Intrado Single Sign On (SSO) Options

Overview

This document provides additional information for incorporating Single Sign On (SSO) into the Intrado environment and the options available to support authenticating Event Participant's information.

SSO is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems. True SSO allows the user to log in once and access services without re-entering authentication factors. When Event Participants join the Event using the login URL, they will be prompted to log in via their SSO login page. When signing in, the Event Participant's information is authenticated via the SSO and are logged into the Event, bypassing the need for additional login credentials.

As SSO provides access to many resources once the user is initially authenticated ("keys to the castle"), it also increases the negative impact in cases when credentials are available to other users and misused. Therefore, SSO requires an increased focus on the protection of user credentials and should be combined with strong authentication methods and one-time password tokens.

The below protocols are currently supported for use in the configuration of SSO access to Intrado:

- SAML - Security Assertion Markup Language

  SAML is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.

- ADFS - Active Directory Federation Services

  A software component developed by Microsoft can run on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries. It uses a claims-based access-control authorization model to maintain application security and to implement federated identity

- OAUTH 2.0 – Open Authentication

  An open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords. This mechanism is used to permit users to share information about their accounts with third-party applications or websites.

- Using Intrado API – Intrado Restful API - OpCode T

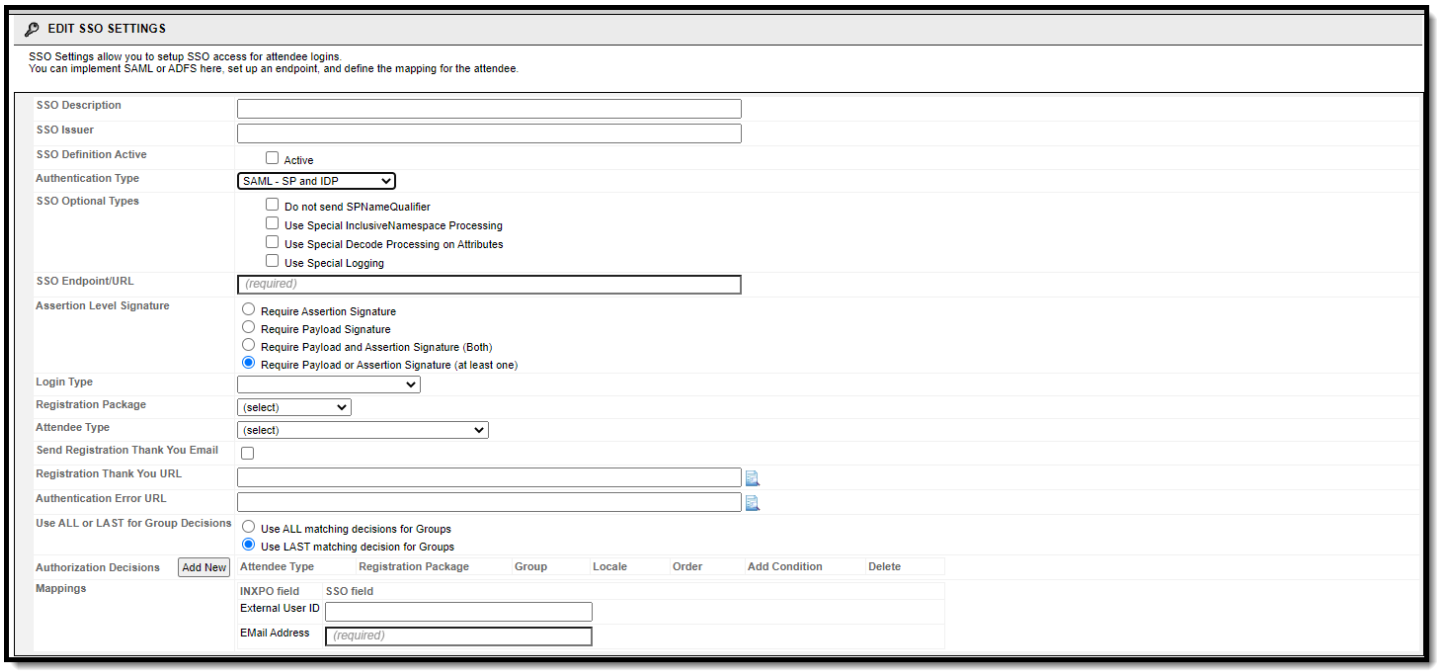
  This Intrado OpCode is used to create a login authorization ticket that is valid for 1 minute. This ticket token can be returned to the client browser with a specific redirect URL, allowing the client to launch the show without having to transmit the API credentials to their browser.

