SAML Identity Provider Configuration

Last Modified on 10/20/2026 12:16 pm CDT

This tool is only available upon request to Campus.

The SAML Identity Provider Configuration tool turns Campus into a SAML Identity Provider (IdP). This is the opposite direction from what most people think of when they hear "SAML SSO in Campus."

Most districts use SAML so that an external system (such as Azure AD, Google, or ADFS) authenticates users and redirects them to Campus. In that scenario, Campus is the Service Provider (SP) and the external system is the Identity Provider. That's configured in the SAML - SSO Service Provider Configuration tool.

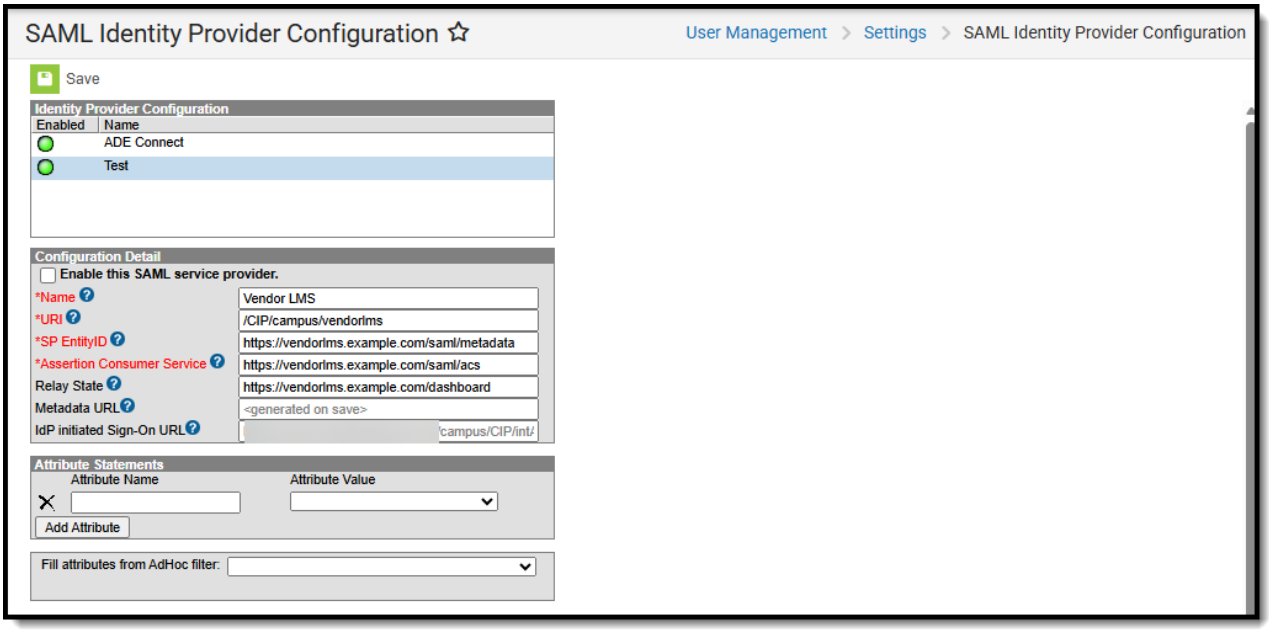
The SAML Identity Provider Configuration tool is for the reverse scenario: an external application needs to trust Campus as the identity source. When a user is already logged in to Campus, they can seamlessly access a third-party application without re-authenticating because Campus generates a signed SAML assertion that verifies their identity.

Before you start

- You must have the SIS security role assigned to your user account.
- You need the following Information from the external Service Provider:
  - Their Entity ID
  - Their ACS URL (Assertion Consumer Service)
  - What attributes/claims they need (e.g., email, name, student ID)
- The external Service Provider administrator available for coordination (they'll need to configure their side too).

