SSO Service Provider Configuration [.2128 - .2211]

Last Modified on 10/22/2022 10:47 am CDT

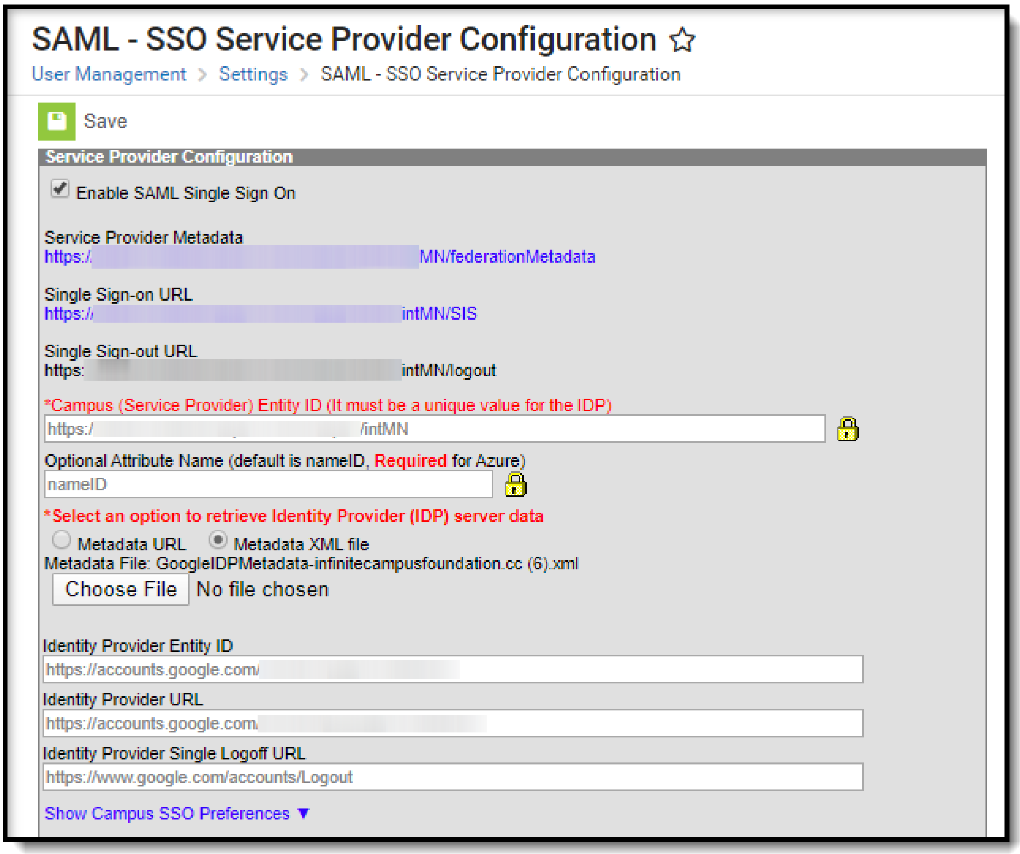
You are viewing a previous version of this article. See SSO Service Provider Configuration for the most current information.

Classic View: *System Administration > User Security > SAML Management > SSO Service Provider Configuration*

Search Term: *SSO Service Provider Configuration*

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

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



SAML - SSO Service Provider Configuration ☆

User Management > Settings > SAML - SSO Service Provider Configuration

Save

Service Provider Configuration

☑ Enable SAML Single Sign On

Service Provider Metadata
https:/[redacted]MN/federationMetadata

Single Sign-on URL
https:/[redacted]intMN/SIS

Single Sign-out URL
https:[redacted]intMN/logout

*Campus (Service Provider) Entity ID (It must be a unique value for the IDP)
https:/[redacted]/intMN

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 (6).xml
Choose File No file chosen

Identity Provider Entity ID
https://accounts.google.com/[redacted]

Identity Provider URL
https://accounts.google.com[redacted]

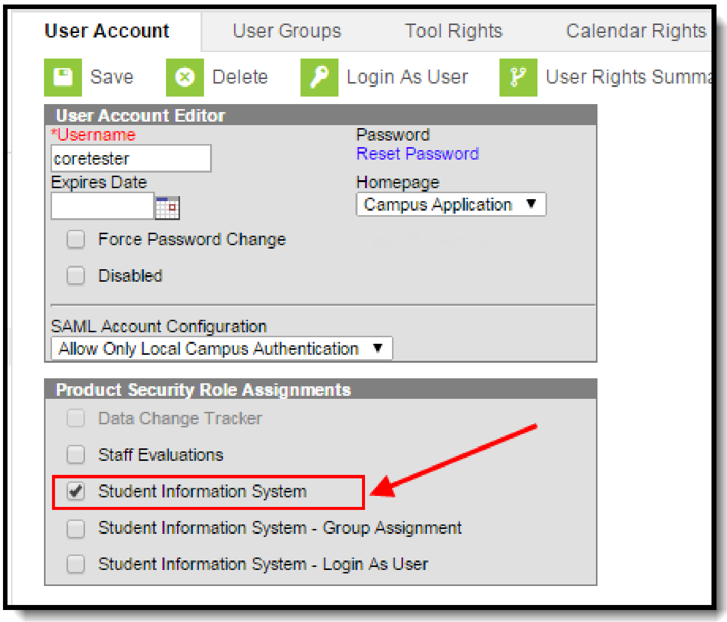
Identity Provider Single Logoff URL
https://www.google.com/accounts/Logout

Show Campus SSO Preferences ▼

Image 1: SSO Service Provider Configuration

Prerequisites

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



User Account | User Groups | Tool Rights | Calendar Rights

Save | Delete | Login As User | User Rights Summa

User Account Editor

*Username
coretester

Password
Reset Password

Expires Date

Homepage
Campus Application ▼

□ Force Password Change

□ Disabled

SAML Account Configuration
Allow Only Local Campus Authentication ▼

Product Security Role Assignments

□ Data Change Tracker

□ Staff Evaluations

☑ Student Information System

□ Student Information System - Group Assignment

□ Student Information System - Login As User

Additional Things to Consider

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

- When considering the configuration of user accounts, please note that Cafeteria Serve and Service Layout functionality only authenticates with a local Campus or LDAP account; therefore, please reserve a separate local Campus or LDAP account for access to Cafeteria Serve and Service Layout
- Schedule Wizard will authenticate with a SSO enabled account; however, it is important to note that the SSO authentication only occurs once. Users will be required to re-log into the Schedule Wizard.
- 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 Azure Active Directory, Google Apps IDP, Shibboleth IDP and OmnID. Since the Campus SSO Service Provider is part of the SAML specification, any IDP that is SAML compliant should connect with minimal intervention.
- Users are encouraged to provide a local domain account that can be linked to a Campus test user so that Campus Support can troubleshoot any SSO issues you may encounter.

When a test/sandbox environment is being refreshed, districts will need to reconfigure SAML each time a refresh occurs.

POS Service Layout and Cafeteria Serve are currently not compatible with the SSO user configuration.

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

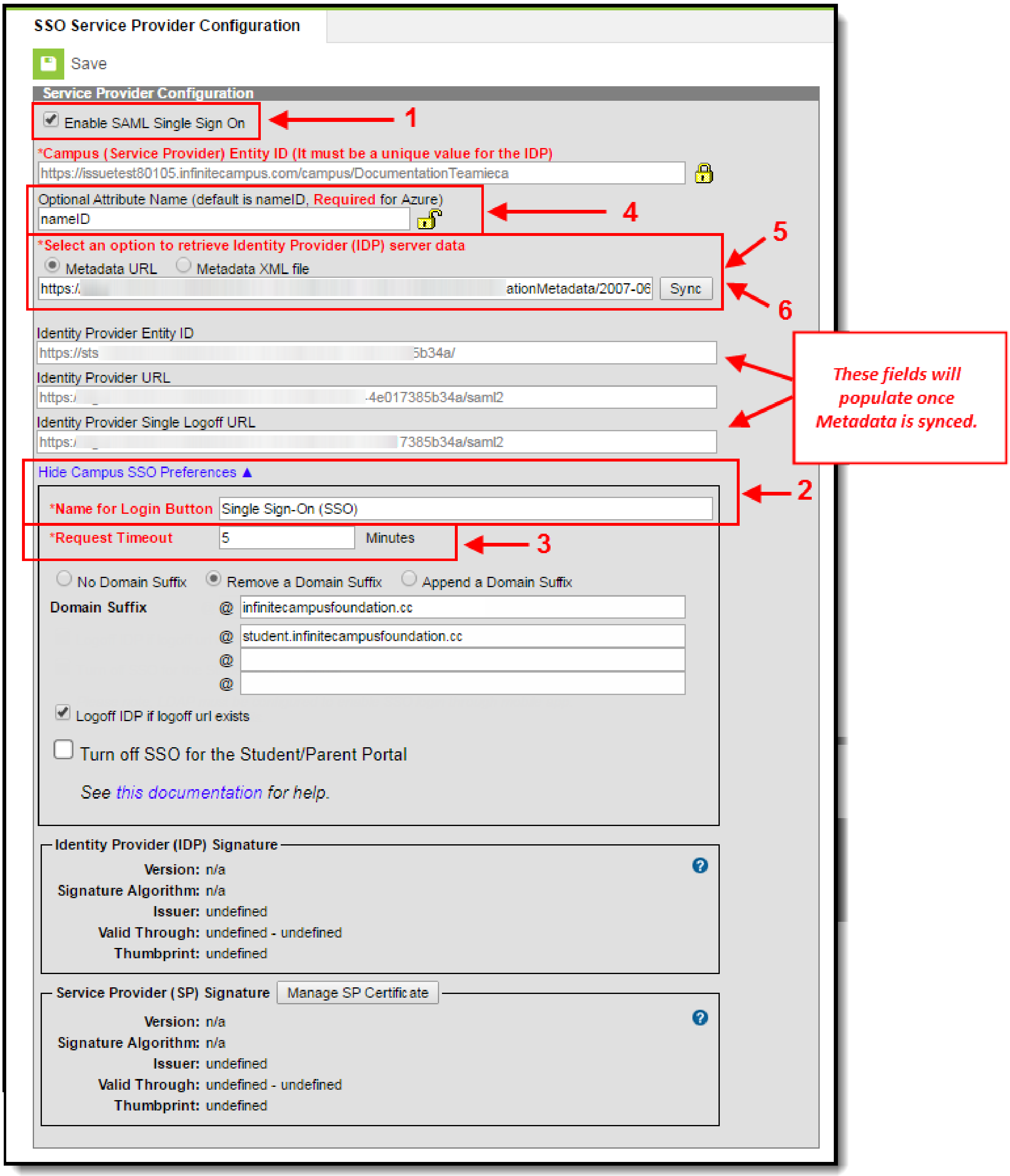
The first step to configuring SAML SSO is to enable SAML SSO functionality, define the Login button and sync IDP server metadata.

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

1. Mark the **Enable SAML Single Sign On** checkbox. This will enable SAML Single Sign On functionality within Campus.
2. Expand the **Campus SSO Preferences** area and 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.
3. Set the **Request Timeout**. This field indicates the number of minutes that can pass before a request between Campus and the IDP produces a timeout error.
4. If connecting Campus to Microsoft Azure, enter the **Optional Attribute Name** (or skip this step if not connecting to Azure). This is the attribute Campus will look for as a response from Azure in order to match the username in Campus to Azure.

   For more information about unique Azure configuration, please see the Configuring a Unique Azure Active Directory section below.

5. Retrieve the IDP server metadata by either entering the **Metadata URL** or by uploading the **Metadata XML File**.
6. If the **Metadata URL** was entered, hit the **Sync** button. This will populate Identity Provider fields below.
7. Move on to Step 2.



SSO Service Provider Configuration

Save

Service Provider Configuration

☑ Enable SAML Single Sign On

*Campus (Service Provider) Entity ID (It must be a unique value for the IDP)

https://issuetest80105.infinitecampus.com/campus/DocumentationTeamieca

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

https:/[redacted]ationMetadata/2007-06 Sync

Identity Provider Entity ID

https://sts[redacted]5b34a/

Identity Provider URL

https:/[redacted]-4e017385b34a/saml2

Identity Provider Single Logoff URL

https:/[redacted]7385b34a/saml2

Hide Campus SSO Preferences ▲

*Name for Login Button: Single Sign-On (SSO)

*Request Timeout: 5 Minutes

○ No Domain Suffix ● Remove a Domain Suffix ○ Append a Domain Suffix

Domain Suffix
@ infinitecampusfoundation.cc
@ student.infinitecampusfoundation.cc
@
@

☑ Logoff IDP if logoff url exists

☐ Turn off SSO for the Student/Parent Portal

See this documentation for help.

Identity Provider (IDP) Signature

Version: n/a
Signature Algorithm: n/a
Issuer: undefined
Valid Through: undefined - undefined
Thumbprint: undefined

Service Provider (SP) Signature Manage SP Certificate

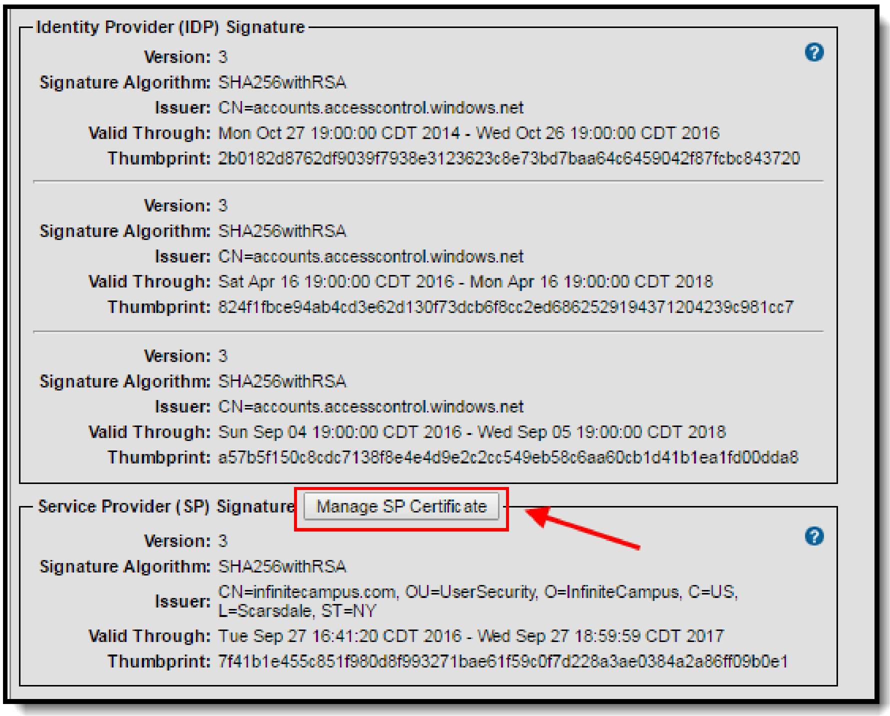
Version: n/a
Signature Algorithm: n/a
Issuer: undefined
Valid Through: undefined - undefined
Thumbprint: undefined

These fields will populate once Metadata is synced.

