immersive

SSO Guide

Single Sign On (SSO) Setup Guide & FAQs

www.immersivelabs.com

immersive

Single Sign On (SSO) Setup Guide

1. Add Immersive to your IdP

To begin implementing SSO, as the customer, you must first set up your side of the integration through your Identity Provider (IdP).

All IdPs are slightly different in their interface, but the basics are all the same (just with potentially different names).

To begin, you will need to open your IdP and under create Immersive as a new SAML application.

Here are some examples of a couple of popular IdPs and how that looks in each one:

AZURE

Go to Azure Active Directory > Enterprise Applications > + New Application > SAML

OKTA

Go to Applications > Applications > Add Application > Create New App > SAML 2.0

2. Immersive Metadata

The Immersive platform is hosted in AWS, and when you begin your subscription with Immersive, your data center region is auto-provisioned based on your geographic region. This will be one of the following regions:

- EU (Ireland eu-west-1)
- US (us-east-1)
- UAE (me-central-1)

The Immersive metadata (links to view this below) contains all the technical details you need to integrate with Immersive, and is fully dependent on which region you have been provisioned, so it is important that you select the correct Immersive SAML Configuration below corresponding to your data center region:

- EU Region Metadata - https://api.immersivelabs.online/saml
- US Region Metadata - https://api.us.immersivelabs.com/saml
- UAE Region Metadata - https://api.uae.immersivelabs.com/saml

Immersive Labs LTD | Registered Company Number: 10553244
5th Floor, The Programme, All Saints' St, Bristol BS1 2NB
+44 (0)345-646-1544
www.immersivelabs.com

If you are unsure which region to choose, please verify this with your Customer Success Manager.

3. Configuring SAML in your IdP

Our SAML Configuration information can be found below, and this again can appear as slightly different names/fields within your IdP, depending on which one you have.

Once again, this information must match the region your data is hosted in, otherwise the connection will not work.

Here are some examples of a couple of popular IdPs and how that looks in each one:

AZURE

Basic SAML Configuration:

- Identifier (Entity ID):
  - EU = https://api.immersivelabs.online/saml
  - US = https://api.us.immersivelabs.com/saml
  - UAE = https://api.uae.immersivelabs.com/saml
- Reply URL (Assertion Consumer Service URL):
  - EU = https://api.immersivelabs.online/accounts/saml/auth
  - US = https://api.us.immersivelabs.com/accounts/saml/auth
  - UAE = https://api.uae.immersivelabs.com/accounts/saml/auth

OKTA

SAML Settings:

- Single sign on URL:
  - EU = https://api.immersivelabs.online/accounts/saml/auth
  - US = https://api.us.immersivelabs.com/accounts/saml/auth
  - UAE = https://api.uae.immersivelabs.com/accounts/saml/auth
- Tick the box ‘Use this for Recipient URL and Destination URL’
- Audience URL SP entity ID:
  - EU = https://api.immersivelabs.online/saml
  - US = https://api.us.immersivelabs.com/saml
  - UAE = https://api.uae.immersivelabs.com/saml

4. Attribute Mapping

Also known as Attributes & Claims, or Attribute Statements, you will need to add at least the mandatory two attributes in order for the connection to work.

We require you to set up one attribute for **EMAIL**, and one attribute for **UNIQUE IDENTIFIER** or UID.

For the UID, the value of this attribute you send can be anything that is unique and unchanging for a user, so select a value that makes the most sense from your IdP, a couple of examples from different IdPs are:

- user.mail
- user.userprincipalname

Once you have selected the values, you MUST add the attribute using the following naming format, otherwise, the connection will not work.

