Background

Conferences i/o supports authentication integration with single sign-on (SSO) identity providers. This integration gives Conferences i/o customers direct control over who can access their Conferences i/o apps.

The Conferences i/o team strongly recommends SSO authentication integration to all customers looking to enhance the security and auditability of their Conferences i/o apps.

Document contents

Limitations with Virtual Apps

The Conferences i/o app for Zoom, MS Teams and Webex will not work for Conferences i/o apps with SSO enabled due to a technical limitation in the virtual platforms.

Supported SSO protocols

The following SSO protocols are directly supported by Conferences i/o:

- SAML 2.0
- OAuth 2.0

Other external authentication methods

Other authentication patterns and protocols may be available as a custom development (please talk to a Conferences i/o account manager).

Features of Conferences i/o SSO integration

Authentication scope

SSO authentication can be required for all users of a Conferences i/o app, or authentication can be limited to just administrative users.

Authentication timeout

An optional timeout can be added to require re-authentication at a regular cadence (for example, once per week). Without using a timeout, users will not be automatically required to re-authenticate.

On-the-fly provisioning

User accounts are provisioned on the fly, as users are authenticated.

User management portal

Accounts that have been provisioned in Conferences i/o can be reviewed, and their roles can be manually adjusted (making someone a moderator, an administrator, etc).

Before-leaving and after-returning splash pages

Optional splash pages can help explain to users why they are being redirected to authenticate, and then advise users about the success or failure of authentication.

OAuth 2.0

Setup process for OAuth 2.0

- A sandbox app may be created on Conferences i/o for the purpose of evaluating SSO.
- Credentials and endpoints are shared between Conferences i/o and customer (client ID, client secret, endpoints, etc).
- Customer identifies the scope of who should be authenticated through SSO (all users or only administrators).
- Customer selects the identity fields they would like mapped to user accounts in Conferences i/o.
- Integration is tested, primarily by the customer. Conferences i/o team is available to assist with testing if dummy accounts are created on identity provider.

OAuth-specific notes

- Conferences i/o only supports one endpoint for obtaining profile information. All identifying data that needs to be mapped to user records in Conferences i/o should be at this one endpoint.
- A unique user identifier field must be included with profile information about users.

SAML 2.0

Setup process for SAML 2.0

- A “sandbox” app may be created on Conferences i/o for the purpose of evaluating SSO.
- SAML metadata is created and exchanged.
- Customer identifies the scope of who should be authenticated through SSO (all users or only administrators).
- Customer selects the identity fields they would like mapped to user accounts in Conferences i/o. More information available below in “Consuming identifying information” section.
- SAML metadata and configuration is fully applied in both the identity provider (IdP) and service provider (SP).
- SSO is tested; Conferences i/o can assist if dummy accounts have been created in the IdP.

SAML-specific notes

- Only SP-initiated authentication is supported.
- NameID passed from the IdP can be any format, but should be a unique and consistent user identifier.
- Signed requests are supported, but not required.

Certificate expiration

The x509 certificate generated on the Conferences i/o side is typically set to expire in five years. This means that roughly once every five years, a new metadata exchange is required (unless certificate expiration is ignored).

SAML single log-out (SLO)

Conferences i/o supports IdP-initiated logout. If a user has been logged out from the IdP, and the logout endpoint of the SAML has been contacted by the IdP, then that user will be logged out of Conferences i/o.

Conferences i/o does not currently support SP-initiated SLO. All “logout” mechanisms within Conferences i/o are specific to Conferences i/o.

Mapping data from identity provider (IdP) to Conferences i/o

The only field automatically mapped to a user record in Conferences i/o is the unique user identifier the identity provider shares with Conferences i/o. For SAML, this is the NameID; for OAuth, this will be whatever is specified as the user ID field.

First name (given name), last name (family name), email address, and up to five (5) additional fields can be mapped to the user record. It is the customer’s responsibility to identify these fields and advise Conferences i/o before the integration configuration is finalized.

More information

- Standardized SAML2 attribute names:
  https://commons.lbl.gov/display/IDMgmt/Attribute+Definitions

Costs & fees associated with SSO

In most cases, there are setup and annual fees associated with SSO for Conferences i/o customers, beyond the costs of the core Conferences i/o license.

Next steps & turnaround time

Customers interested in adding SSO should reach out to their Conferences i/o account manager to inquire about pricing and get the SSO integration started.

When ready to proceed, customers should have responses for the following set of questions:

- What protocol will be used? (SAML or OAuth)

- Will all users be required to authenticate through SSO, or will authentication be limited to administrator-role users?
- What Conferences i/o apps (URLs) will be connected to SSO?
- Who is the customer's technical point of contact that Conferences i/o will be working with to complete the integration?

In most cases, SSO can be integrated and ready for testing within three (3) business days.

History & changes to this document

Version	**Date**	**Change Notes**
1.0	March 2022	Newly created document that merges separate SAML and OAuth information to provide a single source regarding SSO.
1.1	February 2023	Added information about Zoom App limitations