

SSO Service Provider Configuration

Last Modified on 08/19/2025 9:59 am CDT

Tool Search: SSO Service Provider Configuration

The SAML SSO Service Provider Configuration tool allows you to configure and enable SSO authentication(s) for Campus accounts in your district.

- Additional Things to Consider
- Enable and Configure SAML SSO Functionality
- Export the Service Provider Certificate
- Delete the Service Provider Certificate
- Certificate Expiration Warnings
- <u>Replacing Expired Certificates</u>
- Logging into Campus and Campus Portal Using SAML SSO
- <u>Understanding Service Provider Configuration Fields</u>
- Deleting an Existing SSO Configuration
- <u>Configuring a Unique Entra Active Directory</u>
- Configuring a Google IDP
- <u>Sandbox/Staging/Non-Production Environments</u>
- <u>Matching Campus Fields to IDP Fields</u>
- Troubleshooting SSO Login Issues

Campus accounts can be converted from using the Campus login authentication to SSO authentication by using the <u>User Account Type Wizard</u>.

SAML - SSO Service Provider Configuration $rac{d}{d}$	User Management > Settings > SAML - SSO Service Provider Configuration
Save 🗴 Delete 🕂 New	
Service Provider Configurations	
Single Sign-On (SSO) - New	
Service Provider Configuration	
Enable SAML Single Sign On	
*Note: The authentication type for user accounts will need to be updated to use this authentication	tion method.
*Name for Login Button	
Single Sign-On (SSO) - New	
Identity Provider Details	
Select an option to retrieve identity Provider (IDP) server data	
Metadata File: GoogleIDPMetadata (10).xml Choose File No file chosen	
Show Identity Provider Values V	
- Identity Provider (IDP) Certificate Details	
Version: 3	0
Signature Algorithm: SHA2	
Issuer: ST=California, C=US, OU=Google For Work, CN=Google, L=Mountain View, O=Google Inc.	ι,
Valid Through: Mon Oct 17 13:49:44 CDT 2022 - Sat Oct 16 13:49:44 CDT 2027	
Thumbprint: 212c39d4e98544211d4f4fdc4185b	3
Version: 3	-



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

Additional Things to Consider

Please consider the following when enabling and using SAML SSO authentication within Campus:

Once SSO is enabled, the authentication type for user accounts will need to be updated to use this authentication method. This can be done on a user-by-user basis in the <u>User Account</u> tool or updated en masse via the <u>User Account Type Wizard</u>.

- When considering the configuration of user accounts, please note that <u>Cafeteria Serve</u> and <u>Service Layout</u> functionality only authenticates with a non-SSO account (LDAP account or Local Campus Authentication); therefore, please reserve a separate LDAP or Local Campus Authentication account for access to <u>Cafeteria Serve</u> and <u>Service Layout</u>
- In an effort to be as inclusive as possible to the SAML Identity Providers (IDPs) the Infinite Campus user base engages, we have tested the Campus SSO Service Provider against Microsoft Active Directory Federated Services (ADFS), Microsoft Entra Active Directory, Google Apps IDP, Shibboleth IDP, and OmnID. <u>Since the Campus SSO Service Provider is part of</u> <u>the SAML specification, any IDP that is SAML compliant should connect with</u> <u>minimal intervention.</u>
- Users may be asked to provide Campus Support with a test user to assist in troubleshooting any SSO issues they may encounter.

Admins and Authorized Contacts are expected to have a contingency plan for site access in the event your Identity Provider has an issue that makes it impossible to sign in through SSO. Admins should consider setting up a second user account under their own person record that uses an authentication type other than SSO (such as LDAP or Local Campus Authentication). We recommend securing this account with <u>Time-Based Multi-Factor Authentication</u>.

Note that some governing agencies, such as the North Carolina Department of Public Instruction, do not allow the use of Local Campus Authentication. Ensure you comply with your governing agency's security practices.

Enable and Configure SAML SSO



Functionality

The following steps will guide you in enabling and configuring SAML SSO functionality within Campus:

- Step 1. Enable SAML SSO and Sync IDP Server Data
- Step 2. Generate or Upload the Service Provider Certificate

Step 1. Enable SAML SSO and Sync IDP Server Data

The first step in configuring SAML SSO is to enable SAML SSO functionality, define the Login button and sync IDP server metadata.

Please see the table below for detailed information about each of these fields.

- 1. Click the **New** button. The Service Provider Configuration editor will appear below.
- 2. Mark the **Enable SAML Single Sign On** checkbox. This will enable this SAML Single Sign-On configuration within Campus.
- 3. Enter a **Name for the Login Button**. This will be the text that appears on the button for users to select when signing into Campus via SSO or if multiple IDPs are configured, enabled, and made visible, what appears in the dropdown list for selecting which SSO Login to use on the Campus login screen.





NOTE: Users are highly encouraged to give the button a name recognizable to staff and students/parents, ESPECIALLY if configuring more than one IDP. For example, one configuration is labeled as Staff Login, and another configuration is labeled as Student and Parent Login

4. Retrieve the IDP server metadata by either entering the **Metadata URL** or by uploading the **Metadata XML File**.

Campus SSO logic will first use an IDPs HTTP-POST binding if one is present and then only look for an HTTP-Redirect binding if the HTTP-POST binding is not found.

- 5. If the **Metadata URL** was entered, hit the **Sync** button. This will populate Identity Provider fields below.
- If connecting Campus to Microsoft Entra (formerly Azure), leave the **Optional Attribute Name** field as **nameID**. This is the attribute Campus will look for as a response from Entra in order to match the username in Campus to Entra.

For more information about a unique Entra configuration, please see the <u>Configuring a</u> <u>Unique Entra Active Directory</u> section below.

- In the Campus SSO Preferences area, set the Request Timeout. This field indicates the number of minutes that can pass before a request between Infinite Campus and the IDP produces a timeout error.
- 8. Determine the Domain Suffix Handling:
 - No Change This option indicates the domain name does not contain a suffix.
 - **Remove a Domain Suffix** This option allows you to remove the domain name from an IDP attribute value (such as an email address) to compare only the prefix of the value to the Campus username.
 - **Append a Domain Suffix** This option allows you to append a suffix to the domain name.
- 9. Check the **Logoff IDP when logging off Campus if logoff url exists** checkbox if you want the Logoff button in Campus to also log users out of the IDP.
 - This option only works if the **Identity Provider Single Logoff URL** field is populated and correct. This field is defaulted as marked.

This checkbox will automatically be unmarked and grayed out if the **Identity Provider Single Logoff URL** references Google.



- 10. Designate which Campus Login screen(s) the SSO login button will not appear on:
 - **Turn off this SSO configuration for the Main Login page** Marking this checkbox means this SSO configuration will not appear as a button or option on the login screen for accessing the Infinite Campus application.
 - **Turn off this SSO configuration for the Parent Portal** Marking this checkbox means this SSO configuration will not appear as a button or option on the login screen for the Parent Portal.
 - **Turn off this SSO configuration for the Student Portal** Marking this checkbox means this SSO configuration will not appear as a button or option on the login screen for the Student Portal.

NOTE: If 2 or more IDPs are configured and enabled, to lessen confusion, users are highly encouraged to use these options to hide configurations from users who would not use them (i.e., hide the Staff-specific login from the Parent and Student Portals).

11. Move on to Step 2.

Step 2. Generate or Upload the Service Provider Certificate

You must now generate or upload the Service Provider Certificate. To do this, click the **Manage SP Certificate** button.

-Identity Provider (IDP) Signature
Version:	3 🕜
Signature Algorithm:	RSA
Issuer:	CN=accounts.accesscontrol.windows.net
Valid Through:	Mon Oct 27 19:00:00 CDT 2014 - Wed Oct 26 19:00:00 CDT 2016
Thumbprint:	3123623c8e73bd7baa64c6459042f87fcbc843720
Version:	3
Signature Algorithm:	hRSA
Issuer:	CN=accounts.accesscontrol.windows.net
Valid Through:	Sat Apr 16 19:00:00 CDT 2016 - Mon Apr 16 19:00:00 CDT 2018
Thumbprint:	73dcb6f8cc2ed6862529194371204239c981cc7
Version:	3
Signature Algorithm:	withRSA
Issuer:	CN=accounts.accesscontrol.windows.net
Valid Through:	Sun Sep 04 19:00:00 CDT 2016 - Wed Sep 05 19:00:00 CDT 2018
Thumbprint:	2cc549eb58c6aa60cb1d41b1ea1fd00dda8
- Service Provider (SP)	Signature Manage SP Certificate
Version	
Signature Algorithm:	nla
Signature Algorithm	
Issuer:	undefined
Valid Through:	undefined - undefined
Thumbprint:	undefined

Service Provider Certificates can either be automatically generated by Campus using the Generate

the SP Certificate feature or manually uploaded via the Upload a Java Keystore (.jks) feature.