Review the information below for additional information for incorporating SSO in the Intrado environment.

Authentication Types:

Note: The Authentication Type selected will determine what information needs to be provided for configuration.

SAML



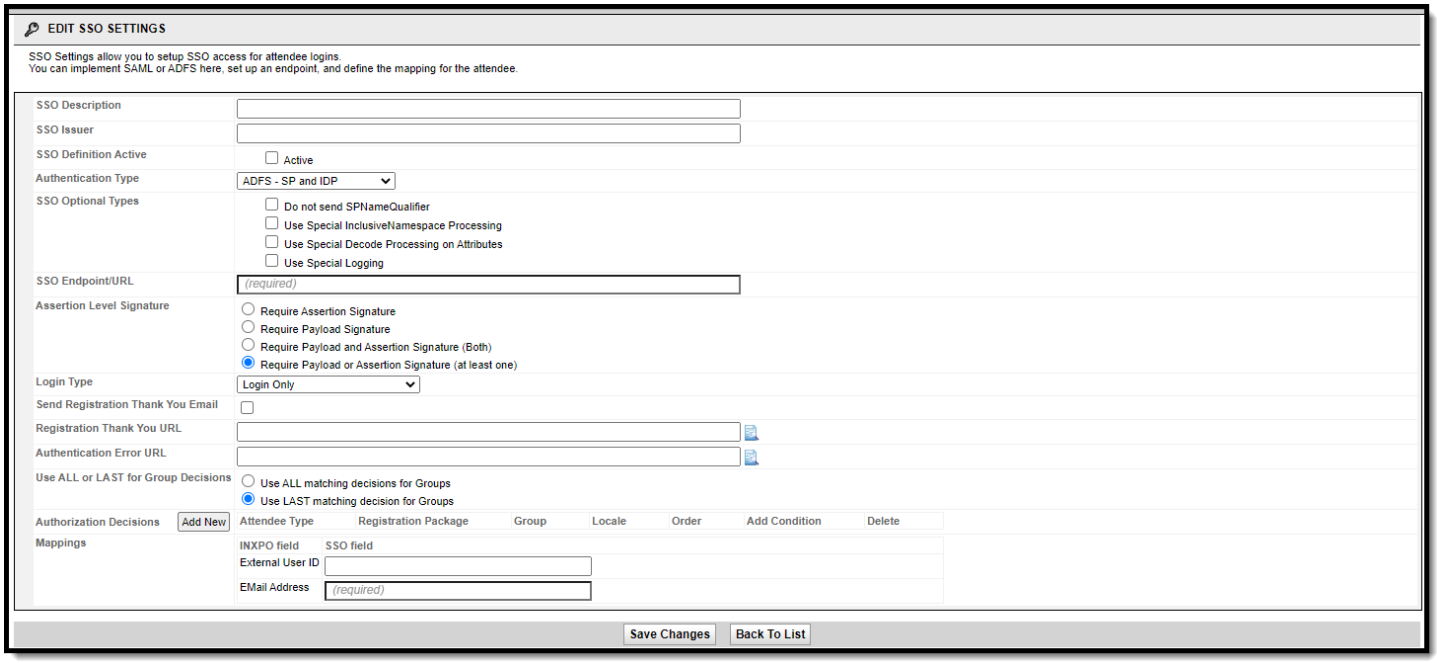
SAML options:

- SAML – SP and IDP
- SAML – SP only
- SAML – Signed SP and IDP
- SAML – Signed SP only
- SAML – Signed 2.0 SP only
- SAML – IDP only

The below configuration screen contains the input fields for the SSO definition settings:

