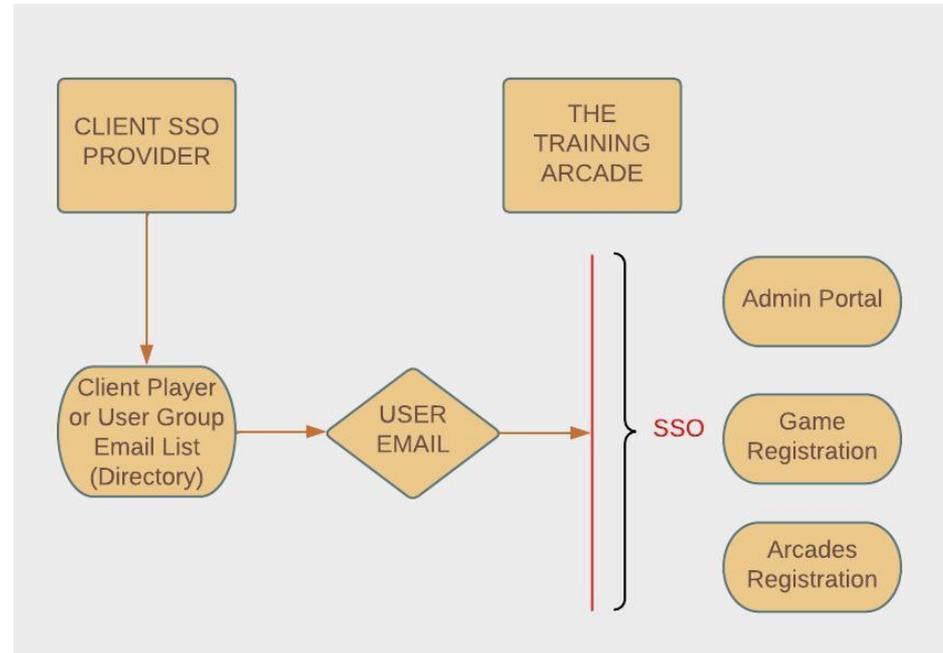


Single Sign On User Guide

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

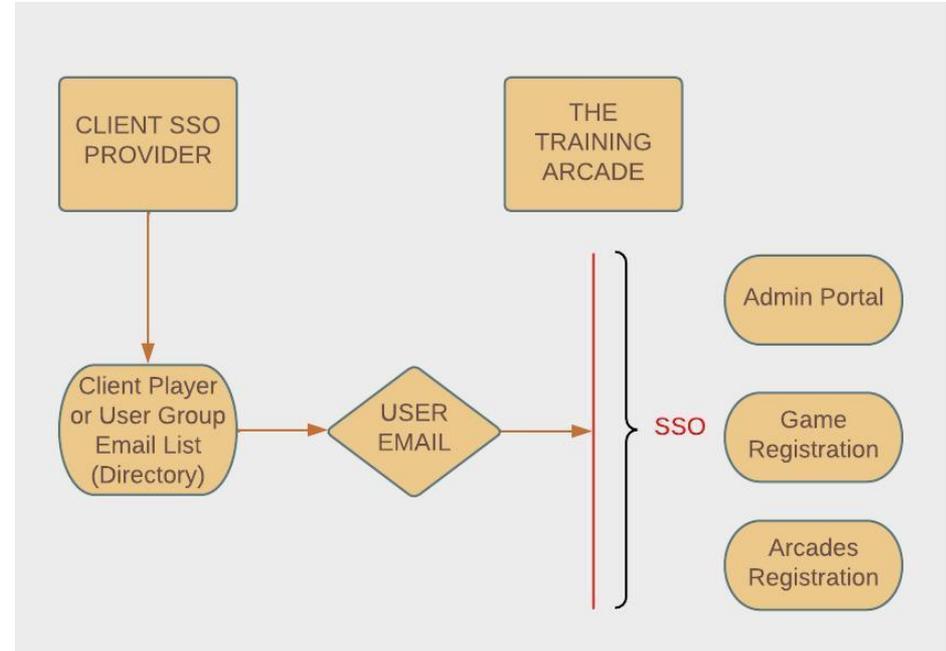
The unique credential users will authenticate with when logging into The Training Arcade® Admin Portal, Games, or Arcades™ will be their email address.