To have Campus generate the Service Provider certificate:

Service Provider Certifica	te Managemen	t	×
Certificate Options: Generate the SP Certificate Upload a Java Keystore (.jks) Export the SP Certificate Delete the SP Certificate	DN Locality Name State Name Alias Alias Password *Expiration Date	CN=inf Scarsdale NY ny_66 Fri, 7 Apr 2017]
		Genera	ite

- 1. Click the **Generate the SP Certificate** radio button.
- 2. Enter an **Expiration Date**. This is the date in which the certificate will expire and will no longer be valid. This field defaults to one year from the current date.
- 3. Click the **Generate** button. Fields within the Service Provider SP (Signature) section of the SSO Service Provider Configuration editor will automatically populate with data generated from this certificate.

If a Service Provider certificate already exists within Campus, generating a new Service Provider certificate will automatically overwrite any existing certificate and associated data.

4. Click Save at the top of the editor. If the IDP was configured correctly, a green circle in the Enabled column will appear next to the IDP name in the Service Provider Configurations window. Users can now log into Infinite Campus via an SSO button on the login screen (see the Logging into Campus and Campus Portal Using SAML SSO section).

SAML - SSO Service Provider Configuration ☆	User Man
Save Save Delete	
Service Provider Configurations Enabled Name for Login Button Image: Single Sign-On (SSO)	
1	
Service Provider Configuration	
C Enable SAML Single Sign On	
*Name for Login Button	
Single Sign-On (SSO)	
Service Provider Metadata	

To upload the Service Provider certificate:

Campus

Service Provider Certifica	te Management	:	*
Certificate Options:	Choose File No file cho	osen	
Generate the SP Certificate	*Alias	Enter alias name	
Upload a Java Keystore (.jks)	*Alias Password	Enter password for your alias	
Export the SP Certificate	*Keystore Password	d Enter the password for your keystore (.jks)	
			Upload
			Cancel

- 1. Click the Upload a Java Keystore (.jks) radio button.
- 2. Click the **Choose File** button and locate the .jks file from your local hard drive or network.
- Once the file is selected, click the Upload button. Fields within the Service Provider SP (Signature) section of the SSO Service Provider Configuration editor will automatically populate with data uploaded from this certificate.

More than one certificate can be uploaded. For example, Microsoft Entra requires two certificates.

If a Service Provider certificate already exists within Campus, uploading a new Service Provider certificate will automatically overwrite any existing certificate and associated data.



4. Click Save at the top of the editor. If the IDP was configured correctly, a green circle in the Enabled column will appear next to the IDP name in the Service Provider Configurations window. Users can now log into Infinite Campus via an SSO button on the login screen (see the Logging into Campus and Campus Portal Using SAML SSO section).

 Save Delete New Service Provider Configurations Enabled Name for Login Button Google Test 2 Google - Parent/Student Login Azure - Staff Login TestLogon2-NotFunctional 	SAML - User Manage	SAML - SSO Service Provider Configuration ☆ User Management > Settings > SAML - SSO Service Provider Configuration		
Tani and Mail under a	Save Settings SAML - SSO Service Provider Configuration Save Delete New Service Provider Configurations Enabled Name for Login Button Google Test 2 Google - Parent/Student Login Azure - Staff Login TestLogon2-NotFunctional			

Export the Service Provider Certificate

To export the Service Provider certificate stored within Campus, select the **Export the SP Certificate** radio button and click the **Export** button. A .cer file of the certificate will appear, which you can save locally to your hard drive or network.

- Identity Provider (IDP) Signature			
Version: 3		0	
Signature Algorithm: SH/			
Issuer: CN=accounts.acces			
Valid Through: Mon Oct 27 19:00:00 CDT 2014 - Wed	Oct 26 19:00:00 CDT 20	16	
Thumbprint: 2b0182d)D42f8	7fcbc843720	
Version: 3			
Signature Algorithm: SHA			
Issuer: CN=accounts.access			
Valid Through: Sat Apr 16 19:00:00 CDT 2016 - Mon	Apr 16 19:00:00 CDT 201	3	
Thumbprint: 824f1fbce	04	239c981cc7	
Signature Algorithm: SHA Valid Th Certificate Options:	te Manageme	nt	×
Generate the SP Certificate	Expiration Date	Wed 05 Apr 2017 23:59:59 CMT	
Upload a Java Keys ore (.jks)		Wed, 05 Apr 2017 25.59.59 GWT	
Delete the SP Certificate			
	1		Export
			Cancel

Delete the Service Provider Certificate

To delete the Service Provider certificate stored within Campus, select the **Delete the SP Certificate** radio button and click the **Delete** button.



Deleting the certificate will wipe all service provider certificate data from Campus and will remove the ability for Campus users to properly use Single Sign On functionality within Campus.

Once you have deleted the certificate, you **MUST** generate or upload a new certificate and resync with your IDP.

- Identity Provider (IDP) Signature			
Version: 3		0	
Signature Algorithm: SH/			
Issuer: CN=accounts.acces			
Valid Through: Mon Oct 27 19:00:00 CDT 2014 - Wed C	oct 26 19:00:00 CDT 2016		
Thumbprint: 2b0182d	9042f87fe	obo843720	
Version: 3			
Signature Algorithm: SHA			
Issuer: CN=accounts.access			
Valid Through: Sat Apr 16 19:00:00 CDT 2016 - Mon Ap	r 16 19:00:00 CDT 2018		
Thumbprint: 824f1fbce	0423	9c981cc7	
- Service Provider (SP) Signature Manage SP Certificate			
		0	
Version: 3			
Signature Algorithm: SHA			
Service Provider Certifica	te Manageme	nt	×
Valid Th	-		
Thum			
Certificate Options			
oci induce o pitolio.			
Concerts the SD C difference	Alias to Delete	ny 662001	
Generate the SP Certificate	Expiration Date	Wod. 05 Apr 2017 23:59:59 CMT	
Upload a Java Keystore (.jks)	Expiration Date	Wed, 03 Apr 2017 23:33:33 OWT	
Export the SP Certificate			
Delete the SP Certificate			
			Delete
			Cancel
			Cancel

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.

You must have proper <u>Messenger Email Settings</u> established in order to receive email notifications.

You can upload a new certificate without removing the expiring or expired certificate and Infinite 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.

Replacing Expired Certificates

If you have received notice from Infinite Campus that your IDP certificate is set to expire or has expired, there are 3 simple ways to resolve this (depending on how you want to resolve this).

- <u>Method 1 Upload a New Java Keystore (.jks)</u>
- Method 2 Resync Metadata via URL
- Method 3 Resync Metadata via XML File

Method 1 - Upload a New Java Keystore (.jks)

- 1. Select the SSO configuration needing an updated certificate.
- 2. Click the **Manage SP Certificate** button. The Service Provider Certificate Management editor will appear.
- 3. If you have an updated cert key from your IDP server, select the **Upload a Java Keystore** (.jks) radio button.
- 4. Click Choose File, locate the Java Keystore file, and click Ok.
- 5. Click the **Upload** button. The **Alias**, **Alias Password**, and **Keystore Password** will populate automatically from the uploaded file.
- 6. Click **Save** at the top of the SSO Service Provider Configuration tool. Your new certificate has been uploaded, and you should no longer receive expiration warnings until this new certificate approaches its expiration date.



Method 2 - Resync Metadata via URL



- 1. Select the SSO configuration needing an updated certificate.
- 2. Select the Metadata URL radio button.
- 3. If the Metadata URL for your IDP server has changed, enter the URL in this field and click Sync.
 If the Metadata URL for your IDP server has not changed, click Sync.
- 4. Once Sync is selected, the updated metadata should insert an updated certificate. Click **Save**. Your certificate has been updated.