For the name (not the value) of the EMAIL attribute, you must name it exactly as follows:

- **urn:mace:dir:attribute-def:email**

For the name (not the value) of the UNIQUE IDENTIFIER attribute, you must name it exactly as follows:

- **urn:mace:dir:attribute-def:uid**

So once these attributes are set up you should have something that looks similar to this:

Attribute Name	Attribute Value
urn:mace:dir:attribute-def:email	user.email
urn:mace:dir:attribute-def:uid	user.userprincipalname

We also have two optional attributes that you can add for a user's first name and last name. If you choose to use either or both of these attributes, the names must be

formatted exactly as follows, and for the value, choose whatever is appropriate from your IdP:

Attribute Name	Attribute Value
urn:mace:dir:attribute-def:first-name	user.firstname
urn:mace:dir:attribute-def:last-name	user.lastname

If you require Team Mapping, we do offer an additional attribute that can be included.

5. Download your Metadata and send to us

Once you have completed all necessary sections of the SAML integration, you will then be given the option to download the metadata file from your IdP.

Download and save this metadata file as an .xml file (if possible) and share it with the Immersive Customer Support Team at support@immersivelabs.com.

Once we receive this, we will then be able to complete the setup of the SSO integration on our side.

6. Your SSO Enabled Landing Page

As part of the integration, we will create you a bespoke landing page that must be used in order to utilize SSO access. Depending on your data region, your new landing page will be a version of one of the following URLs:

- EU - https://yourcompanyname.immersivelabs.online
- US - https://yourcompanyname.us.immersivelabs.com
- UAE - https://yourcompanyname.uae.immersivelabs.com

Once the SSO integration has been completed, we will give you the green-light to test out your new landing page.

Important! Before testing your landing page, we strongly recommend that you add these new URLs to your allow list, depending on your region:

- **EU Region**
  - yourcompanyname.immersivelabs.online
  - yourcompanyname.api.immersivelabs.online
- **US Region**
  - yourcompanyname.us.immersivelabs.com
  - yourcompanyname.api.us.immersivelabs.com
- **UAE Region**
  - yourcompanyname.uae.immersivelabs.com
  - yourcompanyname.api.uae.immersivelabs.com

When testing the new SSO landing page, click on the blue '**Sign in with single sign on**' button, and on your first time you will be re-directed to your IdP to log in. After this, unless you are signed out for any reason, clicking this button should take you directly to the main dashboard.

7. Customized Landing Page (Optional feature)

If you would like to have a customized landing page, this can be done by sending the Immersive Customer Support Team the following information to support@immersivelabs.com:

- Background image (Max File Size: 1MB)
- Company logo (Max file size: 512kb)
- Text to be included on landing page
- FAQFAQs: Single Sign-On (SSO)

immersive

Single sign-on (SSO) set-up FAQs

Does Immersive support SP and IDP initiated SAML SSO?

The Immersive One platform supports both SP and IdP initiated SAML SSO.

How can I update my expiring (X.509) certificate?

When your current certificate is about to expire, please contact Immersive Customer Support. You will need to provide your new certificate, and a time and date that best suits you for when you want to make the change over.

Can I use the same SSO for a second Immersive organization or department?

Yes! We are able to leverage an additional attribute claim which can be used to identify which organization a customer will have access to.

This additional attribute claim is called: *urn:mace:dir:attribute-def:organisation-id*

Note that this will require maintenance on your end (e.g., as new learners are added to your IdP, there needs to be a way of identifying which organization they belong to), but it is possible.

To enable this feature, contact Customer Support.

Can I manage teams using SSO?

Yes! Your teams will have to be managed through your organization's Identity Provider (IdP). If teams are captured in your IdP, users can be assigned teams automatically when they log in via SSO.

Teams will not need to be created in-platform.

This can be achieved via an additional attribute claim to identify the team(s) the user should be assigned to. The additional attribute claim is called:

urn:mace:dir:attribute-def:team-title

Immersive Labs LTD | Registered Company Number: 10553244
5th Floor, The Programme, All Saints' St, Bristol BS1 2NB
+44 (0)345-646-1544
www.immersivelabs.com

Can multi-factor authentication (MFA) or Time-based one-time password (TOTP) be implemented with SSO?

The service provider (IdP) is responsible for the verification of a user. If your IdP supports MFA/TOTP features, you will be able to implement this there. We recommend working with your IdP to explore options that are available to you.

What is the authentication flow?

