SSO Service Provider Configuration

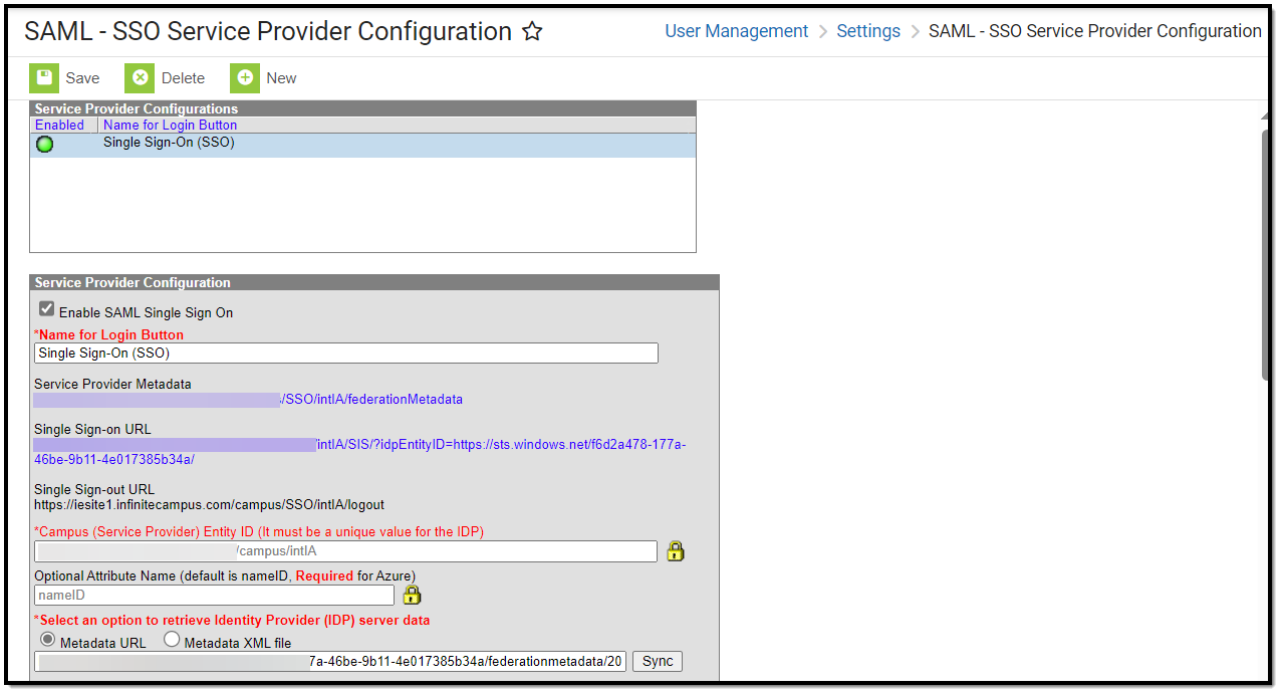
Last Modified on 06/06/2024 2:37 pm CDT

Tool Search: SSO Service Provider Configuration

The SSO Service Provider Configuration tool allows you to configure and enable SSO authentication(s) 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.

Copyright © 2010-2024 Infinite Campus. All rights reserved.



Only users assigned a Product Security Role 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:

- 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 an SSO-enabled account; however, it is important to note that the SSO authentication only occurs once. Users will be required to log back 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 they may encounter.

Copyright © 2010-2024 Infinite Campus. All rights reserved.

The district system administrator's account SHOULD NOT only authenticate through SSO. He/she should have two accounts: one account that authenticates through SSO and a backup account set to authenticate using Local Campus Authentication in the event the SSO IDP's service is unavailable.

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

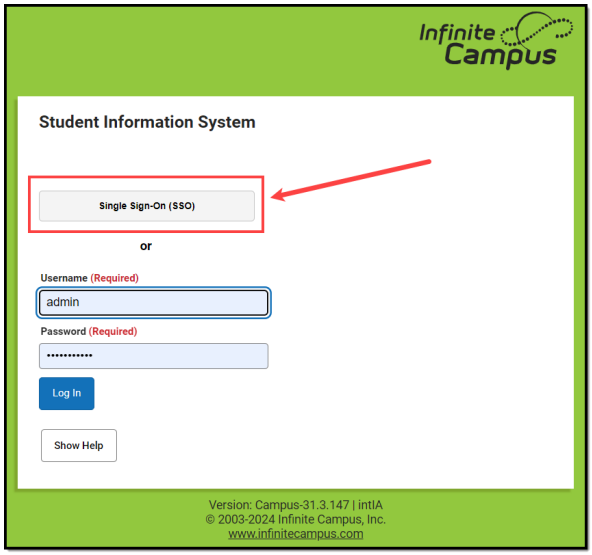
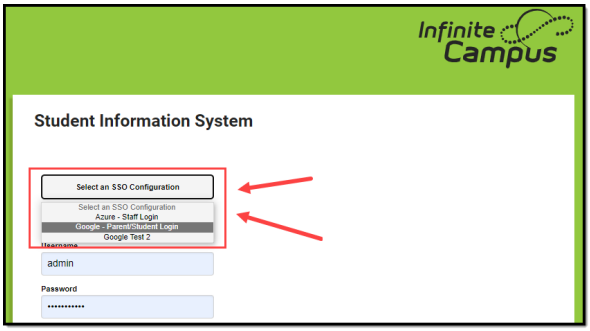
The first step in configuring SAML SSO is to enable SAML SSO functionality, define the Login button and sync IDP server metadata.

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.

Copyright © 2010-2024 Infinite Campus. All rights reserved.

One Enabled/Visible SSO Configuration	Two or More Enabled/Visible SSO Configurations
	

NOTE: Users are highly encouraged to give the button a name recognizable for 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. If connecting Campus to Microsoft Azure, the **Optional Attribute Name,** leave this field as **nameID**. 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**.

   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.

6. If the **Metadata URL** was entered, hit the **Sync** button. This will populate Identity Provider fields below.

7. Expand the **Campus SSO Preferences** area and set the **Request Timeout**. This field

Copyright © 2010-2024 Infinite Campus. All rights reserved.

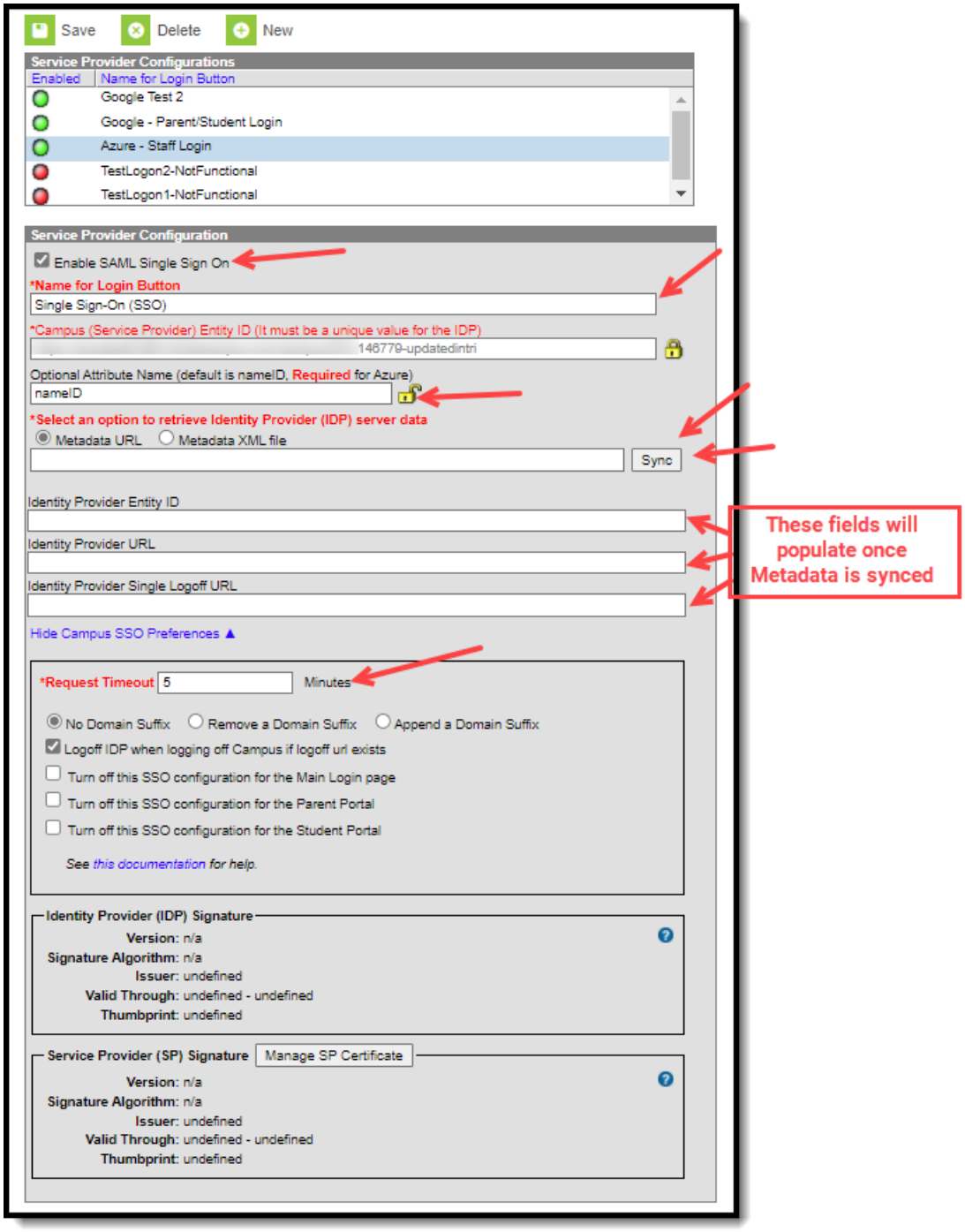
indicates the number of minutes that can pass before a request between Infinite Campus and the IDP produces a timeout error.

8. 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).

9. Move on to Step 2.

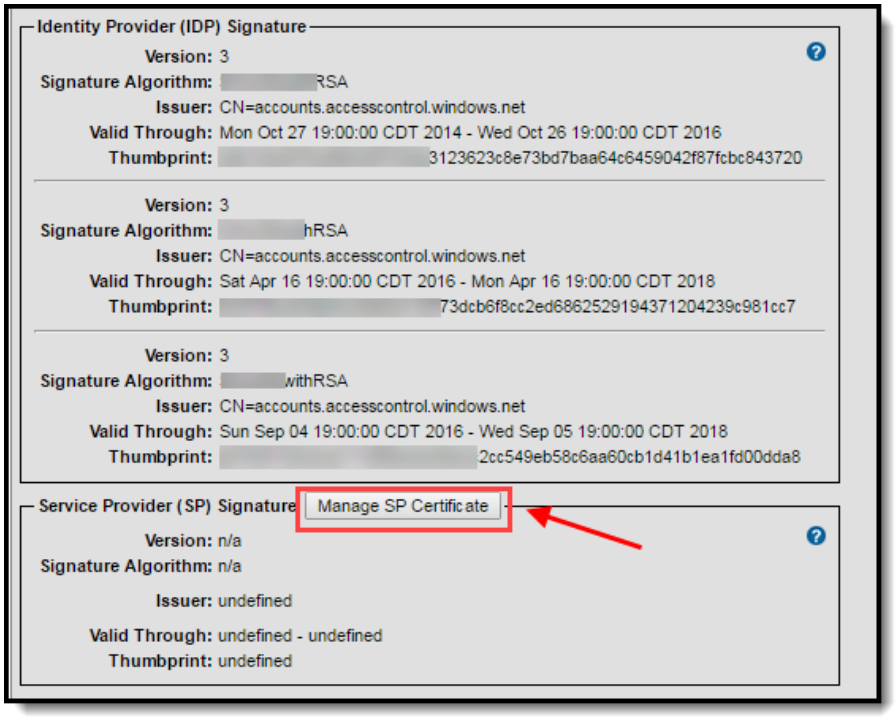
Copyright © 2010-2024 Infinite Campus. All rights reserved.



Step 2. Generate or Upload the Service Provider Certificate

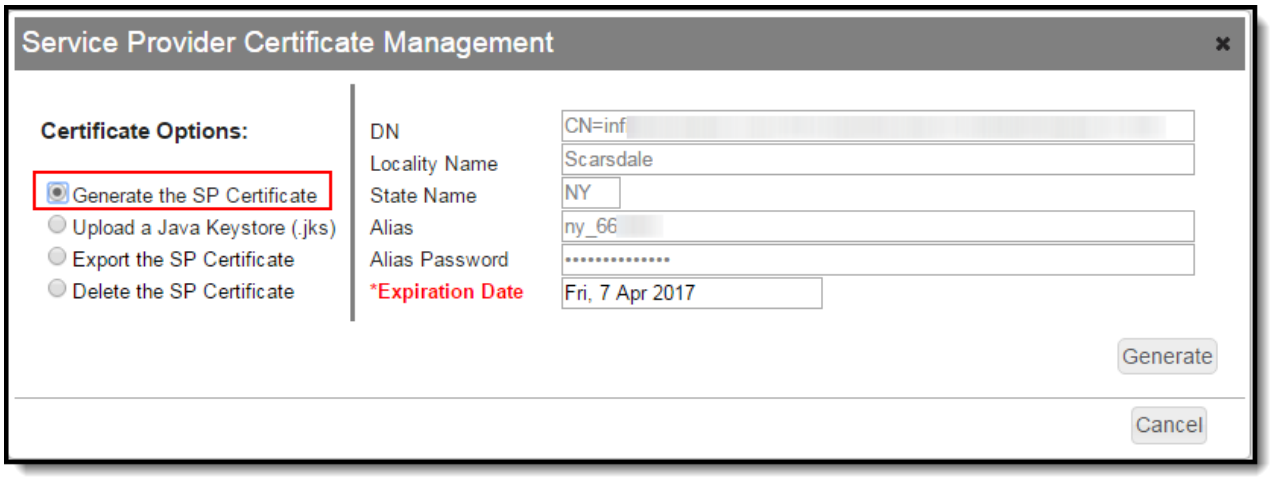
You must now generate or upload the Service Provider Certificate. To do this, click the **Manage SP Certificate** button.