Enabled Name for Lo	ginations oin Button	
Single Sign-C	On (SSO) - New	
Service Provider Config	guration	
Enable SAML Single	e Sian On	
*Note: The authenticati	ion type for user accounts will need to be updated to use this authentic	cation metho
*Name for Login Buttor	n	
Single Sign-On (SSO) -	New	
Identity Provider D	etails	
*Select an option to ret	trieve Identity Provider (1997) server data	- L
Metadata URL	Metadata XML file	
file:GoogleIDPMetadata	a (10).xml	Sync
Show Identity Provider V	/alues 🔻	
		Т
- Identity Provider (ID)	P) Certificate Details	.
		0
Version	Y* 3	
Version Signature Algorithm	1: 3 1:	•
Version Signature Algorithm	1: 3 I: ST=California. C=US. OU=Google For Work. CN=Google. L=Mountain Vie	ew.
Version Signature Algorithm Issuer	1: 3 1: , ST=California, C=US, OU=Google For Work, CN=Google, L=Mountain Vie • O=Google Inc.	ew,
Version Signature Algorithm Issuer Valid Through	1: 3 2: ST=California, C=US, OU=Google For Work, CN=Google, L=Mountain Vie 0=Google Inc. 1: Mon Oct 17 13:49:44 CDT 2022 - Sat Oct 16 13:49:44 CDT 2027	ew,
Version Signature Algorithm Issuer Valid Through Thumbprint	i: 3 ST=California, C=US, OU=Google For Work, CN=Google, L=Mountain Vie O=Google Inc. i: Mon Oct 17 13:49:44 CDT 2022 - Sat Oct 16 13:49:44 CDT 2027 i:	ew,
Version Signature Algorithm Issuer Valid Through Thumbprint	1: 3 ST=California, C=US, OU=Google For Work, CN=Google, L=Mountain Vie O=Google Inc. 1: Mon Oct 17 13:49:44 CDT 2022 - Sat Oct 16 13:49:44 CDT 2027 1:	ew,
Version Signature Algorithm Issuer Valid Through Thumbprint Version	1: 3 I: ST=California, C=US, OU=Google For Work, CN=Google, L=Mountain Vie O=Google Inc. I: Mon Oct 17 13:49:44 CDT 2022 - Sat Oct 16 13:49:44 CDT 2027 I: I: I: 3	ew,
Version Signature Algorithm Issuer Valid Through Thumbprint Version Signature Algorithm	1: 3 ST=California, C=US, OU=Google For Work, CN=Google, L=Mountain Vie O=Google Inc. 1: Mon Oct 17 13:49:44 CDT 2022 - Sat Oct 16 13:49:44 CDT 2027 1: 2: 3 2: 3 2: 5 2: 5	ew,
Version Signature Algorithm Issuer Valid Through Thumbprint Version Signature Algorithm Issuer	S S	ew,
Version Signature Algorithm Issuer Valid Through Thumbprint Version Signature Algorithm Issuer Valid Through	 s ST=California, C=US, OU=Google For Work, CN=Google, L=Mountain Vie O=Google Inc. Mon Oct 17 13:49:44 CDT 2022 - Sat Oct 16 13:49:44 CDT 2027 Mon Oct 17 13:49:44 CDT 2022 - Sat Oct 16 13:49:44 CDT 2027 ST=California, C=US, OU=Google For Work, CN=Google, L=Mountain Vie O=Google Inc. Wed Dec 07 11:54:10 CST 2022 - Mon Dec 06 11:54:10 CST 2027 	ew,
Version Signature Algorithm Issuer Valid Through Thumbprint Version Signature Algorithm Issuer Valid Through Thumbprint	 s ST=California, C=US, OU=Google For Work, CN=Google, L=Mountain Vie O=Google Inc. Mon Oct 17 13:49:44 CDT 2022 - Sat Oct 16 13:49:44 CDT 2027 Mon Oct 17 13:49:44 CDT 2022 - Sat Oct 16 13:49:44 CDT 2027 ST=California, C=US, OU=Google For Work, CN=Google, L=Mountain Vie O=Google Inc. Wed Dec 07 11:54:10 CST 2022 - Mon Dec 06 11:54:10 CST 2027 	ew,

Method 3 - Resync Metadata via XML File

- 1. Select the SSO configuration needing an updated certificate.
- 2. Select the Metadata XML File radio button.
- 3. Click **Choose File**, locate your metadata XML file and click OK. The SSO Service Provider Configuration tool will automatically attempt to sync with the IDP and if successful you should get a popup message stating "IDP Synchronization successful".
- 4. Click Save. Your certificate has been updated.

nfinite C Campus	
Save Delete New Service Provider Configurations Enabled Name for Looin Button Staff Login Service Provider Configuration Enable SAML Single Sign On Name for Login Button	
Staff Login Service Provider Metadata S/SSO ptA7/federationMetadata	
Single Sign-on URL 46be-9b11-4e017385b34a/ Single Sign-out URL	iesite1.infinitecampus.com says IDP Synchronization successful
SS O/intAZ/logout Campus (Service Provider) Entity ID (It mult be a unique value for the IDP) pus: ntAZ Optioned Attribute Name (default in page ID Required for Agure)	ок
	ta.xml

Logging into Campus and Campus Portal Using SAML SSO

The following displays how users will log into Campus using SAML SSO functionality:

Campus	District/State Edition
Users will click the SSO button (named whatever was determined in Step 1 of this document).	S District/State Edition
	Log In Show Help Version: Campus-31.3.147 intIA © 2003-2024 Infinite Campus, inc. www.infinitecampus.com
Campus	Student/Parent Portal



Users will click the SSO button (named whatever was determined in Step 1 of this document).

	Infinite Campus
Campus Student Newton	Announcements
Single Sign-On (SSO)	There are no district announcements.
Or OrStudent Username (Required)	
admin Password (Required)	
Log In	
Help Log in to Campus Parent	
© 2003-2024 Infinite Campus, Language: English <u>Get Di</u>	Inc. Version:Campus-31.3.147 v strict ID

Campus Login Page (two or more Enabled SSO Configurations)

Districts with two or more configured and enabled IDPs will see a button that requires the user to select which SSO Configuration to use when logging in.

This is why it is important to have clear and recognizable Name of Button values for each IDP configuration so users do not have to guess which one they are supposed to use.

	Campus
Student Information System	
Select an SSO Configuration Select an SSO Configuration Azure - Staff Login Google - Parent/Student Login Google Test 2 admin	
Password	

To lessen confusion, you can set each SSO configuration to be hidden for specific login screens.

For example, if your district has a separate SSO configuration for Staff member logins, you can mark the **Turn off this SSO configuration for the Parent Portal** and **Turn off this SSO configuration for the Student Portal** checkboxes so it does not appear for students and parents logging into Infinite Campus.

If hiding this configuration limits the number of options for SSO configurations to 1 for these users, the button will change from a dropdown list to a button labeled their one SSO configuration option.



Understanding Service Provider Configuration Fields

Use the following table to understand each available field.

Field	Description
Enable SAML Single Sign-On	Mark this box to enable SAML SSO functionality for your district. SAML SSO functionality will not function properly until all other fields in this editor are correctly populated and saved.
Name for Login Button	This field indicates the name of the SSO login button on the Campus login page. For example, a value of Staff Login' is entered.

This becomes even more important when two or more IDPs are configured and enabled for a site. Clear login button names ensure users can clearly identify and use the correct SSO login choice.

For example, one IDP is labeled 'Azure - Staff Login' and another is labeled 'Google - Parent/Student Login'. This way, each user knows which one to select.

Field	Description Infinite Campus		
	Student Information System Select an SSO Configuration Select an SSO Configuration Azure - Staff Login Google - Parent/Student Login Google Test 2 admin Password		
	Main Login page, Turn off this SSO configuration for the Parent Portal, and Turn off this SSO configuration for the Student Portal checkboxes described later in this table.		
Service Provider Metadata	This URL is automatically generated by Campus for the SSO Identity Provider (IDP). The link can either be copied and sent electronically to the local IDP administrator or opened and saved in XML format and sent to the IDP administrator.		
Single Sign-On URL	This URL is automatically generated by Campus for use in District customized HTML links or icons. This URL will bypass the standard login page and make calls directly to the SSO Identity Provider (IDP) for user identification and authentication.		
	If the user is logging in for the first time of the day or session, the IDP will require the user's username and password credentials and display its login page. If the user has already logged into the SSO Identity Provider (IDP), identification and authentication of the user will be processed without credentials, and once authenticated, the user will be redirected to the applicable Campus homepage.		
	Assertion Consumer Service (ACS) URL is the equivalent of the Single Sign-On URL		
Single Sign-On Logout URL	This URL is automatically generated by Campus for use with any IDP that requires a URL for redirect to the local application logoff screen upon logout. Microsoft Entra AD is one known IDP that requires the local Campus logout URL in order to properly redirect to the Campus logoff page.		

Infinite Campus



Field	Description				
Campus (Service Provider) Entity ID	This value is automatically generated by Campus for the SSO Identity Provider (IDP). It can be edited by selecting the lock icon. This value is used to identify the Infinite Campus Service Provider to the SSO Identity Provider.				
	Changing this value is NOT recommended for non-Entra users. If the decision is made to change the value, the SSO Identity Provider must resync the Service Provider Metadata URL or reload the Service Provider metadata using the Service Provider Metadata URL .				
	For Entra users, this value MUST equal the Entra Client ID.				
	For Non-Production Sites: The site refresh process will revert this Campus Service Provider Entity ID value to your Production site's Campus Service Provider Entity ID value, followed by _[siteType].				
	To avoid any disruption, ensure the value here matches the value in Production, followed by _[siteType], before providing this value to your Identity Provider.				
Optional Attribute Name	This is the attribute Campus will look for in the IDP response from an IDP in order to match the username within Campus to the value attached to the specified attribute. If this field is left blank, the default attribute Campus will use for comparison is the Name ID.				
	This field is required for use with Microsoft Entra AD (formerly Azure) as the Name ID attribute is reserved by Entra and cannot be used for comparisons. For Entra, leave this field value as nameID.				
	To change this value, click the Lock icon.				
	*Campus (Service Provider) Entity ID (It must be a unique value for the IDP)				
	An incorrect Optional Attribute Name value will break the connection between Campus and the IDP.				