1. User Initiates SSO: The user starts the SSO process by attempting to access a protected resource or application (the Service Provider or SP).
2. SP Generates SAML Request: The Service Provider (SP) generates a SAML Authentication Request. This request asks the Identity Provider (IdP) to authenticate the user.
3. Browser Relays SAML Request to IdP: The user's browser acts as an intermediary. It takes the SAML Request from the SP and sends it to the user's Identity Provider (IdP) (e.g., Azure AD, Okta, ADFS).
4. IdP Authenticates User: The IdP verifies the user's identity. This might involve prompting the user to enter their credentials (username and password) or using an existing session.
5. IdP Generates SAML Assertion: If authentication is successful, the IdP creates a SAML Assertion. This document contains information about the user, including their identity and attributes (e.g., email, name).
6. IdP Sends SAML Assertion to Browser: The IdP sends the SAML Assertion back to the user's browser.
7. Browser Relays SAML Assertion to SP: The user's browser forwards the SAML Assertion to the SP.
8. SP Validates SAML Assertion: The SP validates the SAML Assertion to ensure it's from a trusted IdP and that the user is authenticated.
9. SP Grants Access: If the assertion is valid, the SP grants the user access to the protected resource or application.

Does Immersive support Single Log Out (SLO)?

The platform currently offers partial support for Single Log Out (SLO) to help you manage secure session termination across your organization.

SP-Initiated SLO

Immersive Labs LTD | Registered Company Number: 10553244
5th Floor, The Programme, All Saints' St, Bristol BS1 2NB
+44 (0)345-646-1544
www.immersivelabs.com

We support Service Provider (SP)-initiated SLO. This means that when a user signs out directly from our platform, the system sends an SLO request to your Identity Provider (IdP). This request prompts the IdP to sign the user out of all other active sessions linked to that provider.

The SingleLogoutService Location and Response Location URLs are included in the SSO metadata for your region, available in the Single Sign On (SSO) Setup Guide.

IdP-Initiated SLO

Please note that the platform does not yet support IdP-initiated SLO. If your users sign out from your Identity Provider's dashboard, they may remain signed into our platform until their session expires via an Idle or Maximum timeout.

Note: If IdP-initiated SLO is a critical requirement for your organization, please contact your Customer Success Manager to discuss your needs.

User Access

How do I add users to the platform using SSO?

The SSO handles new user registration automatically. You do not need to take any action on your end.

You should direct users to the platform's login page. Your organization could have its own URL for this. Users can then select the 'Sign in with single sign on' button:

Note: this automatic process will only work as long as there are licenses available. If you'd like to add more licenses, please contact your Immersive Customer Success Manager or Account Manager.

Do I need to do anything so that existing users on the platform can use SSO?

This depends. The SSO uses 'email address' as the point of truth.

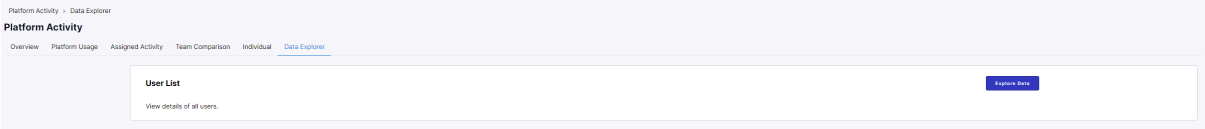
If you have users on the platform that have registered with an email address that does not match the email address available from your Identity Provider (IdP), such as Azure or Okta,

for example, these email addresses need to be updated on the platform. This is so the users can be identified.

If the email addresses aren't updated, a second user account will be created for the user, with the email address stored in your IdP. There will not be any completion data associated with this new account. This will also use up a second license.

If you would like assistance with generating a list of your users and their respective email addresses, you can contact your Immersive Customer Success Manager or Account Manager. If you're an Organization Manager on the platform, you'll have access to this information yourself.

You can do this by navigating to Reports > Platform Activity > Data Explorer and selecting to explore your User List data:



How can I restrict Immersive access to only specific users via SSO?

