

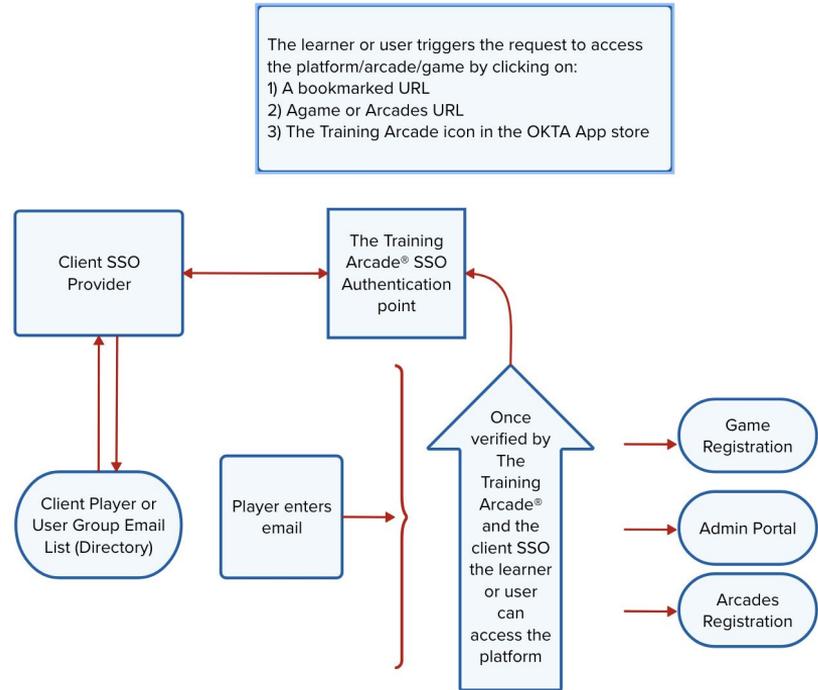


Single Sign On User Guide

Overview

In simple terms <**Single Sign On**> is an authentication method that enables users to securely authenticate in one validated place across multiple related, yet, independent applications such as The Training Arcade® and an LMS by using just one set of credentials.

Users who do not authenticate with SSO will authenticate when logging into The Training Arcade® Admin Portal, Games, or Arcades™ will be their email address.



Overview

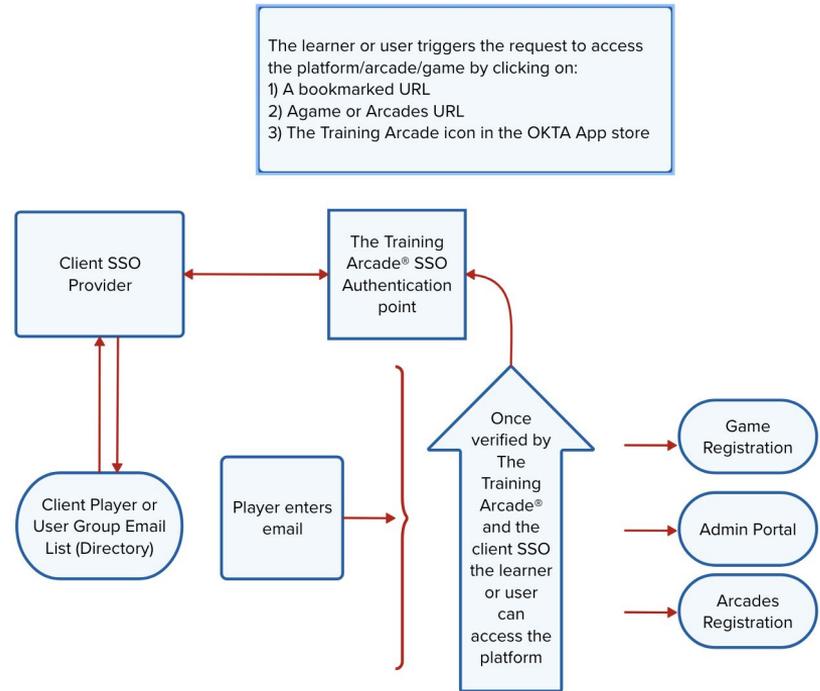
Most SSO providers use a <Directory> style system to <Group> users on the client side.