Field	Description				
Select an option to retrieve Identity Provider (IDP) server data	Indicates how this tool will receive and insert IDP server data. • Metadata URL - IDP server data is pulled from an xml file stored on a network and accessed via a URL. Select an option to retrieve Identity Provider (IDP) server data • Metadata XML File - IDP server data is inserted from a locally stored XML file. Select an option to retrieve Identity Provider (IDP) server data • Metadata URL • Metadata XML file - IDP server data is inserted from a locally stored XML file. Select an option to retrieve Identity Provider (IDP) server data • Metadata URL • Metadata XML file - IDP server data • Choose File No file chosen Once a URL or XML file has been entered, click the Sync button to load the XML server into Compare				
Identity Provider Entity ID	The Identity Provider Entity ID as indicated in the IDP server data XML file.				
Identity Provider URL	The Identity Provider URL as indicated in the IDP server data XML file.				
Identity Provider Single Logoff URL	The Identity Provider Single Logoff URL as indicated in the IDP server data XML file. This URL is required if users wish to use the Logoff IDP if Logoff URL Exists feature.				
Campus SSO Preferences					
Request Timeout	Indicates the number of minutes that can pass before a request between Campus and the IDP produces a timeout error.				
No Change	This option indicates the domain name does not contain a suffix.				



Field	Description		
Remove a Domain Suffix	This option allows you to remove the domain name from an IDP attribute value (such as an email address) to compare only the prefix of the value to the Campus username.This option eliminates the need to store fully qualified domain addresses in the Campus User Account username value.Users can remove the domain suffix for up to 4 IDP attribute values.		
	A Domain Suffix value is required.		
	No Domain Suffix Remove a Domain Suffix Append a Domain Suffix Domain Suffix Infinitecampusfoundation.cc Image: Infinite and the second student is a second student infinite and student infinite and the second student i		
Append a Domain Suffix	This option allows you to append a suffix to the domain name.		
	A Domain Suffix value is required.		
Domain Suffix	Indicates the domain suffix that will be removed or appended based on the value set in the Append a Domain Suffix or Remove a Domain Suffix radio buttons. If this text box is left blank, the SAML response will not be checked for a domain suffix.		
Logoff IDP if Logoff URL Exists	Marking this checkbox means if the Logoff button is selected in Campus, you are also logged off the IDP.		
	This option only works if the Identity Provider Single Logoff URL field is populated and correct. This field is defaulted as marked.		
	This checkbox will automatically be unmarked and grayed out if the Identity Provider Single Logoff URL references Google.		
Turn off this SSO configuration for the Main Login page	Marking this checkbox means this SSO configuration will not appear as a button or option on the login screen for accessing the Infinite Campus application.		



Field	Field Description				
Turn off this SSO configuration for the Parent Portal	Marking this checkbox means this SSO configuration will not appear as a button or option on the login screen for the Parent Portal.				
Turn off this SSO configuration for the Student Portal	Marking this checkbox means this SSO configuration will not appear as a button or option on the login screen for the Student Portal.				
	Identity Provider Signature				
Inf	inite Campus allows for more than one IDP certificate				
Signature	The Identity Provider Signature Algorithm as indicated in the IDP				
Algorithm	certificate. This value is supplied by the SSO Identity Provider's (IDP) metadata.				
Issuer	The Issuer as indicated in the IDP certificate. This value is supplied by the SSO Identity Provider's (IDP) metadata.				
Certificate Valid From	The first date and time for which the certificate is considered valid. This value is supplied by the SSO Identity Provider's (IDP) metadata.				
Certificate Valid To	The final date and time for which the certificate is considered valid. All time after this value is considered invalid and the certificate will no longer work. This value is supplied by the SSO Identity Provider's (IDP) metadata.				
	Service Signature				
Manage SP Certificate	See the <u>Enable and Configure SAML SSO Functionality</u> , <u>Export the Service</u> <u>Provider Certificate</u> , and <u>Delete the Service Provider Certificate</u> sections for more information about functionality.				
Signature Algorithm	The Signature Algorithm as indicated in the Campus certificate.				
Issuer	The Issuer as indicated in the Campus certificate.				
Certificate Valid From	The first date and time for which the certificate is considered valid.				
Certificate Valid To	The final date and time for which the certificate is considered valid. All time after this value is considered invalid and the certificate will no longer work.				

Deleting an Existing SSO Configuration

You can delete an existing SSO configuration however, when doing so you will receive a pop-up notice indicating the number of users who will be affected by the deletion (users who are currently using this SSO configuration). If you proceed to delete the SSO configuration, impacted users will automatically be set to Local Campus Authentication to ensure their accounts are still accessible and you will need to manually convert them back to SSO authentication if another configuration is created.



Configuring a Unique Entra Active Directory

The following section will describe how to configure a unique Entra (formerly Azure) Active Directory.

This section is only relevant for Microsoft Entra customers.

Infinite Campus is now available in the Microsoft Azure Marketplace.

- Infinite Campus in the Marketplace: <u>https://azuremarketplace.microsoft.com/en-us/marketplace/apps/aad.infinitecampus?tab=overview</u>
- Entra Active Directory Integration with Campus Tutorial: <u>https://learn.microsoft.com/en-us/entra/identity/saas-apps/infinitecampus-tutorial</u>

Two main actions need to be taken to ensure Entra has an active connection between Campus and your Entra AD environment.

- 1. Utilize the Infinite Campus Azure Marketplace workflow within your Microsoft Entra environment for initial configuration.
- 2. Update the logout URL in the Entra AD manifest with the Campus logout URL.

The following sections will walk you through this process:

- Infinite Campus Azure Marketplace Workflow
- Add the Infinite Campus Logout URL to the Microsoft Entra SAML SSO Configuration
- Complete a Single Sign-On Login

Infinite Campus Azure Marketplace Workflow

Step 1.

In your Entra AD environment, navigate to Enterprise applications > + New application registration.

Enter "Infinite Campus" in the search box in the **Add from the gallery** section of the page and click on the Infinite Campus icon that appears.

nfinite Campus						
Microsoft Azure						
+ Create a resource	Home > Infcampustest > Enterprise applications Categories ×	- All applications > Categories > Add an application	Add an application	x 🗆 x		
All services	All (3035)	Add your own app				
Dashboard	Business management (333)	Application	On-premises	Non-gallery		
All resources	Contruction (419)	Register an app you're working on to integrate it with Azure AD	Configure Azure AD Application Proxy to enable secure remote	Integrate any other		
 Resource groups App Services 	Consumer (40)			application that you don't find in the gallery		
SQL databases	Content management (138)		access	_		
🖓 SQL data warehouses	CRM (146)	Add from the gallery				
Azure Cosmos DB	Data services (143)					
Virtual machines	Developer services (99)	Infinite Campus		~		
Load balancers Storage accounts	E-commerce (75)	1 applications matched "In	ifinite Campus".			
Virtual networks	Education (131)	NAME		CATEGORY		
Monitor	ERP (70)	Infinite Campus		Education		
Advisor	Finance (248)					

Step 2.

Click the **Add** button in the lower right-hand corner of the screen.

Home > Infcampustest > Enterprise applications - All applications > Categories > Add an application > Infinite Campus							
Categories	× Add an application	Add an application $\Rightarrow \times$			Infinite Campus 🛛 🗠 X		
All (3035)	Add your own app	Add your own app			Infinite Campus, Inc.		
Business management (333)	Application	On-premises	Non-gallery		Our simple vet nowerful SIS supports student		
Collaboration (419)	you're developing	application	application		learning by ensuring school districts		
Construction (8)	Register an app you're	Register an app you're Application Proxy to application that you don't working on to integrate it endour solution that you don't the callery			streamine educational processes, promote stakeholder collaboration and personalize		
Consumer (40)	with Azure AD	enable secure remote access	find in the gallery		learning.		
Content management (138)	_				Use Microsoft Azure AD to enable user access		
CRM (146)	Add from the gallery				to Infinite Campus.		
Data services (143)					Requires an existing Infinite Campus		
Developer services (99)	Infinite Campus			subscription.			
E-commerce (75)	1 applications matched	1 applications matched "Infinite Campus".			Name 🚯		
Education (131)	NAME	NAME CATEGORY			Infinite Campus		
ERP (70)	nfinite Camp	nfinite Campus Education			Publisher 🚯		
Finance (248)					Infinite Campus, Inc.		
Health (61)					Single Sign-On Mode 👩		
Human resources (265)					SAML-based sign-on		
IT infrastructure (181)					URL 🙃		
Mail (33)					https://www.infinitecampus.com/		
management (1)				-			
Marketing (208)	-				A00 ~		

Step 3.