Step 1. Add a SAML Identity Provider configuration

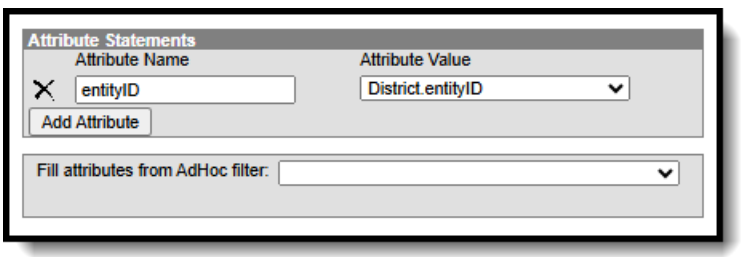
This section will walk you through the steps of adding a new SAML IDP configuration.



1. Enter the **Name** of IDP configuration. This will help you identify which Service Provider this configuration applies to when viewing the list of entries.
2. Enter the **URI**. This is the path segment used to build the IdP endpoint URLs.
3. Enter the **SP Entity ID**. This is the full URL identifier of the external Service Provider.
4. Enter the **Assertion Consumer Service** (ACS). This is the URL where Campus will POST the SAMLResponse.
5. Enter the **Relay State** (optional). This is where users should be directed to upon login.
6. The **Metadata URL** will be generated upon save.
7. The **IdP initiated Sign-on URL** is hardcoded by Campus.
8. If you have attributes, they will be addressed in the next step.
9. Click **Save**. The configuration is now saved, and several important data elements are present, including the Identity Provider (IDP) Signature section and a test button. If you have Identity Claims (also known as Attribute Statements) move to Step 2. If not, move on to Step 3.

Step 2. Configure Attribute Statements - Optional

It is likely your Service Provider wants specific attributes passed to them during the authentication process and expects each piece of data to have a specific name. In the Attribute Statements section, you need to define each Attribute Name and its Attribute Value (where in the database the data for this attribute is stored).

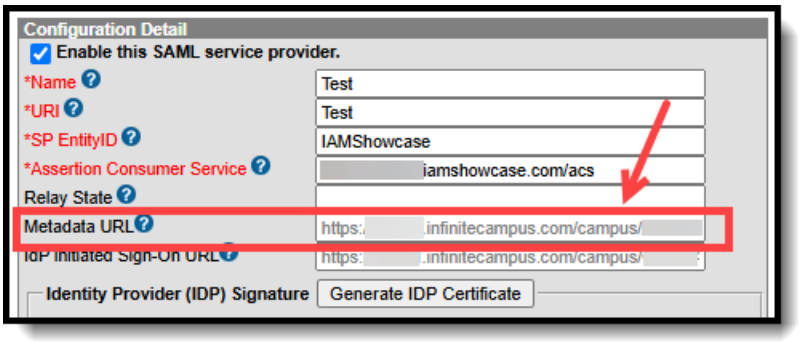


1. Enter the **Attribute Name**. This is the label the Service Provider is expecting for this

attribute. For example, the Service Provider requires all EntityID values be sent as 'entityID'.
2. Enter the **Attribute Value**. This is the database location of this data within Campus.
3. To add additional attributes, click **Add Attribute** and repeat steps 1 and 2.
    - If you need custom district data not supported by the Attribute Values listed, you can create an Ad hoc filter and select it in the **Fill attributes from AdHoc filter** dropdown list. The filter's columns will become additional attributes in the SAML assertion.
4. Once all attributes have been added, click **Save**. Move on to Step 3 below.

Step 3. Provide IdP information to the Service Provider administrator

Now that you have your IdP configured, you need to provide this information to your Service Provider so they can configure their side of the trust.