Copyright © 2010-2024 Infinite Campus. All rights reserved.



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:

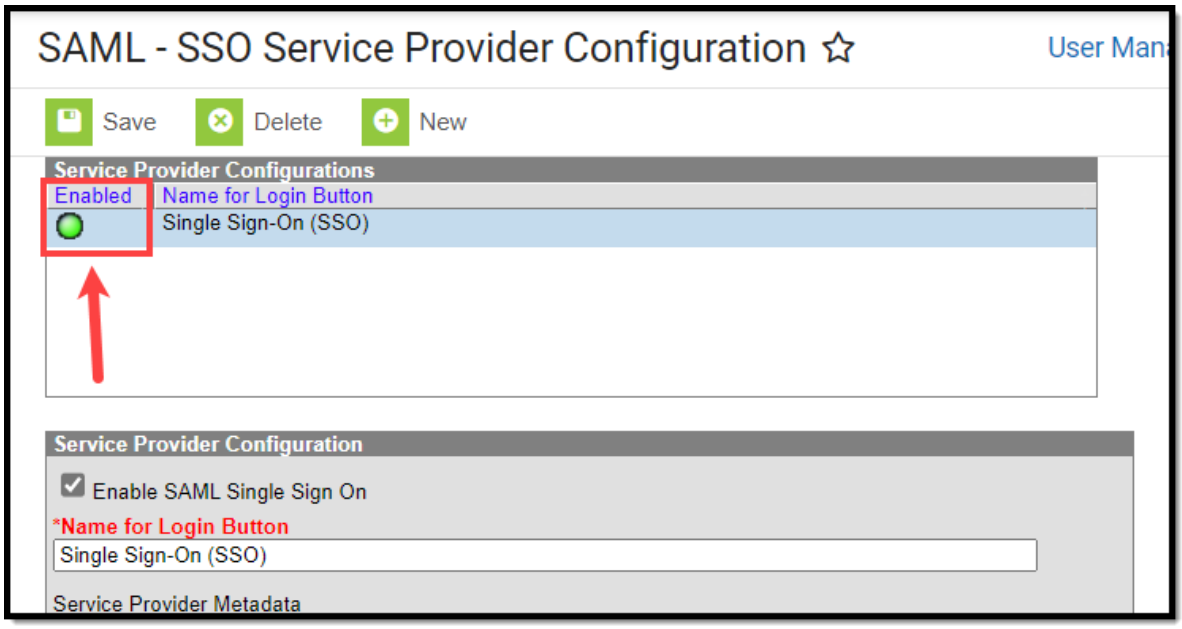


1. Click the **Generate the SP Certificate** radio button.
2. Enter an **Expiration Date**. This is the date in which the certificate will expire and will no longer be valid. This field defaults to one year from the current date.
3. Click the **Generate** button. Fields within the Service Provider SP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

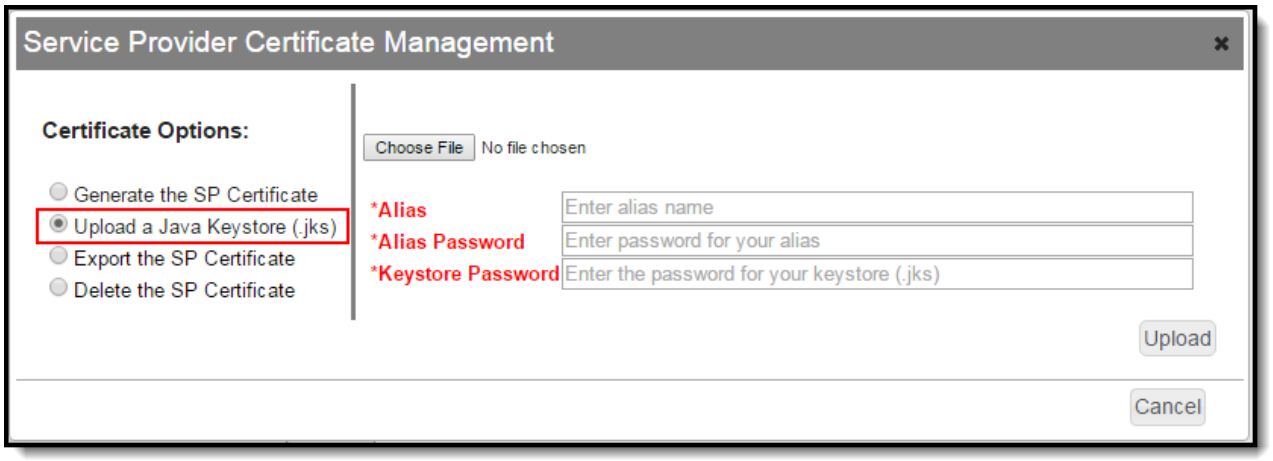
> If a Service Provider certificate already exists within Campus, generating a new Service Provider certificate will automatically overwrite any existing certificate and associated data.

Copyright © 2010-2024 Infinite Campus. All rights reserved.

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).



To upload the Service Provider certificate:



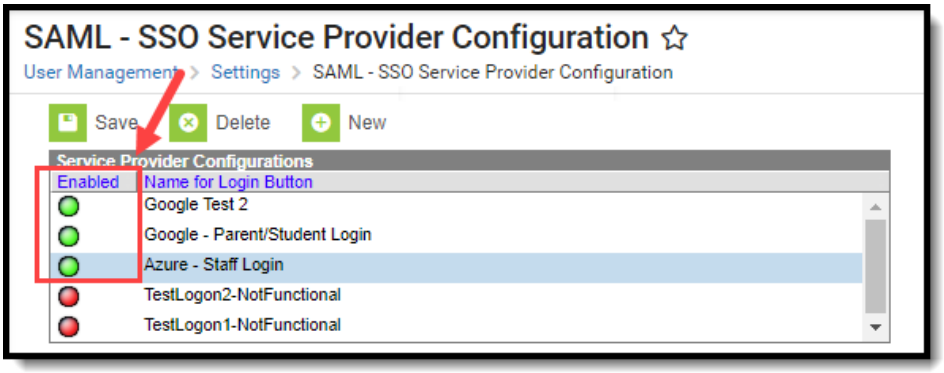
1. Click the **Upload a Java Keystore (.jks)** radio button.
2. Click the **Choose File** button and locate the .jks file from your local hard drive or network.
3. Once the file is selected, click the **Upload** button. Fields within the Service Provider SP (Signature) section of the SSO Service Provider 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.

Copyright © 2010-2024 Infinite Campus. All rights reserved.

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

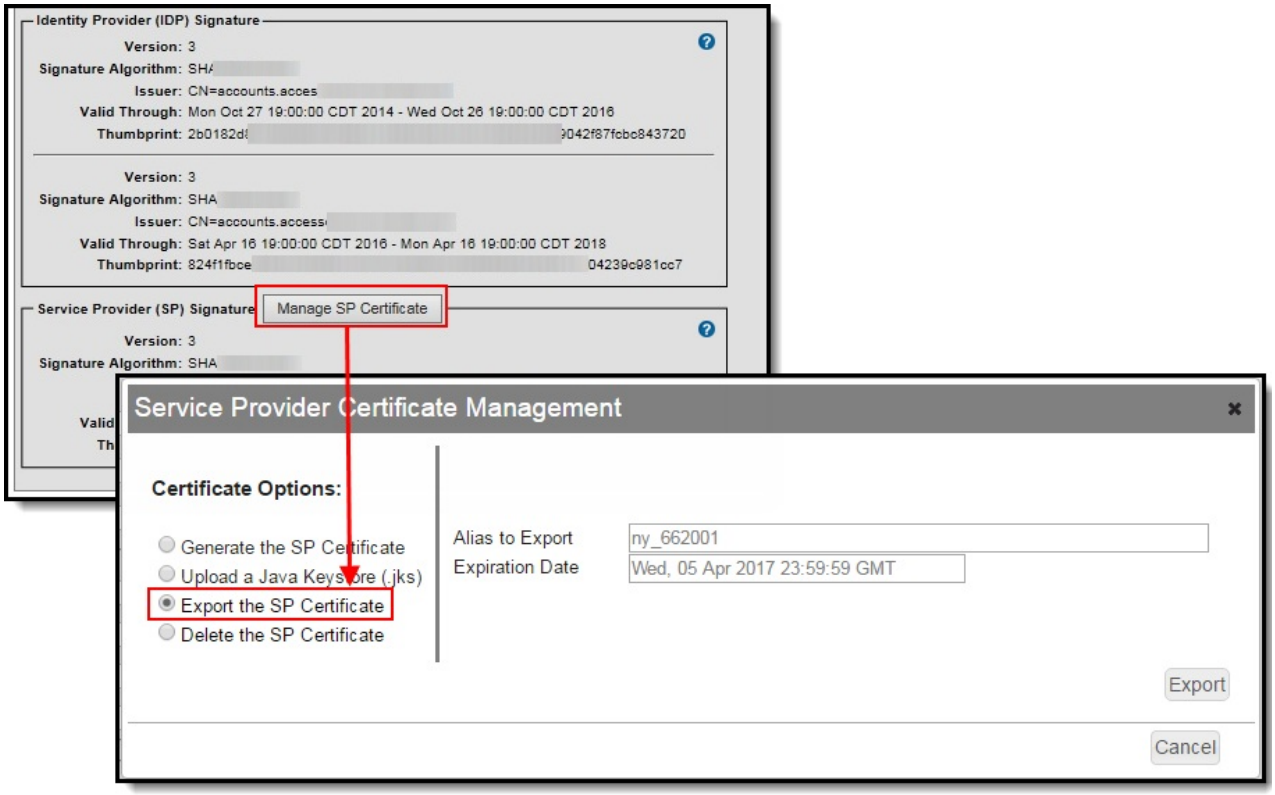
4. Click **Save** at the top of the editor. If the IDP was configured correctly, a green circle in the Enabled column will appear next to the IDP name in the Service Provider Configurations window. Users can now log into Infinite Campus via an SSO button on the login screen (see the Logging into Campus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



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.

Copyright © 2010-2024 Infinite Campus. All rights reserved.



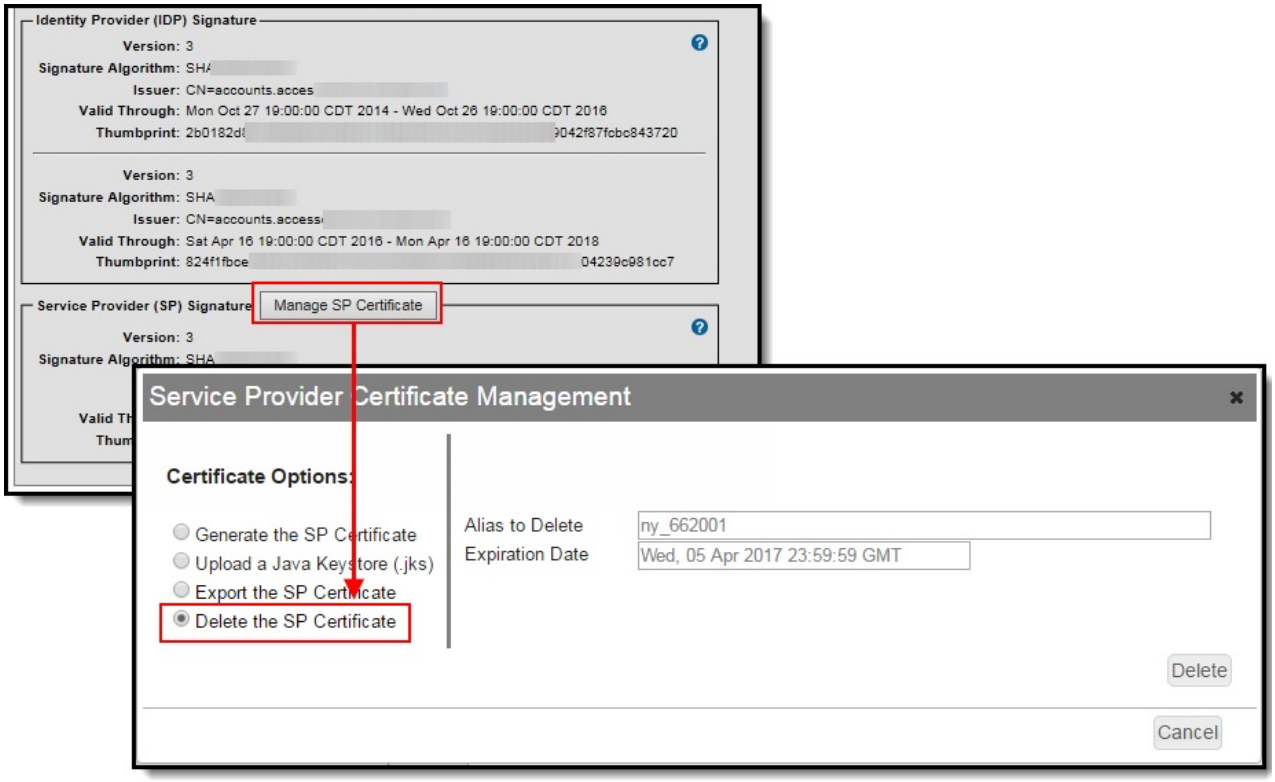
Delete the Service Provider Certificate

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.

Copyright © 2010-2024 Infinite Campus. All rights reserved.



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 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).