Once the Infinite Campus application has been added to the Entra environment, you will need to configure SAML SSO. Click on the **Single sign-on** button of the Enterprise Application index and



Step 4.

Single sign-on

ProvisioningSelf-service

The Microsoft Azure Marketplace workflow will display. Follow the sequence of events laid out on the screen, and if you have any questions, click the **View step-by-step instructions** hyperlink for more information. To edit data, click the edit icons in the upper right corner of each section. Once the data on this page has been reviewed and corrected accordingly, move on to the <u>Add the Infinite</u> <u>Campus Logout URL to the Microsoft Entra SAML SSO Configuration</u> section of this article.

分



up	o Single Sign-On with SAML - P	review	
the	e configuration guide 🖉 for help integrating Infini	ite Campus Int VT.	
	Basic SAML Configuration		1
	Sign on URL	https://ie.infinitecampus.com/ie/SSO/ievt/SIS	
	Reply URL (Assertion Consumer Service URL)	https://ie.infinitecampus.com/ie/SSO/ievt/SIS/	
	Identifier (Entity ID)	https://ie.infinitecampus.com/ie/ievt	
	Relay State	Optional	
[User Attributes & Claims		
	Givenname	user.givenname	
	Surname	user.surname	
	Emailaddress	user.mail	
	Name	user.userprincipalname	
	Unique User Identifier	user.userprincipalname	
	SAML Signing Certificate		1
	Status	Active	
	Thumbprint	368AD52230BD1853C5768AF8281236B3B756EE2A	
	Expiration	11/15/2021, 2:33:14 PM	
	Notification Email	devazure@infinitecampus.com	
	App Federation Metadata Url	https://login.microsoftonline.com/f6d2a478-177a-4	
	Certificate (Base64)	Download	
	Certificate (Raw)	Download	
	Federation Metadata XML	Download	
	Set up Infinite Campus Int VT		
	You'll need to configure the application to link	with Azure AD.	
	Login URL	https://login.microsoftonline.com/f6d2a478-177a-4	
	Azure AD Identifier	https://sts.windows.net/f6d2a478-177a-46be-9b11	
	Logout URL	https://login.microsoftonline.com/common/wsfede	
	View step-by-step instructions		
	Test single sing on with Infinite Computer	Tet V/T	
	rest single sign-on with fininte campus		



Add the Infinite Campus Logout URL to the Microsoft Entra SAML SSO Configuration

Step 1.

This step requires the SAML configuration in Campus to be enabled (check the "Enable SAML Single Sign On" checkbox), along with a metadata upload or synchronization and a subsequent Save, for the Service Provider Configuration screen to publish the applicable URLs. The Single Sign-on Logout URL will be needed for Step 2 below.

In the SSO Service Provider Configuration tool, locate the **Single Sign-on Logout URL** and copy this value.

Save Solution Delete Solution New
Service Provider Configurations Enabled Name for Login Button Single Sign-On (SSO)
Service Provider Configuration
C Enable SAML Single Sign On
*Name for Login Button
Single Sign-On (SSO)
Service Provider Metadata campus/SSO/intlA/federationMetadata
Single Sign-on URL
SSO/intlA/SIS/?idpEntityID=https://sts.windows.net/ f6d2a478-177a-46be-9b11-4e017385b34a/
Single Sign-out URL https://infinitecampus.com/campus/SSO/intlA/logout
*Campus (Service Provider) Entity ID (It must be a unique value for the IDP)
https .com/campus/intlA
Optional Attribute Name (default is nameID, Required for Azure) nameID
*Select an option to retrieve Identity Provider (IDP) server data
Metadata URL O Metadata XML file
i-46be-9b11-4e017385b34a/federationmetadata/2007-C Sync

Step 2.

Next, the Entra AD app registration properties Logout URL needs to be updated so that the proper



redirect upon Campus logout can occur.

- 1. Click on the Settings button (gear icon)
- 2. Click on **Properties** in the Settings list that has appeared to the right.
- 3. In the **Logout URL** field, paste the Single Sign-out URL value copied from the SSO Service Provider Configuration tool.
- 4. Select the **Save** icon.

Home > Infcampustest - App registrations >	JimcampusMaster > Settings > Properties			
JimcampusMaster Registered app	× \$\$	Settings	×	Properties 🛛
🌣 Settings 💉 Manifest 🗴 🛍 Delete				Save X Discard
Display name JimcampusMaster	Application ID d9327c82-9cb1-476b-b037-50a49ae2b8e7	GENERAL		* Name 🚯
Application type Web app / API	Object ID f784bf33-dbdd-4873-b4a6-23e8818519ed	11 Properties	>	Object ID 🚯
Home page https://publictest24.infinitecampus.com/c	Managed application in local directory	📃 Reply URLs	>	f784bf33-dbdd-4873-b4a6-23e8818519ed
https://pasiecest	*	Sources Owners	>	Application ID
		API ACCESS		4932/c82-9cb1-4/6b-b03/-50a49ae2b8e/
		Required permissions	>	https://publictest24.infinitecampus.com/c
		📍 Keys	>	Logo
		TROUBLESHOOTING + SUPPORT		Infinite Configuration
		X Troubleshoot	>	
		New support request	>	Upload new logo 🚯
				Select a file
				Home page URL
				Logout URL
				>
				Terms of service URL 🗿
				Privacy statement URL 🕐

Complete a Single Sign-On Login

The final step is to log out of the administrative account, log into Infinite Campus, and attempt a Single Sign-On user login. Please ensure you have followed the configuration steps outlined throughout this article.

To log in, navigate to the Campus login page and click the SSO button created during the configuration process (covered in steps within this article).

This button may be named something other than Single Sign-On (SSO).

Proper first-time login behavior will be a redirect to the Microsoft Entra AD credentials page. A successful logon to Entra AD results in a successful re-direct to the Infinite Campus application.

	Infinite Campus
Student Information System	
Single Sign-On (SSO)	
Username (Required) admin	
Password (Required)	
Log In Show Help	
Version: Campus-31.3.147 © 2003-2024 Infinite Camp www.infinitecampus.c	7 intlA ous, Inc. om

Infinite 🔶 📿

To log out of Campus, click the **Log Off** button in the upper right corner of the page.

Proper logout behavior will be a brief re-direct to the Microsoft Entra AD homepage, then another instant re-direct to the Infinite Campus logoff page. In a later version of Microsoft Entra AD, the redirect may be simultaneous.

≡	Q	Infinite (Camp	ous		23-24	Ŵ	?		•
		*	3		User: admin				Ζ
Main	Menu	I	B	et bur (Stieby v)	Instruction Se	ttings			
					Password and	d Security	Settings		
+ Inst	truction			and 177330	About Campu	s SIS	Open		
+ Stu	dent Inf	ormation		Int	Try New Look	i 🗤	6		
+ Atte	endance	Office		racker is reporting problems. 🎓					_
+ Beł	navior O	ffice		e2	Log Off	¥			
+ Cer	ารบร						D	01	/09/2024
				e2			De	01	/09/2024
+ Cor	mmunic	ation					De	lete	

Please ensure to contact the Infinite Campus Support team or your CE or other internal contact(s) with any questions or concerns.



Configuring a Google IDP

The following section will describe how to configure the Google IDP to utilize Campus SSO functionality.

Prerequisites

• You need a Google Admin account.

Step 1.

Log in to your Google Administrator account (https://admin.google.com) and select Apps.



Step 2.

Select Web and mobile apps.

≡ Google Adn	Imin Q Search for users, group	ps or settings		
Apps Apps Goog Goog II II Goog II II Goog Goog II II Goog Goog	ogle Workspace	Additional Google services Blogging, photos, video, social tools and more 64 SERVICES	Web and mobile apps Manage SAML, Android and iOS apps 4 APPS	Google Workspace Marketplace apps Add and manage third party apps NO APPS MANAGE

Step 3.

Infinite Campus

Click the Add app button and select Add custom SAML app.

