SSO Implementation

Last Modified on 27.09.2023

About SSO

Single Sign-On is a convenient, yet secure way of authenticating a user.

Most customers are already running an Identity Provider (IDP) that supports Single Sign-On through the SAML 2 protocol, e.g. Active Directory, OneLogin, or Okta.

Benefits of using SSO

Integrating SSO into Userlane makes sure that

- your user can benefit from its content by using credentials they are using each day and in multiple places
- Userlane is silently and seamlessly rolled out to all end users
- your users do not have to do anything in order to see Userlane.

How it works

In the following section, we refer to three different stakeholders who need to align in order to get the integration up and running smoothly:

Company IT Administrator	Company Application Owner	Userlane Customer Success Manager
Sets up the installation on the customer's side.	Has requested that Userlane runs on their application	Point of contact at Userlane for the installation and person who supports App Owner regarding any requirements

In concept, this is how users are seamlessly authenticated for Userlane:

User authentication logic

First time authentication is triggered immediately when User opens the browser with an installed Userlane Browser Extension. If the authentication is not successful, the attempt is repeated exponentially (every 2, 4, 8 minutes and further) until it reaches the frequency of 48h. After that the re-try is triggered every 48h until successfully authenticated.

An already authenticated user will try to refresh the user attributes according to the setting in the Userlane Portal. The refresh is done by re-authenticating.

Configuration

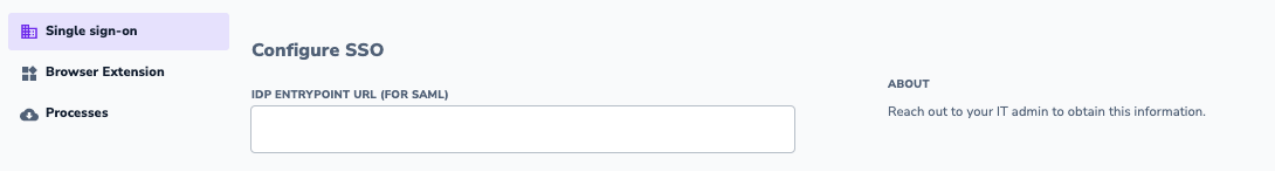
1. Receive relevant data

Reach out to your IT to receive the

- IDP entrypoint URL
- IDP certificate

2. Add to the Userlane Portal

Sign in to **Userlane Portal > Settings > Single Sign On**



Add Userlane to your IDP to connect SSO

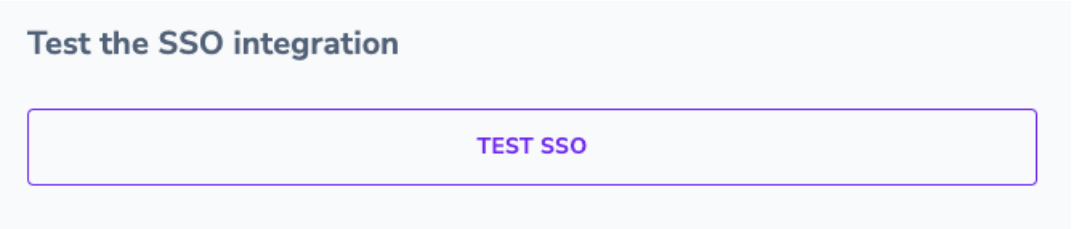
You need to pass the Userlane metadata to your IT.

You can find detailed instructions per provider:

- ADFS
- Azure Active Directory
- Google Workspace

3. Testing in Userlane Portal

Test the SAML connection with the test link in the Userlane Portal.

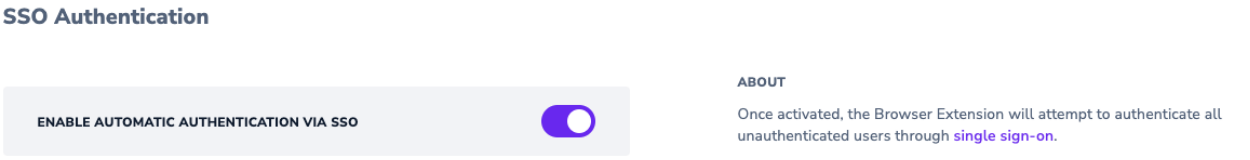


It should bring the user to your IDP login page or (if they are already logged in to their IDP), then to the Chrome or Edge extension store to install the Userlane BE or (if they already have the extension installed) they are brought to a Userlane page with a list of Userlane properties.

Any of these results mean that SSO has been successfully configured.

4. Authenticating the user via Single-Sign-On

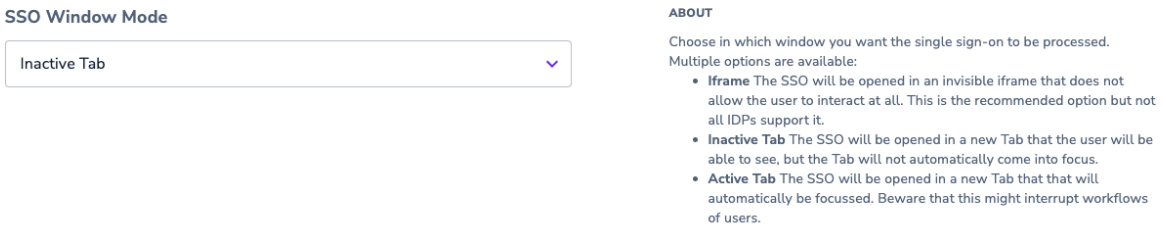
To authenticate the current user towards Userlane, a Single-Sign-On (SSO) flow can be started in a new tab or in the background. Through this, it is also possible to provide more details about a user to Userlane so that specific content can be shown to user segments. This can be done by simply enabling automatic authentication via SSO under the Browser extension tab within your Userlane Portal.



5. Choose the SSO window mode

Choose in which window you want the single sign-on to be processed. Multiple options are available:

- **Iframe** The SSO will be opened in an invisible iframe that does not allow the user to interact at all. This is the recommended option but not all IDPs support it.
- **Inactive Tab** The SSO will be opened in a new Tab that the user will be able to see, but the Tab will not automatically come into focus.
- **Active Tab** The SSO will be opened in a new Tab that will automatically be focussed. Beware that this might interrupt the workflows of users.



Alternatives to SSO

As an alternative to authenticating via SAML, Userlane offers the option to authenticate via Browser Policy.

See here more information on this.