

SSO Implementation

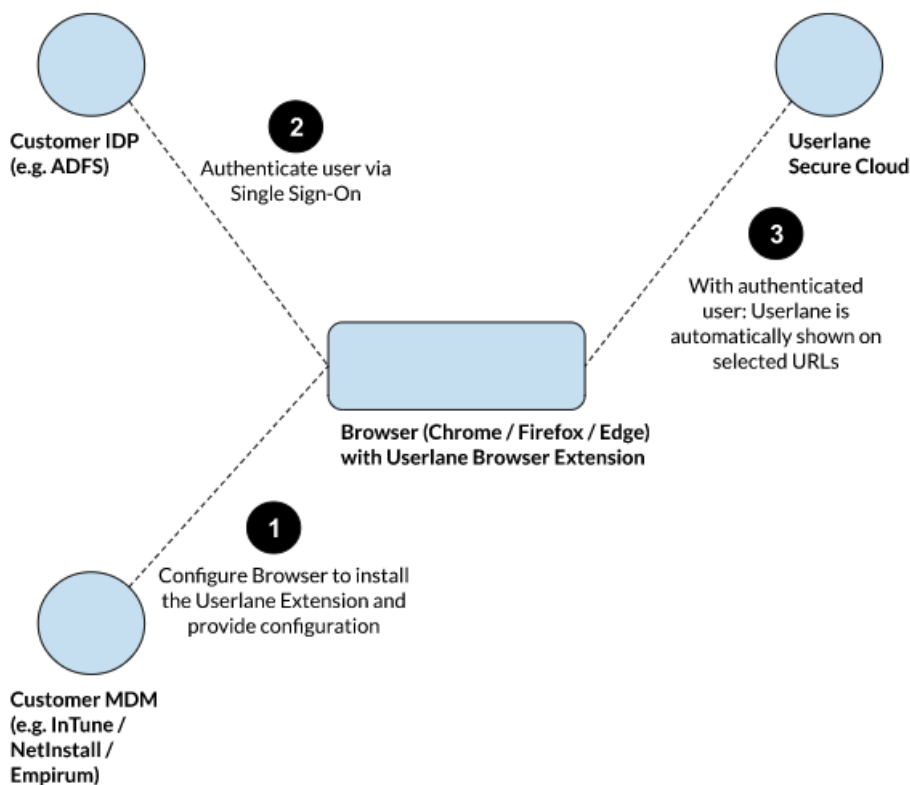
Single Sign-On is a convenient, yet secure way of authenticating a user.

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 (short IT Admin) | Company Application Owner (short App Owner) | Userlane Solution Architect / Implementation Consultant (short SA) |
|--|---|--|
| 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:



Step 1: Configure Browser to install the Userlane Extension and provide configuration

Browsers can be configured via so-called Enterprise policies. Those policies are provided by the Browser manufacturers (Mozilla, Google, or Microsoft) and allow IT Admins to regulate what users can or can't do with the Browser. To do that, companies use a tool to manage devices and software packages (MDM) such as Microsoft InTune, Entel or Matrix42 Empirum. It is possible to automatically install specific Browser Extensions and to provide configuration parameters to them.

To seamlessly rollout Userlane

1. We need to configure the Browser to install the Userlane Extension and
2. Provide the customer's CompanyId and CompanyIntegrity and Region (eu, us) to the Browser. By default your region is set to "eu".

through the given options by the respective browser.

- [Microsoft Edge on Windows](#)
- [Chrome on Windows](#)
- [Chrome on macOS](#)
- [Firefox on macOS](#)
- [Firefox on Windows](#)

Step 2: 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 entirely 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.

Step 3: Userlane is automatically shown on selected URLs

Once a user was authenticated, the Browser Extension can load the runtime configuration which contains the whitelist of URLs on which Userlane will be shown. The list is automatically refreshed once every hour.

Related articles

[Enabling Single Sign-On \(SSO\) via SAML](#)

[Expanding SSO Settings](#)