You can implement this on your side in your Identity Provider (IdP). Create a security group within your IdP; a security group is a collection of users who are given permission to access specific applications.

The way this is created differs slightly in each IdP, but you'll need to create the security group and then add the users that you want to grant access to our platform to this group. You then assign/add the application (Immersive platform) to the group.

For assistance in the specifics of your IdP, we recommend contacting your internal technical team(s), or reaching out to your IdP directly.

Can I force my users to sign in via SSO only?

Yes, this can be enabled (or disabled) at any time. Please contact Customer Support for assistance.

We recommend letting your users know about this before we make this change to avoid confusion. Making this change will mean that they will not be able to log in using their Immersive credentials. Some of them may have been using this method previously, so it's best to communicate with them and let them know they will no longer be able to do so.

Does SSO update when user info changes in the IdP?

No, our current iteration of SSO does not yet support all these features. If a change to user information is made within your IdP, these changes also should be made on the Immersive platform.

To do so, please contact our Customer Support Team.

Will deactivated users be reactivated via SSO sign in?

No, signing in with SSO does not reactivate users. Users must be reactivated manually, via a SCIM sync, or an import.

Immersive Labs LTD | Registered Company Number: 10553244
5th Floor, The Programme, All Saints' St, Bristol BS1 2NB

+44 (0)345-646-1544
www.immersivelabs.com

Personalization & customization

Can we have our own bespoke URL name?

Of course! Please let us know what name you would like to use and when you would like us to have it in place by. If the URL you're after is already in use, we'll not be able to use it. Please do check this beforehand, but we'll let you know if this is the case.

We recommend you inform your users of the new URL name (if this has changed).

Can I customize the landing page with our own branding?

Yes, your landing page can be altered slightly to reflect your organization's branding. This customization is limited to:

- Background image
- Logo
- Bespoke colors and text

To do so, please contact our Customer Support Team.

Immersive Labs LTD | Registered Company Number: 10553244
5th Floor, The Programme, All Saints' St, Bristol BS1 2NB
+44 (0)345-646-1544
www.immersivelabs.com

Issues & Troubleshooting

What do the errors mean and how do I troubleshoot them?

If you are receiving errors, please use the table below to troubleshoot the more common causes. If you cannot see your specific error here, then please contact the Customer Support Team.

Error message or issue	What does it mean?	Troubleshooting
404 or 302 error Or another HTTPS-related error appearing	This is likely to be an error on your end of the configuration in setting up Immersive as a Service Provider in your Identity Provider (IdP).	• Check that you have used the correct metadatafile provided by Immersive. • If you're using Azure or Okta as your IdP, review our guides on adding a service provider application in both Okta and Azure • Ask your technical team to check for any errors occurring in your IdP

Immersive Labs LTD | Registered Company Number: 10553244
5th Floor, The Programme, All Saints' St, Bristol BS1 2NB
+44 (0)345-646-1544
www.immersivelabs.com

SSO login failures A user is selecting the landing page URL to login but: • They receive a SAML error • They receive a HTTPS error	This can either happen because: • Your IdP cannot authenticate the user (this will not be the case if it has resulted in a SAML error) • The user has been authenticated successfully by your IdP and is directed back to our environment, but something isn't quite right Both issues are likely to be resolved by checking the attribute names and values within your IdP configuration - see the troubleshooting	The attribute claims specified aren't quite right (AttributeStatement.saml2:Attribute) . There must be a minimum of two claims, and they must be named exactly as follows in order to work: • Urn:mace:dir:attribute-def:email • Urn:mace:dir:attribute-def:uid These claims must have corresponding values from your IdP (they cannot be null), otherwise the login will fail. Note: the email attribute claim value should be the full email address. -OR- Depending on the configuration you have required, there may be other claims that you have specified. If present, check that these claims are correct and that they also have been named correctly: urn:mace:dir:attribute-def:first-name

	steps on the right for details.	urn:mace:dir:attribute-def:last-name urn:mace:dir:attribute-def:team-title (Required for team mapping) urn:mace:dir:attribute-def:organisation-id (Required for organization mapping)