Central Browser Extension Rollout

Last Modified on 27.09.2023

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.

Requirements

- Userlane Customer Success Manager needs to provide companyID and information on region
- IT Admin with access to Browser Installation and Policies
- IT Admin creates integrityToken
- Userlane Account Admin to set Integrity Token in Userlane Portal

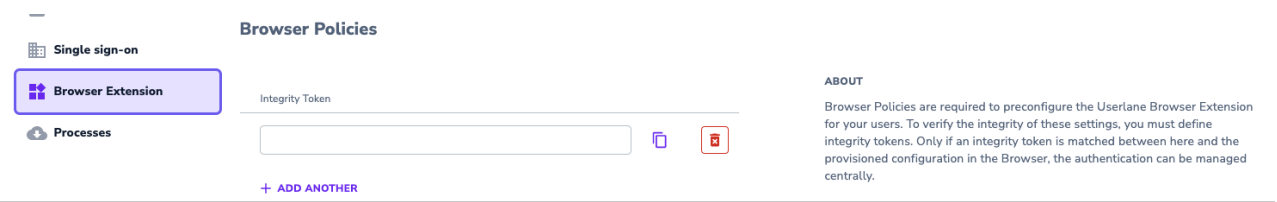
Installation and Configuration

1. Userlane Browser Extension must be added to the ExtensionInstallForceList browser policy
2. Browser Policies must be configured for the Userlane Browser Extension

You need to configure the Browser to install the Userlane Extension through the given options by the respective browser:

- Microsoft Edge on Windows
- Chrome on Windows
- Chrome on macOS
- Firefox on macOS
- Firefox on Windows

Then, sign in to **Userlane Portal > Settings > Browser extension**



Here, you can add your Integrity Token to verify the integrity of the settings and be able to manage authentication centrally. The integrity token secures the configuration for legitimate users.