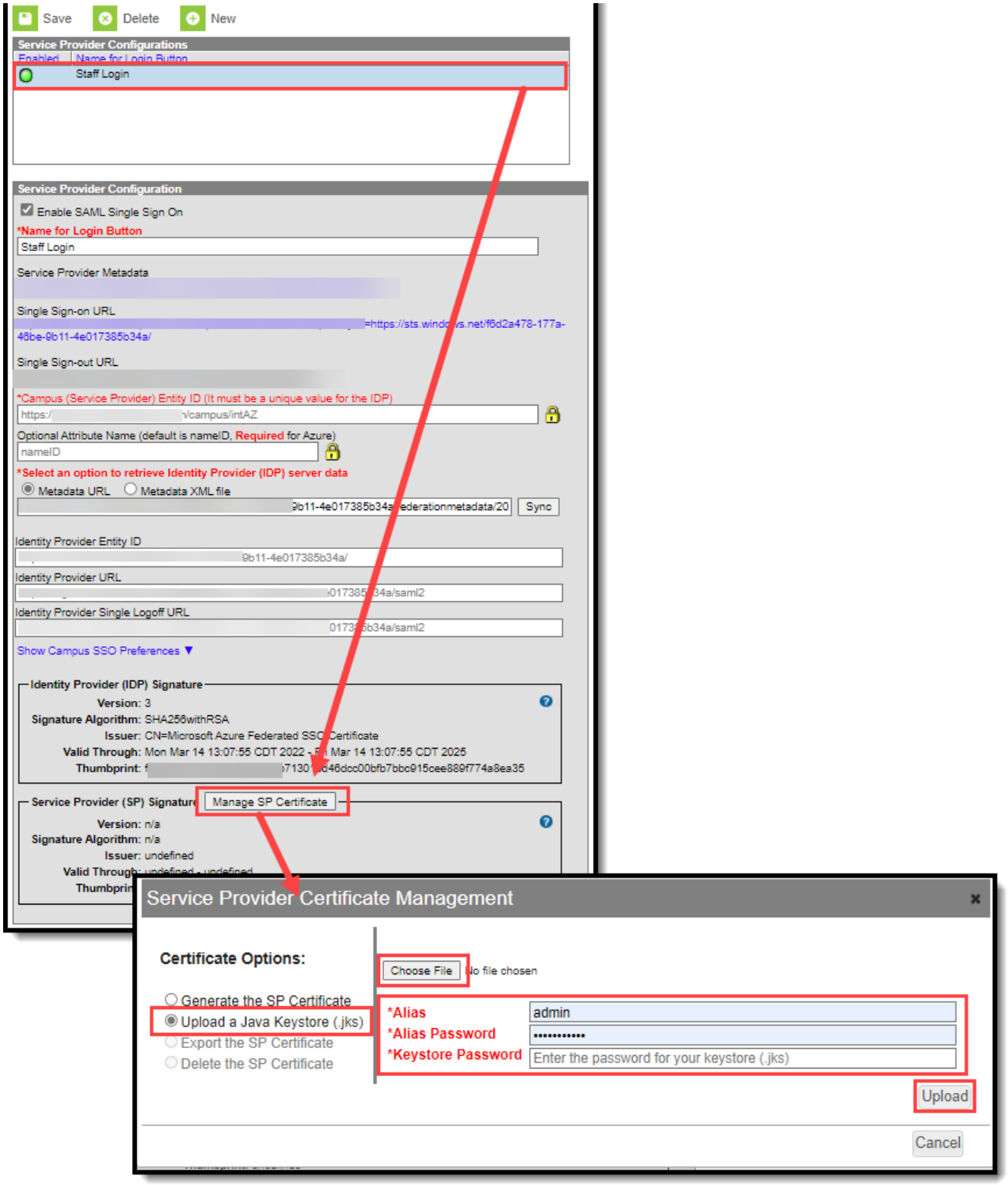
- Method 1 - Upload a New Java Keystore (.jks)

Copyright © 2010-2024 Infinite Campus. All rights reserved.

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.

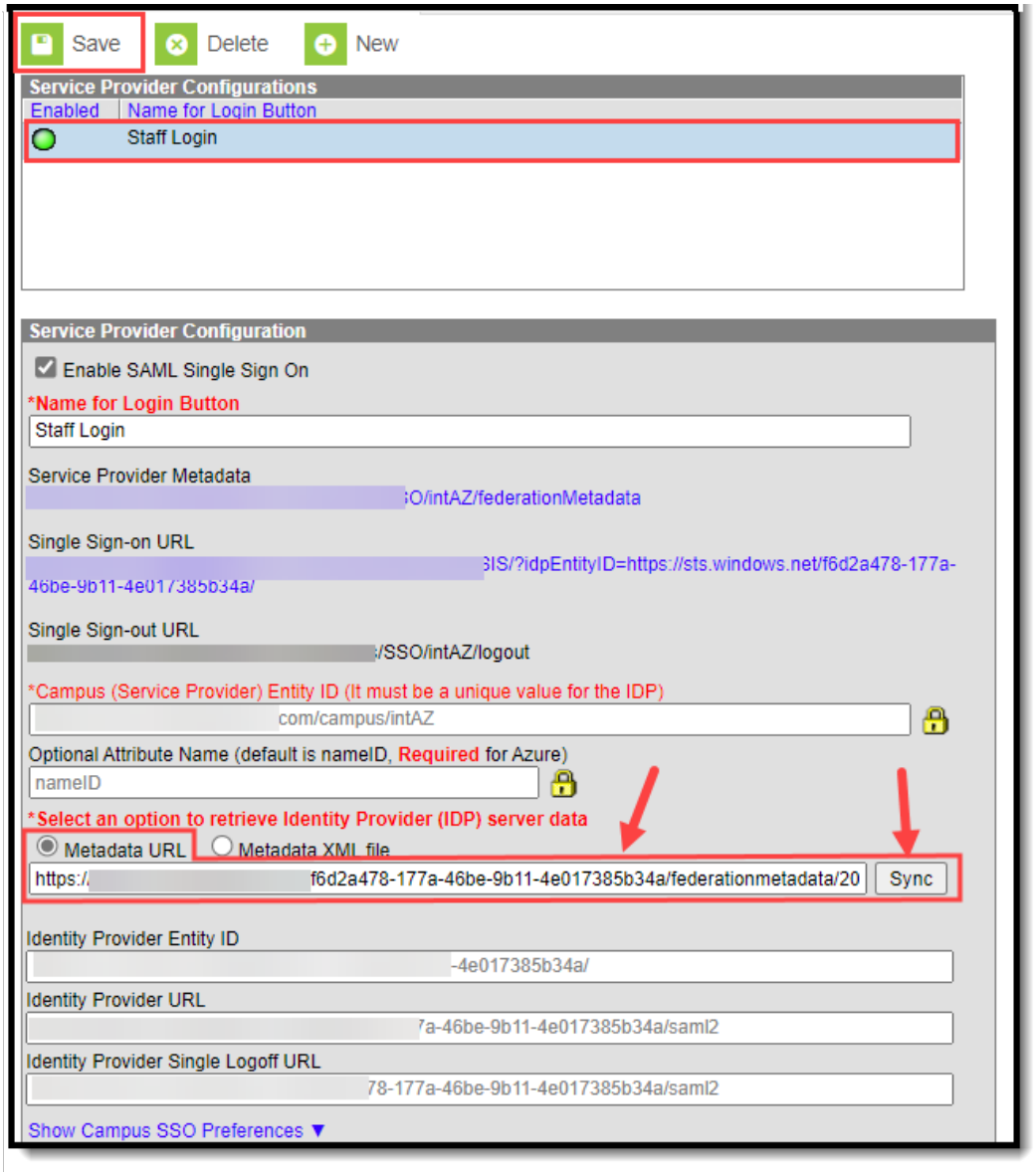
Copyright © 2010-2024 Infinite Campus. All rights reserved.



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.

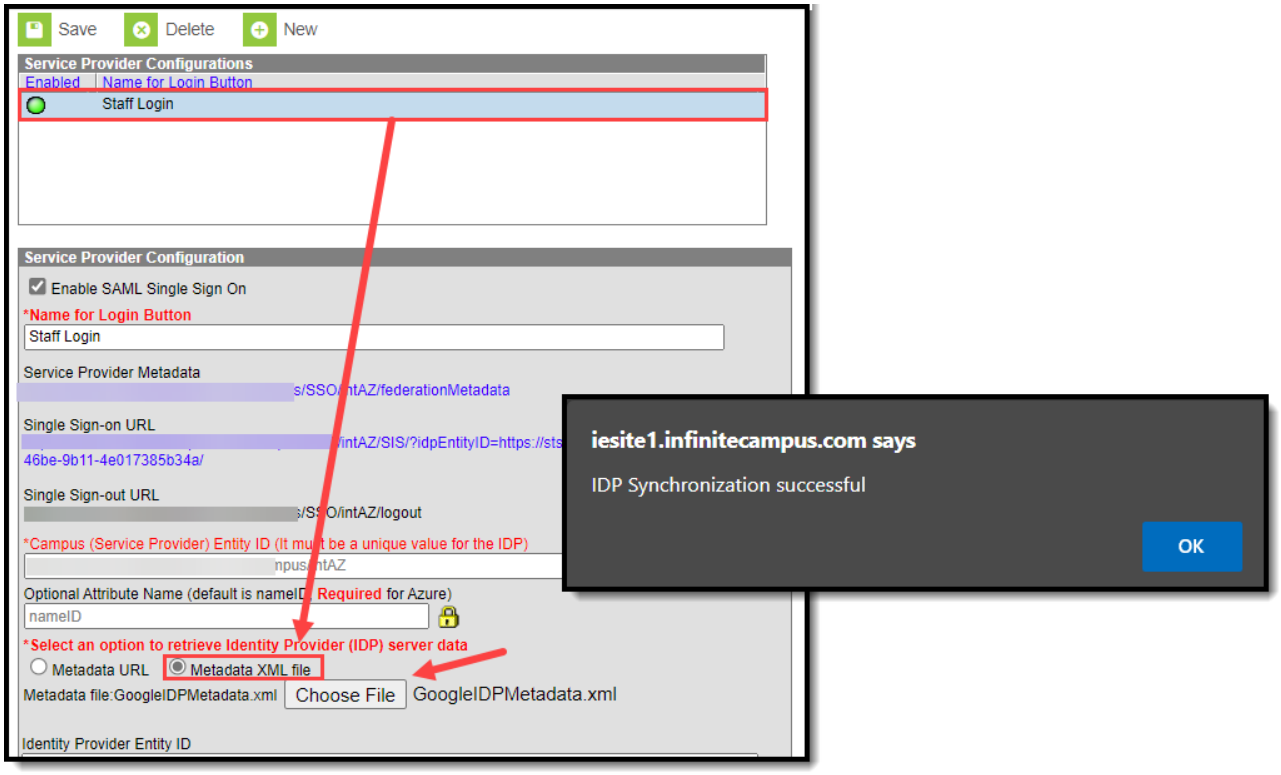
Copyright © 2010-2024 Infinite Campus. All rights reserved.



Method 3 - Resync Metadata via XML File

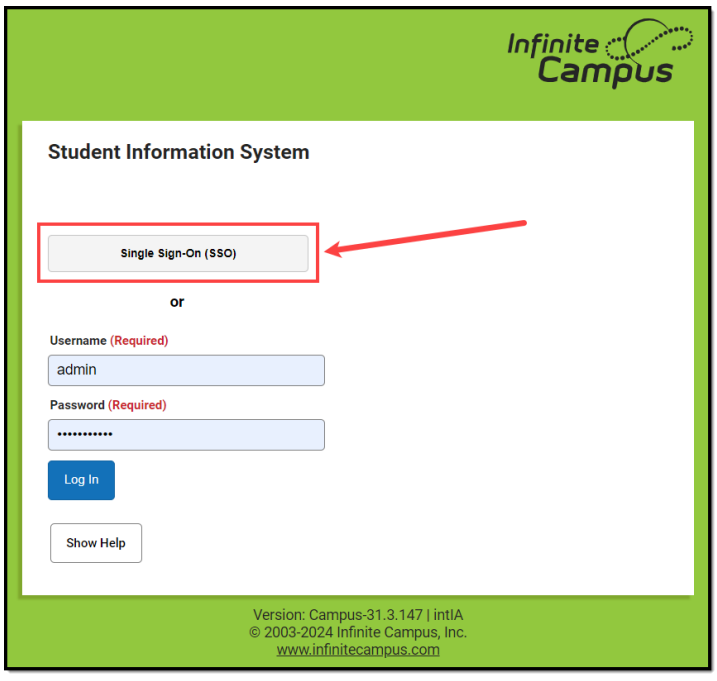
1. Select the SSO configuration needing an updated certificate.
2. Select the **Metadata XML File** radio button.
3. Click **Choose File**, locate your metadata XML file and click OK. The SSO Service Provider Configuration tool will automatically attempt to sync with the IDP and if successful you should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

Copyright © 2010-2024 Infinite Campus. All rights reserved.



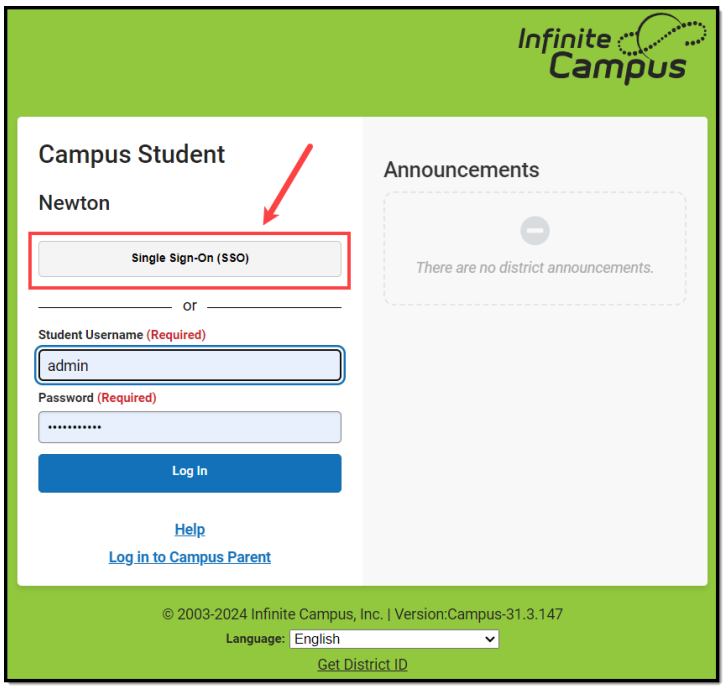
Logging into Campus and Campus Portal Using SAML SSO

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).	
Campus Student/Parent Portal	

Copyright © 2010-2024 Infinite Campus. All rights reserved.