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 the add the following attributes:

- First Name
- Last Name
- Email

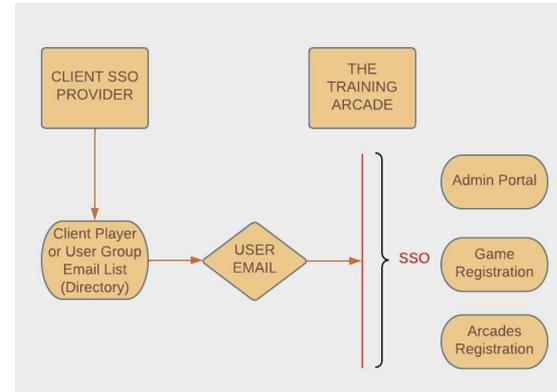
The players email is a Unique Identifier, when a player from the client <Game Player> group arrives at our registration page. The Training Arcade quickly checks the email against the clients group list, if we find the email listed, the player is granted access. If not, the player is shown an <error message> the error message, usually details why the player has been blocked.



Microsoft Azure SSO does not support iFrame use, this is unique to the Azure SSO platform.

The Azure user experience when logging on will have an additional step.

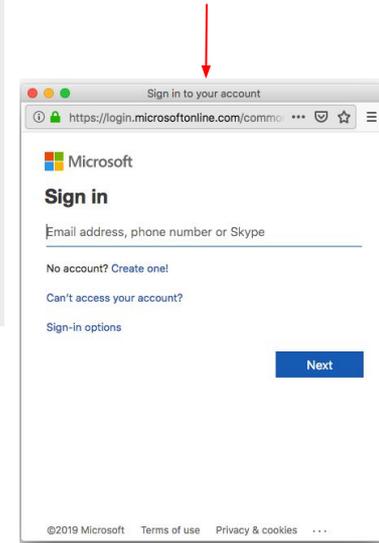
- **Learner Login:** When a learner is not logged into the Azure SSO, a popup window will appear prompting the learner to log in to their Microsoft account or select an existing account from the list of already logged-in accounts. Once the learner is logged into Azure SSO The Training Arcade® will then 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 event:** The instructor of the event will also follow the same login process as the learner, however, this process will take place via the Instructor portal window.



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

[How to disable popup blockers - internet link](#)

This is the Pop-Up that could be blocked by a Pop-Up blocker.



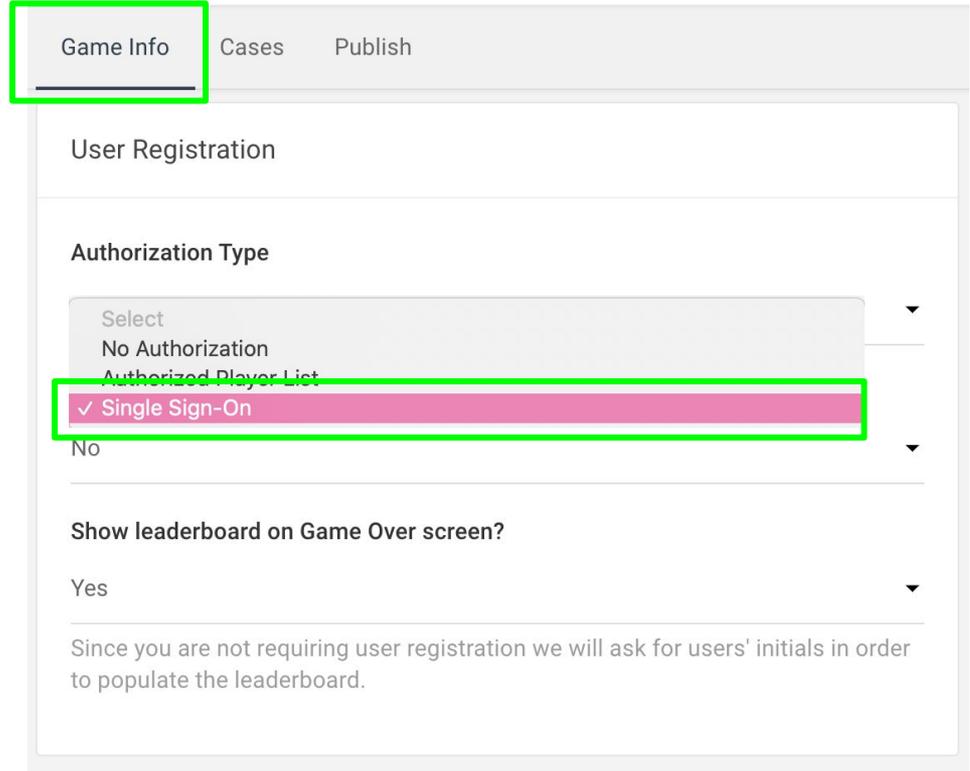
SSO for Games

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 <**SSO**>



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.