Image 2: Enabling SSO, Entering the Login Button Name, and Retrieving IDP Metadata

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 (see Image 3).



Identity Provider (IDP) Signature

Version: 3
Signature Algorithm: SHA256withRSA
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: 2b0182d8762df9039f7938e3123623c8e73bd7baa64c6459042f87fcbc843720

Version: 3
Signature Algorithm: SHA256withRSA
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: 824f1fbce94ab4cd3e62d130f73dcb6f8cc2ed686252919437120423 9c981cc7

Version: 3
Signature Algorithm: SHA256withRSA
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: a57b5f150c8cdc7138f8e4e4d9e2c2cc549eb58c6aa60cb1d41b1ea1fd00dda8

Service Provider (SP) Signature

Version: 3
Signature Algorithm: SHA256withRSA
Issuer: CN=infinitecampus.com, OU=UserSecurity, O=InfiniteCampus, C=US, L=Scarsdale, ST=NY
Valid Through: Tue Sep 27 16:41:20 CDT 2016 - Wed Sep 27 18:59:59 CDT 2017
Thumbprint: 7f41b1e455c851f980d8f993271bae61f59c0f7d228a3ae0384a2a86ff09b0e1

Image 3: Manage SP Certificate

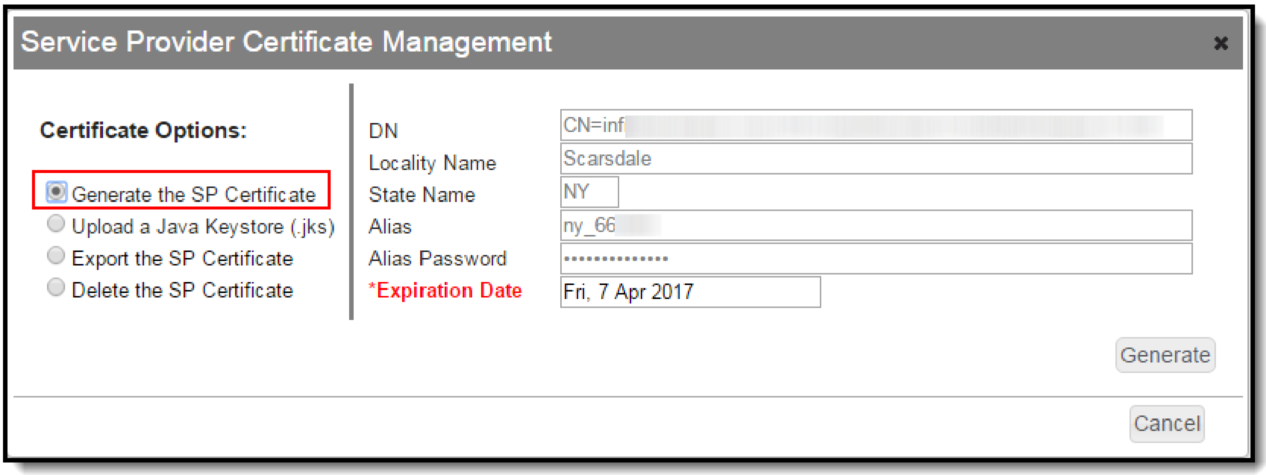
Service Provider Certificates can either be automatically generated by Campus using the Generate the SP Certificate feature or manually uploaded via the Upload a Java Keystore (.jks) feature.

To have Campus generate the Service Provider certificate:

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.
5. Move on to Step 3.



Service Provider Certificate Management

Certificate Options:

● Generate the SP Certificate
○ Upload a Java Keystore (.jks)
○ Export the SP Certificate
○ Delete the SP Certificate

DN: CN=inf
Locality Name: Scarsdale
State Name: NY
Alias: ny_66
Alias Password: ••••••••••••••
*Expiration Date: Fri, 7 Apr 2017

Image 4: Generate the SP Certificate

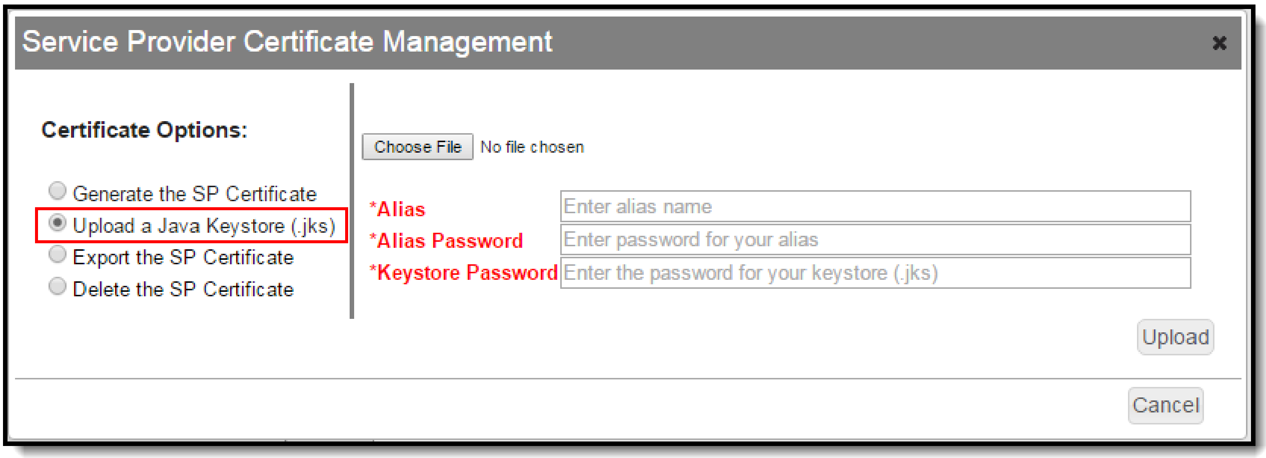
To upload the Service Provider certificate:

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.
3. 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 Azure 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.
5. Move on to Step 3.



Service Provider Certificate Management ×

Certificate Options:

○ Generate the SP Certificate
● Upload a Java Keystore (.jks)
○ Export the SP Certificate
○ Delete the SP Certificate

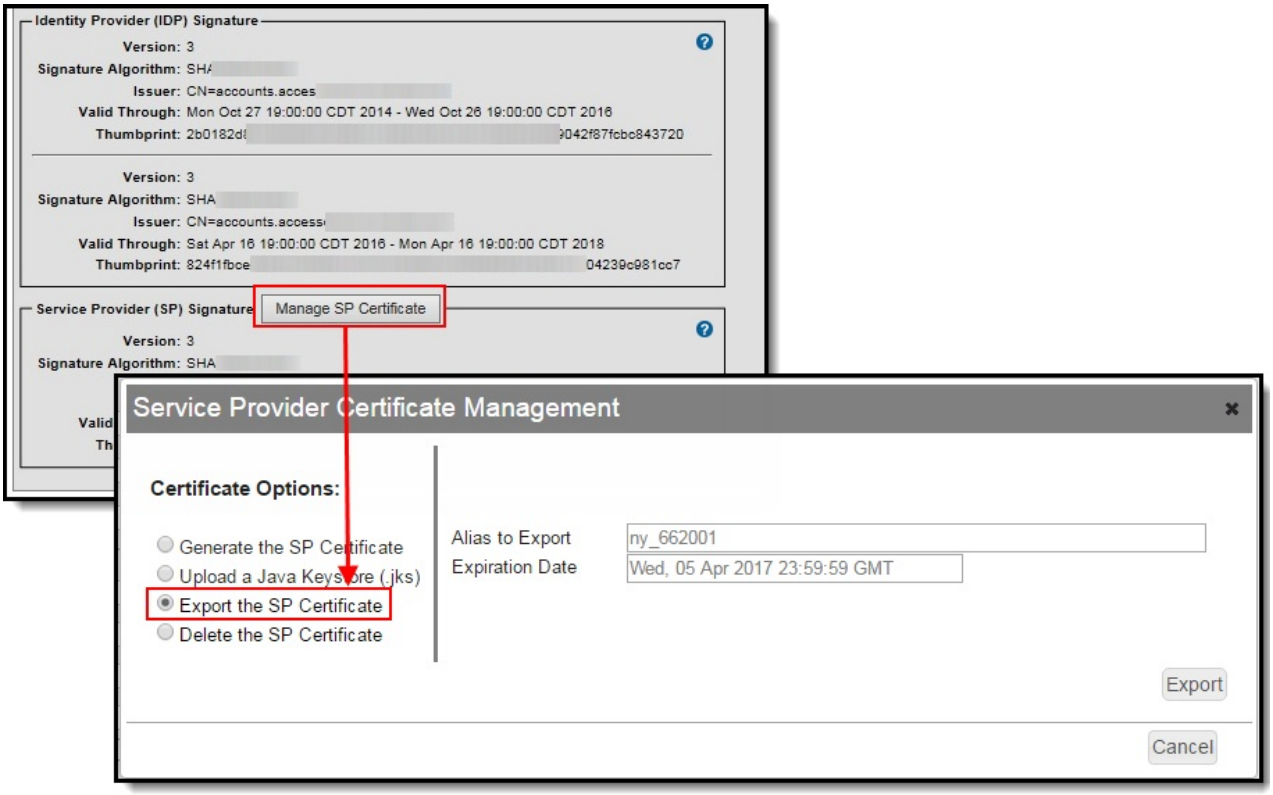
Choose File No file chosen

*Alias: Enter alias name
*Alias Password: Enter password for your alias
*Keystore Password: Enter the password for your keystore (.jks)

Image 5: Upload the Service Provider Certificate

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 for saving locally to your hard drive or network.



Identity Provider (IDP) Signature

Version: 3
Signature Algorithm: SHA[redacted]
Issuer: CN=accounts.acces[redacted]
Valid Through: Mon Oct 27 19:00:00 CDT 2014 - Wed Oct 26 19:00:00 CDT 2016
Thumbprint: 2b0182d[redacted]9042f87fcbc843720

Version: 3
Signature Algorithm: SHA[redacted]
Issuer: CN=accounts.access[redacted]
Valid Through: Sat Apr 16 19:00:00 CDT 2016 - Mon Apr 16 19:00:00 CDT 2018
Thumbprint: 824f1fbce[redacted]04239c981cc7

Service Provider (SP) Signature

Version: 3
Signature Algorithm: SHA[redacted]

Service Provider Certificate Management ×

Certificate Options:

○ Generate the SP Certificate
○ Upload a Java Keystore (.jks)
● Export the SP Certificate
○ Delete the SP Certificate

Alias to Export: ny_662001
Expiration Date: Wed, 05 Apr 2017 23:59:59 GMT

Image 6: Exporting the Service Provider Certificate

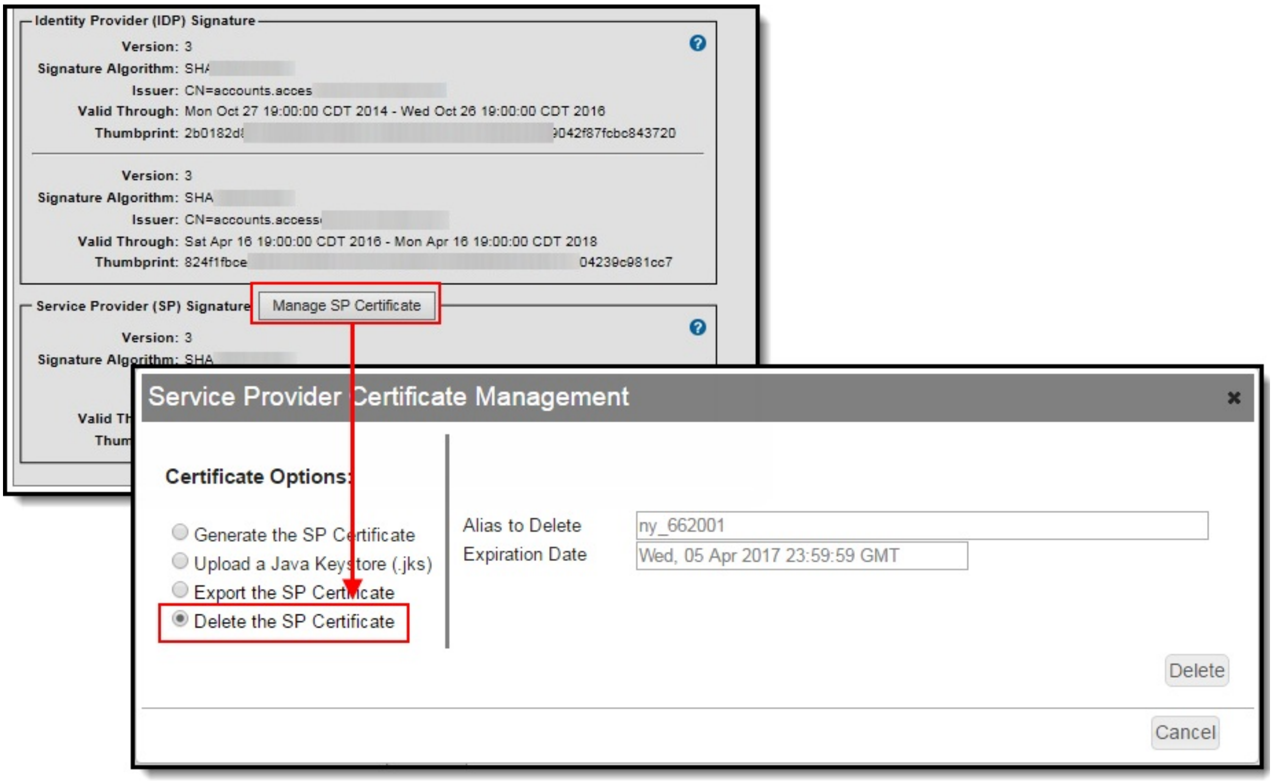
Delete the Service Provider Certificate

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
Signature Algorithm: SHA[redacted]
Issuer: CN=accounts.acces[redacted]
Valid Through: Mon Oct 27 19:00:00 CDT 2014 - Wed Oct 26 19:00:00 CDT 2016
Thumbprint: 2b0182d[redacted]042f87fcbc843720

Version: 3
Signature Algorithm: SHA[redacted]
Issuer: CN=accounts.access[redacted]
Valid Through: Sat Apr 16 19:00:00 CDT 2016 - Mon Apr 16 19:00:00 CDT 2018
Thumbprint: 824f1fbce[redacted]04239c981cc7

Service Provider (SP) Signature

Version: 3
Signature Algorithm: SHA[redacted]

Service Provider Certificate Management

Certificate Options:

○ Generate the SP Certificate
○ Upload a Java Keystore (.jks)
○ Export the SP Certificate
● Delete the SP Certificate

Alias to Delete: ny_662001
Expiration Date: Wed, 05 Apr 2017 23:59:59 GMT

Image 7: Deleting the Service Provider 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.