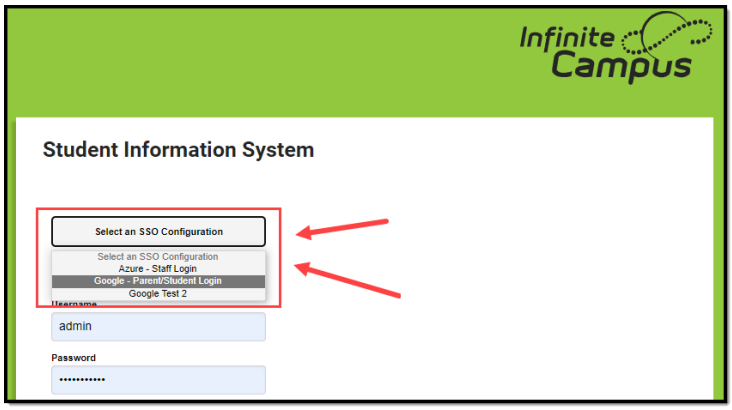
Users will click the SSO button (named whatever was determined in Step 1 of this document).



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.



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

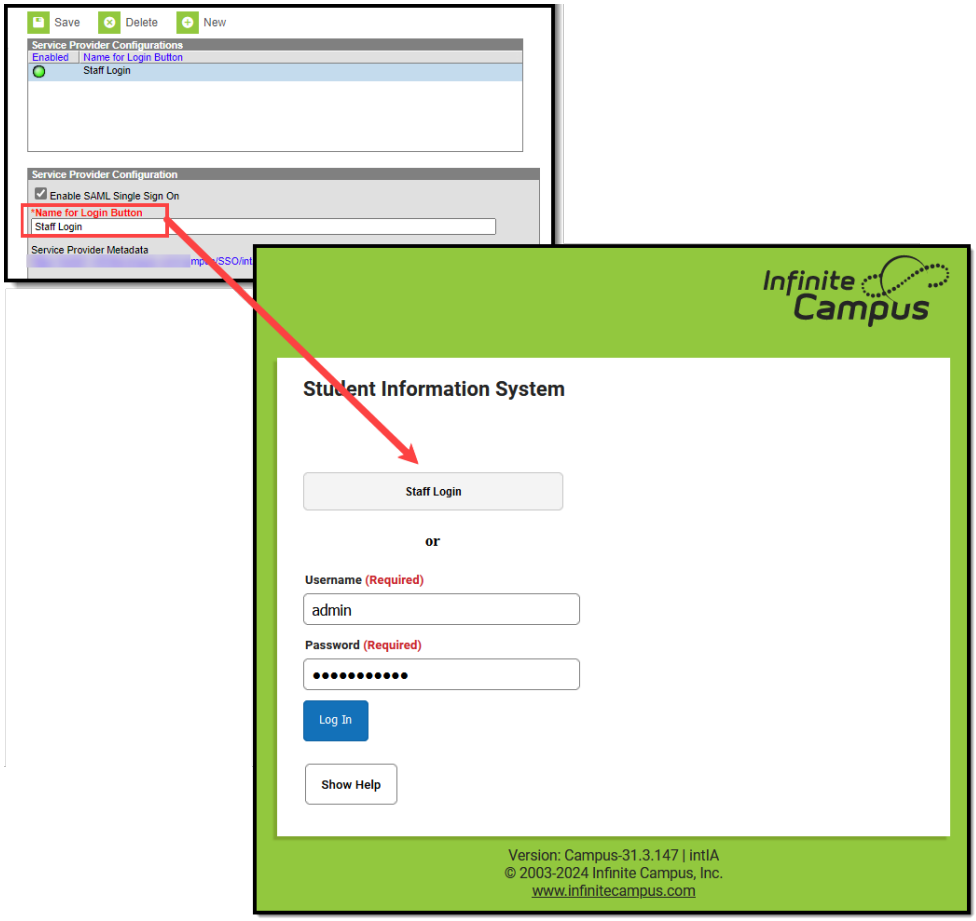
For example, if your district has a separate SSO configuration for Staff member logins, you can mark the **Turn off this SSO configuration for the Parent Portal** and **Turn off this SSO configuration for the Student Portal** checkboxes so it does not appear for students and parents logging into Infinite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

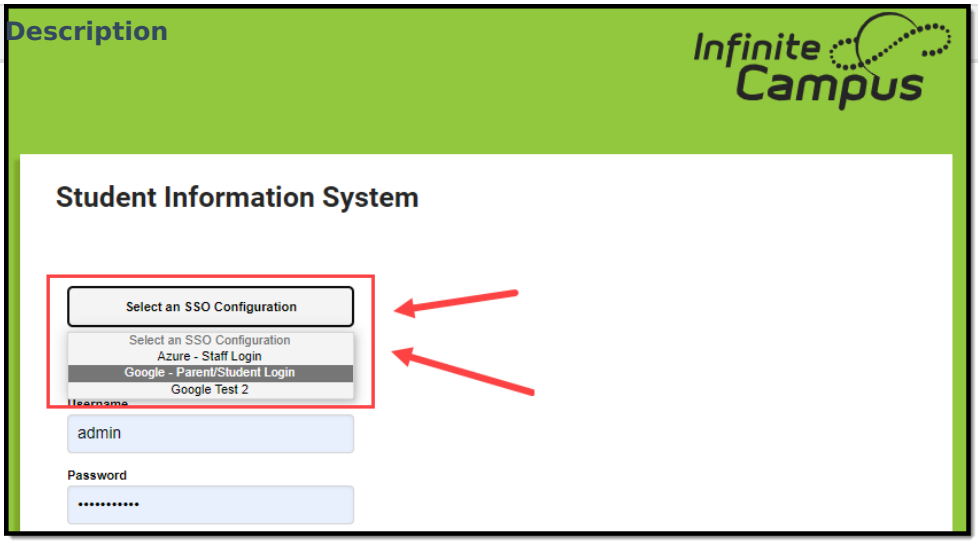
Copyright © 2010-2024 Infinite Campus. All rights reserved.

Understanding Service Provider Configuration Fields

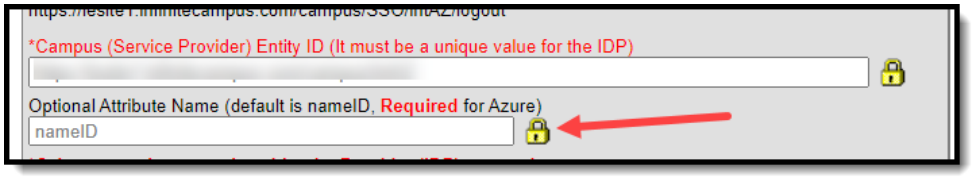
Use the following table to understand each available field.

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 what the name of the SSO login button will be named 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 are able to 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.

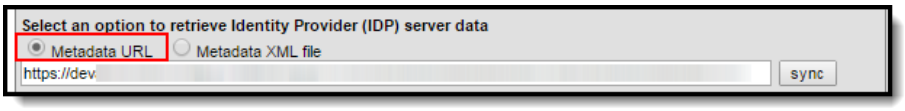
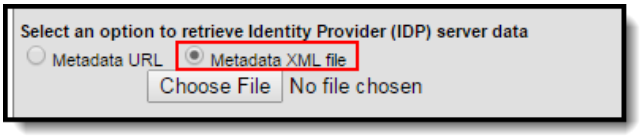
Copyright © 2010-2024 Infinite Campus. All rights reserved.

Field	Description
	 You can hide specific SSO configurations from specific login screens (staff, parent, student) by using the **Turn off this SSO configuration for the 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 Azure AD is one known IDP that requires the local Campus logout URL in order to properly redirect to the Campus logoff page.

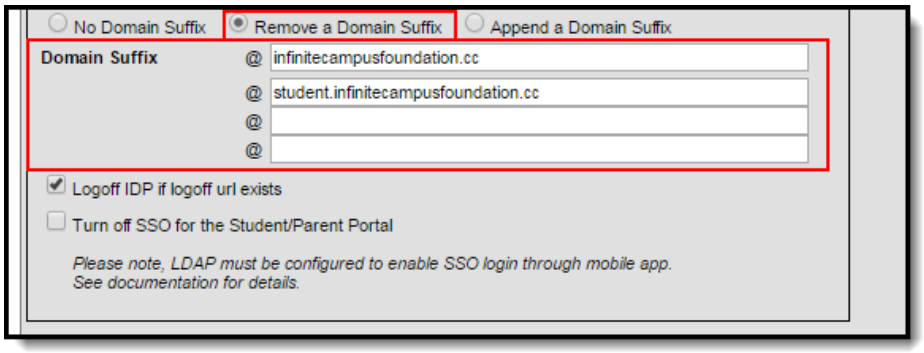
Copyright © 2010-2024 Infinite Campus. All rights reserved.

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-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.
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 Azure AD as the Name ID attribute is reserved by Azure and cannot be used for comparisons. For Azure, leave this field value as nameID. To change this value, click the Lock icon.  An incorrect Optional Attribute Name value will break the connection between Campus and the IDP.

Copyright © 2010-2024 Infinite Campus. All rights reserved.

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.  • **Metadata XML File -** IDP server data is inserted from a locally stored XML file.  Once a URL or XML file has been entered, click the **Sync** button to load the XML values into Campus.
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 Domain Suffix	This options indicates the domain name does not contain a suffix.

Copyright © 2010-2024 Infinite Campus. All rights reserved.

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. 
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.

Copyright © 2010-2024 Infinite Campus. All rights reserved.

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	
Infinite 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.

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.

Copyright © 2010-2024 Infinite Campus. All rights reserved.

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:

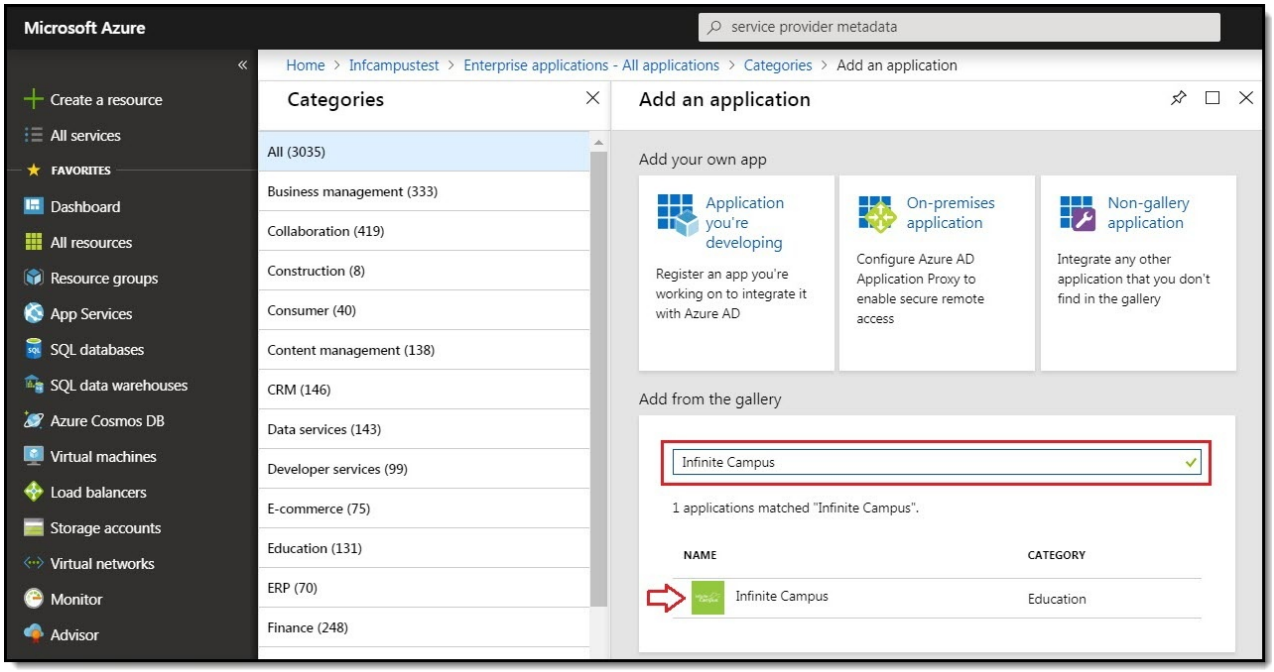
Infinite Campus Azure Marketplace Workflow

Step 1.

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

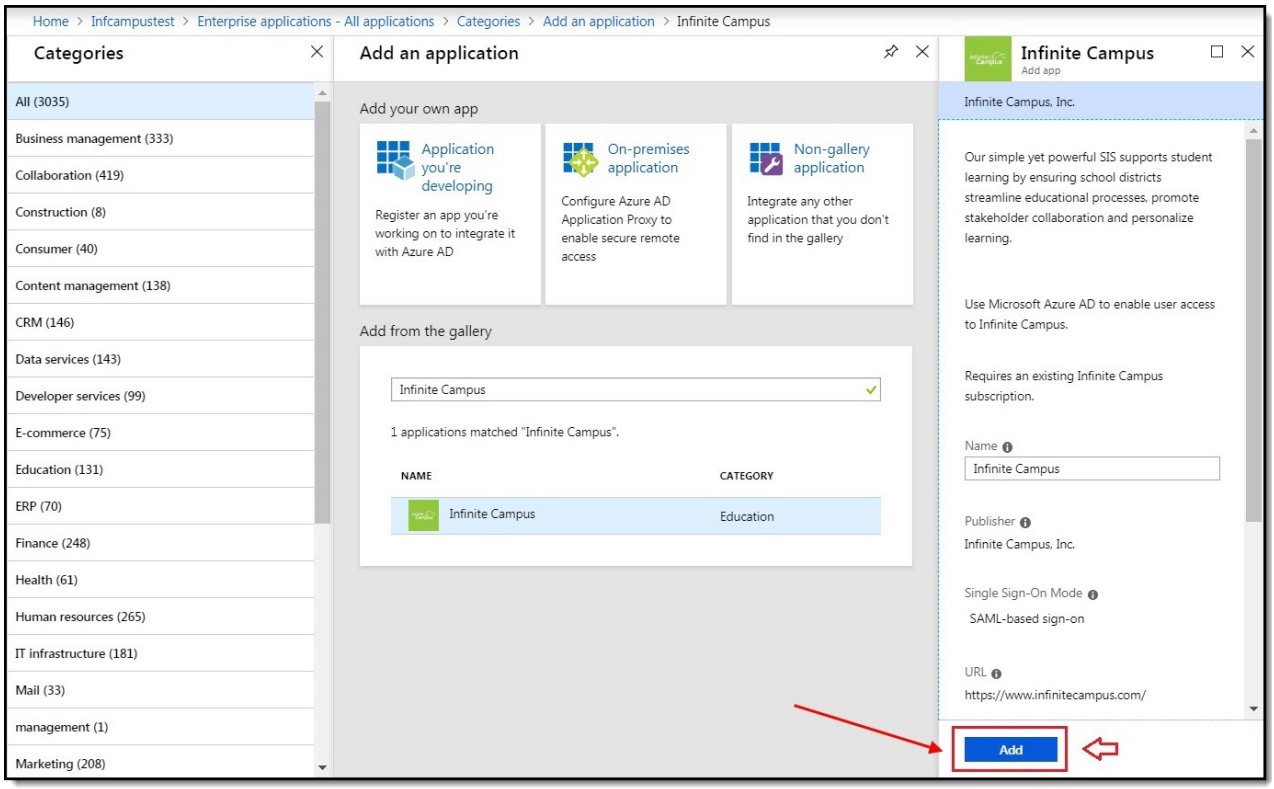
Enter "Infinite Campus" in the search box in the **Add from the gallery** section of the page and click on the Infinite Campus icon that appears.