Clients can create a <Group> at the company called for example <Game Players> in this group they add the following attributes:

- First Name
- Last Name
- Email

The players email is a Unique Identifier, when a player from the client <Game Player> group arrives at our registration page. The Training Arcade quickly checks the email against the clients group list, if we find the email listed, the player is granted access.

If not, the player is shown an <error message> the error message, usually details why the player has been blocked.



Overview

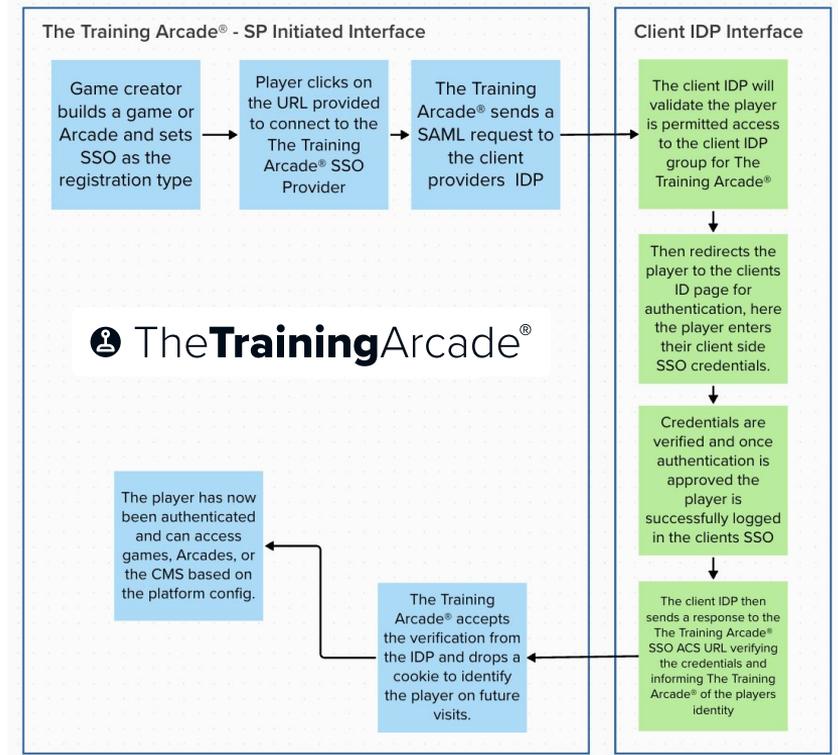
Single Sign On Authentication + Verification Communication Flow

This chart outlines the communication steps between the Service Provider (SP) aka The Training Arcade® and the IDP Identity Provider (IDP) aka the Client.

Our preferred provider is OKTA/SAML, we also integrate with Microsoft Azure out of the box.

The Training Arcade also has an app available via the Okta Store.

For more information on the cost to integrate SSO with The Training Arcade with your Single Sign On service, please reach out to your sales representative.



Overview

Microsoft Azure SSO Users Only

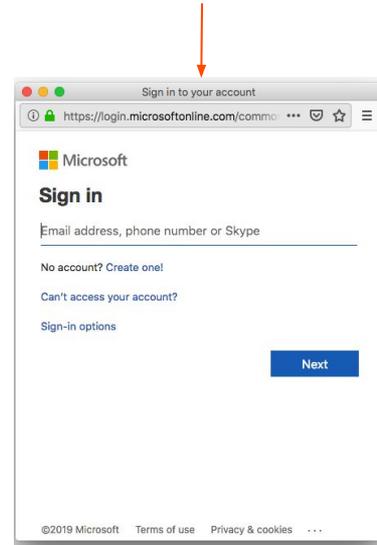
MS Azure is an application, like others, which does not support iFrame use. The Azure user experience when logging on will have an additional step.

- **Learner Login:** When a learner is not logged into the Azure SSO, a pop-up window will appear prompting the learner to log in to their Microsoft account or select an existing account from the list of already logged-in accounts. Once the learner is logged into Azure SSO The Training Arcade® will then allow the learner to access the game or Arcade.
- **Admin Portal:** Administrators, Creators, and Viewers needing to access the admin portal via SSO login will follow the same process as the learner login above.
- **When Facilitating a Virtual or Live Instructor-Led Event:** The instructor of the event will follow the same login process as the learner, however, this process will take place via the instructor portal window.

This is the pop-up that may appear. Please note, this window could be blocked by a pop-up blocker.