ADFS

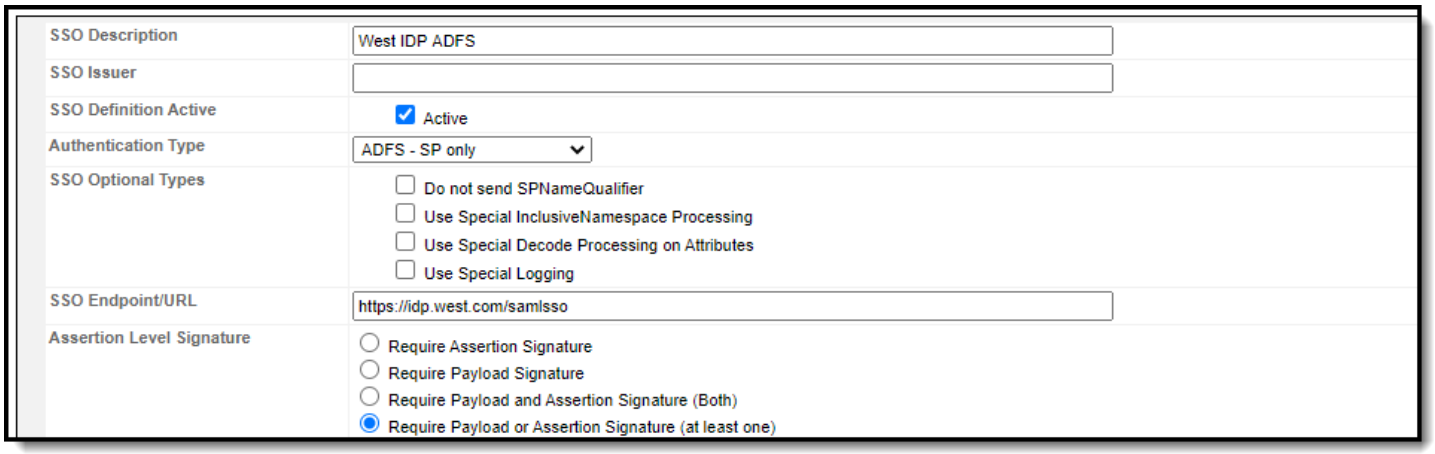
When Event Participants join the Event using the URL provided, they will be prompted to log in with their Customer Portal log in page. When signing in, the Event Participant is authenticated via the Active Directory and are logged into the Event, bypassing the need for additional login credentials.



ADFS options:

- ADFS – SP and IDP
- ADFS – SP only
- ADFS – IDP only

The below configuration screen contains the input fields for the SSO definition settings:

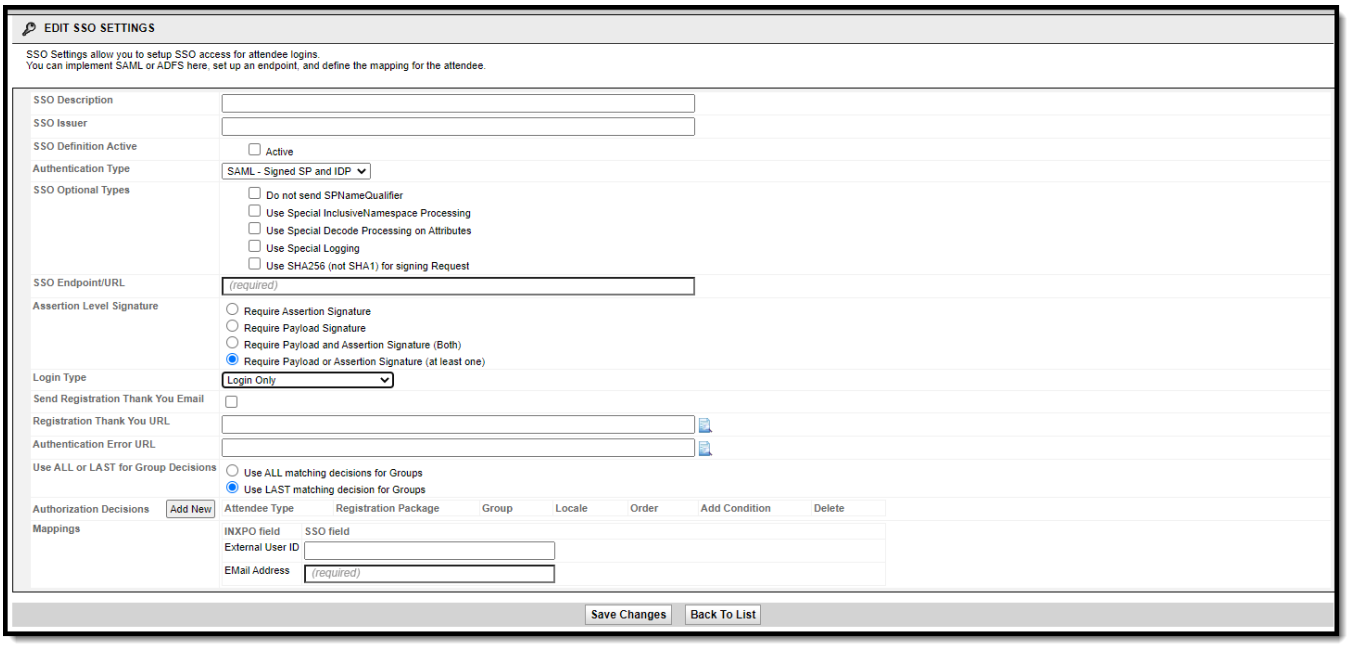


Additional Information:

Login Type options (SAML and ADFS only):

- Login Only: This option is used when Event Participants are already registered, created users, and the information has been provided in the payload.

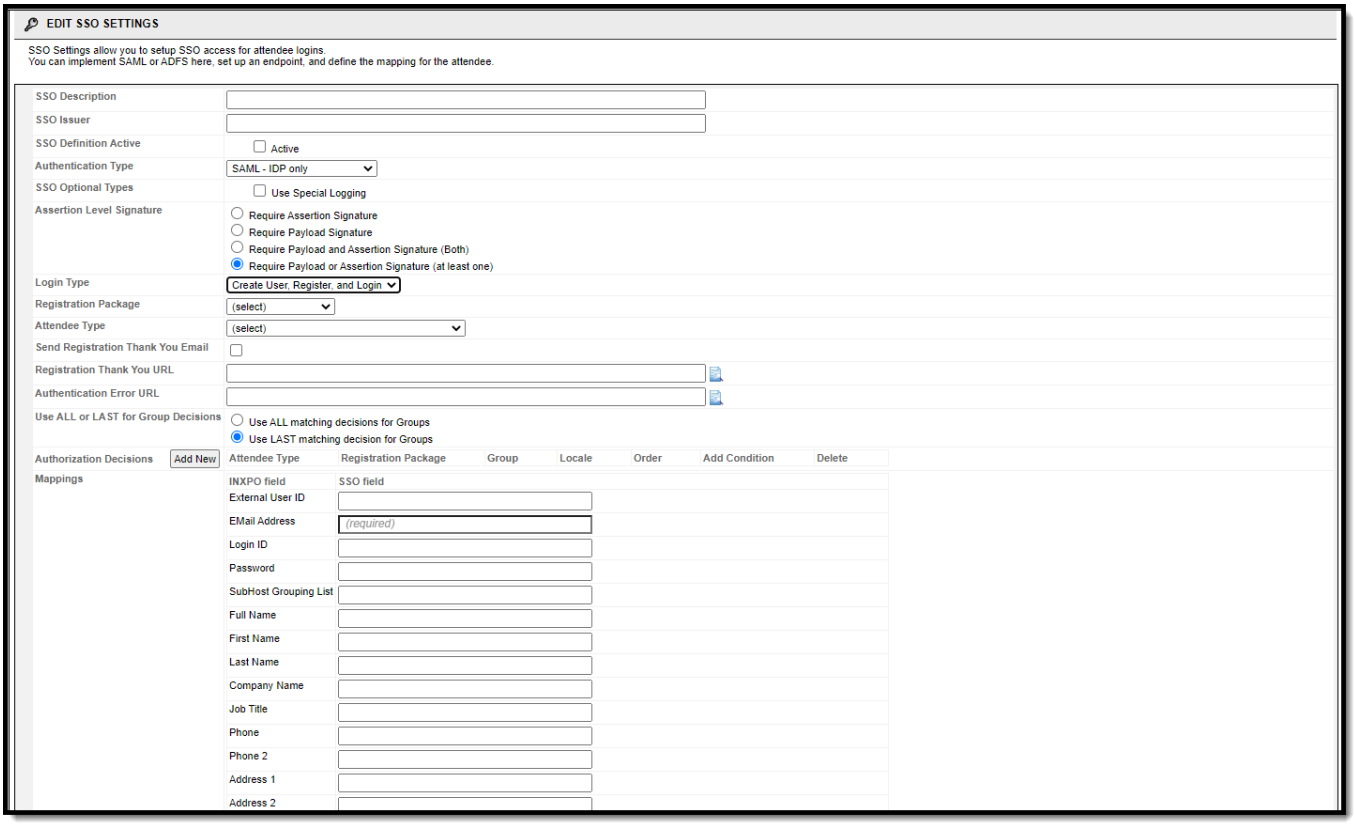
Example:



- Create User, Register, and Login: This option will create, register, and log in the Event Participant seamlessly after obtaining the information from SSO. Additional mapping fields will appear in the Mappings section to determine what information is gathered for registration. The labels in the payload will map to the fields in Intrado, as entered.
    - When selecting this option, the Registration Package and Attendee Type will need to be selected for the user to be registered correctly. Additional logic can be created in the Authorization Decisions section.

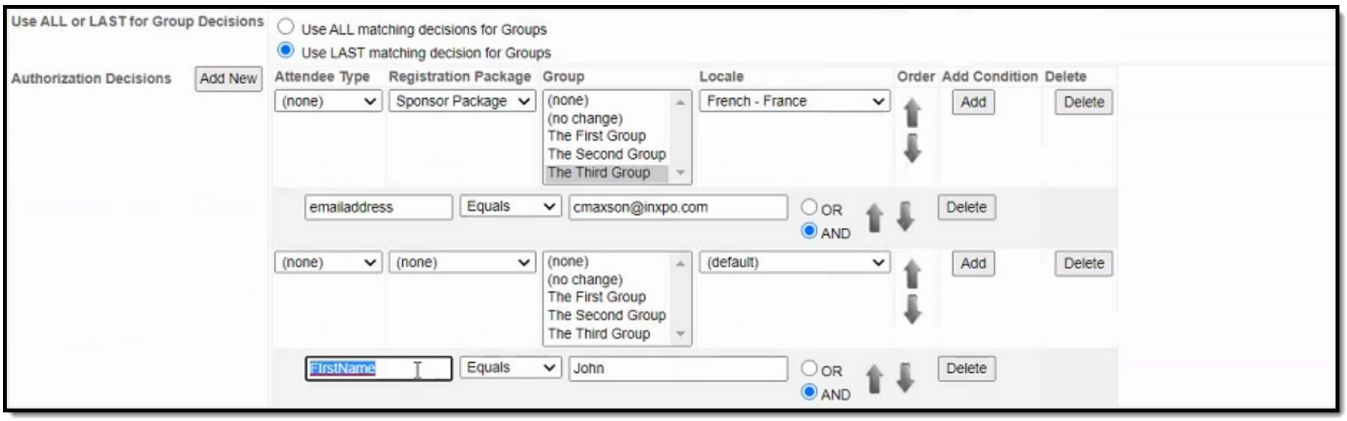
(continued)

Example:



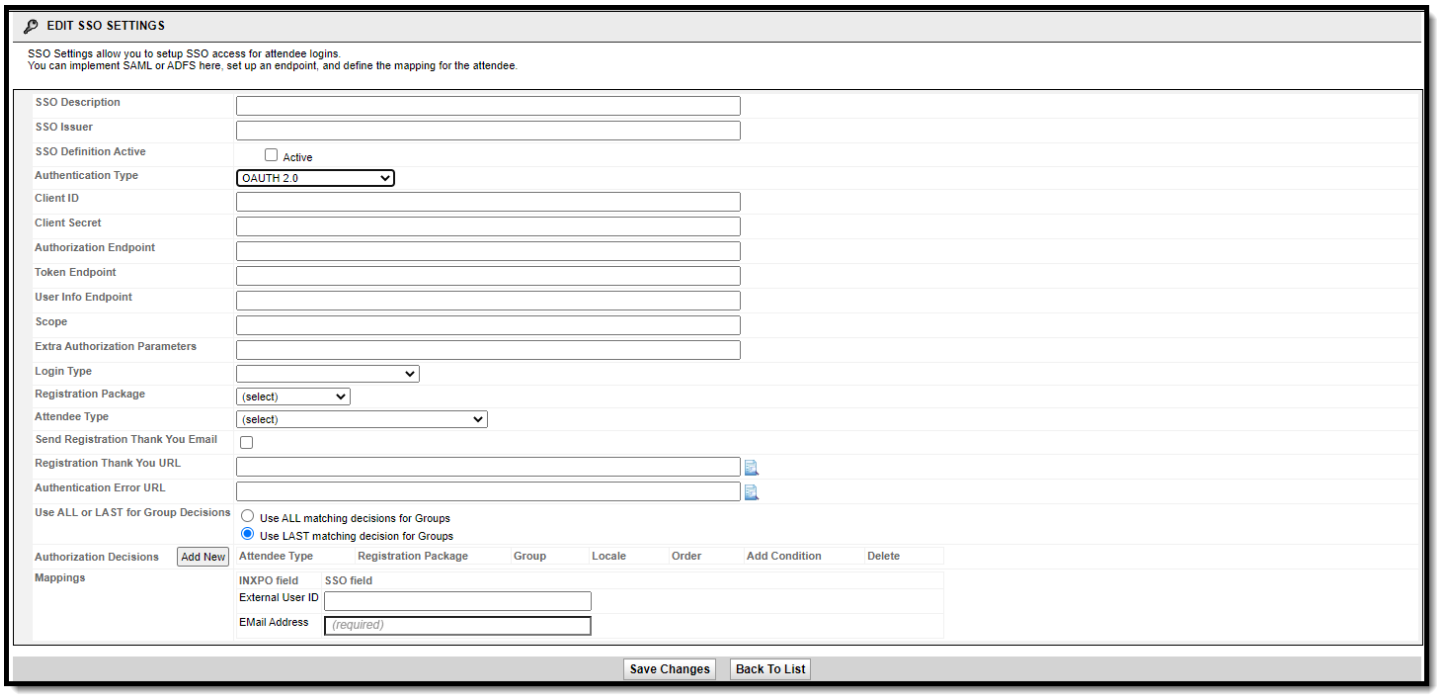
- Authorization Decisions: Authorization Decisions are defined as the controls when using the Create/Register User login function in SSO to auto-provision a user. In some scenarios, there is a need to define the user values at a more distinct level than the basic attendee types and registration packages. These more detailed attributes can be set based on rules that leverage mapping fields to set the attendee types, registration packages, User Groups, and Localization settings.

Example:

