

envi



# OneLogin Single Sign-On

Integration Guide



# Table of Contents

<b>Introduction.....</b>	<b>2</b>
<b>Integration .....</b>	<b>3</b>
<b>Envi Configuration .....</b>	<b>7</b>
<b>Browser Extension.....</b>	<b>9</b>

# Introduction

**OneLogin** is a **single sign-on (SSO)** provider that simplifies the management of application sign-ins and permissions. With **OneLogin SSO** integration, you can effectively control access to your **Envi** application using a secure and scalable identity management system.

**OneLogin** provider prevents common vulnerabilities in the authentication experience, including username and password sign-ins or password reset requests.

You don't need to manually renew or worry about weak sign-in credentials that cause security issues, enforce session timeouts, and require users to sign in again after these timeouts.

This step-by-step guide explains how to configure **SSO** to your **Envi** account with the **OneLogin** provider.

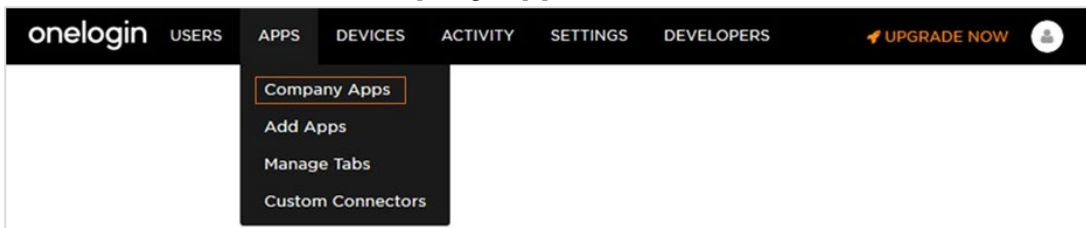
# Integration

Follow the steps below to get your **OneLogin** account linked to your **Envi** account.

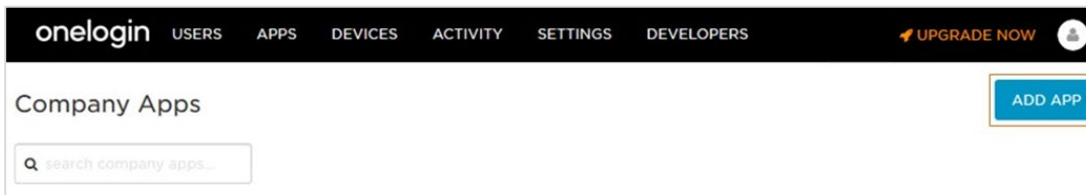
1. Sign in to the [OneLogin](#) site.
2. In the upper-right corner of the page, select **Administration**.



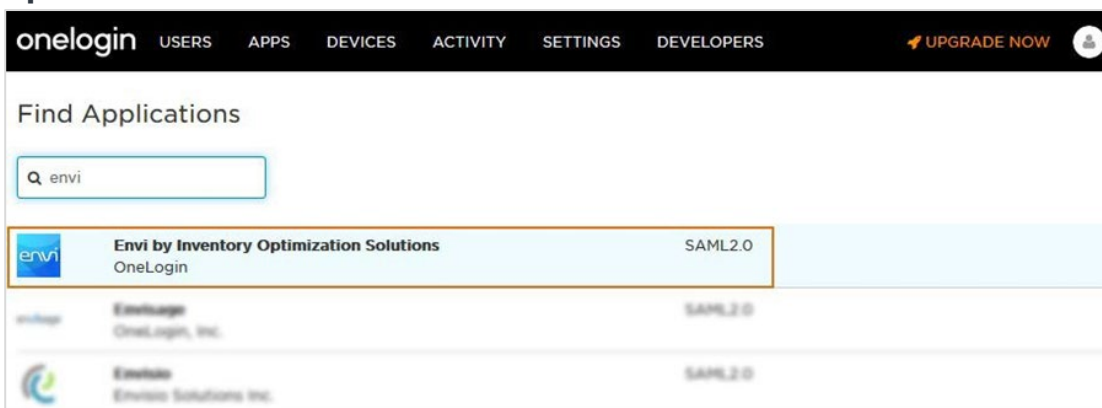
3. On the **APPS** tab, select **Company Apps**.