Copy the **Metadata URL** and provide this to the Service Provider administrator. They can enter this into their system, which will auto-configure:

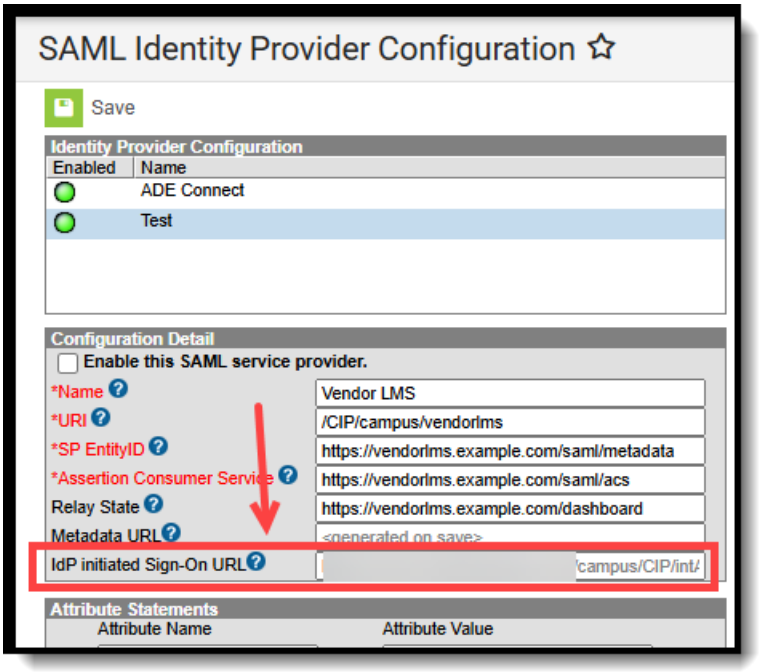
- Campus' Entity ID
- Campus' SSO endpoint
- Campus' signing certificate

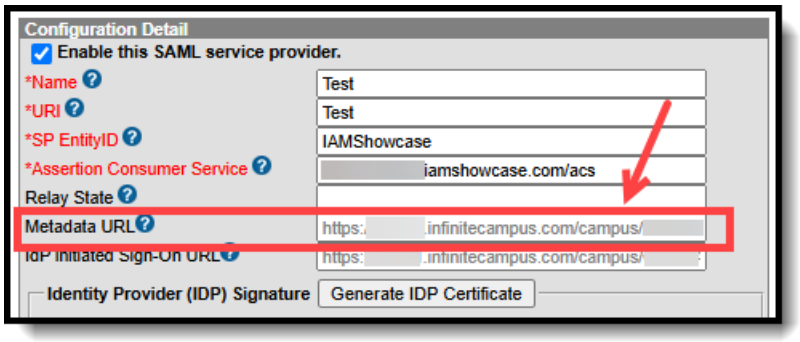
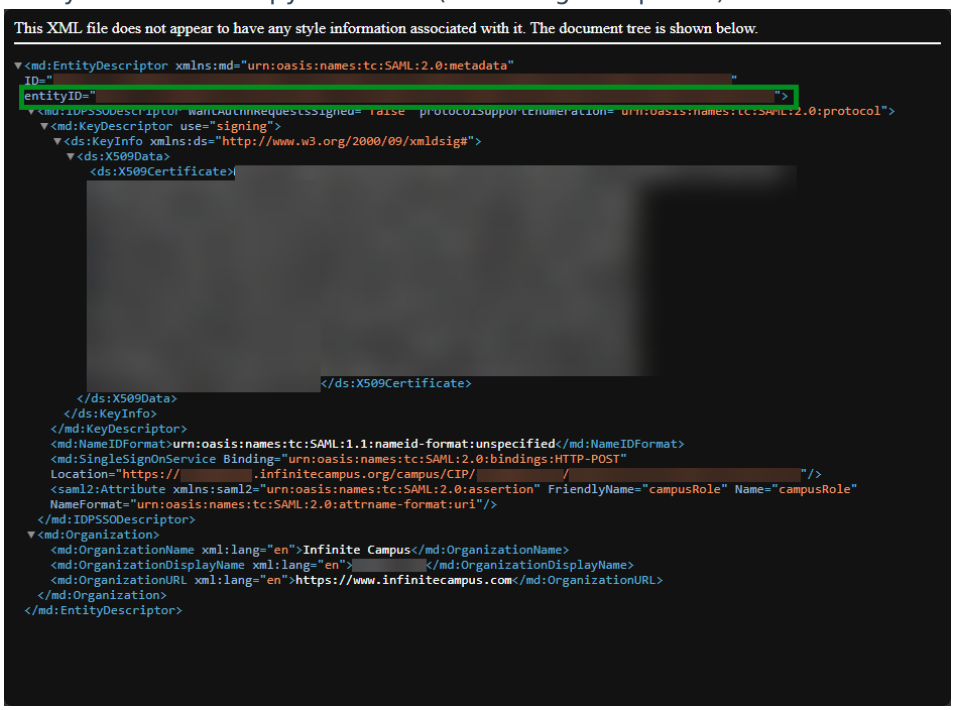
If your Service Provider doesn't support metadata import, follow the guidance below:

Click here to expand...