Copyright © 2010-2024 Infinite Campus. All rights reserved.



Step 2.

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

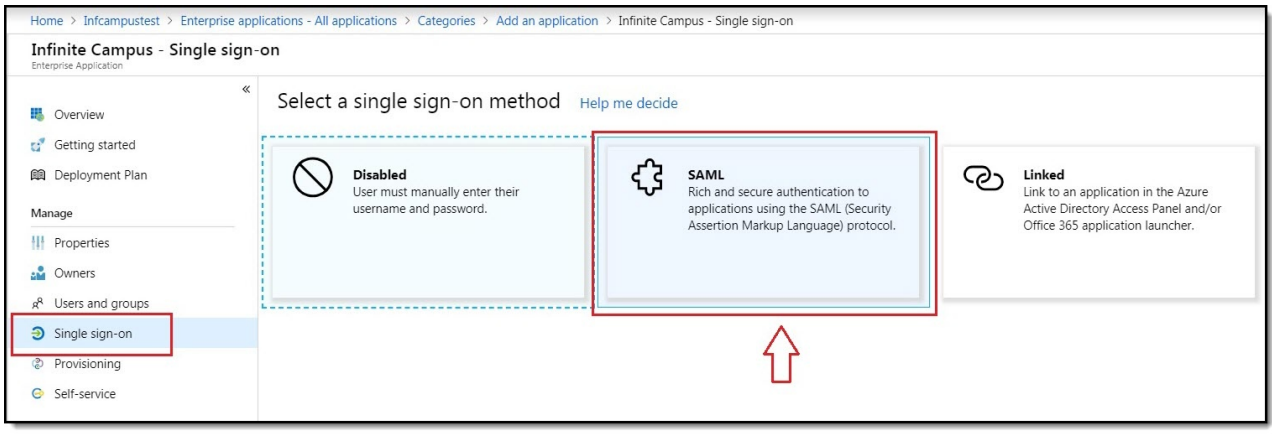


Step 3.

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

Copyright © 2010-2024 Infinite Campus. All rights reserved.

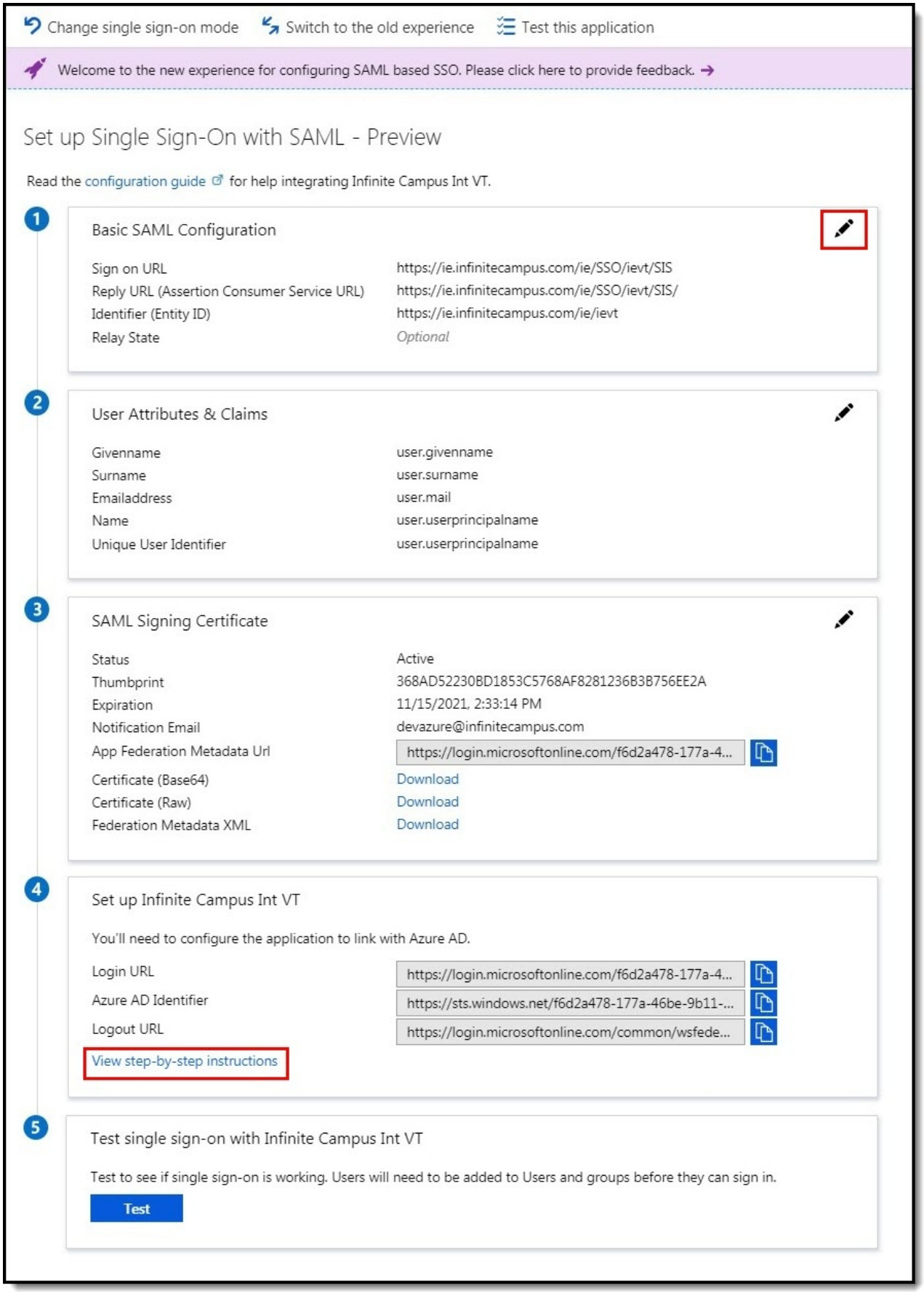
select the **SAML** box:



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. 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.

Copyright © 2010-2024 Infinite Campus. All rights reserved.



Copyright © 2010-2024 Infinite Campus. All rights reserved.

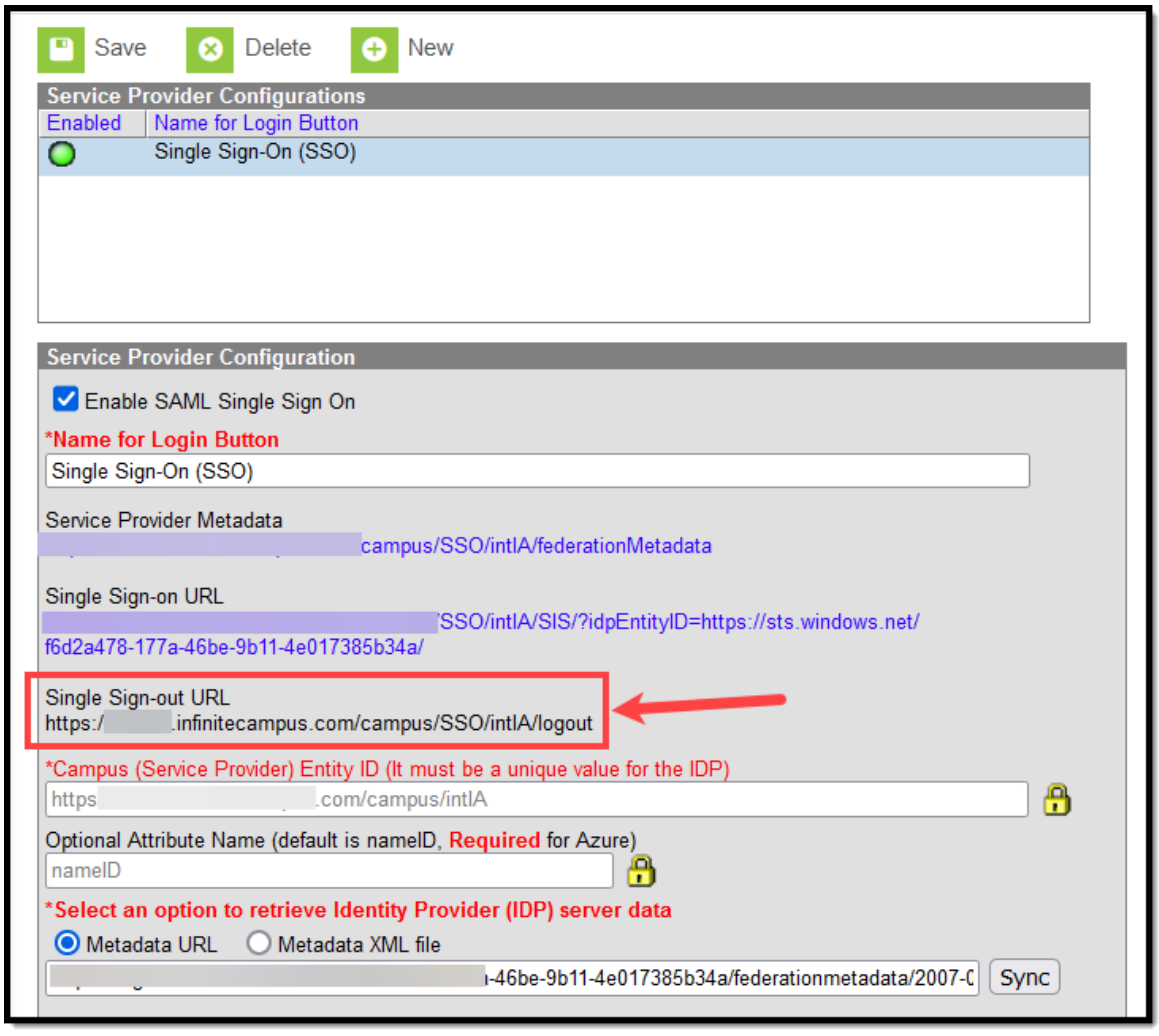
Add the Infinite Campus Logout URL to the Microsoft Azure SAML SSO Configuration

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.

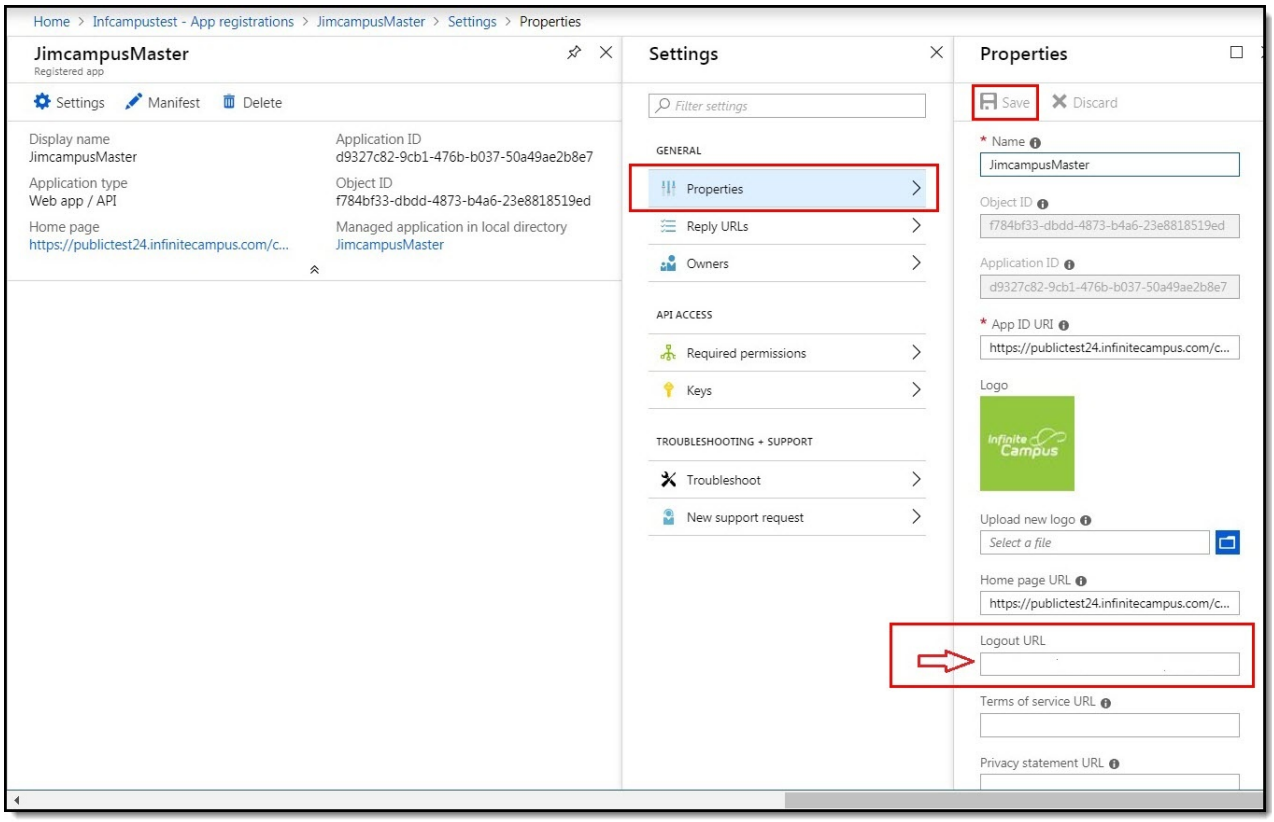


Step 2.

