Single Sign-On for the Userlane Portal

Last Modified on 02.05.2024

What is it?

Single Sign-On (SSO) allows users to authenticate with multiple applications using just one set of credentials. In the context of Userlane, we have two separate SSO configurations:

- Single Sign-On for Managers concerns access to the Userlane Portal, where Managers can add new applications to Userlane, view HEART and content analytics data, as well as manage Userlane content and customize their Userlane application.
- Single Sign-On for End Users authenticates users to see and interact with the Userlane Assistant as well as contribute to HEART data. To set up SSO for End Users please read on here.

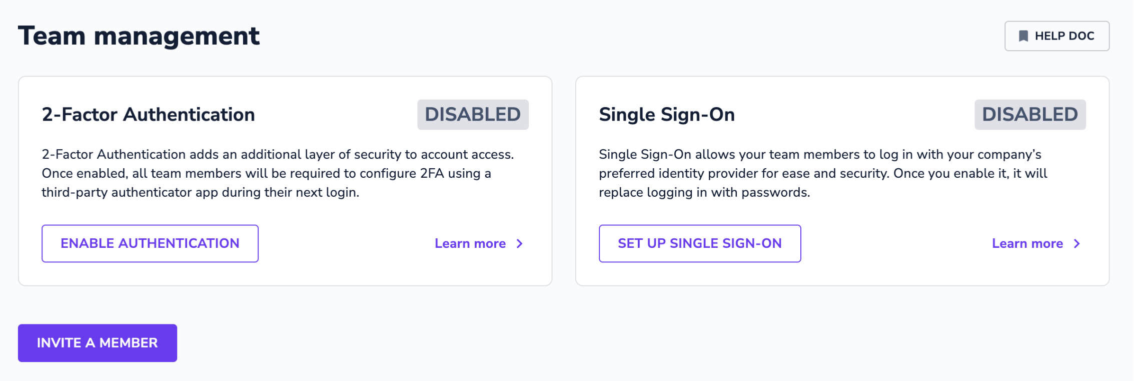
Why use SSO for Managers?

SSO is a secure way to authenticate Userlane Managers that offers two key benefits once enabled:

- **Central User Management:** With SSO enabled, IT Admins can centrally manage who has access to the Userlane Portal. For example, if a user leaves the company, their access can be centrally disabled in the company's Identity Provider and Access Management tool.
- **Increased Security:** SSO also increases security to business-critical data such as that found in the Userlane Portal. By authenticating with one set of credentials, the risk of compromised passwords leading to data breaches is heavily reduced.

How to set up & enable SSO for Managers

On the Team Management page in the Userlane Portal, Managers with the Admin Role will see the option to enable SSO for all Team Members in their Userlane company.