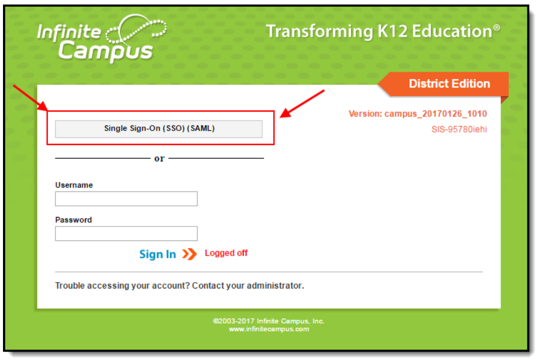
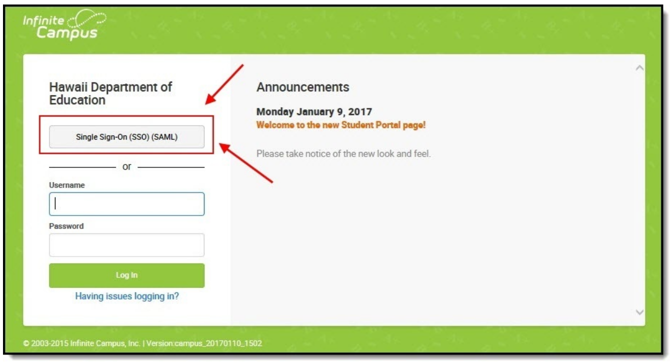
You must have proper Messenger Email Settings established in order to receive email notifications.

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.

Logging into Campus and Campus Portal Using SAML SSO

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

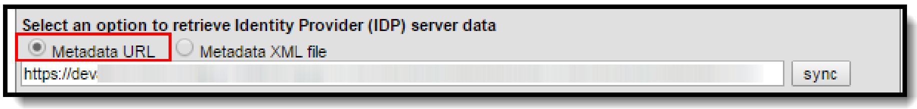
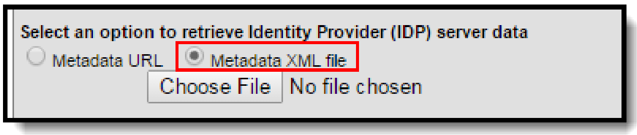
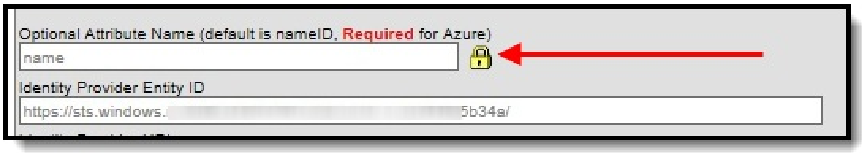
Campus District/State Edition	Campus Student Portal
Users will click the SSO button (named whatever was determined in Step 1 of this document).  Infinite Campus Transforming K12 Education® District Edition Version: campus_20170126_1010 SIS-95780iehi Single Sign-On (SSO) (SAML) or Username Password Sign In Logged off Trouble accessing your account? Contact your administrator. ©2003-2017 Infinite Campus, Inc. www.infinitecampus.com	Users will click the SSO button (named whatever was determined in Step 1 of this document).  Infinite Campus Hawaii Department of Education Single Sign-On (SSO) (SAML) or Username Password Log In Having issues logging in? Announcements Monday January 9, 2017 Welcome to the new Student Portal page! Please take notice of the new look and feel. © 2003-2015 Infinite Campus, Inc. | Version:campus_20170110_1502

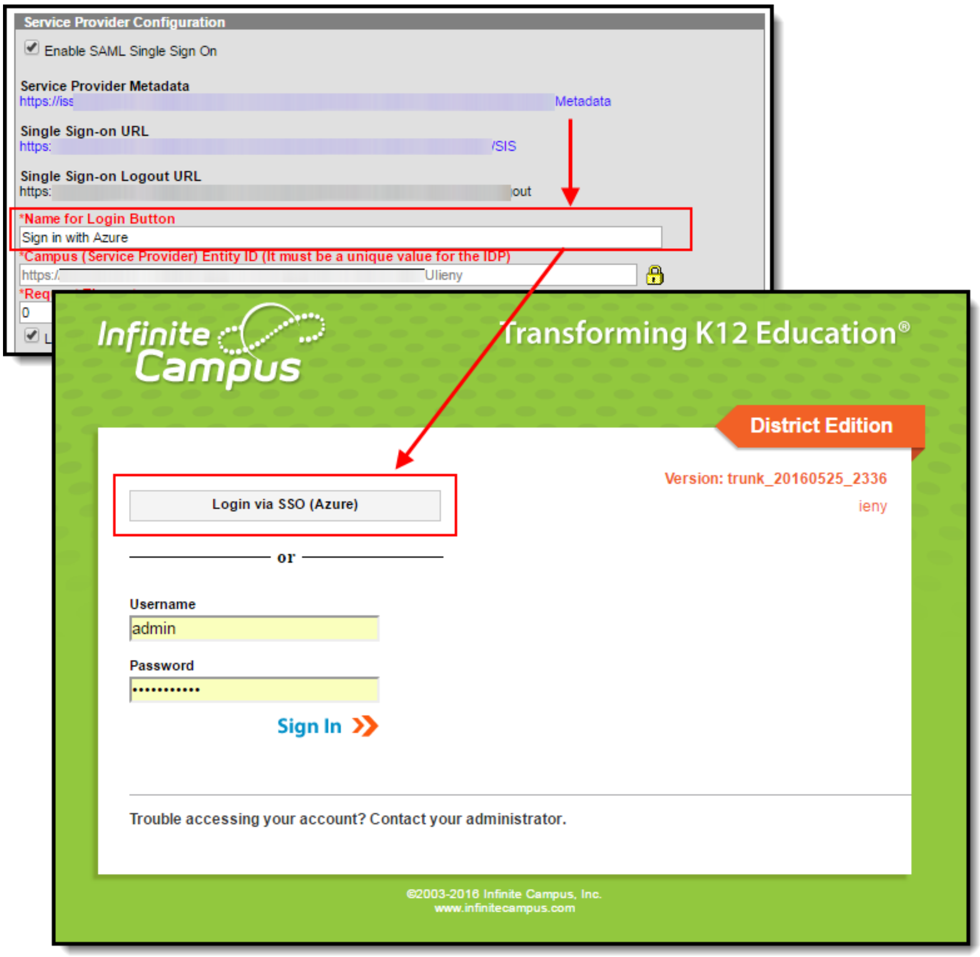
Understanding Service Provider Configuration Fields

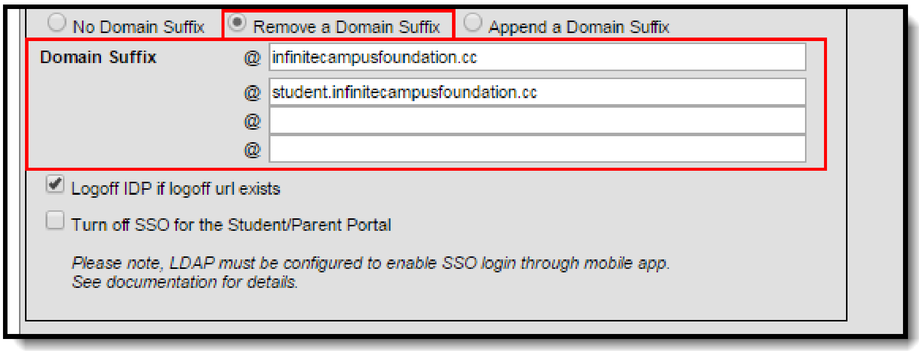
Use the following table to understand each available field.

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.
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 as an XML format and sent to the IDP administrator.

Field	Description
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 process without credentials and once authenticated, will be redirected into the applicable Campus homepage. **Assertion Consumer Service (ACS) URL is the equivalent to 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 Azure AD is one known IDP that requires the local Campus logout URL in order to properly redirect to the Campus logoff page.
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-Azure users. If the decision is made to change the value, the SSO Identity Provider must re-sync the **Service Provider Metadata URL** or reload the Service Provider metadata using the **Service Provider Metadata URL**. For Azure users, this value MUST equal the Azure Client ID.

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 URL ○ Metadata XML file https://dev[redacted] - **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 No file chosen Once a URL or XML file has been entered, click the **Sync** button to load the XML values into Campus.
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 aattribute Campus will use for comparison is the Name ID. This field is required for use with Microsoft Azure AD as the Name ID attribute is reserved by Azure and cannot be used for comparisons. To change this value, click the Lock icon (see image below).  Optional Attribute Name (default is nameID, Required for Azure) name Identity Provider Entity ID https://sts.windows.[redacted]5b34a/ An incorrect Optional Attribute Name value will break the connection between Campus and the IDP.
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	

Field	Description
Name for Login Button	This field indicates what the name of the SSO login button will be named on the Campus login page. For example, in the image below, a value of 'Login via SSO (Azure)' is entered. All users will see a button named this on the Campus login screen and all users with SAML SSO functionality enabled as their authentication method will select this button to log into Campus using their SSO username and password.  Service Provider Configuration ☑ Enable SAML Single Sign On Service Provider Metadata https://iss[redacted]Metadata Single Sign-on URL https:[redacted]/SIS Single Sign-on Logout URL https:[redacted]out *Name for Login Button Sign in with Azure *Campus (Service Provider) Entity ID (It must be a unique value for the IDP) https:/[redacted]Ulieny *Req 0 ☑ L Transforming K12 Education® District Edition Version: trunk_20160525_2336 ieny Login via SSO (Azure) or Username admin Password ••••••••••• Sign In Trouble accessing your account? Contact your administrator. ©2003-2016 Infinite Campus, Inc. www.infinitecampus.com
Request Timeout	Indicates the number of minutes that can pass before a request between Campus and the IDP produces a timeout error.
No Domain Suffix	This options 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 @ student.infinitecampusfoundation.cc @ @ ☑ Logoff IDP if logoff url exists □ Turn off SSO for the Student/Parent Portal *Please note, LDAP must be configured to enable SSO login through mobile app. See documentation for details.*
Append a Domain Suffix	This option allows you 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 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 SSO for the Student/Parent Portal Login Page	Marking this checkbox removes the ability for students and parents to login into the Campus Portal via the SSO login button. These users must log into Portal using their standard Campus username and password.

Field	Description
Identity Provider Signature	
Campus allows for more than one IDP certificate	
Signature Algorithm	The Identity Provider Signature Algorithm as indicated in the IDP 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 Enable and Configure SAML SSO Functionality, Export the Service Provider Certificate, and Delete the Service Provider Certificate 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.

Configuring a Unique Azure Active Directory

The following section will describe configuring a unique Azure Active Directory.

This section is only relevant for Microsoft Azure customers.

Infinite Campus is now available in the Microsoft Azure Marketplace.

- Infinite Campus in the Marketplace: https://azuremarketplace.microsoft.com/en-us/marketplace/apps/aad.infinitecampus?tab=overview
- Azure Active Directory Integration with Campus Tutorial: https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/infinitecampus-tutorial

There are two main actions that need to be taken to ensure Azure has an active connection between Campus and your Azure AD environment;

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

The following sections will walk you through this process:

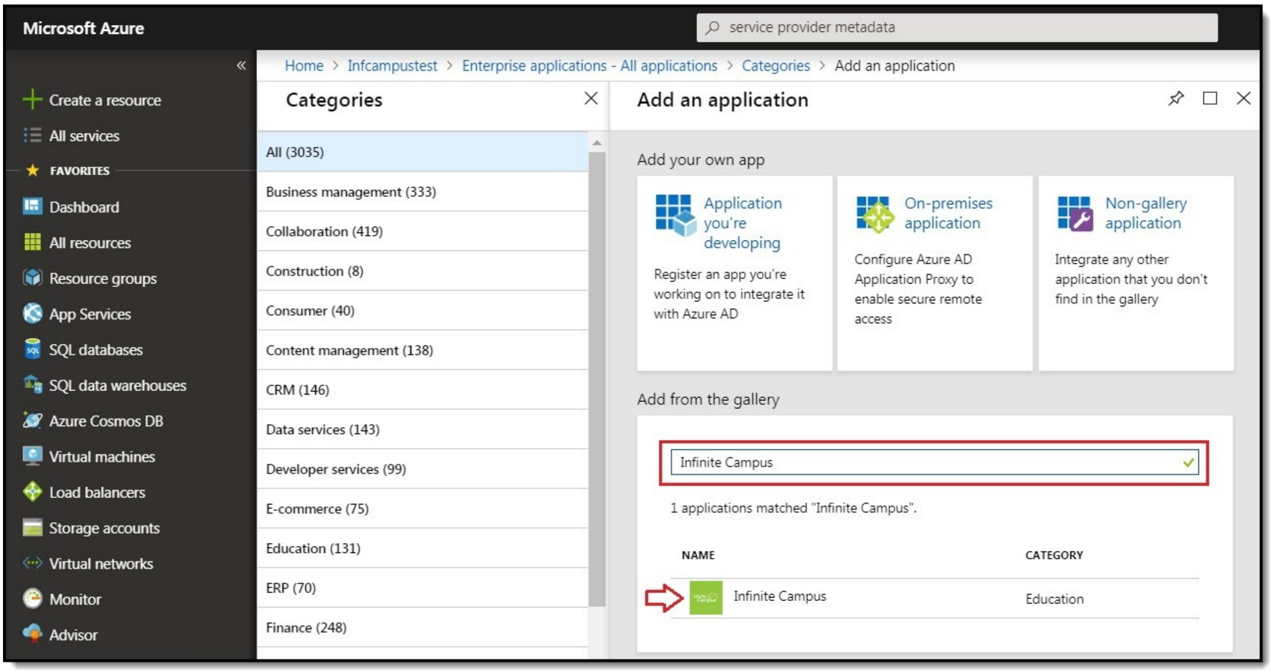
- Infinite Campus Azure Marketplace Workflow
- Add the Infinite Campus Logout URL to the Microsoft Azure SAML SSO Configuration
- Complete a Single Sign-On Login

Infinite Campus Azure Marketplace Workflow

Step 1.