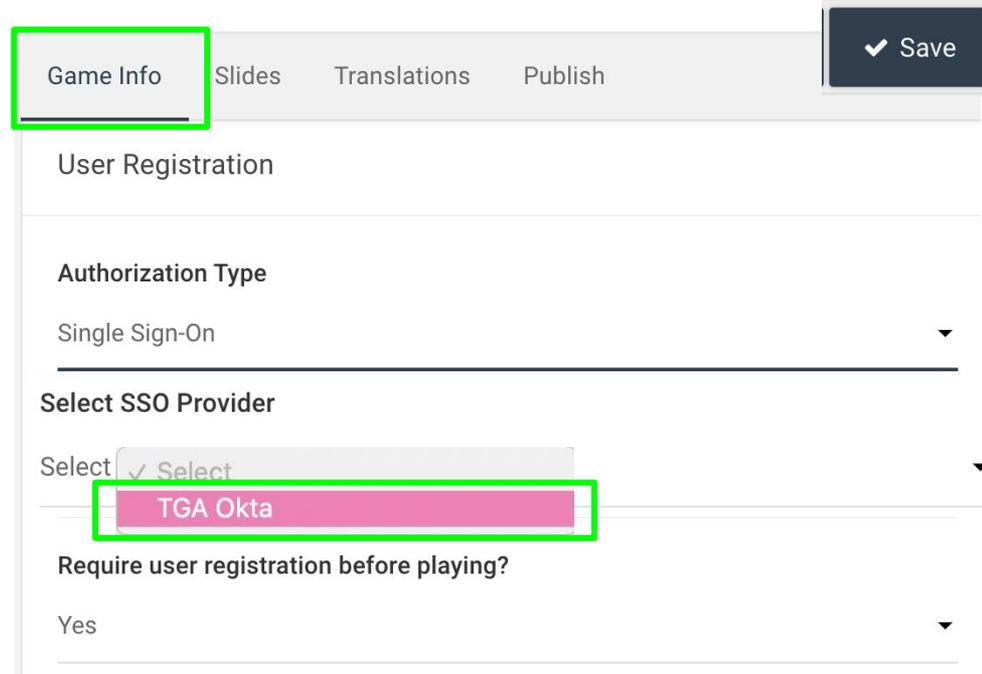
After selecting the <**Authorization Type**> a new dropdown menu is and prompts the user to:

Select an <**SSO Provider**> from a menu

Select 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, there is also a field to determine the time setting available here.

