SAML - SSO Login Report

Last Modified on 07/14/2025 10:30 am CDT

This report displays a record of all SAML login attempts for the past 7 days. Using this data, users can audit SSO logins on their system and troubleshoot issues they may be experiencing.

The table below explains each column in the report:

Column	Description
Timestamp	The exact date and time the user logged into Campus using SSO authentication.
Log ID	A unique identifier given to each login attempt. This identifier is useful when working with Campus Support on SSO-related issues.
Username	The username of the person who logged in (or attempted to log in) using SSO authentication. This field will be blank if the username was not yet passed to our system when the login entry was recorded.
Message Level	Indicates if the record is informational (for example, a login attempt was initiated, or the user successfully logged in) or if an error occurred.

Column	Description
Message	The information recorded regarding the login attempt. Information that may appear here includes an indication that an SSO login attempt was started and received from a specific IDP, whether an identifier was converted to a specific nameID, or whether an error was encountered and what occurred. See the Understand Report Messages section below for detailed information about each report message.
Configuration Name	Name of the SSO configuration used to log into Campus (set in the Name for Login Button field in the SAML - SSO Service Provider Configuration tool).
Identification Attribute	The attribute used for identification (often the username or nameID).

Each column of the report can be filtered by searching for a specific value as well as applying additional search logic to the value entered.
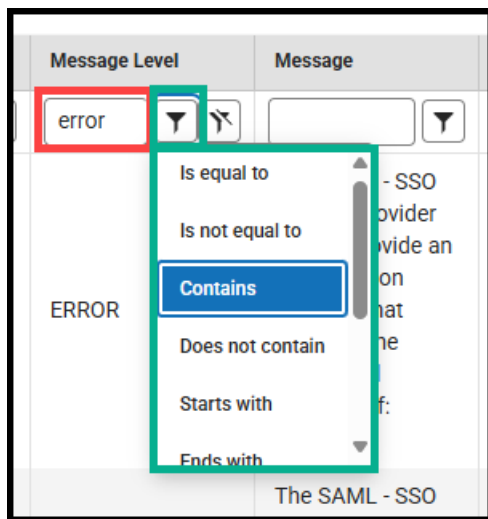
Understand Report Messages

Expand the link below to learn more about each reported message.

Message Level	Message	More Information

Message Level	Message	More Information
WARN	SAML - SSO configuration chosen because it is the only existing config (will cause exception if second config is added). Consider adding idpEntityID to the (single sign-on) URL.	Currently, your Infinite Campus site has only one SAML/SSO configuration set up. If, in the future, another one were to be added, Campus would not be able to distinguish between the two. To correct this and future-proof your connection, you'll need to re-provide the full Single Sign-On URL to your Identity Provider. Navigate to SAML -SSO Service Provider Configuration and copy/paste the full Single Sign-On URL into the corresponding field within your Identity Provider's system. Or, if your Identity Provider obtains that value through metadata, copy/paste the full Service Provider Metadata URL into your Identity Provider, then resync metadata within your Identity Provider.
INFO	"SAML -SSO Login successful for " + username	This message communicates that a SAML/SSO login was successfully completed for the indicated username.
INFO	"Identifier converted to:" + System.lineSeparator() + username	This message communicates that the identifier was converted (usually due to Domain Suffix handling settings) to the identifier recorded above during a login request
INFO	"Identifier from SAML -SSO Identity Provider:" + System.lineSeparator() + username	This message clarifies the identifier the Identity Provider sent during the login request. This identifier must correspond to an Infinite Campus username.
INFO	SAML - SSO login attempt started. SAMLResponse received from " IdPUrl	This message communicates that a SAML/SSO login process has been initiated and includes the Identity Provider URL from which the SIS received a SAML/SSO Response.
ERROR	Missing SAML - SSO Service Provider Configuration	This indicates that Campus could not find the SAML/SSO configuration. Please make sure that the configuration is still set up properly in the SAML-SSO Service Provider Configuration tool in Campus.