In your Azure 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 (Image 8).



Register an app you're working on to integrate it with Azure AD

Configure Azure AD Application Proxy to enable secure remote access

Integrate any other application that you don't find in the gallery

Infinite Campus ✓

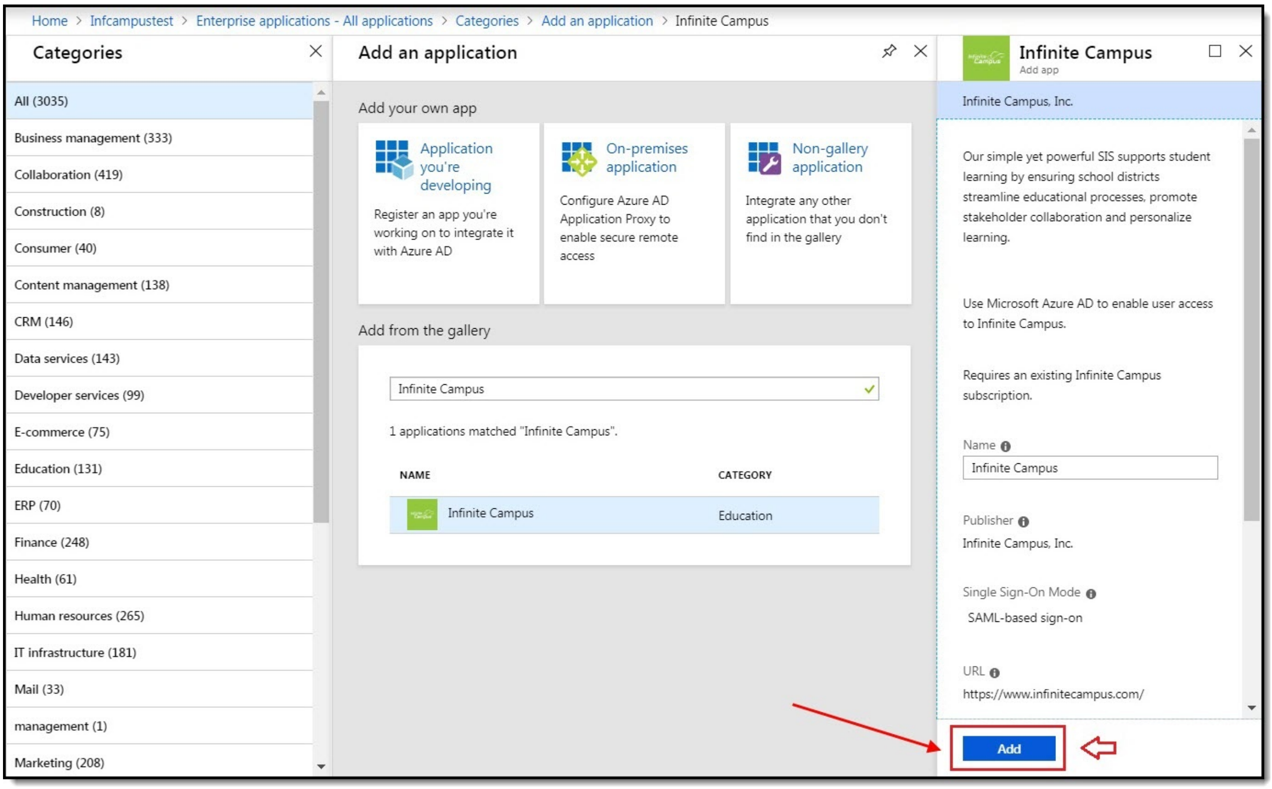
1 applications matched "Infinite Campus".

NAME	CATEGORY
Infinite Campus	Education

Image 8: Azure AD Administrative View of Local Environment Configurations

Step 2.

Click the **Add** button in the lower right-hand corner of the screen (Image 9).



Register an app you're working on to integrate it with Azure AD

Configure Azure AD Application Proxy to enable secure remote access

Integrate any other application that you don't find in the gallery

Infinite Campus ✓

1 applications matched "Infinite Campus".

NAME	CATEGORY
Infinite Campus	Education

Infinite Campus, Inc.

Our simple yet powerful SIS supports student learning by ensuring school districts streamline educational processes, promote stakeholder collaboration and personalize learning.

Use Microsoft Azure AD to enable user access to Infinite Campus.

Requires an existing Infinite Campus subscription.

Name: Infinite Campus

Publisher: Infinite Campus, Inc.

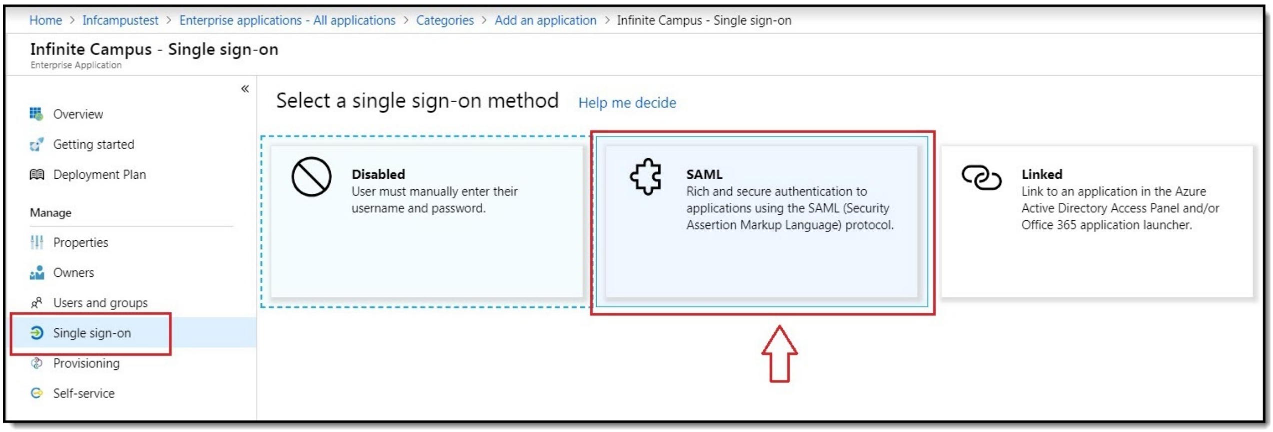
Single Sign-On Mode: SAML-based sign-on

URL: https://www.infinitecampus.com/

Image 9: Azure AD Administrative View of Adding the Infinite Campus Azure Application Configuration

Step 3.

Once the Infinite Campus application has been added to the Azure environment, you will need to configure SAML SSO. Click on the **Single sign-on** button of the Enterprise Application index and select the **SAML** box (Image 10):



Home > Infcampustest > Enterprise applications - All applications > Categories > Add an application > Infinite Campus - Single sign-on
Infinite Campus - Single sign-on
Enterprise Application
«
Overview
Getting started
Deployment Plan
Manage
Properties
Owners
Users and groups
Single sign-on
Provisioning
Self-service
Select a single sign-on method
Help me decide
Disabled
SAML
Linked

User must manually enter their username and password.

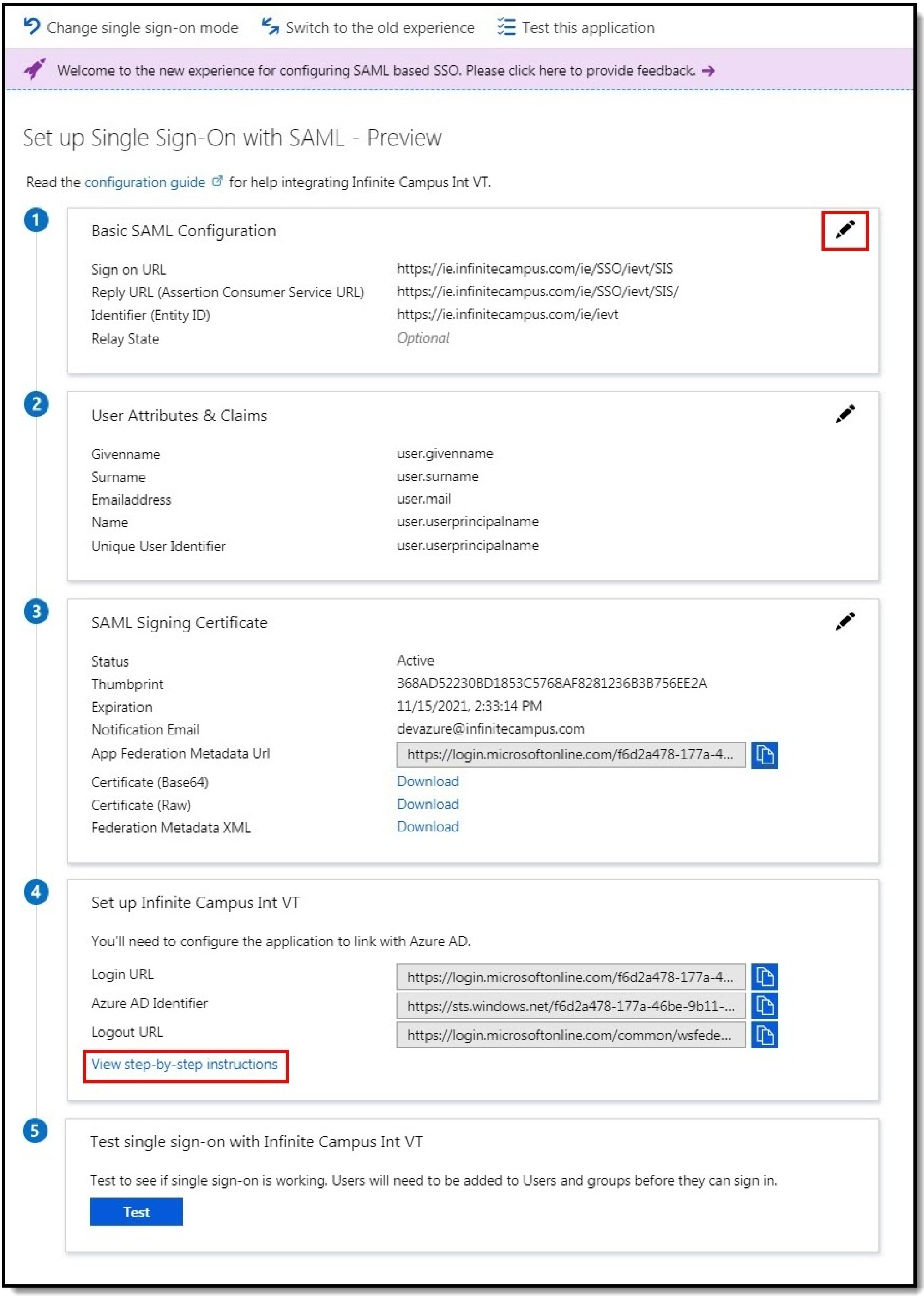
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

Image 10. Adding the SAML SSO Configuration to the Infinite Campus Azure Enterprise Application Configuration

Step 4.

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 (Image 11). Once the data on this page has been reviewed and corrected accordingly, move onto the Add the Infinite Campus Logout URL to the Microsoft Azure SAML SSO Configuration section of this article.



Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback. →

Set up Single Sign-On with SAML - Preview

Read the configuration guide for help integrating Infinite Campus Int VT.

1 Basic SAML Configuration

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*

2 User Attributes & Claims

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate

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

4 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

5 Test single sign-on with Infinite Campus Int VT

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

Image 11: Reviewing the SAML SSO Configuration for the Infinite Campus Application

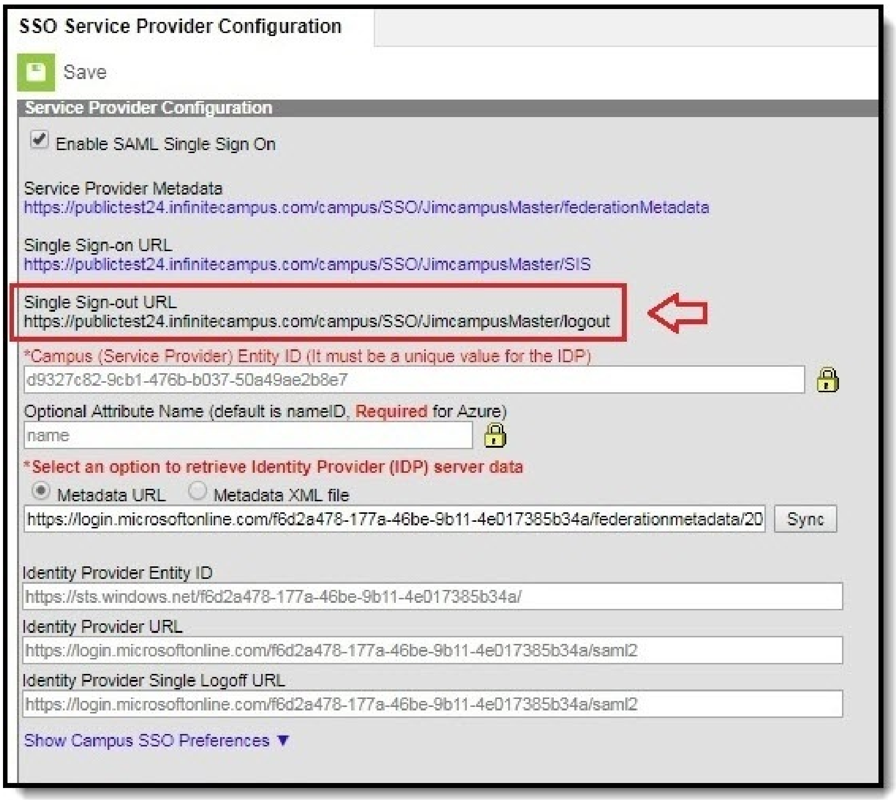
Add the Infinite Campus Logout URL to the Microsoft Azure SAML SSO Configuration

Step 1.