4. Select the **Add App** button.

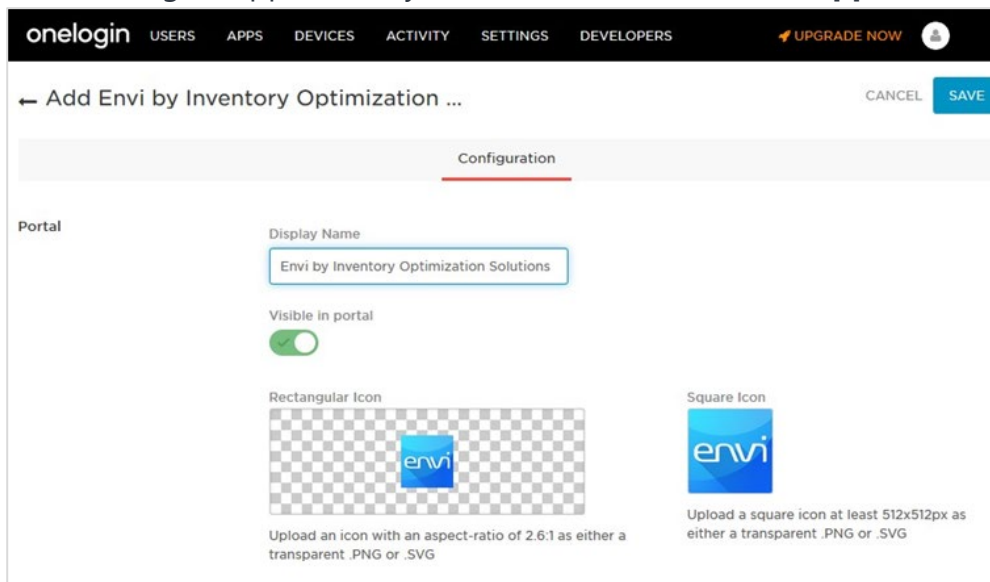


5. In the **Find Applications** search box, enter **Envi** and then select **Envi by Inventory Optimization Solutions** from the list.



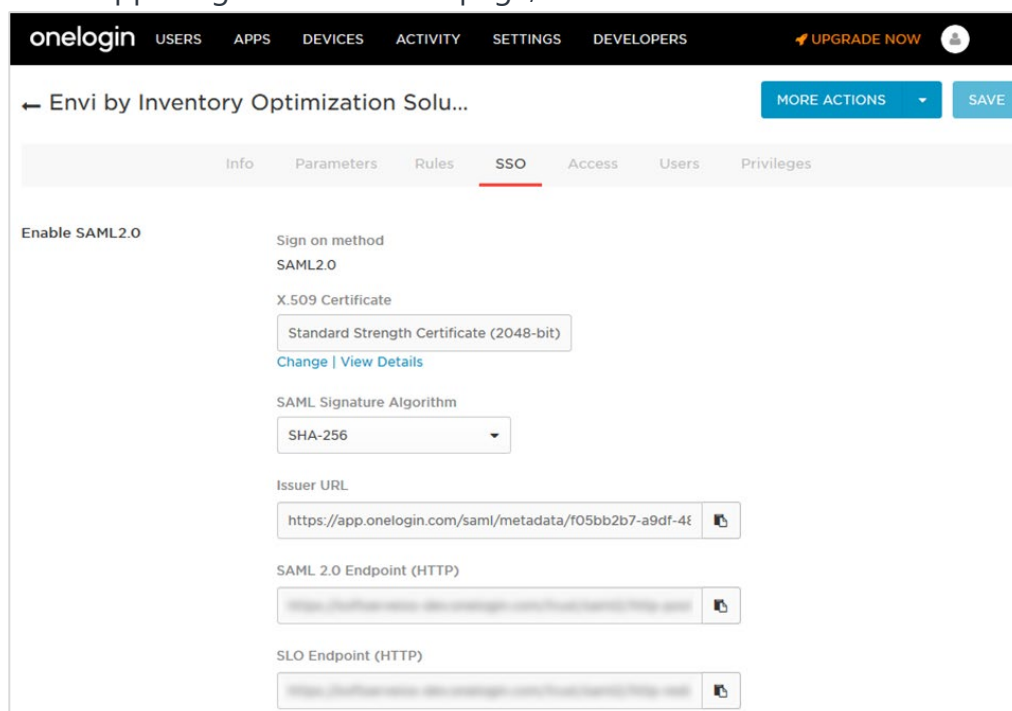
6. On the **Add Envi by Inventory Optimization Solutions Configuration** page, do the following steps:
  - a. Change **Display Name**.
  - b. Upload other icons if needed.
  - c. Select **Save**.