Message Level	Message	More Information
ERROR	"Failed to parse the SAML -SSO message." + e.getMessage() This e.getMessage is any error that happens while parsing the SAML message. Some errors we've seen in the past include: • Input string was null. • InputStream cannot be null	This error can indicate several things. Make sure that your Identity Provider has been provided the correct information from your Infinite Campus site. This could mean your Identity Provider is configured to look for a value other than the one you entered in SAML—SSO Service Provider Configuration > Optional Attribute Name. Ensure that the field is not empty and is set to whatever your Identity Provider is configured to send (usually nameID). This error could also be caused by a networking issue, usually temporarily.
ERROR	Failed to get keystore! Failed to get keystore! Failed to load SAML - SSO Identity Provider Certificate Failed to get keystore! Failed to get cert DB password	This type of error message indicates an issue with the keystore that stores the certificate associated with the SSO connection. Have your Authorized Contact reach out to Campus Support for assistance in identifying and resolving the underlying cause.
ERROR	SAML - SSO validation failed: This category of error indicates an issue during the SAML validation part of the process. Specific examples include: • "SAML -SSO validation failed: SAML -SSO response authn assertion does not contain conditions." • "SAML -SSO validation failed: Authn assertion does not contain conditions."	Ensure the Identity Provider is configured to send the correct conditions. Navigate to SAML -SSO Service Provider Configuration and note the Service Provider Entity ID and Single Sign-on URL. Ensure these values match the corresponding fields in the Identity Provider system. Or, if your Identity Provider supports it, re-provide your Identity Provider with the full Service Provider Metadata URL and resync metadata within your Identity Provider.

Message Level	Message	More Information
ERROR	"SAML -SSO response authn assertion conditions audience restrictions do not contain any audiences." "SAML -SSO response audience does not match expected audience."	This indicates that the "audience" (EntityID) is not configured or not configured correctly within your Identity Provider. Navigate to SAML -SSO Service Provider Configuration and note the Campus (Service Provider) Entity ID value. Ensure this value matches the corresponding Entity ID field in the Identity Provider system; if it doesn't, update your Identity Provider to match what is in Infinite Campus. Or, if your Identity Provider supports it, re-provide your Identity Provider the full Campus (Service Provider) Metadata URL and resync metadata within your Identity Provider.
ERROR	"The SAML -SSO message expired."	The SAML login request has timed out. This value can be modified at SAML -SSO Service Provider Configuration > Campus SSO Preferences > Request Timeout and set to a longer duration if desired.
ERROR	"SAML -SSO response or Authn assertion must be signed."	Please ensure that the Identity Provider is configured to sign the assertions.
ERROR	"Response doesn't have any valid assertion which would pass subject validation"	This can be indicative of a few different issues. Verify that the Identity Provider has a valid certificate and the correct entity ID and Single Sign-on URL: • Navigate to SAML -SSO Service Provider Configuration and note the Campus (Service Provider) Entity ID and Single Sign-On URL values. Ensure these values match the corresponding fields in the Identity Provider system; if they don't, update your Identity Provider to match what is in Infinite Campus. Or, if your Identity Provider supports it, re-provide your Identity Provider the full Campus (Service Provider) Metadata URL and resync metadata within your Identity Provider.

Message Level	Message	More Information
ERROR	"Invalid destination"	The destination value the Identity Provider sent to Campus does not match up with the destination Campus was expecting. This value is case sensitive. Please confirm the Identity Provider has been provided the correct Single Sign On URL: Navigate to SAML -SSO Service Provider Configuration and take note of the Single Sign-On URL value. Ensure this value matches the corresponding field in the Identity Provider system; if it doesn't, update your Identity Provider to match what is in Infinite Campus. Or, if your Identity Provider supports it, re-provide your Identity Provider the full Campus (Service Provider) Metadata URL and resync metadata within your Identity Provider.
ERROR	"Response has invalid issuer: " + <idpEntityID sent from IdP>+ " was expecting: " + <Stored iDPEntityID>	The entityID that was sent by the IDP does not match the one stored in Campus for this configuration.
ERROR	"Failed to refresh metadata"	Campus could not retrieve the metadata, which could indicate a keystore issue. Please have your Authorized Contact contact Campus Support.