Apps 3	Web and mobile app	S		
	Apps (4)	Add app ▼ Settings ▼		
	+ Add a filte	Search for apps		
	📄 Name 🛧	Add private Android app	nentication User access	Details
	🗆 G ,	Add private Android web app	/IL ON for every	one A Certificate expires on Jun 12, 2022
	🗆 Ġ 4	Add custom SAML app	/L ON for every	one 🛕 Certificate expires on Jun 12, 2022
		illy Sandbox Web SAN	AL OFF for every	yone 🛕 Certificate expires on Jun 12, 2022
	Re Re	IMN SSO app Web SAM	AL ON for every	one A Certificate expires on Jun 12, 2022

Step 4.

Enter an **App name**, **attach an app icon** (we highly suggest an Infinite Campus logo for easier identification), and click **Continue**.



Add custom SAML app		
App details — 2 Google Identity Provider detail: —	3 Service provider details — 🕢 Attribute mapping	
	App details Enter details for your custom SAML app. This information is shared with app users. Learn more	
	App name	
	Nate Testing	
	Annicon	
	Attach an app icon. Maximum upload file size: 4 MB	
	affailes of an	
	Campus	

Step 5.

Click **Download Metadata** and save the XML file somewhere you can easily locate it for an upcoming step.

× Add custom SAML app				
App details — 2 Google Identity Provider detail: — 🚳 Service provider details — 🚳 Attribute map	pping			
	To configure single sign-on (SSO) for SAML apps, follow your service provider's instructions. Learn more Option 1: Download IdP metadata			
	DOWNLOAD METADATA			
	OR			
	Option 2: Copy the SSO URL, entity ID, and certificate			
	SSO URL			
	https://accounts.google.com/o/saml2/idp?idpid=C02j2xb4b			
	Entity ID			
	https://accounts.google.com/o/saml2?idpid=C02j2xb4b			
	Certificate			
	Google_2022-6-12-14126_SAML2_0	±		
	SHA-256 fingerprint			
	74:6F:FD:FC:76:80:5D:19:EC:96:FF:82:75:63:DB:EF:8E:CC:2E:7A:58:0C:10:B7:01:6B:95:0C:46:79:92:E9	ē		
ВА	ж	CANCEL CONTINUE		

Step 6.



Open Infinite Campus in a different tab and navigate to the SSO Service Provider Configuration tool (System Administration > User Security > SAML Management > SSO Service Provider Configuration).

Using the Google IDP metadata file downloaded in Step 5:

- 1. Select the Metadata XML File radio button
- 2. Click Choose File.
- 3. Select the Google IDP metadata file from Step 5 and click **Open**.

The Identity Provider Entity ID, Identity Provider URL, and Identity Provider Single Logoff URL will populate.

Campus does not support the use of the **Logoff IDP if Logoff URL Exists** preference when using a Google IDP setup. This checkbox will automatically be unmarked and grayed out if the Identity Provider Single Logoff URL references Google.

Save	1
Service Provider Configuration	- 1
C Enable SAML Single Sign On	
Service Provider Metadata com/campus/SSO/SIS-124425intca/federationMetadata	
Single Sign-on URL com/campus/SSO/SIS-124425intca/SIS	
Single Sign-out URL n/campus/SSO/SIS-124425intca/logout	
*Campus (Service Provider) Entity ID (It must be a unique value for the IDP)	
Optional Attribute Name (default is nameID, Required for Azure) nameID	
*Select an option to retrieve Identity Provider (IDP) server data Metadata URL Metadata XML file Metadata File: GoogleIDPMetadata-infinitecampusfoundation.cc (5).xml Choose File No file chosen	
Identity Provider Entity ID	Once the Google IDP
/sami2?/idpid=C03lbk2xh	Metadata file is
o/saml2/idp?idpid=C03lbk2xh	will automatically
Identity Provider Single Logoff URL https://www.google.com/accounts/Logout	populate.
Show Campus SSO Preferences ▼	

Step 7.

Now it's time to save and enable the Campus SSO. Mark the **Enable SAML Single-Sign On** checkbox and click **Save**.

Save Service Provider Configuration Enable SAML Single Sign On	
Campus (Service Provider) Entity 10 (it must be a unique value for the IDP) Com/campus/intAZ Optional Attribute Name (default is nameID, Required for Azure)	
nameID I *Select an option to retrieve Identity Provider (IDP) server data • Metadata URL • Metadata XML file • Sync	

Step 8.

Go back to your open Google Admin session. Click **Continue**.

Option 1: Download IdP metadata		
DOWNEDAD METADATA		
OR		
Option 2: Copy the SSO URL, entity ID, and certificate		
SSO URL		
https://accounts.google.com/o/saml2/idp?idpid=C02j2xb4b	ē	
Entity ID		
https://accounts.google.com/o/saml2?idpid=C02j2xb4b	Ē	
Certificate		
Google_2022-6-12-14126_SAML2_0) ±	
BEGIN CERTIFICATE MIIDdDCCAlygAwlBAgiGAVyjQuHpMA0GCSqGSib3DQEBCwUAMHaxFDASBgNVBAoTC0dvb2daZSBJ bmMuMRVwFAYDVQQHEw1Nb3VudGFpbiBWaWV3MQ8wDQYDVQQDEwZHb29nbGUxGDAWBgNVBAsTD0dv b2daZSBGb3IgV29yazELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGimb3JuaWEwHhcNMTcwNjEz		
SHA-256 fingerprint		
74:6F:FD:FC:76:80:5D:19:EC:96:FF:82:75:63:DB:EF:BE:CC:2E:7A:58:0C:10:B7:01:6B:95:0C:46:79:92:E9	ē	

Step 9.

On the Service Provider Details screen:

1. Enter the ACS URL as the same value found in the Single Sign-On URL field.



- 2. Enter the Entity ID as the same value found in the Campus (Service Provider) Entity ID (It must be a unique value for the IDP) field.
- 3. Click **Continue**.

Service provider details To configure single sign on, add service provider details such as ACS URL and entity ID. Learn more ACS URL	Save O Delete New Franker Provider Configurations Enabled Name for Login Button Single Sign-On (SSO)
https://lesite3.infinitecampus.com/campus/SSO/intRI/SIS/?idpEntityID=https://accounts.google.com/o/saml2?idpid=C02[2xb4b Enttys:// https://lesite3.infinitecampus.com/campus/intRI	Service Provider Configuration
Start URL (optional) Signed response	Single Sign-On (SSO) Service Provider Metadata comcampusi/SSO/IntRI/federation/Metadata Single Sign-on URL https://estei3.intimiceumpus.com/campusi/SSO/IntRI/SIS7/dpEnthylD=https://accounts.google.com/o/sam/2? rdpis/Cr202a-bb
Name ID Defines the naming format supported by the identity provider. Learn more	Single Sign-out URL comicampus/SSOIntRillogoul Campus (Service Provide) Entry ID (It must be a unique value for the IDP) Into silvesità similare ampus comicampus/IRI Comica del Martine Marcine (che di comica del campo) Comica del Martine Marcine (che di comica del campo) Comica del Martine Marcine (che campo) Comica del Martine Marcine (che campo) Comica del Marcine Marcine (che campo) Comic
Nore D tomat UNSPECIFIED	Cylinida Hallace Traine (Deduct is Talinetto), requires to Azalif InameD InameD *Select an option to retrieve Identity Provider (IDP) server data Mandara 101 Mandara 104
Name D Basic Information > Primary email	Versional V. Comparison on L Be Metadata File: Google DPMetadata xml Choose File No file chosen Identity Provider Entity D Indity. France Condivisiant2.7
BACK CANCEL CONTINUE	

Step 10.

Now we need to turn on the service within Google.

- 1. Navigate to Apps > **Web and mobile apps** and locate your Infinite Campus app.
- 2. Click on the app and then select View details.



3. Click the **ON for everyone** radio button and select **Save**. SSO is now configured. The last thing to do is test the connection to ensure everything is working correctly.

By default, Google SSO matches based on username.

Step 11.

Test the connection by selecting a user account, modifying their **Authentication Type** to SAML: Single Sign-On (SSO), and selecting **Save**.



Note you will need to know the user's Username and Password in order to complete the login process so using a test account is advised.



Now, log out of Infinite Campus and log back in as this user via the SSO Login button, which is now available on the Campus Login Screen.

	Infinite Campus
Student Information System	
Single Sign-On (SSO)	
or	
Username (Required)	
admin	
Password (Required)	
••••••	
Log In	
Show Help	
Version: Campus-31.3.147 © 2003-2024 Infinite Campu www.infinitecampus.com	intIA s, Inc. <u>m</u>

If you are able to log in without a problem you are all set!

If you would like to convert all existing accounts from using local Campus login authentication to SAML SSO, please use the <u>User Account Type Wizard</u>.

Sandbox/Staging/Non-Production Environments

This section indicates the process for setting up SSO in a non-production environment for the first time.