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

The logout URL appears in release Campus.1629 and later.

In the SSO Service Provider Configuration tool, locate the **Single Sign-on Logout URL** and copy this value (Image 12).



SSO Service Provider Configuration

Save

Service Provider Configuration

☑ Enable SAML Single Sign On

Service Provider Metadata
https://publictest24.infinitecampus.com/campus/SSO/JimcampusMaster/federationMetadata

Single Sign-on URL
https://publictest24.infinitecampus.com/campus/SSO/JimcampusMaster/SIS

Single Sign-out URL
https://publictest24.infinitecampus.com/campus/SSO/JimcampusMaster/logout

*Campus (Service Provider) Entity ID (It must be a unique value for the IDP)
d9327c82-9cb1-476b-b037-50a49ae2b8e7

Optional Attribute Name (default is nameID, Required for Azure)
name

*Select an option to retrieve Identity Provider (IDP) server data
● Metadata URL ○ Metadata XML file
https://login.microsoftonline.com/f6d2a478-177a-46be-9b11-4e017385b34a/federationmetadata/20 Sync

Identity Provider Entity ID
https://sts.windows.net/f6d2a478-177a-46be-9b11-4e017385b34a/

Identity Provider URL
https://login.microsoftonline.com/f6d2a478-177a-46be-9b11-4e017385b34a/saml2

Identity Provider Single Logoff URL
https://login.microsoftonline.com/f6d2a478-177a-46be-9b11-4e017385b34a/saml2

Show Campus SSO Preferences ▼

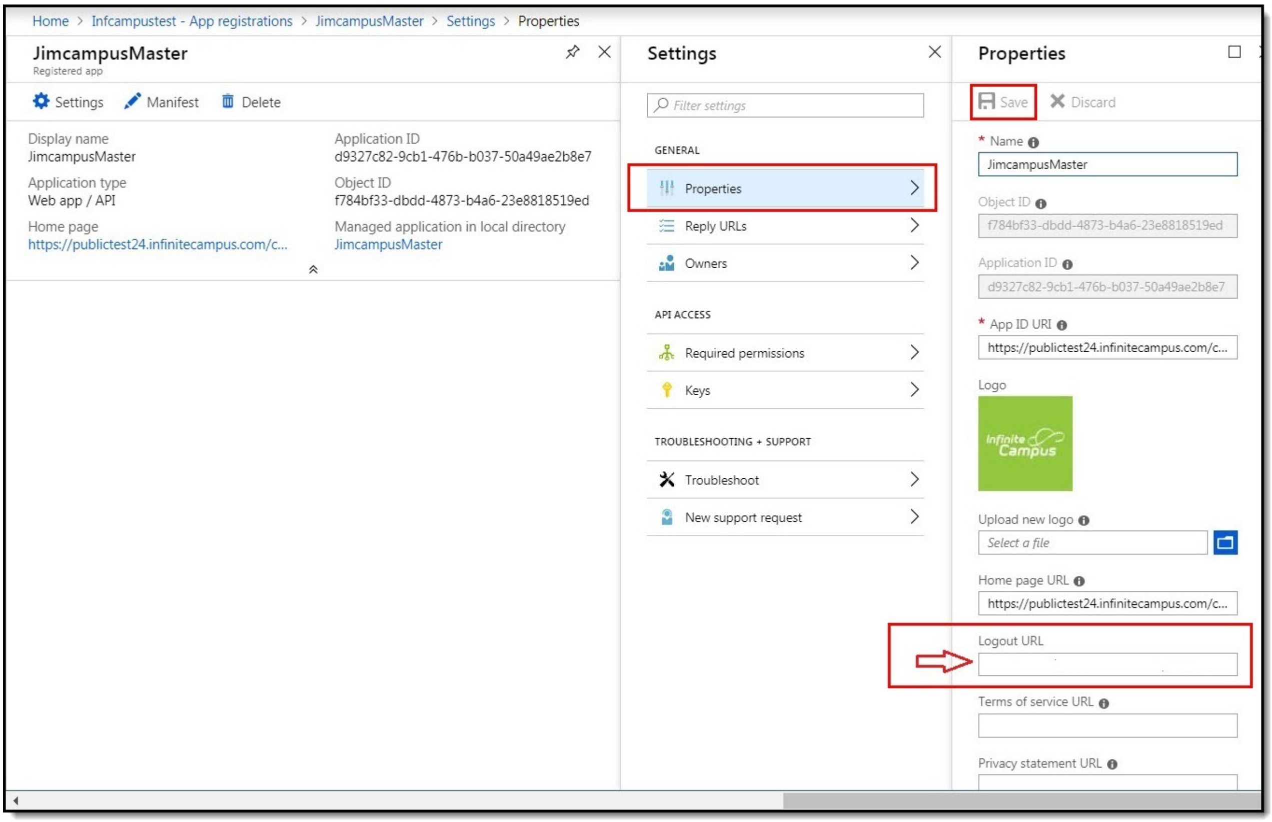
Image 12: Locating the Single Sign-out URL

Step 2.

Next, the Azure AD app registration properties **Logout URL** needs to be updated so the proper re-direct 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. Paste in the Single Sign-out URL value copied from the SSO Service Provider Configuration tool into the **Logout URL** field.
4. Select the **Save** icon.



Display name: JimcampusMaster

Application type: Web app / API

Home page: https://publictest24.infinitecampus.com/c...

Application ID: d9327c82-9cb1-476b-b037-50a49ae2b8e7

Object ID: f784bf33-dbdd-4873-b4a6-23e8818519ed

Managed application in local directory: JimcampusMaster

* Name: JimcampusMaster

Object ID: f784bf33-dbdd-4873-b4a6-23e8818519ed

Application ID: d9327c82-9cb1-476b-b037-50a49ae2b8e7

* App ID URI: https://publictest24.infinitecampus.com/c...

Home page URL: https://publictest24.infinitecampus.com/c...

Logout URL:

Terms of service URL:

Privacy statement URL:

Image 13: Establishing the Logout URL

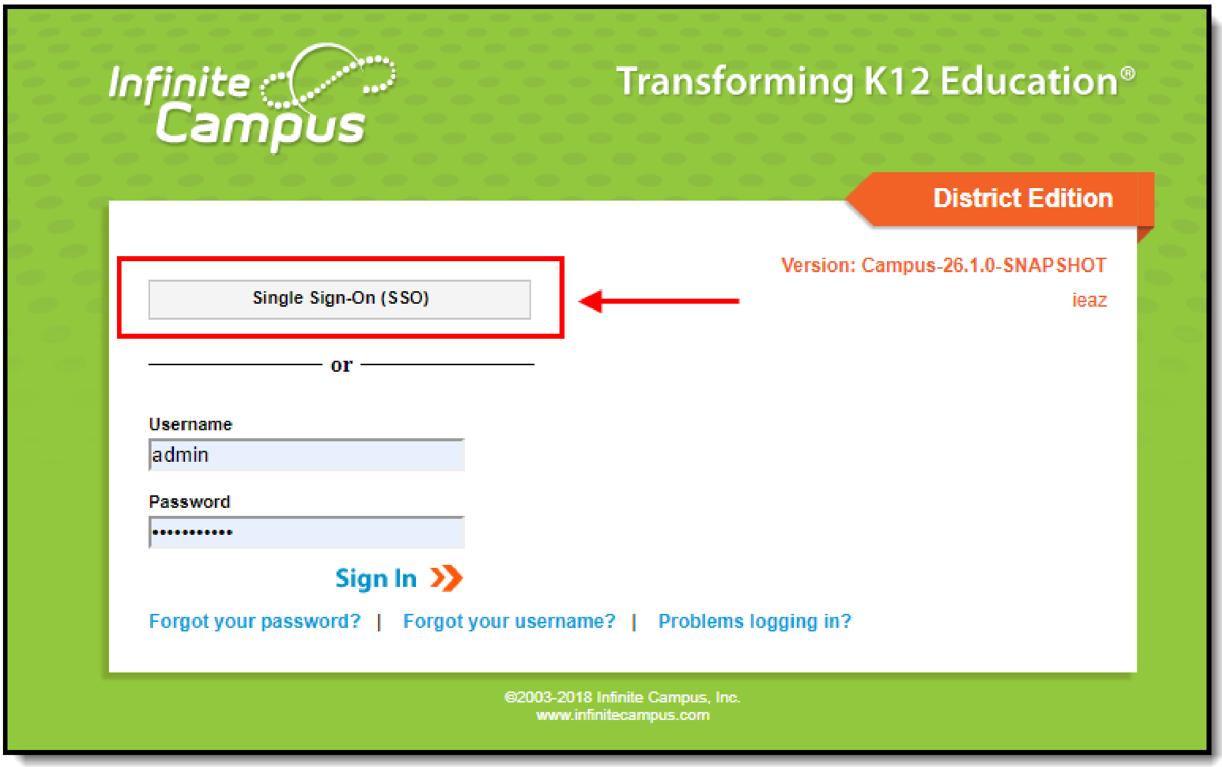
Complete a Single Sign-On Login

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

To login, 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). The image below is for example purposes only.

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



Infinite Campus Transforming K12 Education®

District Edition

Version: Campus-26.1.0-SNAPSHOT
ieaz

Single Sign-On (SSO)

or

Username: admin

Password: •••••••••••

Sign In

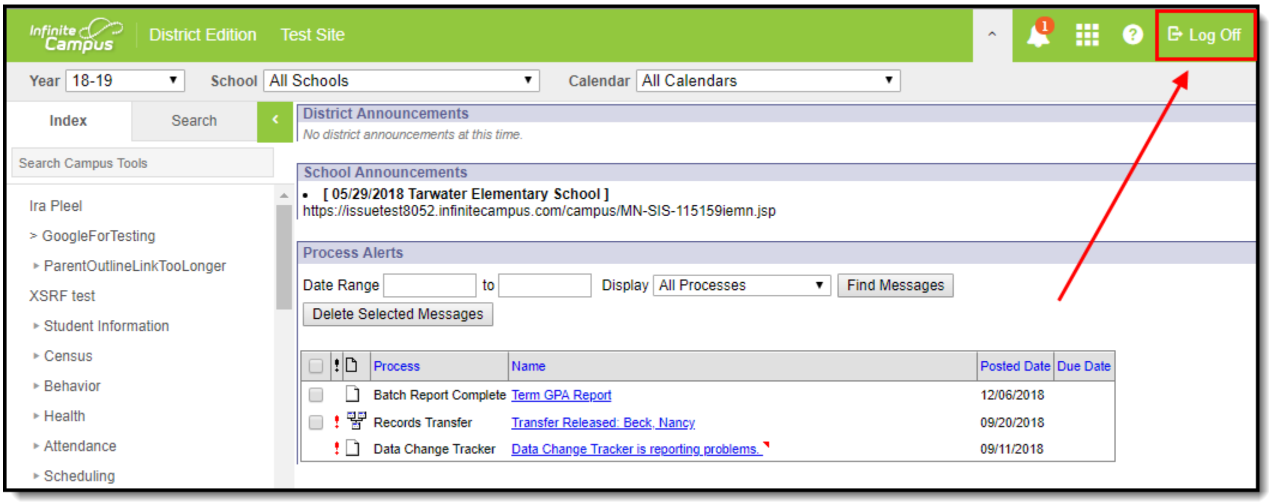
Forgot your password? | Forgot your username? | Problems logging in?

©2003-2018 Infinite Campus, Inc.
www.infinitecampus.com

Image 14: Logging into Campus via SSO

To log out of Campus, click the **Log Off** button in the upper right corner of the page (see Image 15).

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



Year 18-19 School All Schools Calendar All Calendars

District Announcements
No district announcements at this time.

School Announcements
- [05/29/2018 Tarwater Elementary School]
https://issuetest8052.infinitecampus.com/campus/MN-SIS-115159iemn.jsp

Process Alerts

Date Range ____ to ____ Display All Processes Find Messages

Delete Selected Messages

□	!		Process	Name	Posted Date	Due Date
□			Batch Report Complete	Term GPA Report	12/06/2018	
□	!		Records Transfer	Transfer Released: Beck, Nancy	09/20/2018	
	!		Data Change Tracker	Data Change Tracker is reporting problems.	09/11/2018	

Image 15: Logging Out of Campus

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 configuring the Google IDP to utilize Campus SSO functionality.

Prerequisites

- You need a Google Admin account.
- Expand the **Campus SSO Preferences** area:
    - 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.
    - Set the **Request Timeout**. This field indicates the number of minutes that can pass before a request between Campus and the IDP produces a timeout error.

Step 1.

Log into your Google Administrator account (https://admin.google.com) and select **Apps** (Image 16).