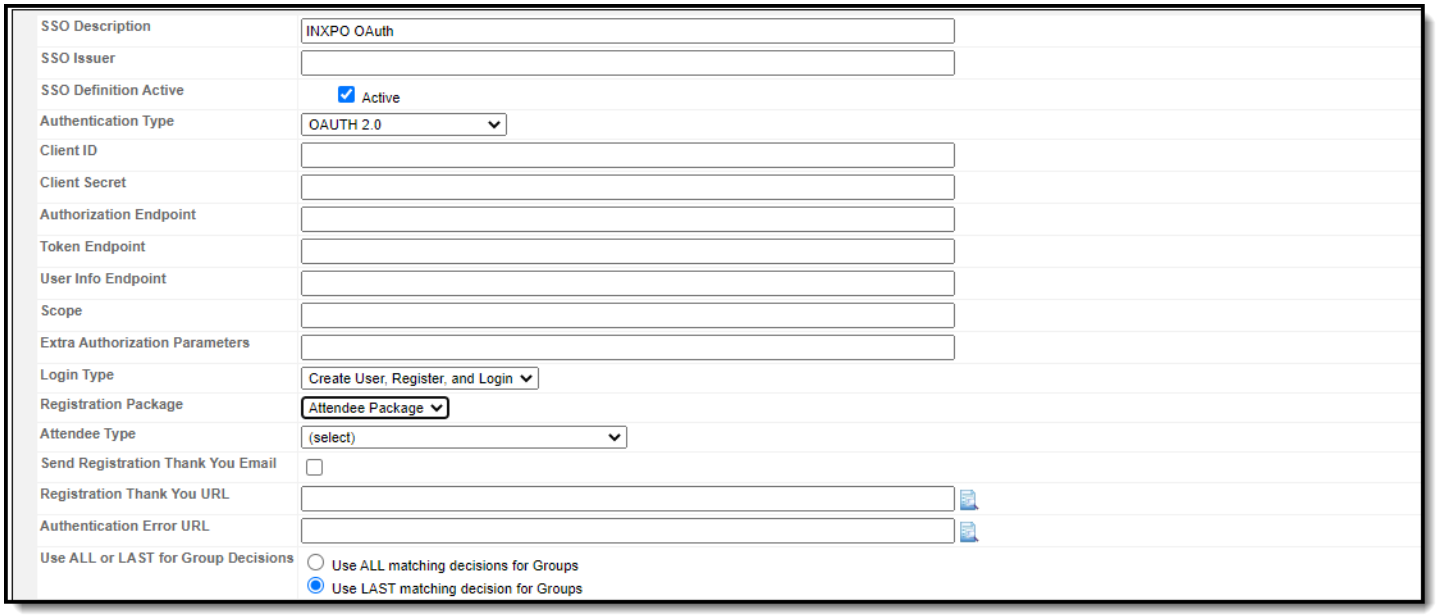


OAUTH 2.0

OAuth 2.0 is an open authentication standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords. This mechanism is used to permit users to share information about their accounts with third-party applications or websites



The below configuration screen contains the input fields for the SSO definition settings:



Using Intrado API when not using an authentication provider

Inrtrado API can be utilized as an alternative option for SSO when not using an authentication provider. This option creates a login authorization ticket that will validate the Event Participant and log them into the Event, bypassing the need for additional login credentials.

OpCode T is used to create a login authorization ticket that is valid for 1 minute. This ticket token can be returned to the client browser with a specific redirect URL, allowing the client to launch the show without having to transmit the API credentials to their browser.

API Parameter	Type/Size	Required	Comment
APIUserAuthCode	varchar 80	Y	Your API authorization code as supplied by Intrado.
APIUserCredentials	Varchar 80	Y	Your API user credentials as supplied by Intrado.
OpCodeList	Varchar 20	Y	Should include T to invoke this function.
OutputFormat	Char 1	N	T for text, H for HTTP URL-encoded, or X for XML. Defaults to T.
LookupByExternalUserID	Bit (0/1)	N	Pass 1 to lookup this person by the supplied ExternalUserID (your internal identifier).
ExternalUserID	Varchar 255	-	Your internal identifier for this person. This value must be unique for each person.
EMailAddress	Varchar 255	-	The person's email address.
ShowKey	Integer	Y	The show identifier to launch.
ShowLaunchInitialDisplayItem	Varchar 20	N	The show module to navigate to upon launch of the show. This consists of a type prefix followed by an item key. The valid type prefixes are S for Show Floors, E for Events, EL for Event Lobbies, EH for Event in the main show area, B for booths, D for documents/links, G for group chats, M for message boards, and U for User Profile,
ShowLaunchErrorRedirectURL	Varchar 500	N	Optional URL to redirect users to if the show launch fails. Embedded variables $[ShowKey]$, $[DisplayItem]$, $[LangLocaleID]$, $[ErrorMsg]$ and $[ShowName]$ may be placed in this URL, and will be replaced by the system.