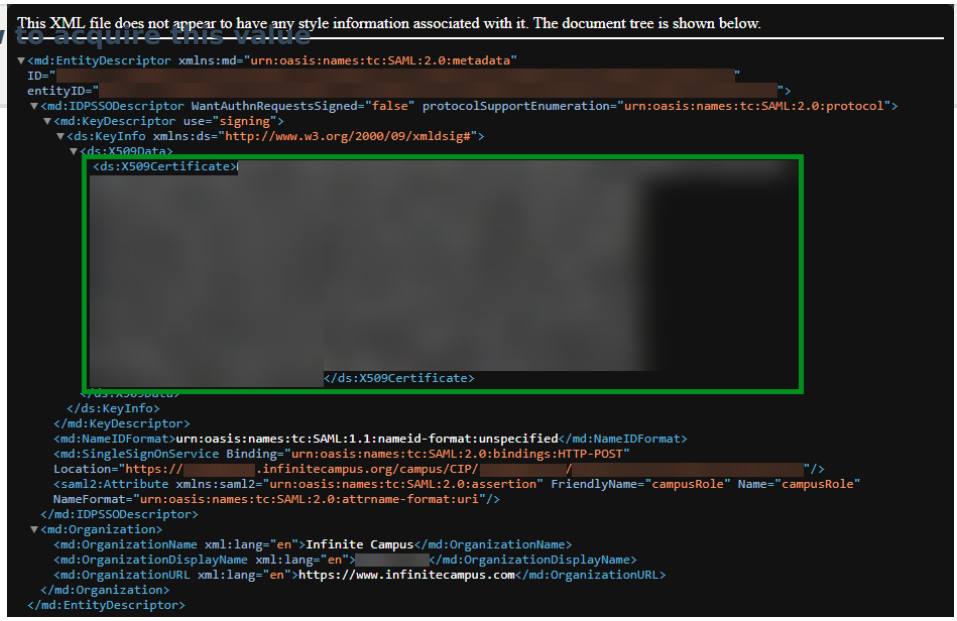
Note: Hit **Save** on the SAML Identity Provider Configuration screen to ensure values are saved and populated.

Metadata value	How to acquire this value

Metadata value	How to acquire this value
IDP Sign In URL	To obtain the IDP Sign In URL, on the SAML IDP Configuration screen, copy the **Idp Initiated Sign-On URL** and paste it into the Service Provider's IDP Sign-On URL field (or whatever related term the Service Provider users for IDP Sign-On URL) 

Metadata value	How to acquire this value
IDP Entity ID	1. Copy the **Metadata URL**. If this isn't showing, click **Save** to generate it.  2. Navigate to the Metadata URL in a browser. In the resulting XML, find entityID="..." and copy the value (excluding the quotes).  3. Paste this entityID into the Service Provider's IDP Entity ID field (or whatever related term the Service Provider uses for IDP Entity ID).
IDP certificate	Infinite Campus' default means of communicating the certificate is through the metadata URL, but when the Service Provider does not support that, it can be exported manually as a file. 1. Navigate to the Metadata URL in a browser. In the resulting XML, find the <ds:X509Certificate> tag.