- 1. Ensure a Non-SSO User Account Exists for Administrators
- 2. Have the Non-Production Infinite Campus Environment Refreshed
- <u>3. In Your SSO IDP's System, Repeat Their Setup Process</u>

1. Ensure a Non-SSO User Account Exists for Administrators

In your production environment, ensure a user account exists for yourself and is set to an Authentication Type of LDAP or Local Campus Authentication before proceeding.

Note that some governing agencies, such as the North Carolina Department of Public Instruction, do not allow use of Local Campus Authentication. Ensure you comply



with your governing agency's security practices.

THIS IS AN IMPORTANT STEP THAT MUST BE FOLLOWED. If this step is not followed, you will not be able to access your non-production environment until you complete this step and have your non-production environment refreshed again.

For the rest of the process, if your district has more than one non-production environment (ex. sandbox and staging), these steps will need to be followed for each environment.

User Account ☆ Terri II: Staff #: DOB:	User Management > User Account Administration > User Account
User Account Detail ttestperson User Account Information	-
User Credentials	Authentication Information
Homepage Authentication Type Campus Tools Ulsername *	Authentication Options Exclude from Multi-Factor Authentication and New Device Notifications Time-Based Two-Factor Authentication
ttestperson Force Password Change	
Account Expiration Date month/day/year Disable Account	

2. Have the Non-Production Infinite Campus Environment Refreshed

Next, follow the steps below:

- 1. Follow your district's typical processes to have your non-production Infinite Campus environment refreshed to match your production Infinite Campus site.
- 2. Use your non-SSO user account to log into the non-production Infinite Campus environment.
- 3. Navigate to the SSO Service Provider Configuration screen and select your configuration. You will need to reference this screen and its values for the next steps.

3. In Your SSO IDP's System, Repeat Their Setup Process

Most Identity Providers (ex. Google, Microsoft Entra, etc.) require you set up a fresh app that is specific to the non-production Infinite Campus environment and distinct from the app that you set up for the production Infinite Campus environment.



Refer to whichever sections of this documentation you referred to originally to configure your production app, repeating this process, but for a fresh app specific to your non-production Infinite Campus site:

- General instructions
 - Enable and Configure SAML SSO Functionality
- IDP-specific instructions
 - Configuring a Unique Entra Active Directory
 - Configuring a Google IDP

These two items are especially important as you complete the setup in the IDP system for your nonproduction Infinite Campus app:

Campus (Service Provider) Entity ID	In your non-production environment, you'll notice the Campus (Service Provider) Entity ID starts the same as it does in production, but ends with an underscore and site type (for example _sandbox or _staging). This is an important distinction to be aware so that when you set up a non-production Infinite Campus app in your SSO IDP's system, you use the non-production Campus (Service Provider) Entity ID.
	Your non-production site's Campus (Service Provider) Entity ID value may not correlate to a valid URL. This is not a concern. What is important is that it is not the same value as your production Campus (Service Provider) Entity ID.
Metadata URL/Metadata XML file	During the process of setting up your non-production Infinite Campus app in your SSO IDP's system, you will either be provided a metadata URL or metadata XML file by your IDP's system. Do not reuse the metadata originally provided for your production Infinite Campus setup. Use the metadata your SSO IDP provides for the non-production app in your non-production site.
	Note: You will need to repeat this step—re-uploading this file or pasting in and resyncing this URL—after each refresh of your non- production site.

Troubleshooting existing SSO config in a non-production environment

If you are encountering issues after a refresh or cutover in an environment that has already been set up and is functional, ensure the following is correct:

Ensure Your Metadata Has Been Re-Uploaded/Resynced:

After each site refresh, your non-production environment must be provided with your Identity Provider's metadata.

If you do not have the metadata for your non-production site:

1. Log in to your SSO IDP system,



- 2. Navigate to the non-production Infinite Campus app you've set up
- 3. Copy the Metadata URL or re-download the Metadata XML file

Once you have obtained the metadata, navigate to your non-production Infinite Campus environment:

- 1. Log in to Infinite Campus using your non-SSO (LDAP or Local Campus Authentication) credentials.
- 2. Navigate to the SSO Service Provider Configuration tool (System Administration > User Security > SAML Management > SSO Service Provider Configuration)
- 3. Select the SSO configuration.
- 4. Resync the metadata by either:
 - 1. Selecting the **Metadata URL** radio button, pasting in the metadata URL, and clicking **Sync**

OR

2. Selecting the **Metadata XML file** radio button, uploading the metadata XML file, and clicking **Sync**

Service Provider Configuration		
Enable SAML Single Sign On		
*Name for Login Button		
Single Sign-On (SSO)		
*Campus (Service Provider) Entity ID (It must be a unique value for the IDP) https://iesite1.infinitecampus.com/campus/intID		
Optional Attribute Name (default is nameID, Required for Azure) nameID		
*Select an option to retrieve Identity Provider (IDP) server data Metadata URL OMetadata XML file Sync		
Identity Provider Entity ID		
Identity Provider URL		
Identity Provider Single Logoff URL		
Show Campus SSO Preferences ▼		

5. Once the metadata has been entered and synced, click Save. Single Sign-On for your nonproduction Infinite Campus site should now function properly.

Campus (Service Provider) Entity ID:

In your Campus non-production environment, on the **SSO Service Provider Configuration** screen, verify that your **Campus (Service Provider) Entity ID** matches your production Campus (Service Provider) Entity ID with the important addition of an underscore and your site type at the end (ex. _sandbox or _staging).

In your SSO IDP system's non-production app, navigate to where you originally provided this value. Ensure that what is listed in your SSO IDP's system exactly matches the Campus (Service Provider) Entity ID listed in your Infinite Campus non-production environment. If it does not, update your SSO IDP system to match Infinite Campus.



Matching Campus Fields to IDP Fields

This section will assist you in understanding how fields within your IDP correlate to fields within Campus.

- <u>SSO Setup Process</u>
- Google (admin.google.com)
- <u>Microsoft Entra Active Directory (entra.microsoft.com)</u>
- <u>Microsoft Active Directory Federated Services (AD FS)</u>
- Classlink (SAML Console)
- <u>Clever (SAML Connector)</u>
- Duo SAML SSO
- Okta (SAML App Integration)
- OneLogin (SAML Custom Connector Advanced)
- <u>OmnID</u>
- RapidIdentity (SAML Integration)

SSO Setup Process

Accessed in the Identity Provider system

Find the metadata within your Identity Provider system as a URL or an XML file download. Then paste/upload it to the Campus SSO Service Provider Configuration screen.

Terms used in Identity Provider systems	Corresponding field in Infinite Campus	
"Federation Metadata URL Path" "IDP Metadata URL" "Live Metadata URL" "Metadata URL"	Select an option to retrieve Identity Provider (IDP) server data Metadata URL	
OR		
"Download Metadata" "Federation Metadata XML" "Metadata (download)" "View IDP Metadata > Save as"	Select an option to retrieve Identity Provider (IDP) server data Metadata XML	

Accessed in Infinite Campus > Provided to the Identity Provider system

Within Infinite Campus, do one of these:

- Copy out the Service Provider Metadata URL and provide it to your Identity Provider. Their system can use this URL to pull in the other values it needs (Single Sign-On URL, Campus (Service Provider) Entity ID, Single Sign-Out URL). For Identity Providers that support intaking the Service Provider Metadata URL, it's a convenient way to get them all the URLs their system needs at once.
- 2. Provide the Single Sign-On URL and Campus (Service Provider) Entity ID, and Single Sign-Out



URL manually. (Not all systems support the Single Sign-*Out* URL, so some will have nowhere to put it on their end.)

Field in Infinite Campus	Terms used for the corresponding field in Identity Provider systems
Service Provider Metadata	"Metadata" "Metadata URL" "Federation metadata address" "Load XML from file or http address"
	OR
Single Sign-On URL	"ACS URL" "Assertion Consumer Service URL" "Destination URL" "Recipient URL" "Relying party SAML 2.0 SSO Service URL" "Reply URL" "Sign on URL"
Campus (Service Provider) Entity ID	"Audience Restriction" "Audience URI (SP Entity ID)" "Entity ID" "Identifier (Entity ID)" "Relying party trust identifier" "Remote Entity Name"
Single Sign-Out URL (Optional)	"Logout Url" "SAML Logout Trusted URL" "Single Logout URL"

Terms Used in Specific Identity Provider Systems

Google (admin.google.com)

See this section for detailed steps on configuring a Google IDP.

Google

Get from Google Provide to Corresponding Field in Campus



Get from Google	Provide to Corresponding Field in Campus
Download Metadata	Select an option to retrieve Identity Provider (IDP) server data Metadata XML

Infinite Campus

Get from Campus	Provide to Corresponding Field in admin.google.com
Service Provider Metadata	N/A - Google does not support intaking Infinite Campus Service Provider Metadata via a Metadata URL
Single Sign-On URL	ACS URL
Campus (Service Provider) Entity ID	Entity ID
Single Sign-Out URL	N/A - Google does not support Single Sign Out
NameID: The default nameID value from Google is the full Google account email	

Microsoft Entra Active Directory (entra.microsoft.com)

<u>See this section</u> for detailed steps on configuring a unique Entra (formerly Azure) Active Directory.

