

Admin App Guide for Okta SAML Integration

Prerequisites AML Background

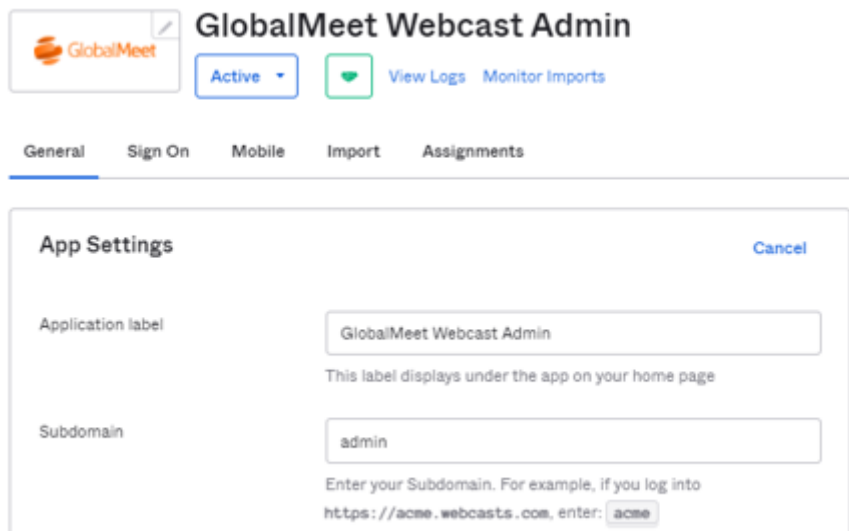
Users that need to be enabled for SAML login will need an existing account and license on the Webcasts Platform.

Supported Features

- IdP-initiated SSO

Procedure

1. From the Okta Integration Network, search and install the "GlobalMeet Webcast Admin" app.
2. During the setup process, in the "General" settings, if you are using a custom subdomain to login on the Webcasts Admin, enter that value into the "Subdomain" field, otherwise enter "admin" and Save."



The screenshot shows the 'GlobalMeet Webcast Admin' app configuration page in Okta. At the top, there's a header with the app name and a status 'Active' with a dropdown arrow. Below this are links for 'View Logs' and 'Monitor Imports'. A navigation bar contains tabs for 'General', 'Sign On', 'Mobile', 'Import', and 'Assignments', with 'General' being the active tab. The main content area is titled 'App Settings' and includes a 'Cancel' button in the top right. It features two input fields: 'Application label' with the value 'GlobalMeet Webcast Admin' and a descriptive text 'This label displays under the app on your home page'; and 'Subdomain' with the value 'admin' and a descriptive text 'Enter your Subdomain. For example, if you log into https://acme.webcasts.com, enter: acme'.

GlobalMeet Webcast Admin

Active ▾ View Logs Monitor Imports

General Sign On Mobile Import Assignments

App Settings Cancel

Application label GlobalMeet Webcast Admin
This label displays under the app on your home page

Subdomain admin
Enter your Subdomain. For example, if you log into https://acme.webcasts.com, enter: acme

- Next, from the "Sign On" tab, click on Identity Provider metadata below the "View Setup Instructions" button. Copy this and email to your GlobalMeet SAML contact.

General

Sign On

Mobile

Import

Assignments

Settings

Edit

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.
Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

Disable Force Authentication ☒

SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

Credentials Details

Application username format

Email

Password reveal ☐ Allow users to securely see their password (Recommended)

- Once your GlobalMeet SAML contact completes the integration, you will be provided with a "Default Relay State" value. On the "Sign On" tab, enter the provided Relay State value.

Settings

[Cancel](#)

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0 is the only sign-on option currently supported for this application.

SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState.

Attributes (Optional) [Learn More](#)

Disable Force

☒

Authentication

Never prompt user to re-authenticate.

[Preview SAML](#)

5. On the "Application Username Format", select "Email" and save.



SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

Credentials Details

Application username format

Email



Password reveal

☐ Allow users to securely see their password
(Recommended)



Password reveal is disabled, since this app is using SAML with no password.

[Save](#)

6. Done! Now you should be able to login to Webcast Admin platform from the Okta User Dashboard.

References

- <https://www.okta.com/integrations/globalmeet-webcast-admin/>
- https://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-GlobalMeet-Webcast-Admin.html

Non-Okta Customers

The workflow is same as Okta; however, setup steps will depend on what platform you are using. From your system we will need the following information or MetaData XML that contains these fields.

- IDP Sign in URL
- IDP Entity ID
- IDP Certificate
- Webcasts Subdomain you are currently using to login into the webcast platform. The default is admin.webcasts.com however you may have a custom URL such as companyname.admin.webcasts.com

Once you provide the above information the configuration will be setup on your GlobalMeet account. We will provide you with a RelayState and Service Provide Consumer URL to complete your SAML SSO setup. Please note, we currently we only support integration where email is part of the NameID.

FAQs

1. Will 2 Factor Authentication work with SAML SSO? **Yes**

2. Do we support Guest logins? **No**
3. Do we support Encrypted Assertions? **No**
4. What is required information for configuration?

GlobalMeet Subdomain:

Metadata containing following items.

IDP Sign In URL:

IDP Entity Id:

IDP Certificate:

5. What happens if there are multiple users with same email?

SAML login will fail. SSO only allows a unique email.

6. What happens if a user's email is assigned to both an Admin account and Guest Admin account? **The user will be logged in with the Admin account.**
7. Reasons why SAML would fail?

- - Mismatching IDP SSO, EntityID, Certificate.
 - Invalid Relay State
 - The user trying to login is not under same License as configured in the setup.
 - Multiple usernames associated with the email.
 - Trying to pass Encrypted assertion.
 - Username passed as nameidentifier instead of email.