Metadata value	How to acquire this value



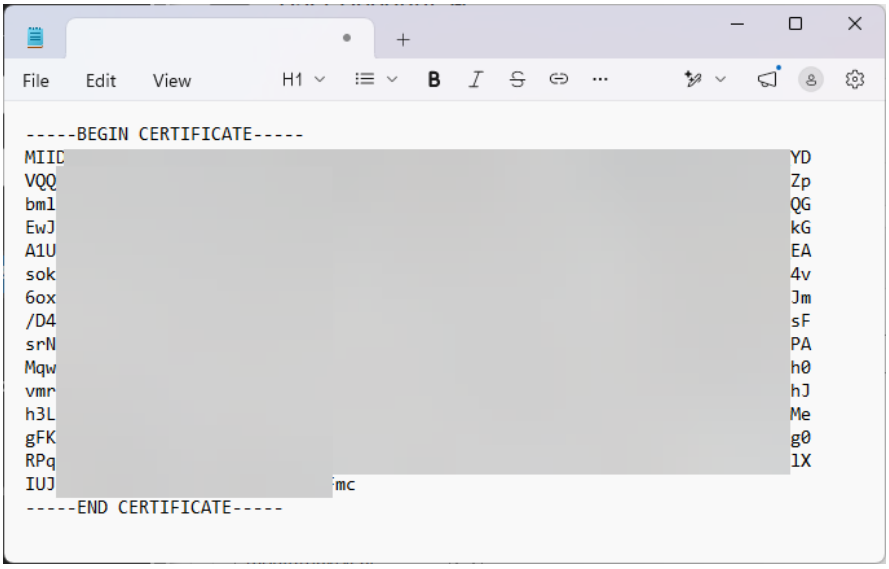
2. Copy the value between those tags. Do not include <ds:X509Certificate> or </ds:X509Certificate>.
3. Create a new text file (use Notepad or something similar). The file will have a header, the certificate contents, and a footer.
   a. Start the file with the line

      ```
      -----BEGIN CERTIFICATE-----
      ```

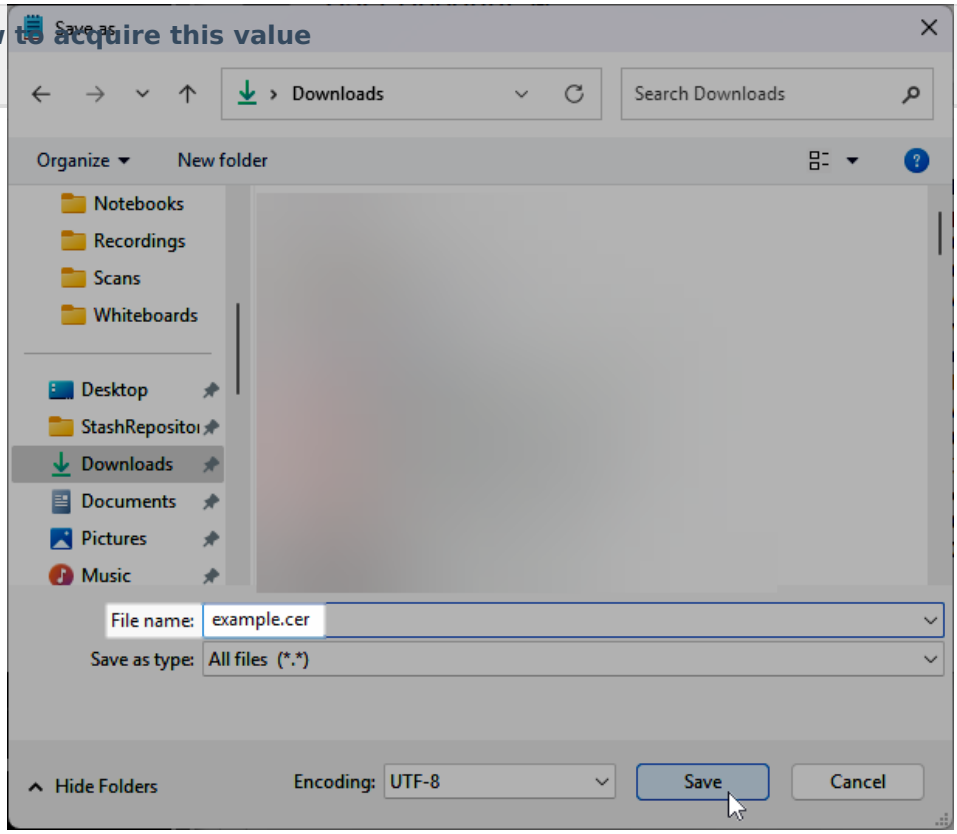
   b. On a new line, paste in your certificate value. (Again, do not include <ds:X509Certificate> or </ds:X509Certificate>.)
   c. On a new line, end the file with the line

      ```
      -----END CERTIFICATE-----
      ```

   d. Once complete, it should look like this.