Team management

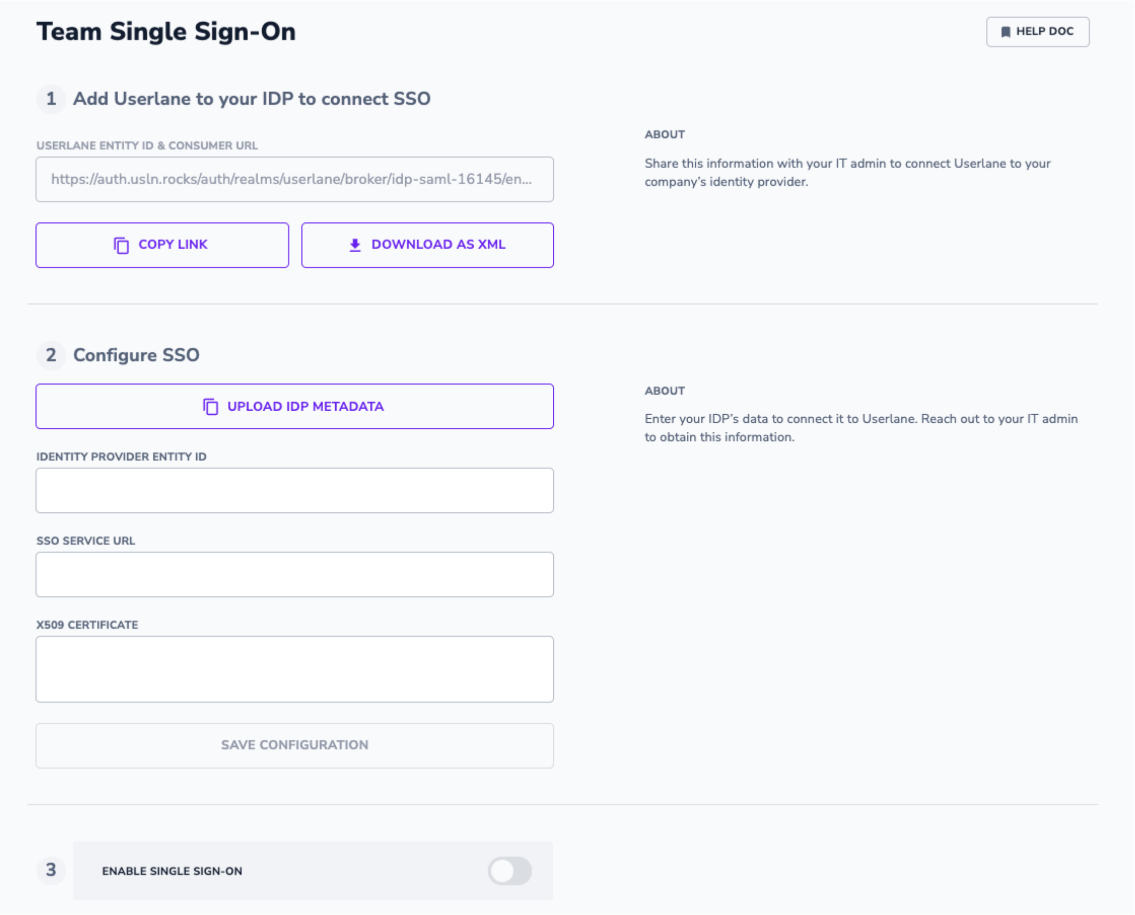
2-Factor Authentication — DISABLED

2-Factor Authentication adds an additional layer of security to account access. Once enabled, all team members will be required to configure 2FA using a third-party authenticator app during their next login.

Single Sign-On — DISABLED

Single Sign-On allows your team members to log in with your company's preferred identity provider for ease and security. Once you enable it, it will replace logging in with passwords.

After clicking 'Set Up Single Sign-On', Admins will be directed to a new page to complete the set up and enable SSO. As shown below, there are 3 steps to setting up and enabling SSO for Managers.



USERLANE ENTITY ID & CONSUMER URL: https://auth.usln.rocks/auth/realms/userlane/broker/idp-saml-16145/en...

ABOUT

Share this information with your IT admin to connect Userlane to your company's identity provider.

IDENTITY PROVIDER ENTITY ID

SSO SERVICE URL

X509 CERTIFICATE

ABOUT

Enter your IDP's data to connect it to Userlane. Reach out to your IT admin to obtain this information.

Step 1

To configure SSO, you must first add Userlane as a trusted application to your Identity Provider (IdP). In this step, you are provided with the metadata needed to do so. You can access that metadata either as a link or by downloading it as an xml file. Please pass it along to your IT team who can add Userlane as a trusted application.

Helpful links from common Identity Providers:

- Microsoft Entra ID
  - Add an Enterprise Application
  - Enable Single Sign-On with SAML

> ℹ If you plan on triggering Userlane from the Microsoft MyApps Portal, make sure you add https://family.userlane.com as the Sign-On URL in the Entra ID configuration.

- Google Workspace
  - Set up your own custom SAML App
- OneLogin
  - SAML Custom Connector (Advanced)

> ℹ For OneLoginensure that: (1) the Recipient field is filled with the EntityID URL; (2) the Login URL is filled with https://family.userlane.com; and (3) the SAML Initiator setting needs to be changed to 'Service Provider'

- Microsoft ADFS
  - Create a Relying Party Trust
  - For AD FS, you must add a claim Rule to your configuration. Please refer to this article on how to do so.

Step 2

In step 2, you need to add the metadata from your own Identity Provider in Userlane to establish the SSO connection. There are two ways to do so:

- If you received the metadata from your IT team in the form of an xml file, you can simply click 'Upload IDP Metadata' and select the MetaData.xml file from your file explorer. This will auto-fill the form fields for you with the right information.
- You can also enter the metadata information manually into the form. Or edit the information as needed, for example, if you need to update a SAML certificate.

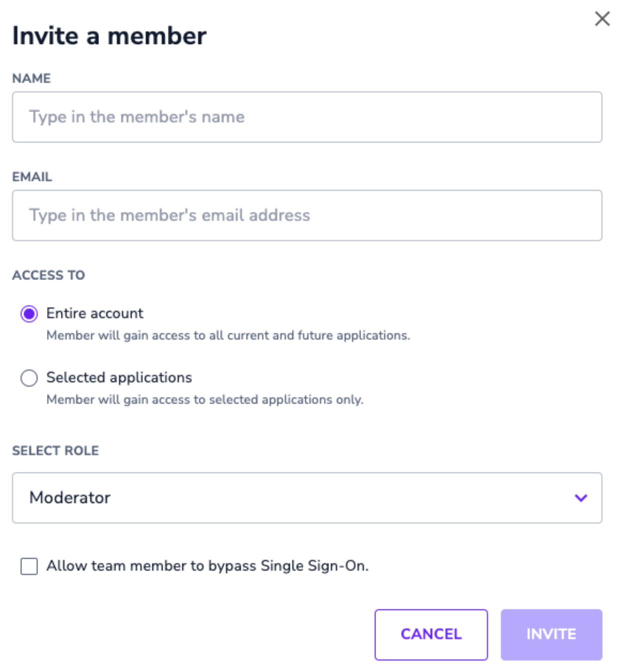
> After the metadata has been entered, be sure to save your configuration. Upon saving, the metadata you entered will be saved in the Userlane Portal but SSO will **not be enabled.**