Message Level	Message	More Information
ERROR	"Invalid public key!"	The certificate that was used for this is likely not correct. If you have more than one SSO configuration within your Identity Provider, ensure you've provided a Metadata URL/Metadata XML file from the correct one. Navigate to SAML -SSO Service Provider Configuration and note the certificate information under Identity Provider (IDP) Signature. Verify that this information matches the certificate the Identity Provider is currently using for their corresponding SSO app. If you're using a Metadata URL, hit Sync and Save, and check again. If you're using a Metadata XML file, you may have to re-export a fresh Metadata XML from your Identity Provider with up-to-date certificate details.
ERROR	"Invalid signature profile" "Invalid signature!"	The certificate that was used for this is not correct. If you have more than one SSO configuration within your Identity Provider, ensure you've provided a Metadata URL/Metadata XML file from the correct one. Navigate to SAML -SSO Service Provider Configuration and note the certificate info under Identity Provider (IDP) Signature. Verify that this info matches the certificate the Identity Provider is currently using for their corresponding SSO app. If you're using a Metadata URL, hit Sync and Save, and check again. If you're using a Metadata XML file, you may have to re-export a fresh Metadata XML from your Identity Provider with up-to-date certificate details. The certificate that was used for this is not correct. Verify that the metadata in the SSO configuration page matches the metadata provided by the IDP.

Message Level	Message	More Information
ERROR	"The SAML -SSO Identity Provider did not provide an identification attribute that matches the configured attribute of: " + usernameAttributeName	This indicates that during login, the SAML/SSO Identity Provider did not send over the attribute Campus was expecting. This could mean your Identity Provider is configured to look for a value other than the one you have entered in SAML –SSO Service Provider Configuration > Optional Attribute Name. Ensure that the field is not empty and is set to whatever your Identity Provider is configured to send (usually nameID).
ERROR	"Not able to find username!"	Ensure that the user account exists in Infinite Campus and verify that the Authorization Type drop-down menu is set to the correct SAML/SSO configuration(not Local Campus Authentication or LDAP).
ERROR	"The identifier '" + userName + "' sent from the SAML -SSO Identity Provider does not exist in SIS."	This indicates that the identifier indicated does not correspond to an Infinite Campus username. That user may not exist in Infinite Campus.
ERROR	"The user '" + userName + "' sent from the SAML -SSO Identity Provider is not configured for SAML authentication in SIS."	This indicates that the user account is not configured to use SAML SSO. Navigate to the User Account screen, change the Authentication Type to the correct SAML (SSO) option, and save.
ERROR	"Incorrect SAML -SSO configuration ID, '" + <auth.samlConfigurationID> + "' doesn't match the configuration ID of: '" + <Stored samlConfigurationID> + "'"	The SAML/SSO configuration that was used to log in does not match the stored SAML/SSO configuration for the user account. Please ensure that the user account is configured to utilize the expected SAML/SSO configuration on the User Account screen.
ERROR	"PIV card authentication is enabled"	This indicates that the account is enabled for PIV card authentication and cannot be authenticated with SAML/SSO. Change the account Authentication Type on the User Account screen to the correct SAML (SSO) option.
ERROR	"User Account is disabled for User " + username	This indicates that the user account is disabled and, therefore, cannot be logged into. If this account was disabled in error, you can enable it on the User Account screen.

Message Level	Message	More Information
ERROR	"User Account is expired for User " + username	This indicates that the user account has expired and cannot be logged into. If the account expired in error, you can remove the Account Expiration Date on the User Account screen.
ERROR	"User Account is invalid for User " + username	This error indicates that something went wrong with the login. Make sure the SAML/SSO configuration is enabled, the User Account is active, and its Authentication Type is set to the correct SAML (SSO) option, and that the SAML/SSO configuration has been done correctly.