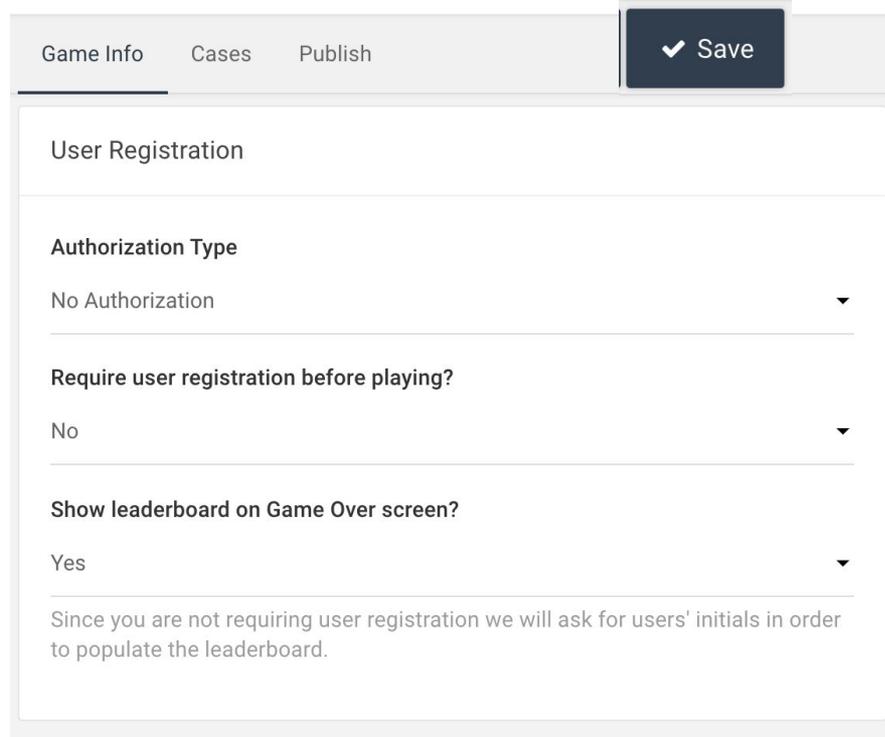


The screenshot shows a configuration interface for a game. At the top, there are tabs for 'Game Info', 'Slides', 'Translations', and 'Publish'. The 'Game Info' tab is selected and highlighted with a green box. In the top right corner, there is a 'Save' button with a checkmark icon. Below the tabs, the 'User Registration' section is visible. Underneath, the 'Authorization Type' is set to 'Single Sign-On'. Below that, the 'Select SSO Provider' section has a dropdown menu with 'TGA Okta' selected and highlighted with a green box. At the bottom, there is a 'Require user registration before playing?' dropdown menu set to 'Yes'.

To turn off SSO:

Select <**Authorization Type**>
select: <**No Authorization**>

Click <**Save**>



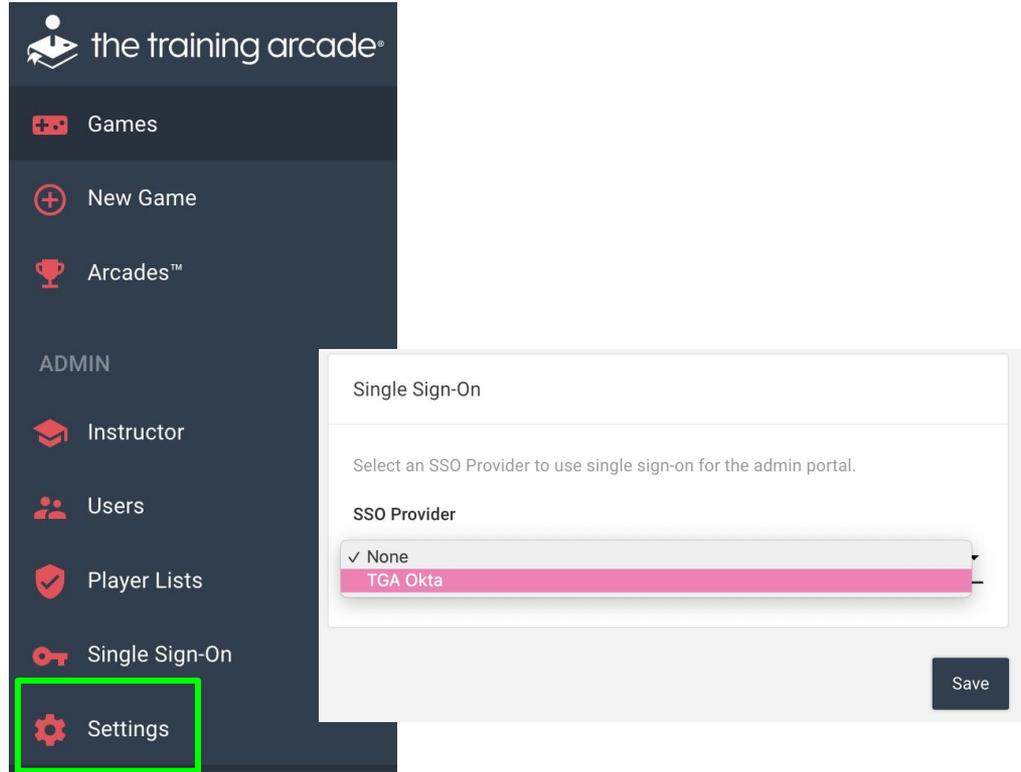
The screenshot shows a configuration panel with a top navigation bar containing 'Game Info', 'Cases', 'Publish', and a highlighted 'Save' button with a checkmark. The main content area is titled 'User Registration' and contains three dropdown menus:

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

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

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

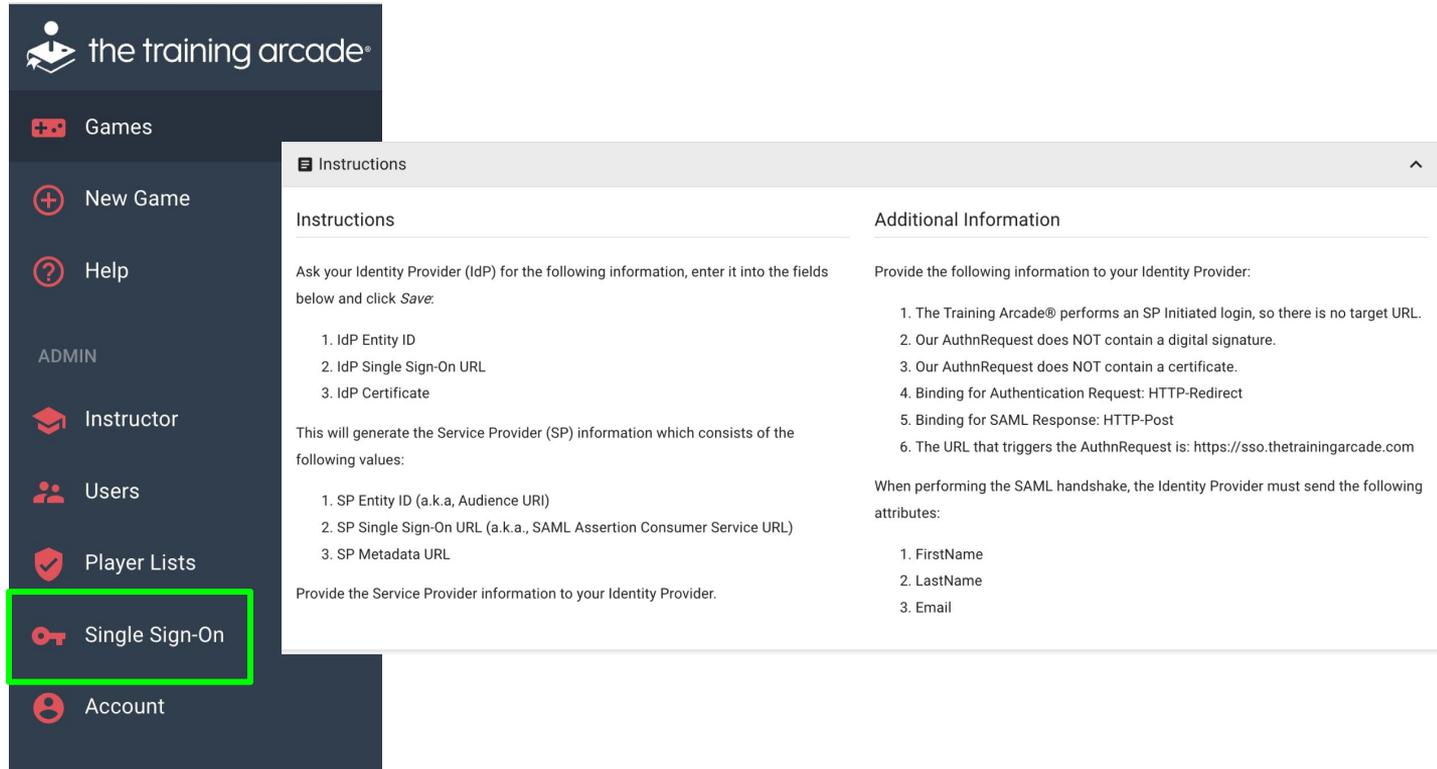
Select the provider, then click **<save>**



The screenshot displays the admin portal interface. On the left, a dark navigation bar contains the following items: Games, New Game, Arcades™, ADMIN, Instructor, Users, Player Lists, Single Sign-On, and Settings. The Settings item is highlighted with a green border. On the right, a modal dialog titled "Single Sign-On" is open. It contains the text "Select an SSO Provider to use single sign-on for the admin portal." Below this is a dropdown menu labeled "SSO Provider" with two options: "None" (selected) and "TGA Okta" (highlighted in pink). A "Save" button is located at the bottom right of the dialog.

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 admin interface for 'the training arcade'. The left sidebar menu includes options for Games, New Game, Help, ADMIN, Instructor, Users, Player Lists, Single Sign-On (highlighted with a green box), and Account. The main content area shows the 'Instructions' page for SSO configuration, which 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:
victoria.keating@thegameagency.com