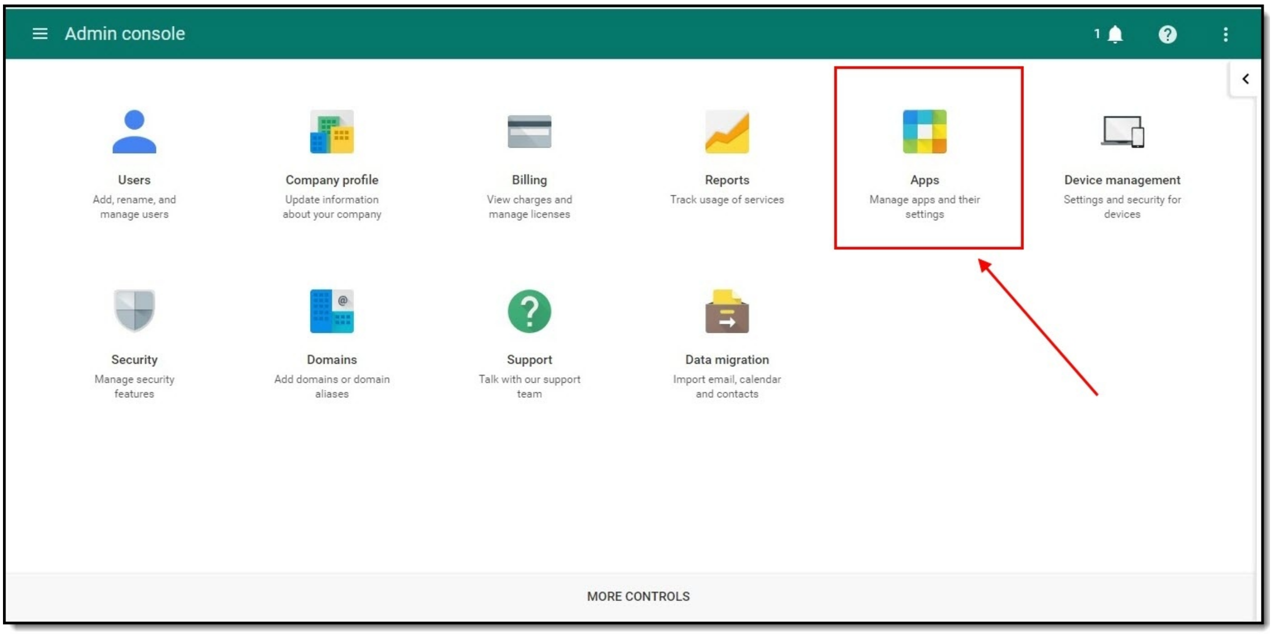

Admin console
Users
Add, rename, and manage users
Company profile
Update information about your company
Billing
View charges and manage licenses
Reports
Track usage of services
Apps
Manage apps and their settings
Device management
Settings and security for devices
Security
Manage security features
Domains
Add domains or domain aliases
Support
Talk with our support team
Data migration
Import email, calendar and contacts
MORE CONTROLS

Image 16: Selecting Apps

Step 2.

Select **SAML apps** (Image 17).

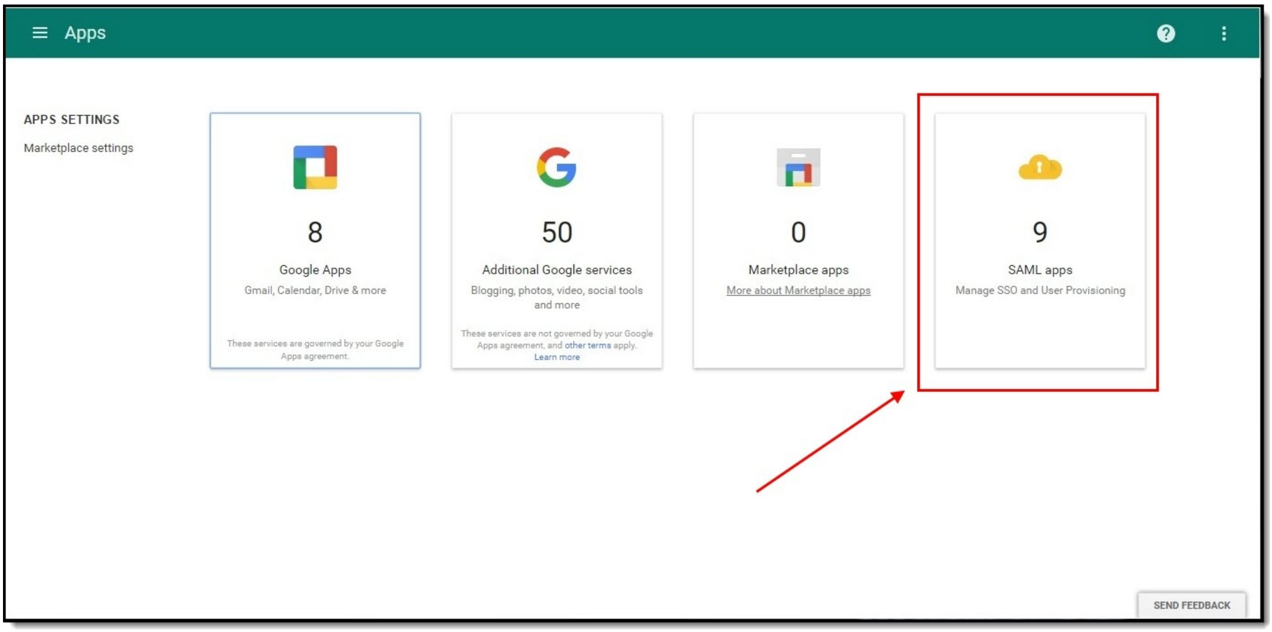
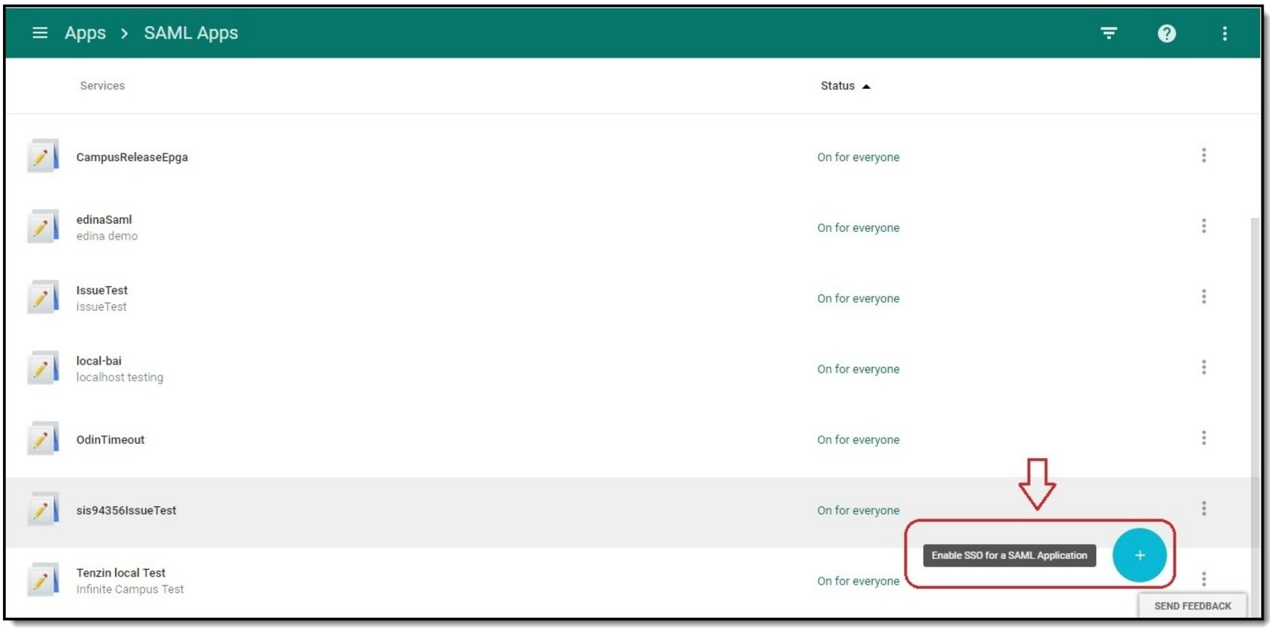

Apps
APPS SETTINGS
Marketplace settings
8
Google Apps
Gmail, Calendar, Drive & more
These services are governed by your Google Apps agreement.
50
Additional Google services
Blogging, photos, video, social tools and more
These services are not governed by your Google Apps agreement, and other terms apply.
Learn more
0
Marketplace apps
More about Marketplace apps
9
SAML apps
Manage SSO and User Provisioning
SEND FEEDBACK

Image 17: Select SAML Apps

Step 3.

Click the plus sign (+) labeled **Enable SSO for a SAML Application** (Image 18).



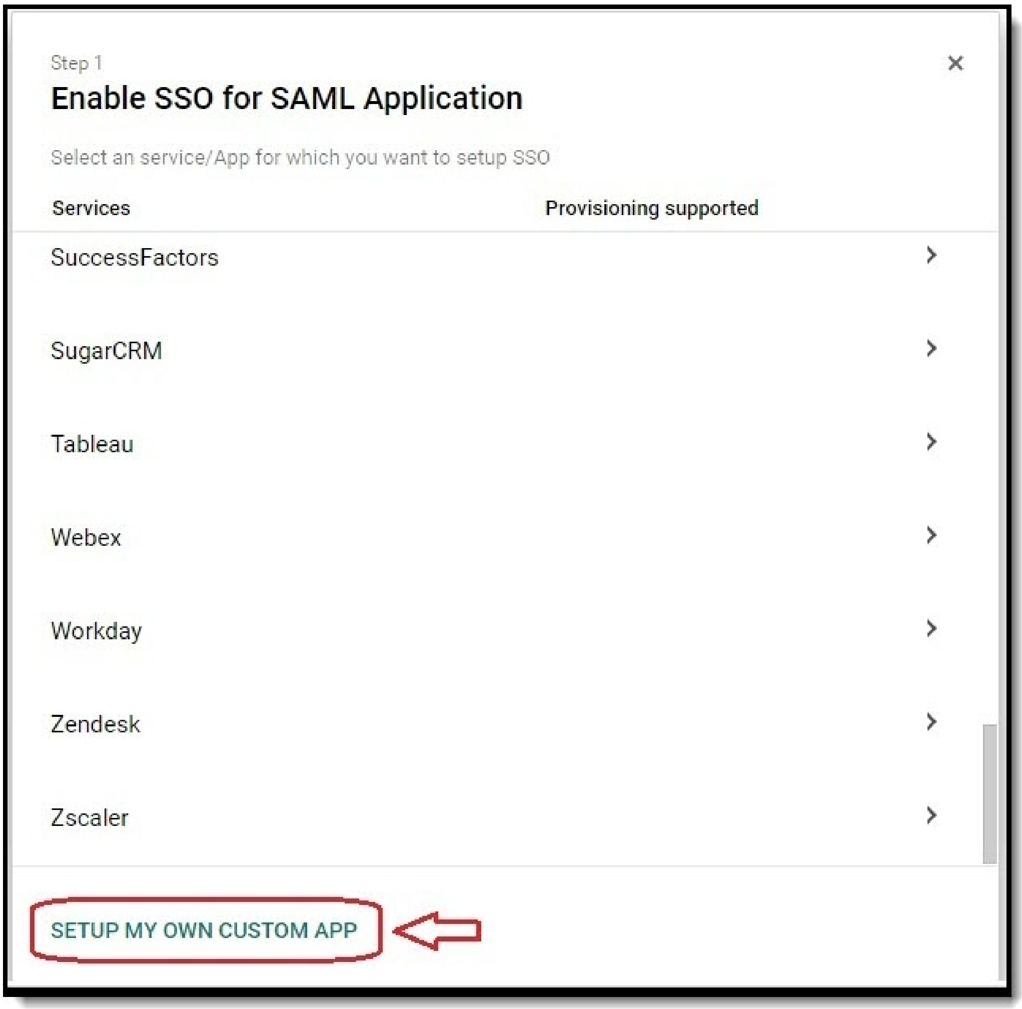
Services	Status
CampusReleaseEpga	On for everyone
edinaSaml edina demo	On for everyone
IssueTest issueTest	On for everyone
local-bai localhost testing	On for everyone
OdinTimeout	On for everyone
sis94356IssueTest	On for everyone
Tenzin local Test Infinite Campus Test	On for everyone

Enable SSO for a SAML Application +

Image 18: Enable SSP for a SAML Application

Step 4.

Select **Setup My Own Custom App** (Image 19).



Step 1

Enable SSO for SAML Application

Select an service/App for which you want to setup SSO

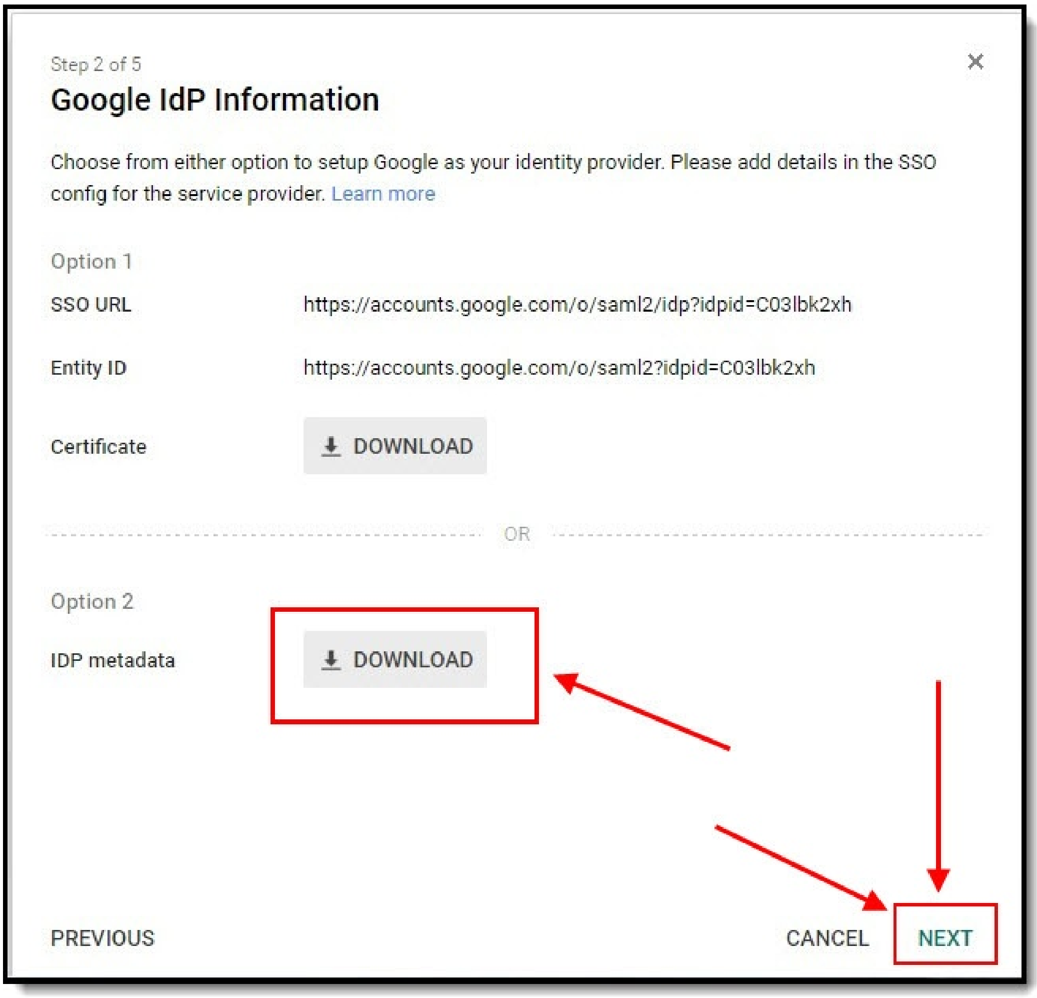
Services	Provisioning supported
SuccessFactors	
SugarCRM	
Tableau	
Webex	
Workday	
Zendesk	
Zscaler	

Image 19: Setup a Custom App

Step 5.