Below is a link to a website detailing how to turn off pop-up blockers on most popular browsers.

[How to disable pop-up blockers—internet link](#)



Using SSO

SSO for Games

Game creators can select SSO as the registration setting on a per game basis. This gives additional flexibility when using games for players who are not in Company user groups but need to be included in a training.

On the Game Info tab scroll down to **<User Registration>**

Click on **<Authorization Type>** and from the dropdown

Select **<Single Sign-On>**

Game Info Cases Publish

User Registration

Authorization Type

Select
No Authorization
Authorized Player List
✓ Single Sign-On

No

Show leaderboard on Game Over screen?

Yes

Since you are not requiring user registration we will ask for users' initials in order to populate the leaderboard.

Using SSO

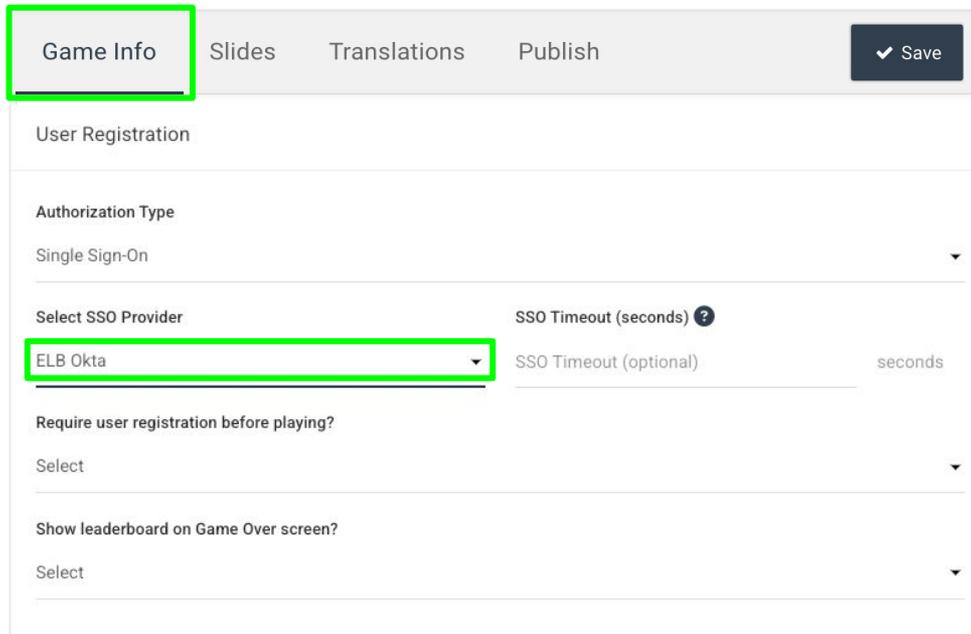
With **<Authorization Type>** set to Single-Sign-On

Select SSO Provider

Click Select ▼ and from the dropdown, click the providers name

Click **<Save>**

If you would like to have the system automatically log players out after a set period of time of inactivity, set the optional **SSO Timeout** field also found in this registration area.



The screenshot shows a configuration interface for a game. At the top, there are tabs for 'Game Info', 'Slides', 'Translations', and 'Publish'. A 'Save' button is located in the top right corner. The 'Game Info' tab is active and highlighted with a green box. Below the tabs, the 'User Registration' section is visible. It contains several settings:

- Authorization Type:** Set to 'Single Sign-On'.
- Select SSO Provider:** A dropdown menu with 'ELB Okta' selected, highlighted with a green box.
- SSO Timeout (seconds):** A field with a help icon (?) and a unit of 'seconds'.
- SSO Timeout (optional):** A field with a unit of 'seconds'.
- Require user registration before playing?:** A dropdown menu set to 'Select'.
- Show leaderboard on Game Over screen?:** A dropdown menu set to 'Select'.