Step 3

In step 3 you can enable SSO for Managers when you are ready. Once enabled, the SSO login flow will be activated for your Userlane Team. All users will be required to authenticate with Userlane via SSO, except for those who have been marked as being able to 'Bypass SSO'.

Bypass SSO

Admins can determine if any of their Userlane Team Members should be able to bypass SSO and still log in to the Userlane Portal with their email and password. For new users, you can activate this setting when inviting them to Userlane for the first time.



Invite a member

NAME

Type in the member's name

EMAIL

Type in the member's email address

ACCESS TO

● Entire account
Member will gain access to all current and future applications.

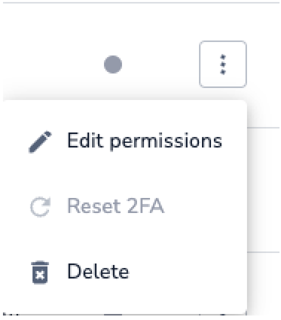
○ Selected applications
Member will gain access to selected applications only.

SELECT ROLE

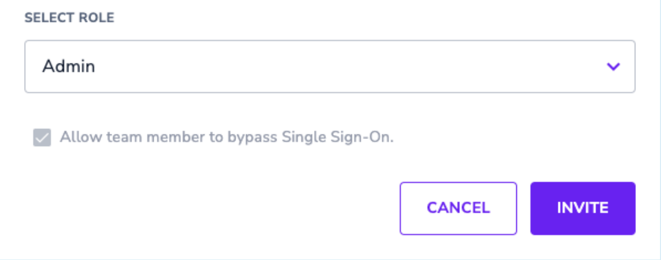
Moderator

□ Allow team member to bypass Single Sign-On.

For existing users, if you would like to activate the bypass SSO setting, simply edit their permissions by clicking on the 3 dots next to their user entry and open the permissions window.



By default, this setting is active and cannot be deactivated for Admins!


SELECT ROLE

Admin

☑ Allow team member to bypass Single Sign-On.

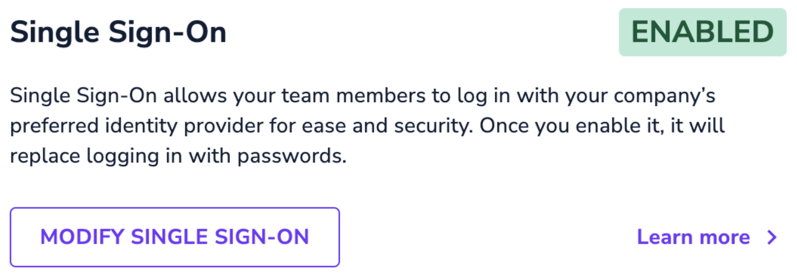
Why would I activate bypass SSO?

There are two primary use cases for which the bypass SSO setting is used:

- In the event that the SSO connection does not work, it is necessary that at least one Manager can access the Userlane Portal in order to update or deactivate SSO and allow other Managers to access the Portal.
    - As SAML certificates often need to be updated, it can happen that the SSO configuration has expired and needs to be updated with a new certificate from your identity provider.
    - This is why Admins have bypass SSO activated by default.
- If your company works with any external contractors or consultants to manage Userlane, it is possible that these users are not managed in your identity provider, meaning that SSO will not work for them. To ensure that they can still access the Userlane Portal, we recommend that bypass SSO is activated for them.

Modify or Disable SSO

Once SSO for Managers is enabled, Admins can easily and quickly Modify the SSO configuration from the Team Management page.



Single Sign-On

ENABLED

Single Sign-On allows your team members to log in with your company's preferred identity provider for ease and security. Once you enable it, it will replace logging in with passwords.

Upon clicking 'Modify Single Sign, Admins are brought to the configuration page where they can:

- Edit the existing configuration
- Delete the existing configuration
- Disable SSO using the toggle at the bottom of the page

Deleting the configuration will permanently remove the IdP metadata from Userlane!