Copyright © 2010-2024 Infinite Campus. All rights reserved.

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.



Complete a Single Sign-On Login

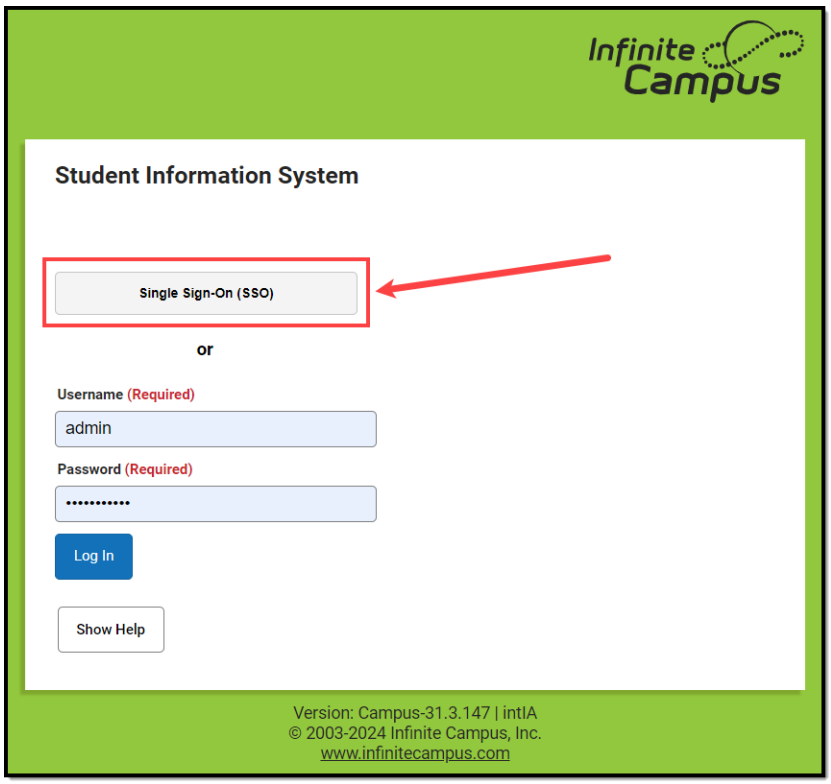
The final step is to log out of the administrative account and log into Infinite Campus and attempt a Single Sign-On user login. Please ensure you have followed the configuration steps outlined throughout this article.

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).

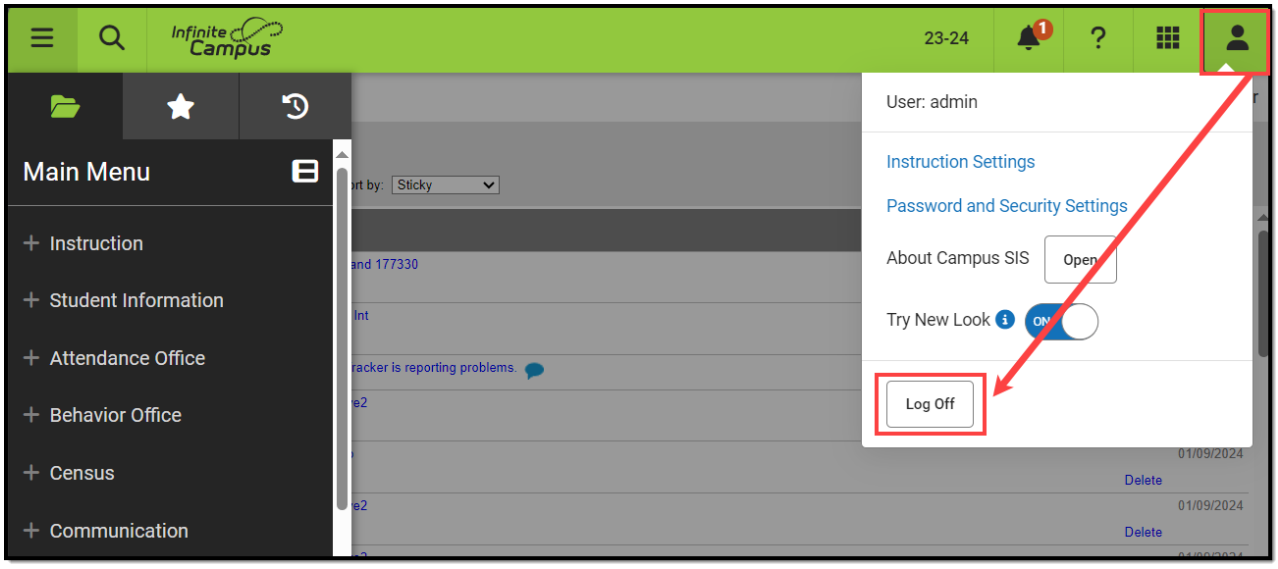
Proper first-time login behavior will be a redirect to the Microsoft Azure AD credentials page. A successful logon to Azure AD results in a successful re-direct to the Infinite Campus application.

Copyright © 2010-2024 Infinite Campus. All rights reserved.



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



Please ensure to contact the Infinite Campus Support team or your CE or other internal contact(s)

Copyright © 2010-2024 Infinite Campus. All rights reserved.

with any questions or concerns.

Configuring a Google IDP

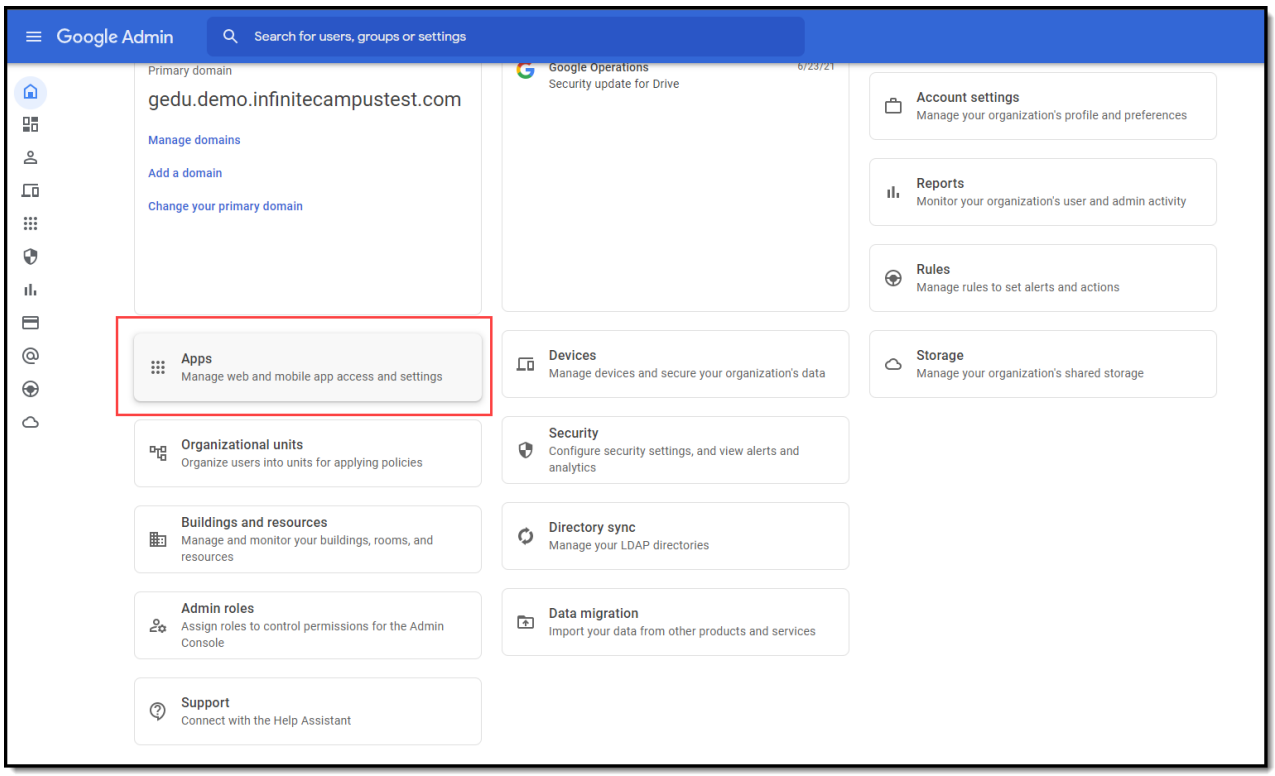
The following section will describe configuring the Google IDP to utilize Campus SSO functionality.

Prerequisites

- You need a Google Admin account.

Step 1.

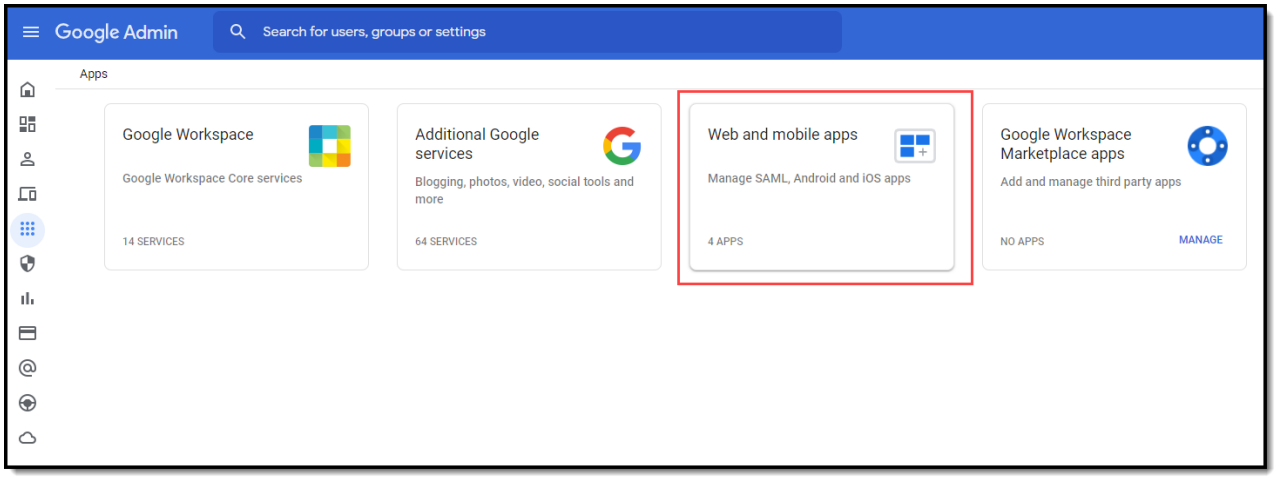
Log into your Google Administrator account (https://admin.google.com) and select **Apps**.



Step 2.

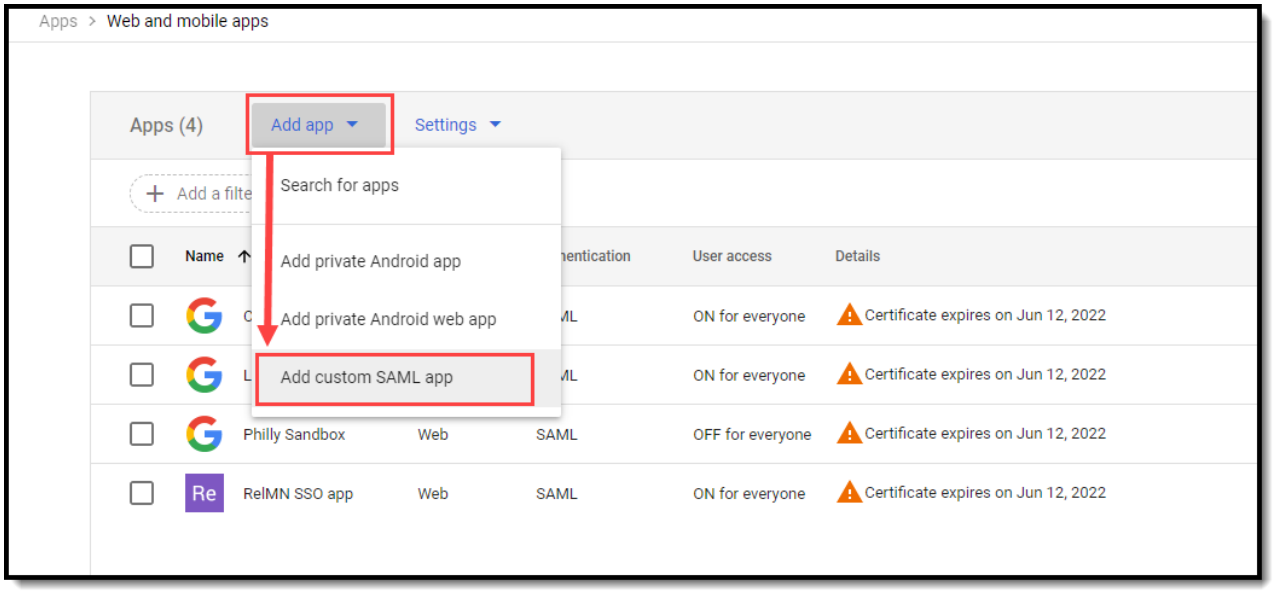
Select **Web and mobile apps**.

Copyright © 2010-2024 Infinite Campus. All rights reserved.



Step 3.

