Installing and Configuring the Userlane Browser Extension for Firefox on Windows (SSO)

Last Modified on 27.09.2023

Microsoft Edge, Mozilla Firefox and Google Chrome allow the silent installation of Browser Extensions. This way, the users do not have to manually install the Browser Extension themselves, but rather the IT Admins can roll out the Browser Extension in the background via a MDM solution, such as Microsoft InTune, Enteo NetInstall, or Matrix42 Empirum.

Each browser needs to be set up separately.

This article explains the configuration for Firefox on Windows.

Browser Extensions in Firefox can be installed and configured through Enterprise Policies.

Requirements

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

Steps to Complete the Setup

1. Installation and Configuration
2. Verification

1 Installation and Configuration

ExtensionInstallForceList browser policy

Add the Userlane Extension (Link for Firefox: https://browser-extension.userlane.com/firefox/userlane.xpi) to the Extension\Install list:

https://github.com/mozilla/policy-templates#extensionsettings

For the *installation_mode* we recommend *force_installed.*

New registry **entry** (example)**:**

Path: HKEY_LOCAL_MACHINE\Software\Policies\Mozilla\Firefox

New entry name: ExtensionSettings

Entry type: REG_MULTI_SZ

Example **value** for the registry entry **:**

```
{
  "{9f6832a6-ec0c-11e8-8eb2-f2801f1b9fd1}": {
    "installation_mode": "force_installed",
    "install_url": "https://browser-extension.userlane.com/firefox/userlane.xpi"
  }
}
```

Note: The Registry Key might need to be modified if multiple Browser Extensions (other than Userlane) are installed to Firefox.

Browser Policy Configuration

Firefox Extensions can be configured in many ways, e.g. through system policies: https://extensionworkshop.com/documentation/enterprise/adding-policy-support-to-your-extension/

On Windows, the easiest way is to use system registry. Prepare the following data that you will find in the Portal: *Settings - Single Sign On* and *Settings - Browser Extension*

- companyId (provided by your Customer Success Manager!)
- companyIntegrity
- region

Here is the registry path to add the configuration:

Software\Policies\Mozilla\Firefox\policies\3rdparty\Extensions\{9f6832a6-ec0c-11e8-8eb2-f2801f1b9fd1}

Example .reg file:

```
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Mozilla\Firefox\3rdparty]


[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Mozilla\Firefox\3rdparty\Extensions]


[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Mozilla\Firefox\3rdparty\Extensions\{9f6832a6-ec0c-11e8-8eb2-f2801f1b9fd1}]

"companyId"="12345"

"companyIntegrity"="12345"

"region"="eu"

"authMethod"="openUrl"

"authToken"=""

"userId"="user123"
```

Here is additional info about the specific values shown above. The first three are **required**:

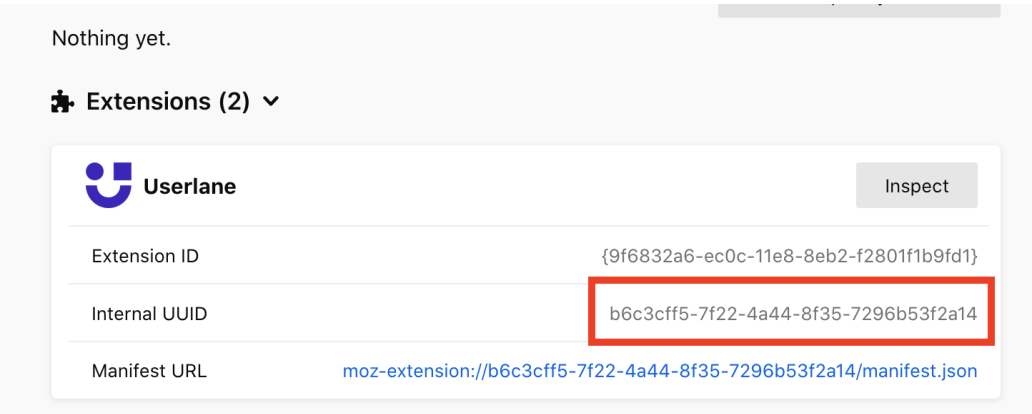
Name	Default value	Description	Required
companyId		Id of the company from Admin Center	yes
companyIntegrity		Value to prove the integrity of the companyId, you can set it in the Portal	for SSO-SAML
region	eu	Region, EU by default; need to be specified for US customers	for US
authMethod		Option to override default Auth method set in Portal	no
authToken		Authentication Token for Passwordless Authentication	only for non SAML
userId		ID of the user, depends on internal settings; e.g. email for SSO	no

userAttributes		User attributes in JSON format	no

2. Verification

Visit

moz-extension://**EXTENSION_INTERNAL_UUID**/options/index.html?stay#/nativeconfig, where **EXTENSION_INTERNAL_UUID** can be found on `about:debugging#/runtime/this-firefox` page:



for example: moz-extension://b6c3cff5-7f22-4a44-8f35-7296b53f2a14/options/index.html?stay#/nativeconfig

Please note that the Internal UUID is always unique.