4. Save that as a file with a .CER extension:

Metadata value	How to acquire this value
	 5. Upload the resulting .CER certificate file into your SAML Service Provider system. Note: If your Service Provider has a field to enter a Sign Out URL, leave it blank. Single Sign Out is not supported by the SAML IdP Configuration tool.

Step 4. The Service Provider administrator configures their side

Once the Service Provider has your IdP information, they must configure their side and confirm completion of this task before you can proceed. Typically, the Service Provider needs to:

1. Import the metadata (or manually enter Entity ID, SSO endpoint, and certificate).
2. Configure which attributes they expect from Campus.
3. Map those attributes to their internal user fields.
4. Enable the trust relationship on their end.

This step is completed entirely outside of Campus. Coordinate timing with the Service Provider administrator so that both sides are ready before testing.

Step 5. Test the IdP-initiated SSO

Once both sides are configured, it is now time to test the IdP-initiated SSO.

1. Log in to Campus, then click the configuration in the SAML Identity Provider Configuration tool.
2. Click the **Test** button.
    - Campus will generate a SAML response with your user data and post it to the Service Provider's ACS URL.
3. If everything is configured correctly, you will be authenticated and redirected to the external application or to the URL specified in the **Relay State** field.

The Service Provider can also test their side of things by accessing the external application utilizing the SSO connection, clicking the Login with SSO (or however the Service Provider presents it), and, if already logged into Campus, ensuring they are authenticated and logged in to the external application. If they are not logged into Campus, they should be presented with a Campus login page, and once logged in, redirected and logged into the external application.

Step 6. Deploy to users and add the link to Campus

Now that your Campus IdP configuration is complete and testing was successful, users can utilize this authentication in two ways:

Authentication Point	Details
Navigating to the external application when in Campus	You can add a link to the external application within Campus by adding it as a URL Link via Custom Tool Setup. This allows the application to appear as a selectable item within Campus, automatically logs them, and redirects them to the application when selected.
Logging into the external application via SSO	Users attempting to log in to the external application can click the SSO login option on that application's login page. If they are already logged in to Campus, they will be automatically logged in to the external application. If they are not logged in to Campus, they will be redirected to the Campus login screen, where they must enter their Campus credentials.

Troubleshooting

Issue	Likely Cause
Metadata URL returns nothing	Entry wasn't saved successfully, or URI is invalid
SP rejects the SAMLResponse	Certificate wasn't imported correctly on the SP side, or SP EntityID/Audience mismatch

"No user in session" redirect loop	Same-site cookie issue, or the user isn't logged into Campus
SP receives a response but can't identify the user	Identity claims not configured, or attribute names don't match what the SP expects
Works for one user but not another	Ad hoc filter doesn't return data for that user, or claims return null for users missing certain data
Stops working after ~1 year	Certificate expired (365-day validity, no auto-renewal)

Ongoing Maintenance

Certificate Renewal	When the certificate expires, regenerate it via the **Generate IDP Certificate** button, then coordinate with the Service Provider administrator to re-import the metadata or upload the certificate on their side. Campus does not warn users when a certificate is expiring, so you will need to monitor the date to generate a new certificate and avoid any disruptions.
Attribute Statement Changes	If the Service Provider changes what attributes they need, you will need to update the Attribute Statements, save the configuration changes, and re-test the configuration.
URI changes	Avoid at all costs. Changing the URI changes all endpoint URLs and breaks the trust relationship on the SP side. It would require full reconfiguration on both sides.