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

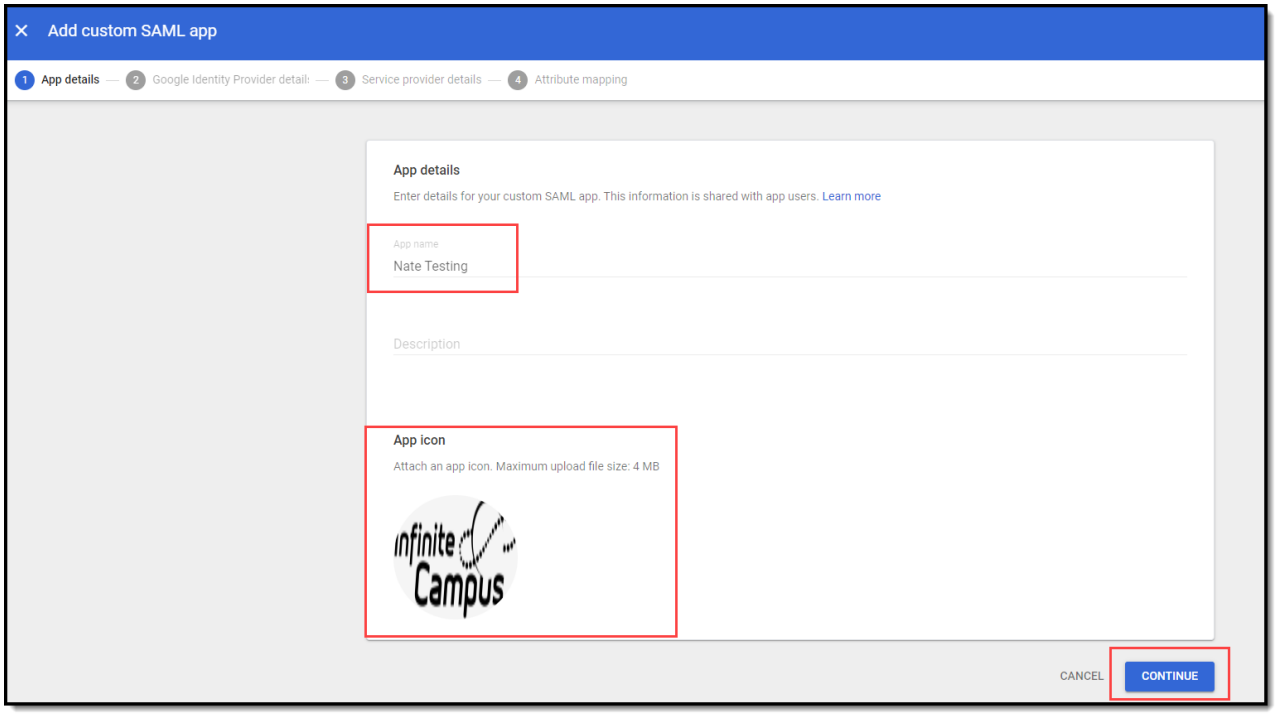


Step 4.

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

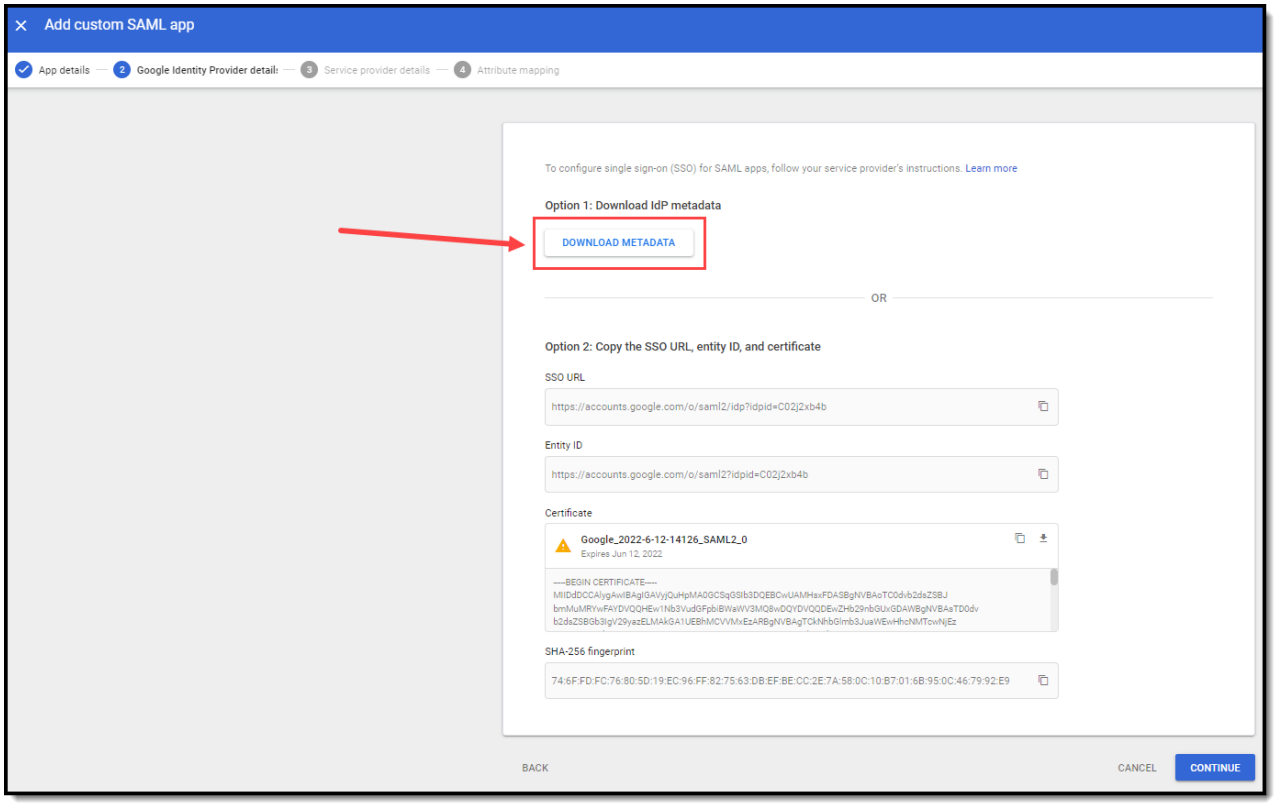
An example of a logo you can use:

Copyright © 2010-2024 Infinite Campus. All rights reserved.



Step 5.

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



Step 6.

Copyright © 2010-2024 Infinite Campus. All rights reserved.

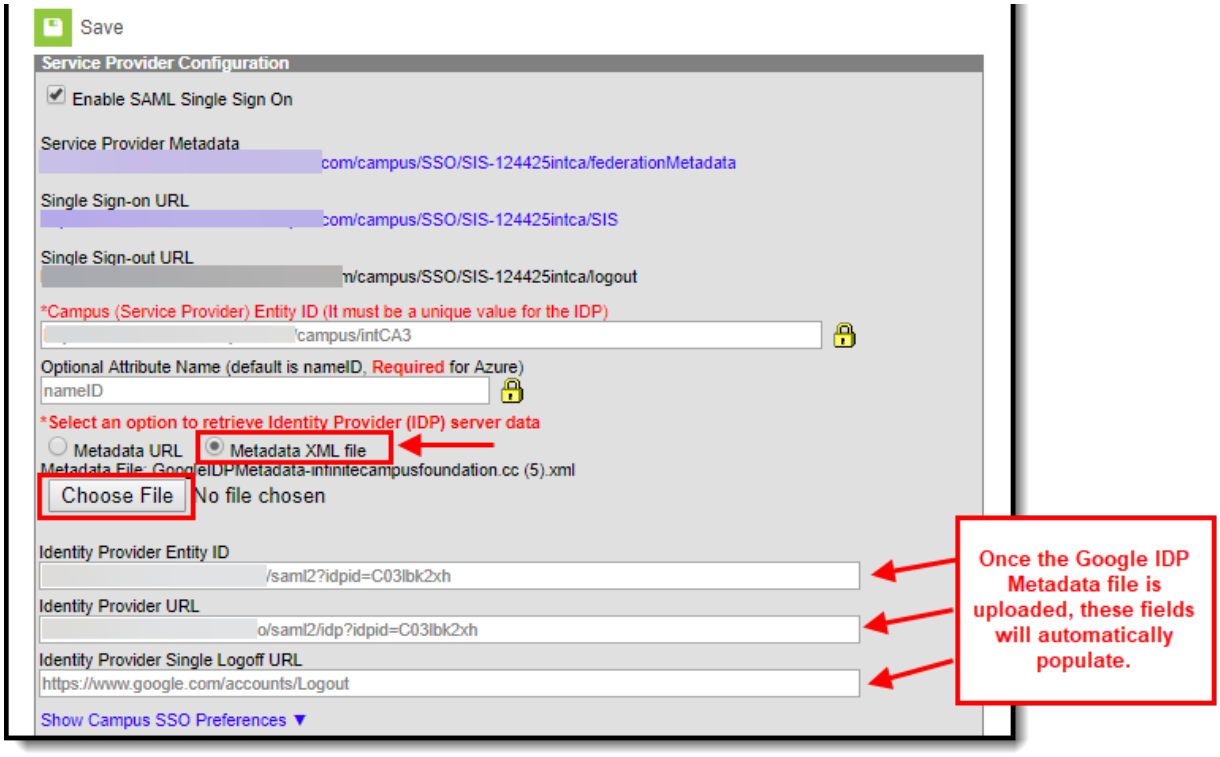
Open Infinite Campus in a different tab and navigate to the SSO Service Provider Configuration tool (System Administration > User Security > SAML Management > SSO Service Provider Configuration).

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.

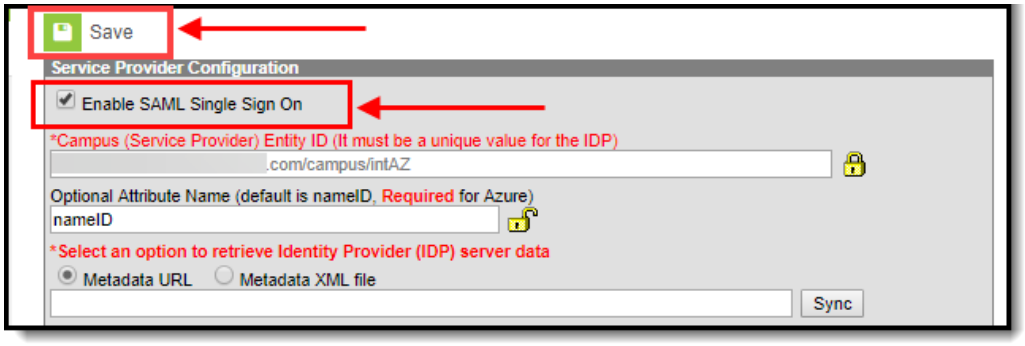
> Campus does not support the use of the **Logoff IDP if Logoff URL Exists** preference when using a Google IDP setup. This checkbox will automatically be unmarked and grayed out if the Identity Provider Single Logoff URL references Google.



Step 7.

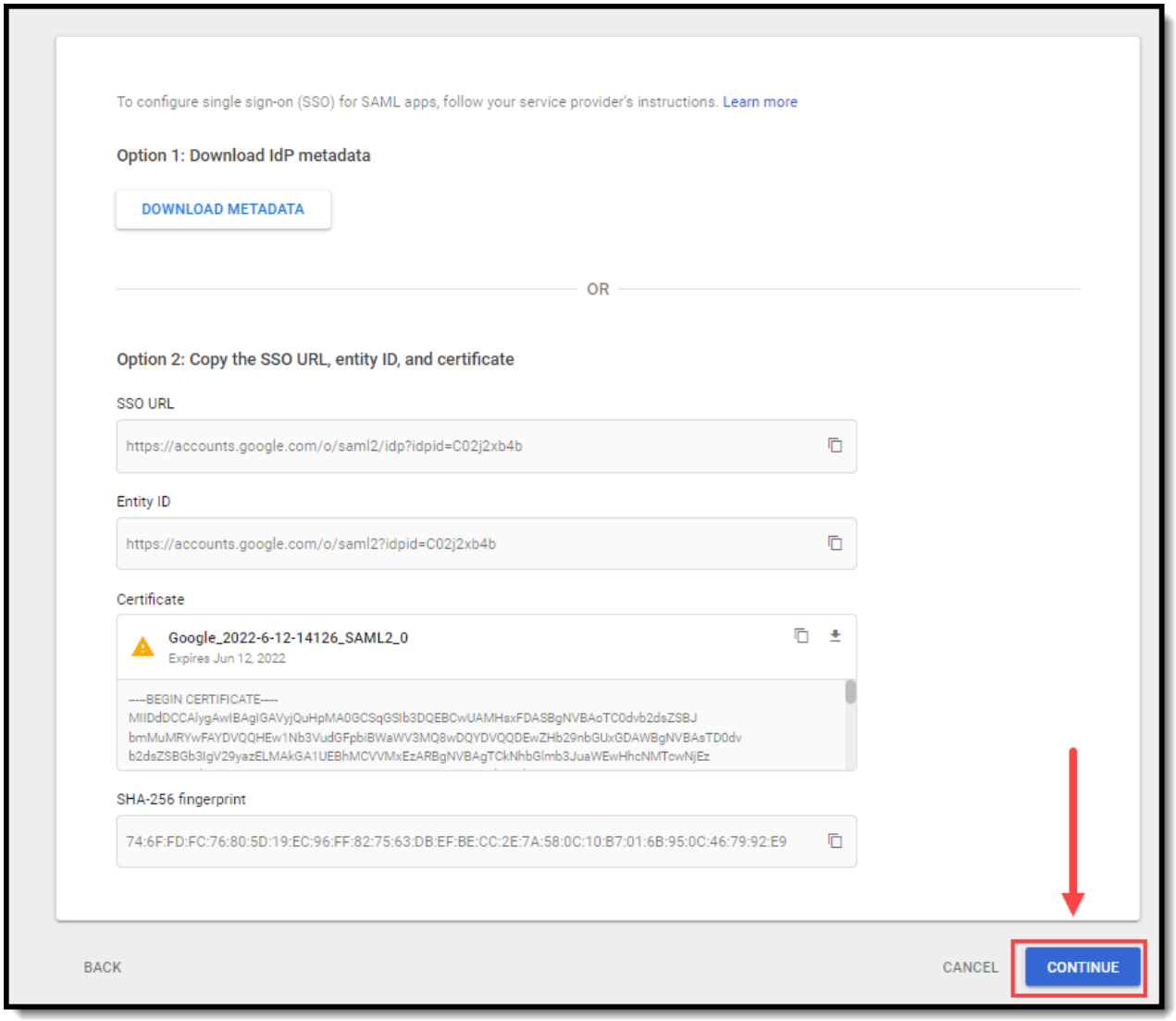
Now it's time to save and enable the Campus SSO. Mark the **Enable SAML Single-Sign On** checkbox and click **Save**.

Copyright © 2010-2024 Infinite Campus. All rights reserved.



Step 8.

