Pool: erver 1 Host erver 2 Host port: first port: erver 3 Host: port:	
DAP Name: mgtest	
DAP Name: mgtest Enable this LDAP Configuration. DAP Server Pool: Server 1 Host. *Port: 636 erver 2 Host. Port. erver 3 Host. Port. erver 4 Host. Port. Use SSL (Strongly Recommended.) dministrator: Simple O SASL Bind User PDN: Test20 12LDAP Nadministrator Gind User Password:	
Labele this LDAP Configuration. DAP Server Pool: Server 1 Host "Port: erver 2 Host: Port: Prever 3 Host: Port: erver 4 Host: Port: Use SSL (Strongly Recommended.) dministrator: Simple O SASL Simple Password: Change Password:	
DAP Server Pool: Server 1 Host: Port: Server 2 Host: Port: Port: Port: Port: Port: Port: Use SSL (Strongly Recommended.) dministrator: Simple SASL Simple SASL Simple SASL Change Password Change Password	
DAP Server Pool: *Port: 636 Server 1 Host: Port: 636 erver 3 Host: Port: Port: erver 4 Host: Port: Port: Use SSL (Strongly Recommended.) dministrator: @ Simple O SASL Simd User DN: Test2012LDAP Nadministrator Bind User Password: Change Password Change Password	
erver 2 Host: Port: B30 erver 2 Host: Port: Por	
erver 3 Host: Port: Port	
erver 3 Host: Port: Port	
erver 4 Host: Port: Use SSL (Strongly Recommended.) dministrator: © Simple O SASL Bind User DN: Test2012LDAP Nadministrator Bind User Password:	
Use SSL (Strongly Recommended.) dministrator: Image: Simple O SASL Sind User DN: Test2012LDAP1\administrator Sind User Password: Change Password	
dministrator: Simple O SASL Simd User DN: Change Password Change Password	
Iministrator Single O SASL Sind User DN: Test2012LDAP1\administrator Sind User Password: Change Password	
Simple USASL Bind User DN: Test2012LDAP1\administrator Bind User Password: Change Password	
Sind User Data Instantialistication Sind User Password Change Password	
Sino User Password Change Password	
ser Search Configuration	
Ser Search Base DC=com	
Iser Search Filter (%AbhertClass=user/(sAMArcountName=(0)))	
A Search entire subtree of the user search base.	
alidation	

Image 6: Testing Your LDAP Configuration and Certificate

Upload a Certificate (SASL)

In order to complete this process, you must first have your SASL client configured for Campus and Certificate and Key Files generated by the client. For a step-by-step process on how to configure Google Suite to work with Campus LDAP, see the LDAP Authentication article.

- 1. Click the **New** icon. The Certificate Upload editor will appear.
- 2. Select **SASL**.
- 3. Under Certificate File click **Browse**. You will be prompted to locate the certificate on your locale hard drive or network. This file is provided to you by your SASL client.
- 4. Under Key File click **Browse**. Locate the key file (likely to be in the same location as the Cert file in Step 3). This file is provided to you by your SASL client.



Infinite Campus

5. The Certificate File and Key File will now appear as selected in the Certificate Upload editor. Click **Upload**.

Upload 🥐 New				
Subject Name	type	Effective Date	Expiration Date	Expires in
· · ·				
Certificate IInload				
			1	
Certificate File (.cer, .crt)	Key Fil	e (.key)	+	
Browse Google_2022_08_18_56400.crt	Brow	wse Google_20	22_08_18_56400	.key

6. The files are now uploaded into Campus and appear in the Certificates window.

P New 😣	Delete				
Certificates					
Subject Name		type	Effective Date	Expiration Date	Expires in
ST=California,C=US,	OU=GSuite,CN=LDAP Client	SASL	Mon Aug 19 10:40:00 CDT 2019	Thu Aug 18 10:40:00 CDT 2022	1078 Days
Certificate					
Certificate Version	3	_		_	_
Certificate Version Type	3 SASL	_	_	_	_
Certificate Version Type Signature Algorithm	3 SASL withRSA	-	-	-	-
Certificate Version Type Signature Algorithm Subject	3 SASL withRSA ST=California,C=US,OU=GSuite	e,CN=LDAP Client	,L=Mountain View	,0=Google Inc.	-
Certificate Version Type Signature Algorithm Subject Valid Through	3 SASL withRSA ST=California,C=US,OU=GSuite 08/19/2019 - 08/18/2022	e, CN=LDAP Client	,L=Mountain View	,0=Google Inc.	_

Infinite Campus

7. The final step in this process is to navigate to the LDAP Authentication tool, ensure LDAP is configured properly, and test your LDAP connection by entering a **Test Username** and selecting **Test Configuration**.

If your LDAP configuration and certificate(s) is valid, a message will appear stating 'Test Configuration Success!'. LDAP is now successfully configured in Campus.

LDAP Config	uration 🏠		User Management > Settings > LDAP Configuration
New Sa	ve S Delete		
Connection Status N	ation ame	Server URL	
Disabled m	gtest		
Configuration Detail			
*LDAP Name:	mgtest		
Enable this LDAP	Configuration.		
LDAP Server Pool:			
*Server 1 Host:		*Port: 636	
Server 2 Host: Server 3 Host:		Port	
Server 4 Host:		Port:	
Use SSL (Strongly	Recommended.)		
Administrator:			
Simple O SASL Second Liser DN:	Test2012LDAP1\administrator		
*Bind User Password:	Change Password		
User Search Configurat	ion		
*User Search Base:	DC=com		
*User Search Filter:	(&(objectClass=user)(sAMAccountName={0}))		
Search entire subtr	ee of the user search base.		
Validation:			
Test Username: Test Configuration Su	testuser Test Configuration		

Replace a Certificate

If a certificate is close to expiring or simply needs to be replaced, you should do so by selecting the certificate, clicking the **Delete** button, and uploading a new certificate using the steps listed in the



Upload a Certificate section above.

You can upload a new certificate without removing the expiring or expired certificate and Campus will know to use the new valid certificate. However, until you remove the expired certificate from this tool, you will continue to receive in-app and email notifications about the expired certificate.

To prevent a potential lockout of users, it is important to replace certificates prior to their expiration. You will receive warning emails when a certificate is getting close to expiring.

	Effective Date	Expiration Date	Expires in
infinitecampus.com,O	Tue Jul 17 19:00:00 CDT 2018	Wed Jul 22 07:00:00 CDT 2020	412 Days
	_	_	
1256withRSA		-	
A256withRSA ,L=Blaine,ST=Minnesota,C=US	OU	=Managed Service	es,O=Infinite Campus∖
	infinitecampus.com,O	Fffective Date infinitecampus.com,O 19:00:00 CDT 2018	infinitecampus.com,O Tue Jul 17 19:00:00 CDT 2018 Ved Jul 22 07:00:00 CDT 2020

Image 7: Replace an Expired Certificate

Certificate Expiration Warnings

Email and in-app notification functionality is built into this tool. Users who have access to this tool will receive an email and in-app notification every 3 days when a certificate will expire in less than 30 days.

When a certificate will expire in 10 or less days, this notification will increase to every day until the certificate is replaced. Users will continue to receive daily notifications until the expired certificate is replaced or removed.





certificate from this tool, you will continue to receive in-app and email notifications about the expired certificate.