Using SSO

To turn off SSO:

Select <**Authorization Type**>

Select <**No Authorization**>

Click <**Save**>

The screenshot shows a settings panel for a game. At the top, there are tabs for 'Game Info', 'Cases', and 'Publish', and a 'Save' button with a checkmark. The main content area is titled 'User Registration'. It contains three settings, each with a dropdown arrow on the right:

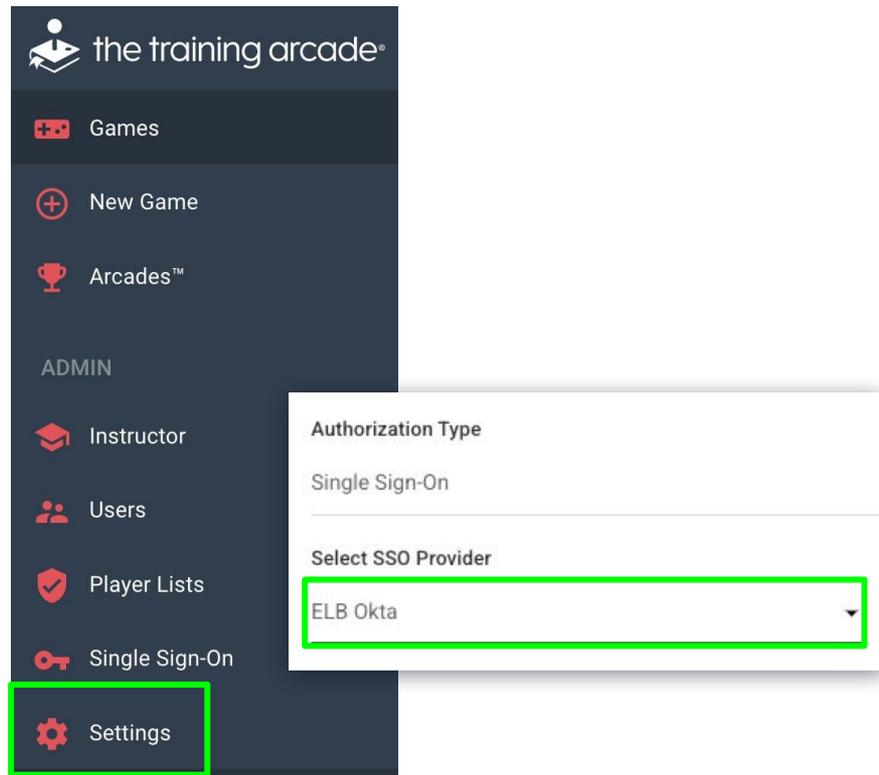
- Authorization Type**: Set to 'No Authorization'.
- Require user registration before playing?**: Set to 'No'.
- Show leaderboard on Game Over screen?**: Set to 'Yes'.

Below these settings, there is a note: 'Since you are not requiring user registration we will ask for users' initials in order to populate the leaderboard.'

Using SSO

To use SSO login on the Admin Portal click **<Settings>** from the side navigation bar.

Select the provider, then click **<Save>**



Using SSO

Once implemented, instructions for editing or changing the SSO metadata can be accessed by clicking on the <**Single Sign On**> button on the menu bar.

*Only account Admins have access to the SSO settings.

The screenshot displays the 'the training arcade' admin interface. The left sidebar menu includes: Games, New Game, Help, ADMIN, Instructor, Users, Player Lists, **Single Sign-On** (highlighted with a green box), and Account. A modal window titled 'Instructions' is open, providing details for configuring SSO. The modal is divided into two columns: 'Instructions' and 'Additional Information'.

Instructions

Ask your Identity Provider (IdP) for the following information, enter it into the fields below and click *Save*.

1. IdP Entity ID
2. IdP Single Sign-On URL
3. IdP Certificate

This will generate the Service Provider (SP) information which consists of the following values:

1. SP Entity ID (a.k.a, Audience URI)
2. SP Single Sign-On URL (a.k.a., SAML Assertion Consumer Service URL)
3. SP Metadata URL

Provide the Service Provider information to your Identity Provider.

Additional Information

Provide the following information to your Identity Provider:

1. The Training Arcade® performs an SP Initiated login, so there is no target URL.
2. Our AuthnRequest does NOT contain a digital signature.
3. Our AuthnRequest does NOT contain a certificate.
4. Binding for Authentication Request: HTTP-Redirect
5. Binding for SAML Response: HTTP-Post
6. The URL that triggers the AuthnRequest is: <https://sso.thetrainingarcade.com>

When performing the SAML handshake, the Identity Provider must send the following attributes:

1. FirstName
2. LastName
3. Email

We hope you find this document helpful,
if you have any questions please send email to: support@elblearning.com