Click the **Download** button for Option 2 and download the Google IDP metadata (Image 20). The file will download to your local hard drive. Remember where this file is located as we will need to use it in Step 6.

Click the **Next** button.



Step 2 of 5

Google IdP Information

Choose from either option to setup Google as your identity provider. Please add details in the SSO config for the service provider. Learn more

Option 1

SSO URL https://accounts.google.com/o/saml2/idp?idpid=C03lbk2xh

Entity ID https://accounts.google.com/o/saml2?idpid=C03lbk2xh

Certificate

Option 2

IDP metadata

Image 20: Download IDP Metadata

Step 6.

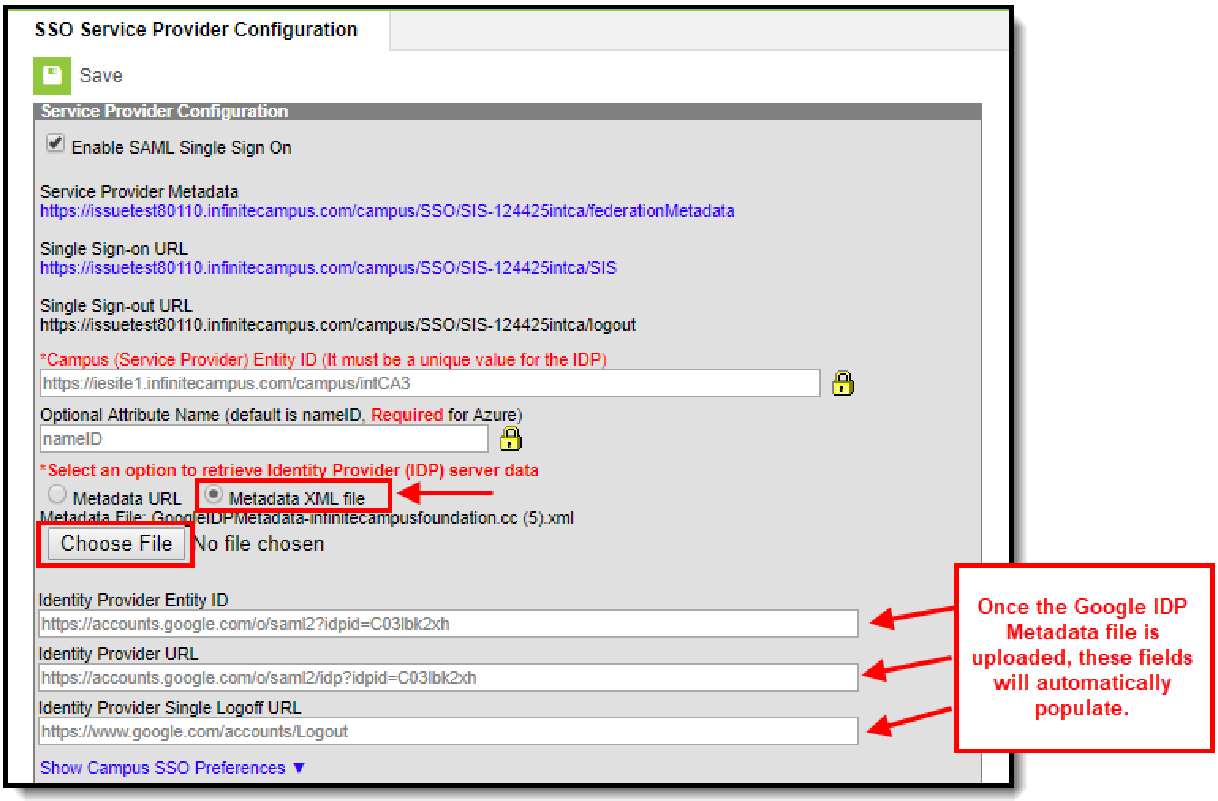
Open Campus in a different tab and navigate to the SSO Service Provider Configuration tool (System Administration > User Security > SAML Management > SSO Service Provider Configuration).

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 (Image 21).

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.



SSO Service Provider Configuration

Save

Service Provider Configuration

☑ Enable SAML Single Sign On

Service Provider Metadata
https://issuetest80110.infinitecampus.com/campus/SSO/SIS-124425intca/federationMetadata

Single Sign-on URL
https://issuetest80110.infinitecampus.com/campus/SSO/SIS-124425intca/SIS

Single Sign-out URL
https://issuetest80110.infinitecampus.com/campus/SSO/SIS-124425intca/logout

*Campus (Service Provider) Entity ID (It must be a unique value for the IDP)
https://iesite1.infinitecampus.com/campus/intCA3

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
https://accounts.google.com/o/saml2?idpid=C03lbk2xh

Identity Provider URL
https://accounts.google.com/o/saml2/idp?idpid=C03lbk2xh

Identity Provider Single Logoff URL
https://www.google.com/accounts/Logout

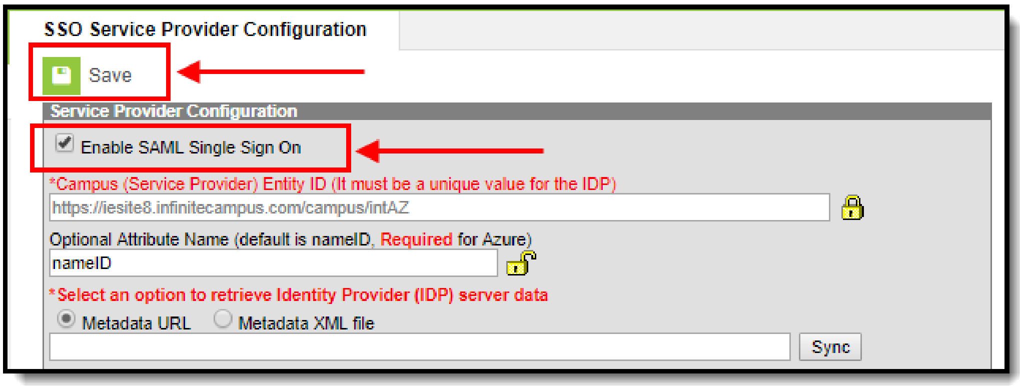
Show Campus SSO Preferences ▼

Once the Google IDP Metadata file is uploaded, these fields will automatically populate.

Image 21: Uploading the Metadata File

Step 7.

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



SSO Service Provider Configuration

Save

Service Provider Configuration

☑ Enable SAML Single Sign On

*Campus (Service Provider) Entity ID (It must be a unique value for the IDP)
https://iesite8.infinitecampus.com/campus/intAZ

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

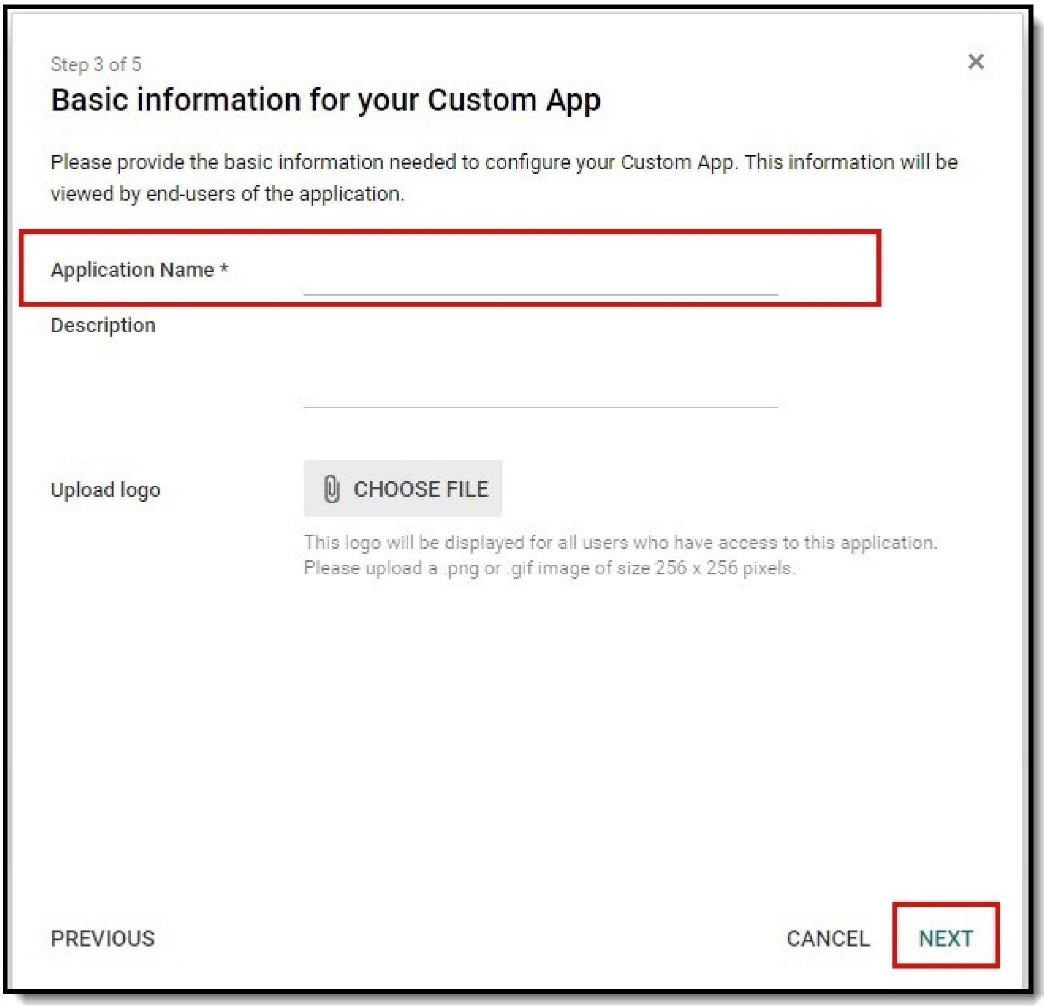
Sync

Image 22: Enable and Save the SSO Configuration

Step 8.

Go back to your Google Admin tab. You should be on the **Basic Information for your Custom App** screen (see image below). Enter an **Application Name** of 'Infinite Campus' and upload an image that will display within the Google App launcher (optional). When finished, click **Next**.

An example of a logo you can use:



Step 3 of 5

Basic information for your Custom App

Please provide the basic information needed to configure your Custom App. This information will be viewed by end-users of the application.

Application Name *

Description

Upload logo

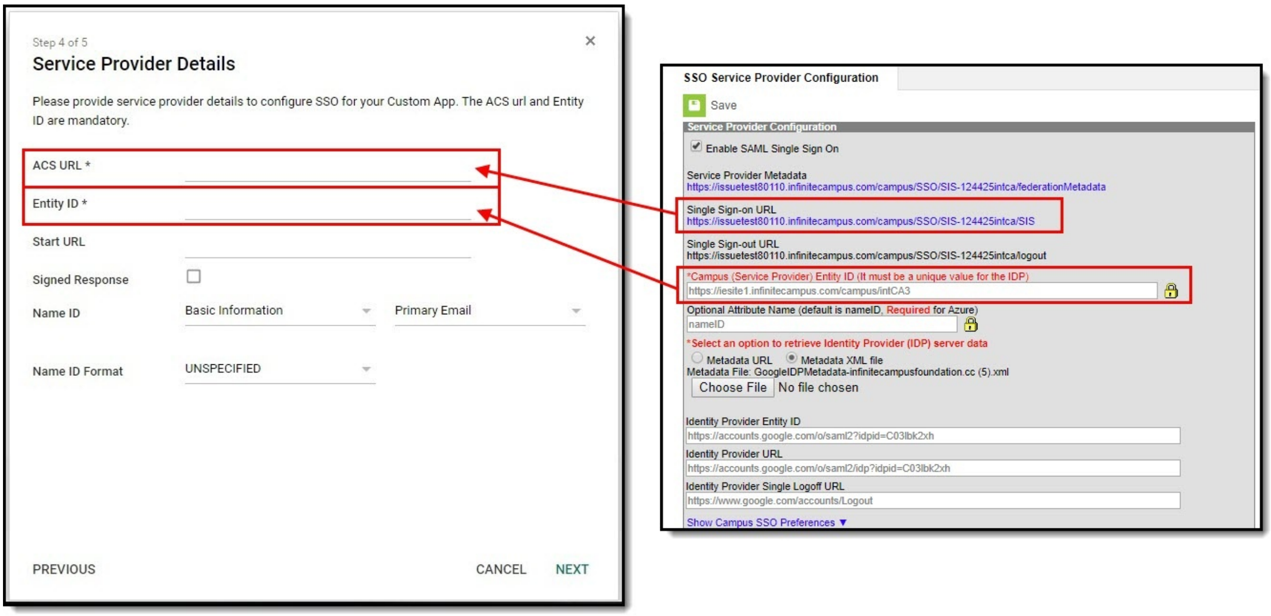
This logo will be displayed for all users who have access to this application. Please upload a .png or .gif image of size 256 x 256 pixels.