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



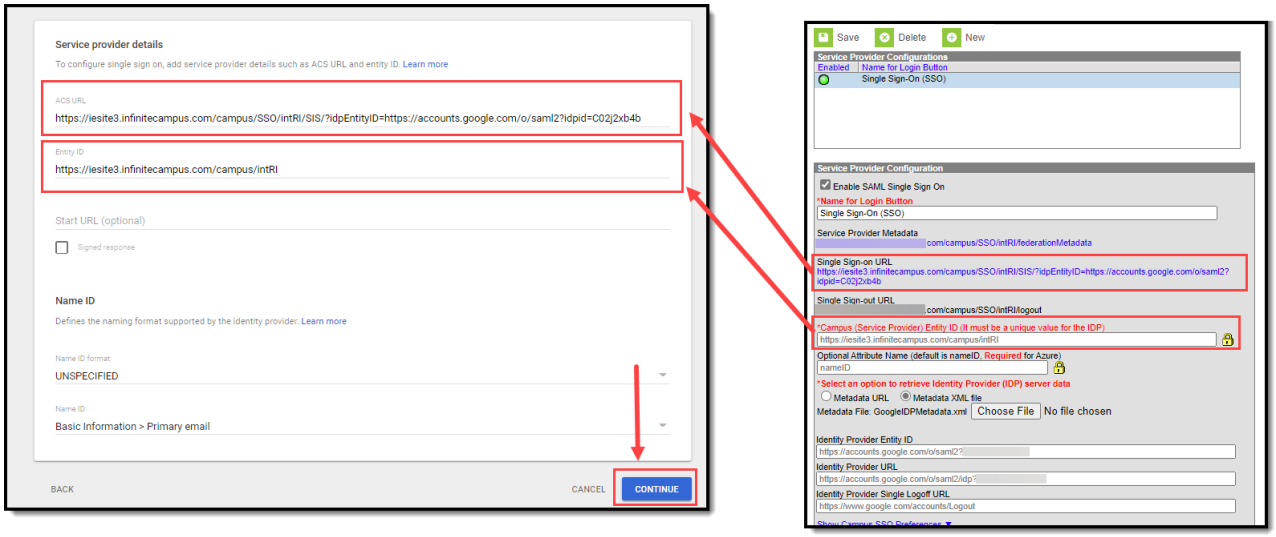
Step 9.

On the **Service Provider Details** screen:

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

Copyright © 2010-2024 Infinite Campus. All rights reserved.

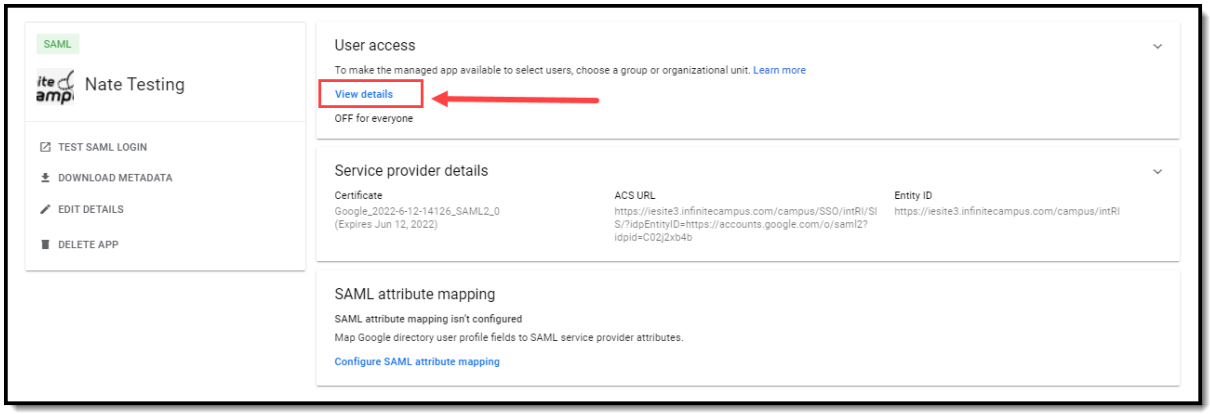
2. Enter the **Entity ID** as the same value found in the **Campus (Service Provider) Entity ID (It must be a unique value for the IDP)** field.
3. Click **Continue**.



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.

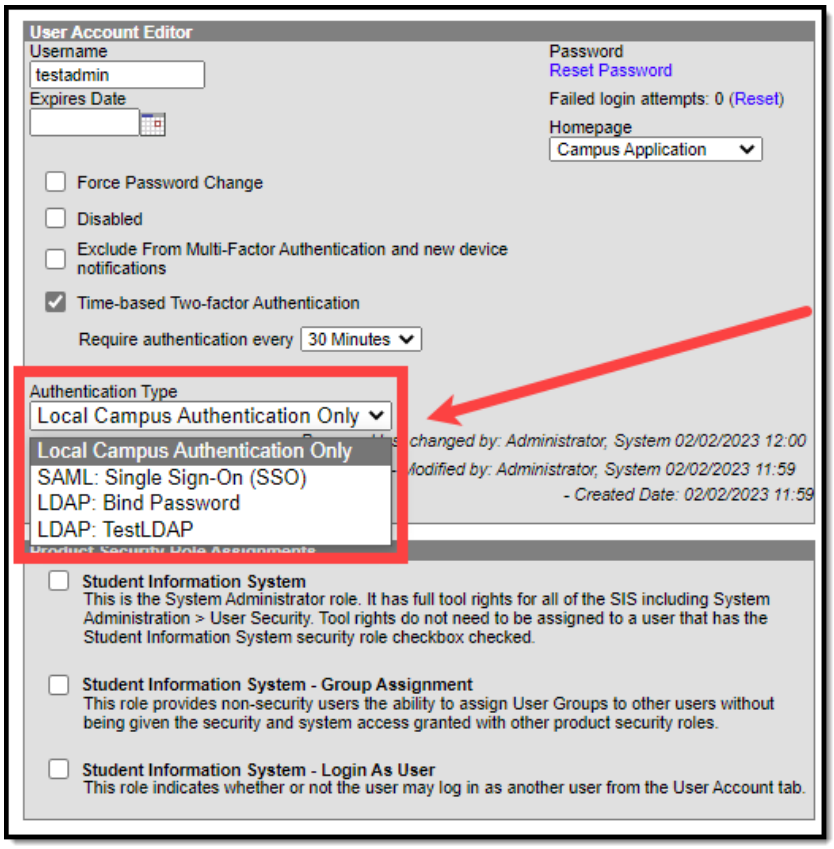
By default, Google SSO matches based on username.

Step 11.

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

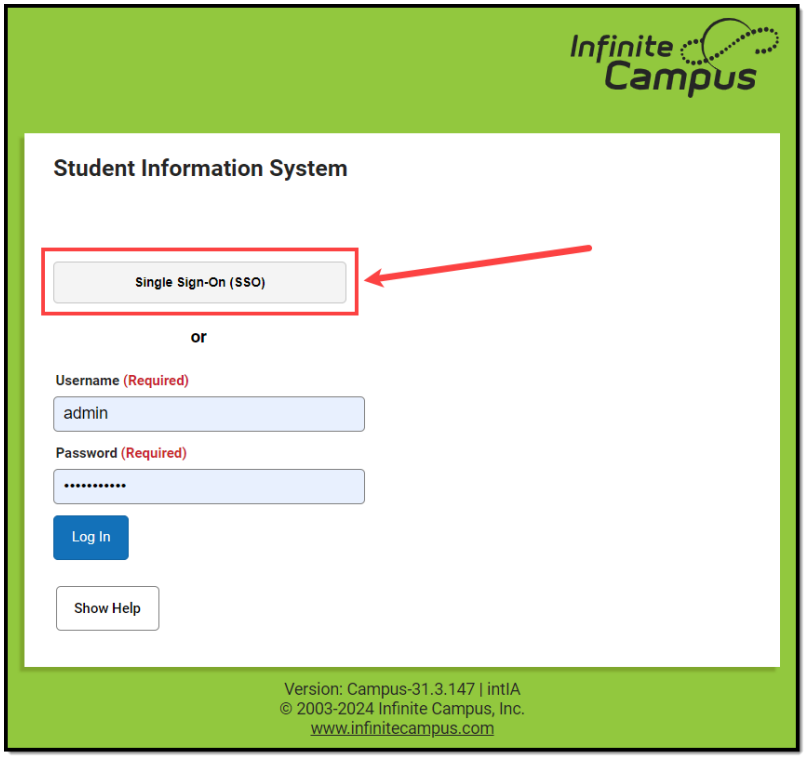
Copyright © 2010-2024 Infinite Campus. All rights reserved.

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.

Copyright © 2010-2024 Infinite Campus. All rights reserved.



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 User Account Type Wizard.

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 Local Campus Authentication User Account Exists for Administrators
- 2. Have the Non-Production Infinite Campus Environment Refreshed
- 3. In Your SSO IDP's System, Repeat Their Setup Process

1. Ensure a Local Campus Authentication User Account Exists for Administrators

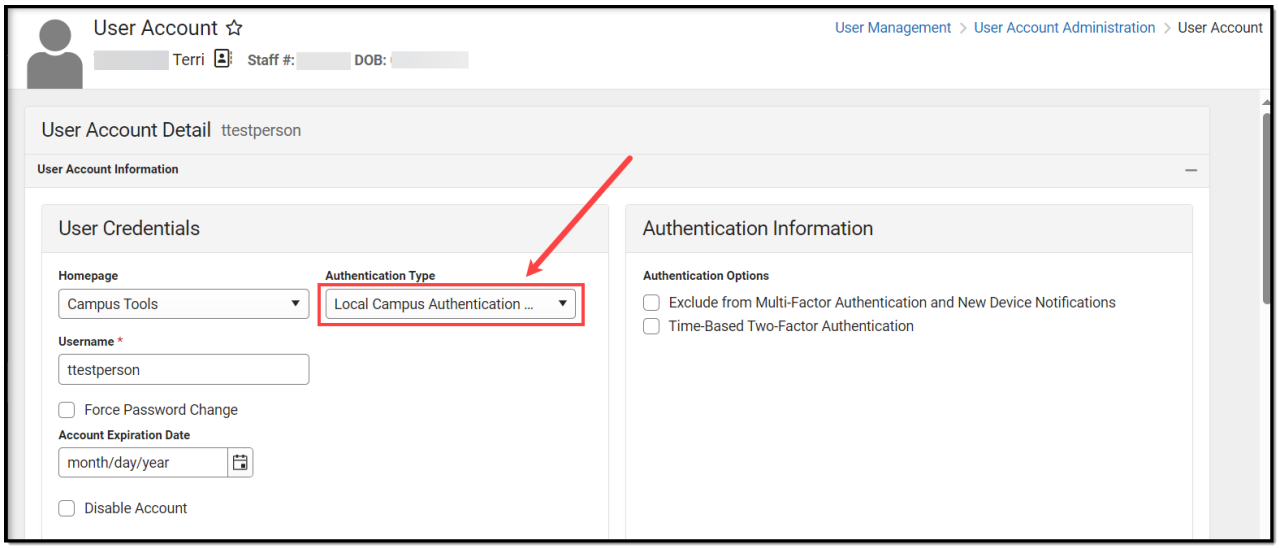
In your production environment, ensure a user account exists for yourself and is set to an Authentication Type of Local Campus Authentication before proceeding.

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

Copyright © 2010-2024 Infinite Campus. All rights reserved.

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.



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 Local Campus Authentication 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 Azure, 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

Copyright © 2010-2024 Infinite Campus. All rights reserved.

- **IDP-specific instructions**
  - Configuring a Unique Azure Active Directory
  - Configuring a Google IDP

These two items are especially important as you complete the setup in the IDP system for your non-production 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 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:

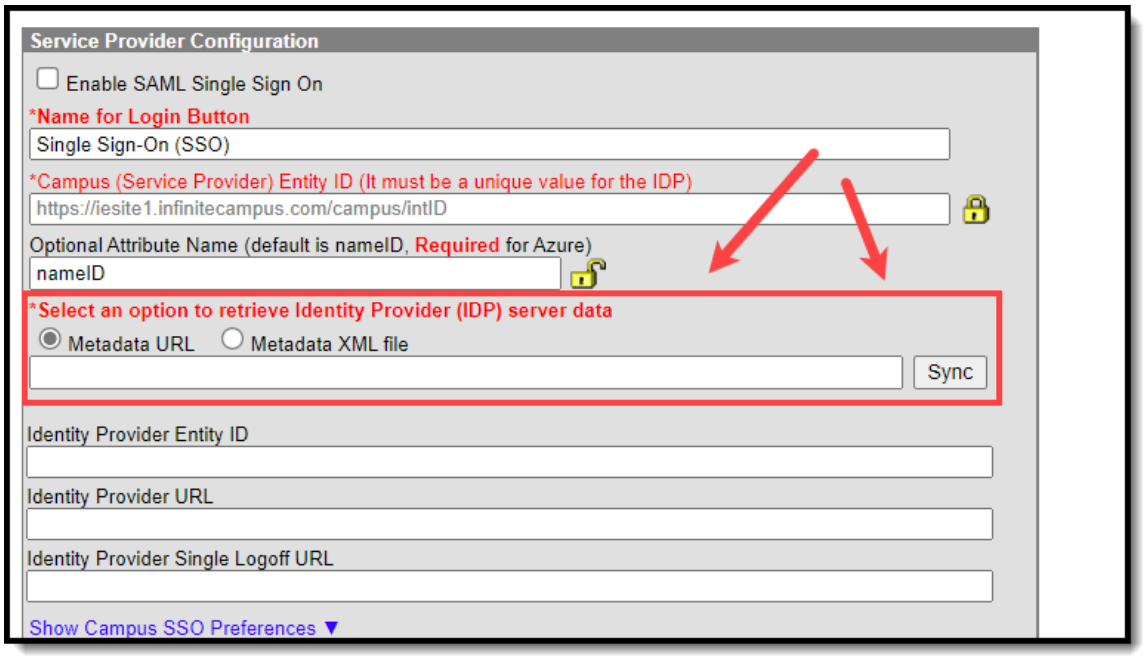
1. Log into your SSO IDP system,
2. Navigate to the non-production Infinite Campus app you've set up
3. Copy the Metadata URL or re-download the Metadata XML file

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

1. Log into Infinite Campus using your Local Authentication credentials.

Copyright © 2010-2024 Infinite Campus. All rights reserved.

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**



5. Once the metadata has been entered and synced, click Save. Single Sign-On for your non-production 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.

Copyright © 2010-2024 Infinite Campus. All rights reserved.