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.

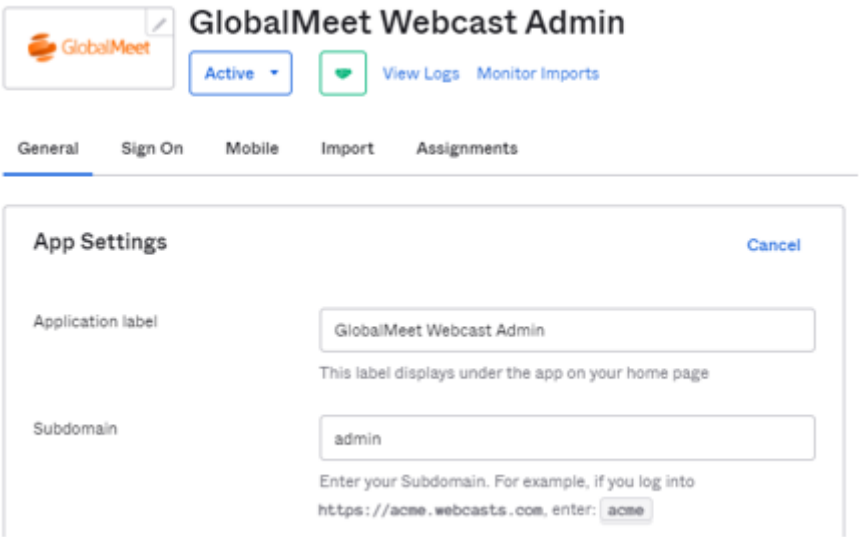
Supported Features

- IdP-initiated SSO

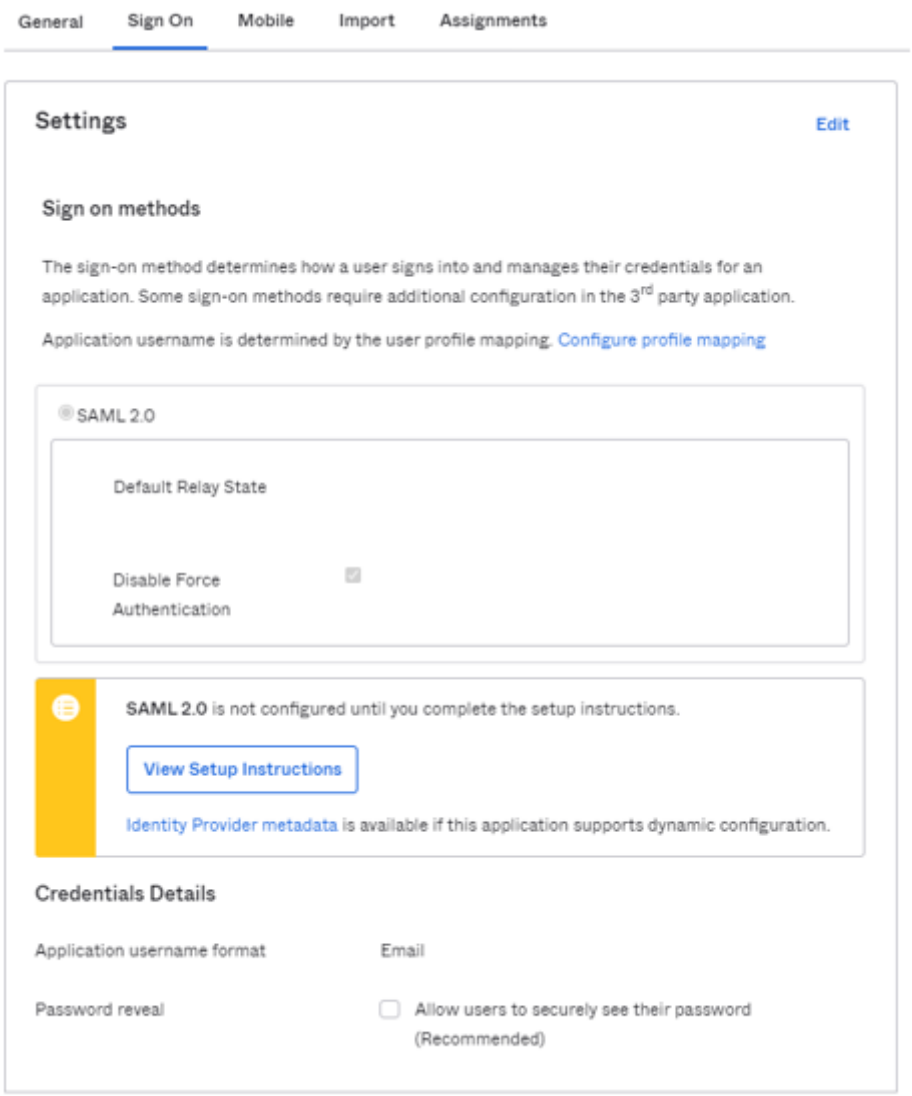
Procedure

1. From the Okta Integration Network, search and install the "GlobalMeet Webcast Admin" app.

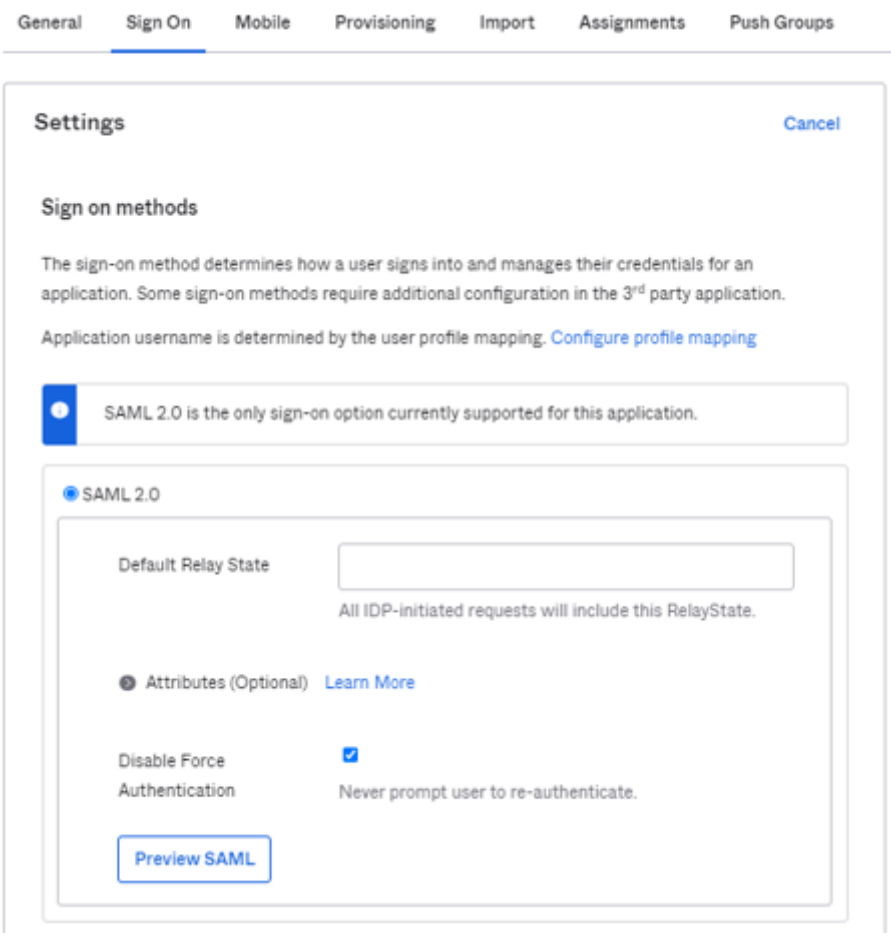
2. During the setup process, in the "General" settings, if you are using a custom subdomain to login on the Webcasts Admin, enter that value into the "Subdomain" field, otherwise enter "admin" and Save."