Image 23: Enter an Application Name

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 (see image below).
3. Click **Next**.



Step 4 of 5

Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL *

Entity ID *

Start URL

Signed Response □

Name ID: Basic Information | Primary Email

Name ID Format: UNSPECIFIED

SSO Service Provider Configuration

Service Provider Configuration

☑ Enable SAML Single Sign On

Service Provider Metadata
https://issuetest80110.infinitecampus.com/campus/SSO/SIS-124425intca/federationMetadata

Single Sign-on URL
https://issuetest80110.infinitecampus.com/campus/SSO/SIS-124425intca/SIS

Single Sign-out URL
https://issuetest80110.infinitecampus.com/campus/SSO/SIS-124425intca/logout

*Campus (Service Provider) Entity ID (It must be a unique value for the IDP)
https://iesite1.infinitecampus.com/campus/intCA3

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

Identity Provider Entity ID
https://accounts.google.com/o/saml2?idpid=C03lbk2xh

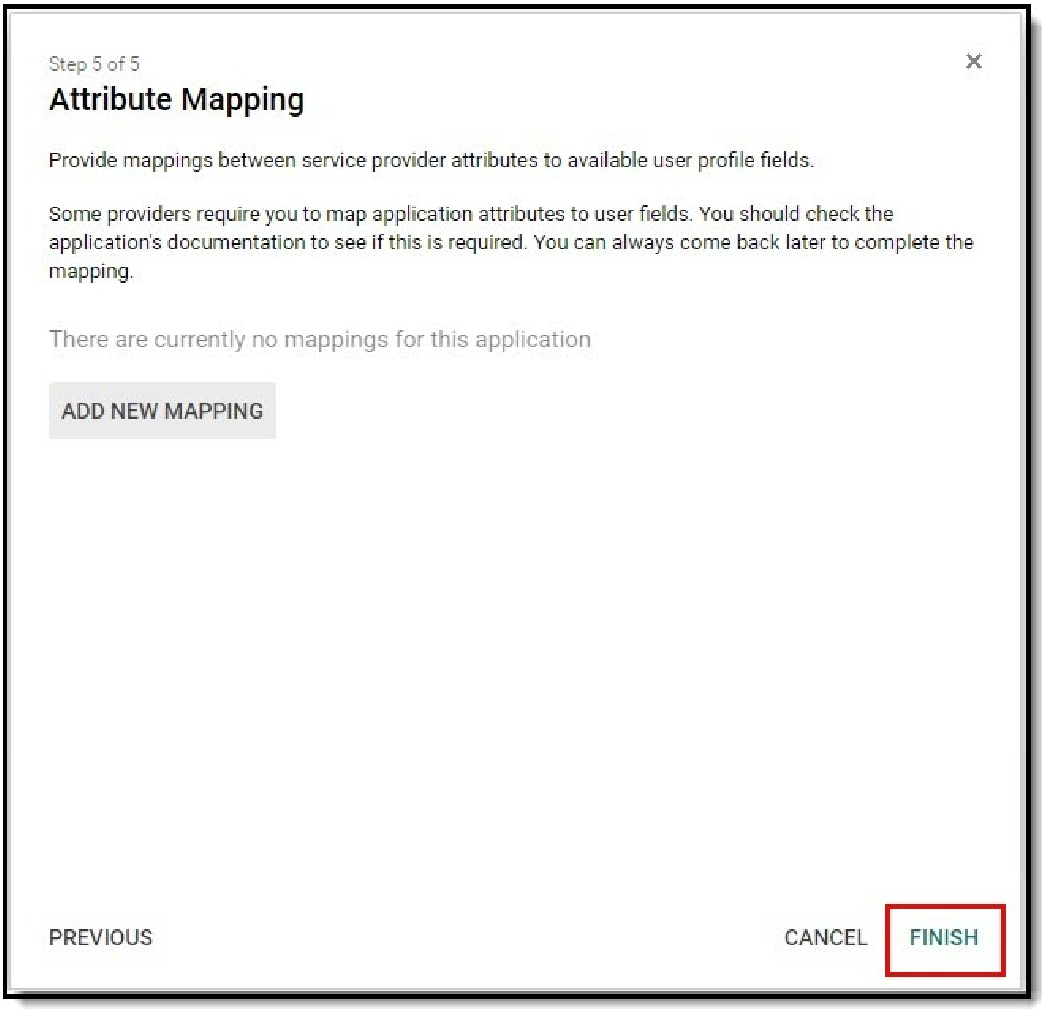
Identity Provider URL
https://accounts.google.com/o/saml2/idp?idpid=C03lbk2xh

Identity Provider Single Logoff URL
https://www.google.com/accounts/Logout

Image 24: Service Provider Details

Step 10.

Click **Finish** on the Attribute Mapping screen.



Step 5 of 5

Attribute Mapping

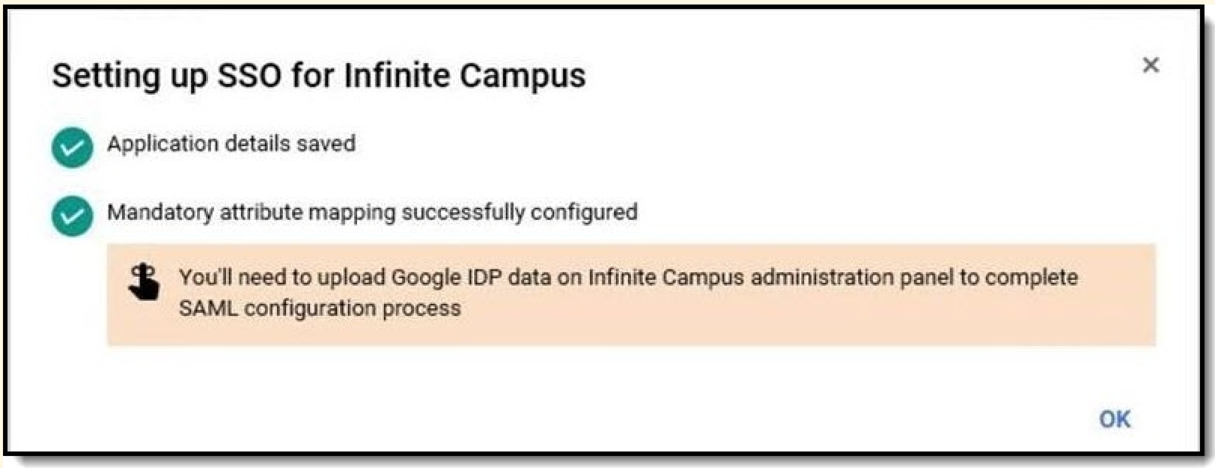
Provide mappings between service provider attributes to available user profile fields.

Some providers require you to map application attributes to user fields. You should check the application's documentation to see if this is required. You can always come back later to complete the mapping.

There are currently no mappings for this application

Image 25: Finish Setup

You may see the following message after hitting the **Finish** button. You can ignore this message.



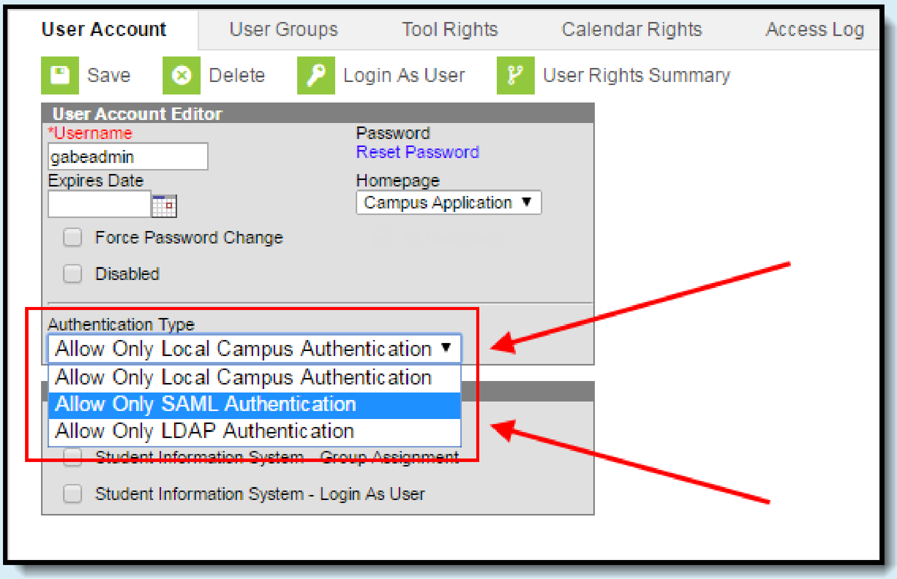
Setting up SSO for Infinite Campus

✓ Application details saved

✓ Mandatory attribute mapping successfully configured

You'll need to upload Google IDP data on Infinite Campus administration panel to complete SAML configuration process

Individual students and staff can have their authentication type modified via the User Account tab (see image below). This is a good method for testing it out using a few users before enabling it for all staff and students.



User Account Editor

*Username: gabeadmin

Expires Date

Password: Reset Password

Homepage: Campus Application

□ Force Password Change

□ Disabled

Authentication Type: Allow Only Local Campus Authentication

- Allow Only Local Campus Authentication
- Allow Only SAML Authentication
- Allow Only LDAP Authentication

□ Student Information System - Group Assignment

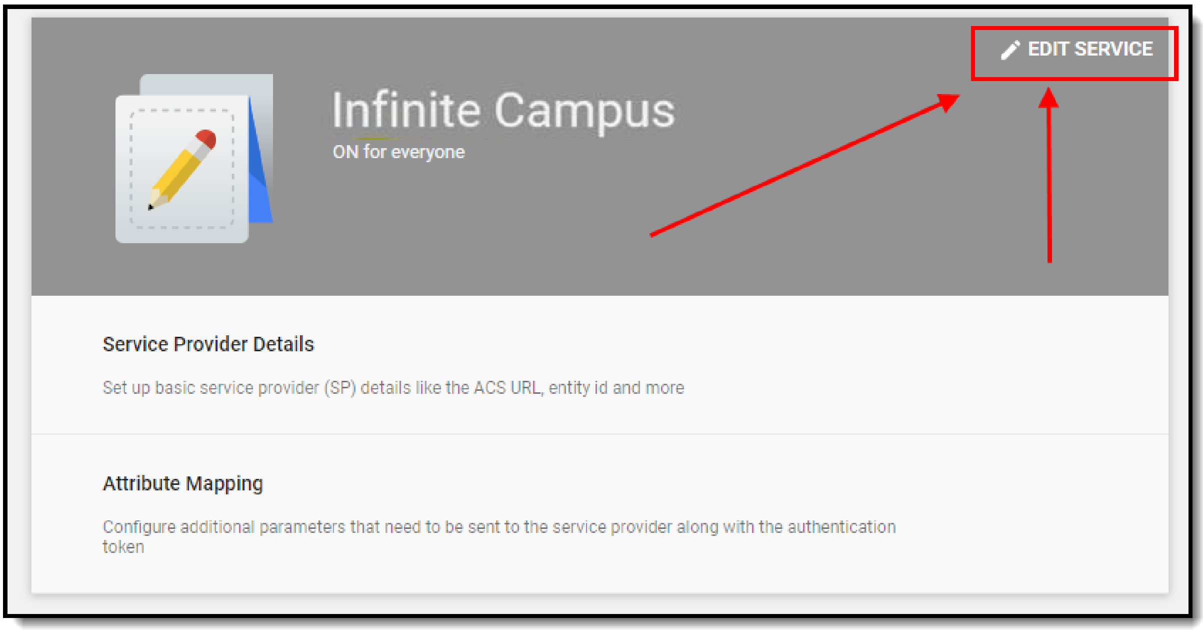
□ Student Information System - Login As User

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

Step 10.

The final step is to turn on the service within Google.

1. Navigate to Apps > SAML Apps and locate your Infinite Campus app.
2. Enter the configuration screen for the Campus app.
3. Click the **Edit Service** button (see below).



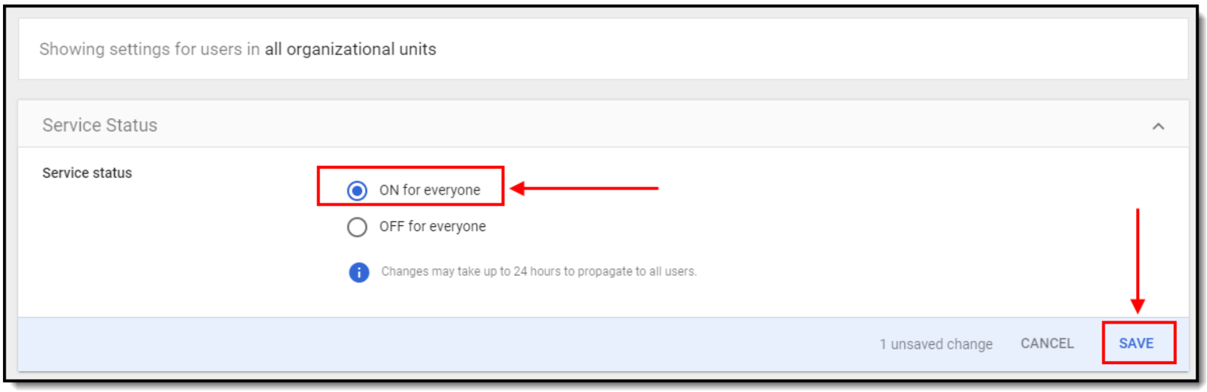
Service Provider Details

Set up basic service provider (SP) details like the ACS URL, entity id and more

Attribute Mapping

Configure additional parameters that need to be sent to the service provider along with the authentication token

4. Under Service Status, mark the **ON for everyone** radio button and click **Save** (see image below).



Showing settings for users in all organizational units

Service Status

Service status

● ON for everyone

○ OFF for everyone

Changes may take up to 24 hours to propagate to all users.

5. That's it! Google and Campus should now be properly connected.

> By default, Google SSO matches based on username.