Not to be confused with AD FS (Microsoft Active Directory Federated Service), which is a different Identity Provider service from Microsoft.

Entra

Get from Entra	Provide to the Corresponding Field in Campus	
IDP Metadata URL	Select an option to retrieve Identity Provider (IDP) server data Metadata URL	
OR		
Federation Metadata XML	Select an option to retrieve Identity Provider (IDP) server data Metadata XML	
There is a "Relay State" field on Entra Active Directory's SAML Configuration screen that you will not fill in		

Infinite Campus



Get from Campus	Provide to the Corresponding Field in Entra
Service Provider Metadata	N/A - Entra Active Directory does not seem to support intaking Infinite Campus Service Provider Metadata via a Metadata URL
Single Sign-On URL	Reply URL (Assertion Consumer Service URL) <i>and</i> Sign on URL
Campus (Service Provider) Entity ID	Identifier (Entity ID)
Single Sign-Out URL	Logout Url (Optional)
NameID: The default nameID value from Entra Active Directory is the full Microsoft account email	

Microsoft Active Directory Federated Services (AD FS)

This is not to be confused with Microsoft Entra Active Directory, which is a different Identity Provider service from Microsoft.

AD FS

Get from AD FS	Provide the Corresponding field in Campus
AD FS > Service > Endpoints URL Path (the one with a type of Federation Metadata, which should end in .xml)	Select an option to retrieve Identity Provider (IDP) server data Metadata URL
OR	
AD FS > Service > Endpoints UBL Path (the one with a type of Federation	<i>Select an option to retrieve Identity Provider (IDP) server data</i>
Metadata, which should end in .xml)	Metadata XML
Navigate to the path in a browser to download the file.	

Infinite Campus



Get from Campus	Provide to Corresponding Field in AD FS
Service Provider Metadata	Select Data Source > Import data about the relying party published online or on a local network
	Federation metadata address (host name or URL)
It is not necessary t	to enter this info manually if you provide ASFS the Infinite Campus Service Provider Metadata, but if you choose manual setup:
Single Sign-On URL	Select Data Source > Enter data about the relying party manually > Choose Profile: AD FS Profile > Configure URL Relying party SAML 2.0 SSO Service URL
Campus (Service Provider) Entity ID	Select Data Source > Enter data about the relying party manually > Choose Profile: AD FS Profile > Configure Identifiers Relying party trust identifier
Single Sign-Out URL	Relying Party Trusts > Properties > Add/Edit > Endpoint Type: SAML Logout > Binding: POST Trusted URL

Classlink (SAML Console)

Classlink

Get from Classlink	Provide to Corresponding Field in Campus
IDP Metadata URL	Select an option to retrieve Identity Provider (IDP) server data Metadata URL

Infinite Campus

Get from Campus	Provide to Corresponding Field in Classlink SSO
Service Provider Metadata	Metadata URL
Single Sign-On URL	N/A - It seems like ClassLink obtains this directly from Infinite Campus' Service Provider Metadata URL
Campus (Service Provider) Entity ID	N/A - It seems like ClassLink obtains this directly from Infinite Campus' Service Provider Metadata URL
Single Sign-Out URL	N/A - It seems like ClassLink obtains this directly from Infinite Campus' Service Provider Metadata URL

Clever (SAML Connector)



Clever

Get from Clever	Provide to Corresponding Field in Campus	
Metadata URL	Select an option to retrieve Identity Provider (IDP) server data	
	Metadata URL	

Infinite Campus

Get from Campus	Provide to Corresponding Field in Clever
Service Provider Metadata	N/A - It doesn't seem like Clever supports intaking Infinite Campus Service Provider Metadata via a Metadata URL
Single Sign-On URL	Assertion Consumer Service URL
Campus (Service Provider) Entity ID	Entity ID
Single Sign-Out URL	N/A - It doesn't seem like Clever supports Single Sign Out

Duo SAML SSO

Duo

Get from Duo	Provide to Corresponding Field in Campus	
Metadata URL	Select an option to retrieve Identity Provider (IDP) server data Metadata URL	
OR		
SAML Metadata	Select an option to retrieve Identity Provider (IDP) server data Metadata XML	

Infinite Campus

Get from Campus	Provide to Corresponding Field in Duo	
Service Provider Metadata	Metadata XML URL	
<i>It is not necessary to enter this info manually if you provide OmnID the Service Provider Metadata, but if you decide to enter it manually:</i>		
Single Sign-On URL	Assertion Consumer Service (ACS) URL	
Campus (Service Provider) Entity ID	Entity ID	
Single Sign-Out URL	Single Logout URL	



Get from Campus

Provide to Corresponding Field in Duo

NameID: Default nameID value from Duo is full email

Okta (SAML App Integration)

Okta

Get from Okta	Provide to Corresponding Field in Campus	
View IDP Metadata > Save as	Select an option to retrieve Identity Provider (IDP) server data	
Additional details: Default RelayState can be left blank. To be able to enter a Single Logout URL,		
you must upload a Signature Certificate (see <u>Generate the Service Provider Certificate</u>) and mark		

Enable Single Logout within Okta.

Infinite Campus

Get from Campus	Provide to Corresponding Field in Okta	
Service Provider Metadata	N/A - Okta does not support intaking Infinite Campus Service Provider Metadata via a Metadata URL	
Single Sign-On URL	Single Sign On URL (Recipient URL and Destination URL are the same as the Single Sign On URL)	
Campus (Service Provider) Entity ID	Audience URI (SP Entity ID) Audience Restriction	
Single Sign-Out URL	Single Logout URL	
NamelD: Default namelD value from Okta is full email		

OneLogin (SAML Custom Connector Advanced)

OneLogin

Get from OneLogin	Provide to Corresponding Field in Campus
SSO > Issuer URL	Select an option to retrieve Identity Provider (IDP) server data Metadata URL

Infinite Campus



Get from Campus	Provide to Corresponding Field in OneLogin
Service Provider Metadata	N/A - OneLogin does not seem to support intaking Infinite Campus Service Provider Metadata via a Metadata URL
Single Sign-On URL	Login URL and ACS (Consumer) URL • (Do not make the mistake of entering it into the ACS (Consumer) URL <u>Validator</u> field, which is for something else.)
Campus (Service Provider) Entity ID	Audience (EntityID)
Single Sign-Out URL	Single Logout URL
NamelD: Default namelD value from OneLogin is full email	

OmnID

OmnID

Get from OmnID	Provide to Corresponding Field in Campus
<i>OmnID Console > Configure > User Managed</i> <i>SAML Settings</i>	<i>Select an option to retrieve Identity Provider</i> <i>(IDP) server data</i>
IDP Metadata URL	Metadata URL
Additional details: Infinite Campus does not support encrypted assertions. Within OmnID	

Additional details: Infinite Campus does not support encrypted assertions. Within OmnID (OmnID Console > SP Provided Metadata Settings), Encrypt Assertion must not be marked.

Infinite Campus

Get from Campus	Provide to Corresponding Field in OmnID	
Service Provider Metadata	Load XML from file or http address	
It is not necessary to enter this info manually if you provide OmnID the Service Provider Metadata, but if you decide to enter it manually:		
Single Sign-On URL	ACS URL	
Campus (Service Provider) Entity ID	Remote Entity Name	
Single Sign-Out URL	Single Logout URL	

RapidIdentity (SAML Integration)

RapidIdentity

Get from RapidIdentity	Provide to Corresponding Field in Campus	
Live Metadata URL Select an option to retrieve Identity Provider (IDP) se data Metadata URL		
OR		
Metadata (download)	Select an option to retrieve Identity Provider (IDP) server data Metadata XML	

Infinite Campus

Get from Campus	Provide to Corresponding Field in RapidIdentity
Service Provider Metadata Navigate to the Service Provider Metadata URL in a browser to view and copy its contents	Metadata > Paste contents of Service Provider Metadata URL into this textbox
Single Sign-On URL	N/A - RapidIdentity obtains this directly from the contents of Infinite Campus' Service Provider Metadata URL
Campus (Service Provider) Entity ID	N/A - RapidIdentity obtains this directly from the contents of Infinite Campus' Service Provider Metadata URL
Single Sign-Out URL	N/A - RapidIdentity obtains this directly from the contents of Infinite Campus' Service Provider Metadata URL

Troubleshooting SSO Login Issues

<u>See this article</u> for assistance in troubleshooting SSO login issues.