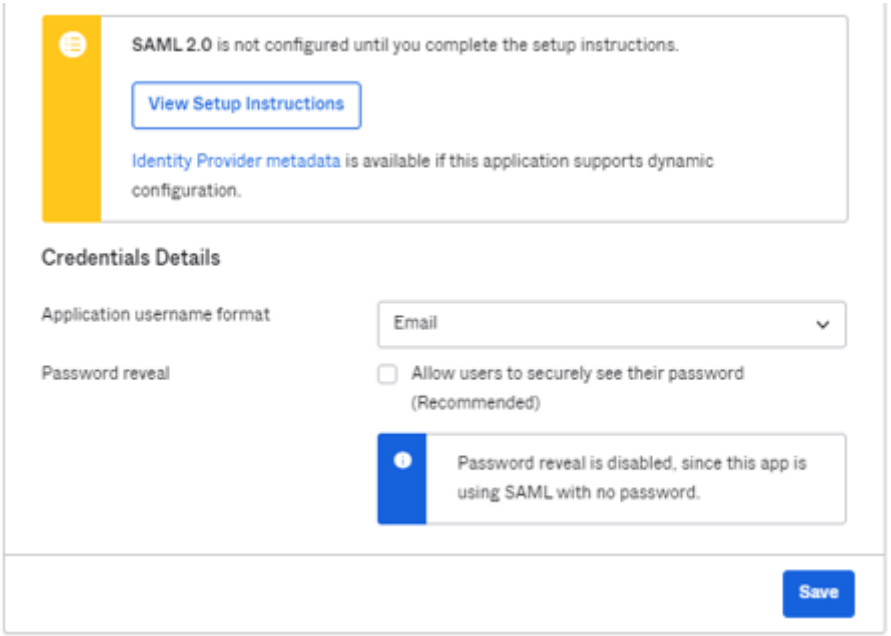
3. Next, from the "Sign On" tab, click on Identity Provider metadata below the "View Setup Instructions" button. Copy this and email to your GlobalMeet SAML contact.



4. 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.



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

Revision #2

Created 6 January 2023 19:13:17 by Matt Engel

Updated 6 January 2023 21:01:21 by Matt Engel