After adding an application, you will be redirected to the **Application Details** page.

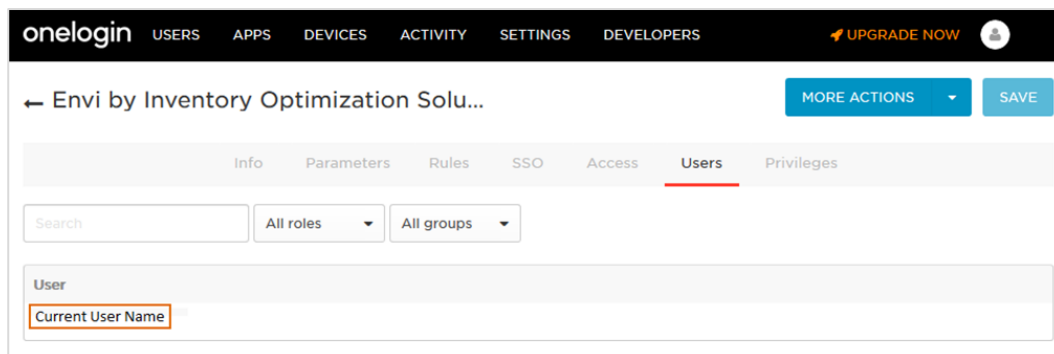


7. On the **Application Details** page, go to the **SSO** tab and do the following steps:
  - a. In the **SAML Signature Algorithm** dropdown list, select **SHA-256**.
 

**Note:** All other boxes will be auto-populated.
  - b. Copy the **Issuer URL** which you will use for the **Envi** configuration later.
  - c. In the upper-right corner of the page, select **Save**.

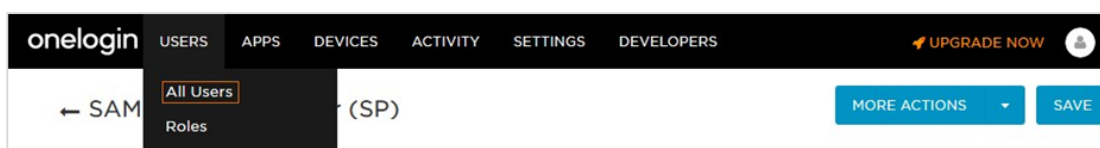


**Note:** Go to the **Users** tab > in the **Users** list to find and view current user details.



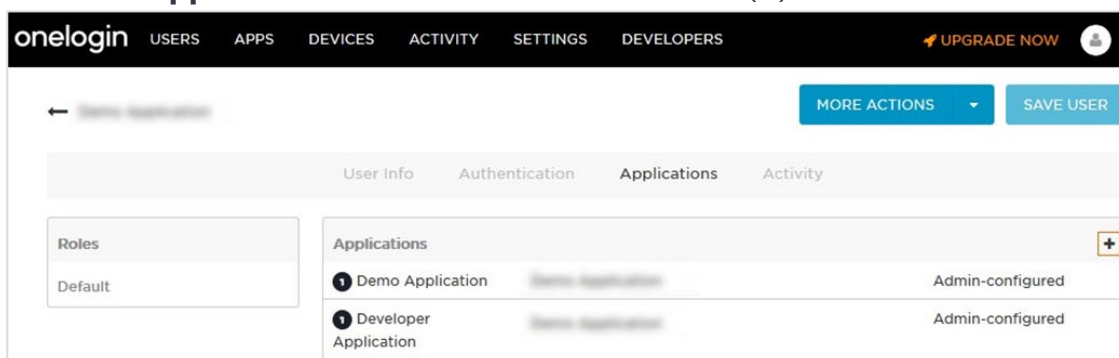
8. To grant access to the application to other existing users, do the following steps:

a. Go to **Users > All Users**.

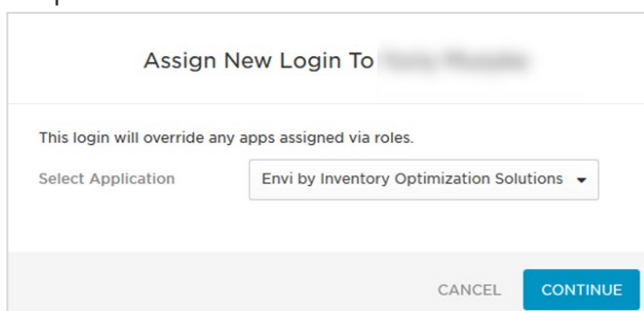


b. Select a needed user.

c. Go to the **Applications** tab and then select the **Plus (+)** icon.



d. In the **Assign New Login To** pop-up window, select your application from the dropdown list and select **Continue**.



- e. In the **Edit Login For** pop-up window, select the **Allow users to sign in** checkbox and select **Save**.

**Note:** The **NameID (Subject)** and **Username** fields should show the current user's email address.

Edit Envi By Inventory Optimization Solutions Login For

Enabled  Allow users to sign in

NameID (Subject)

Username

Email Address

CANCEL DELETE SAVE

Now, the **SSO** configuration is ready for use.

# Envi Configuration

In the **Envi** application, set up the following domain and user configurations:

1. Sign in to the **Envi** application.
2. Go to **My Profile > Domain List**.
3. Select a needed domain and then select **Edit**.
4. In the **Authentication** dropdown list, make sure that **HTTP Redirect** is selected and then select **Upload Metadata**.

Domains > Domain Name Domain\_Name Default Change

**DETAILS** ORGANIZATIONS USERS PASSWORD DICTIONARIES RESOURCES SECURITY

**Update** Cancel

Name\*: Domain\_Name

Description: Description

Session Timeout, m: 20

Mobile Token Expiration, h:

Default UI: Default [Update Users](#)

Status: Active

Authentication: HTTP Redirect **Upload Metadata**

Failed Attempts\*: 255 ⓘ

Endpoint URL:

Identifier URL:

SSO Message\*: Please provide your SSO credentials for further ⓘ

Require force authentication.  
 Require device registration.  
 Restrict IP Addresses.

5. In the **Upload Metadata** pop-up window, perform the following steps:
  - a. In the **Upload From** dropdown list, select **URL**.
  - b. In the **Select File** box, enter the **Issuer URL** (For more information, go to the [Integration](#) section, step 7).
  - c. Select **OK**.

**Upload Metadata** ✕

Upload From: URL

Identifier URL\*:

**OK** Cancel

**Note:** Make sure that the **Endpoint URL** and **Identifier URL** are updated with new values and that the **Certificates** section contains new certificates.

Domains > Domain Name Domain\_Name

**DETAILS** ORGANIZATIONS USERS PASSWORD DICTIONARIES RESOURCES SECURITY

**Edit**

Name: Domain\_Name

Description: Description

Session Timeout, m: 20

Mobile Token Expiration, h:

Default UI: Default [Update Users](#)

Status: Active

Authentication: HTTP Redirect

Failed Attempts: 255

Endpoint URL: http://login.microsoftonline.com/f895cf5e-95fc-493c...

Identifier URL: http://app.onelogin.com/saml/...

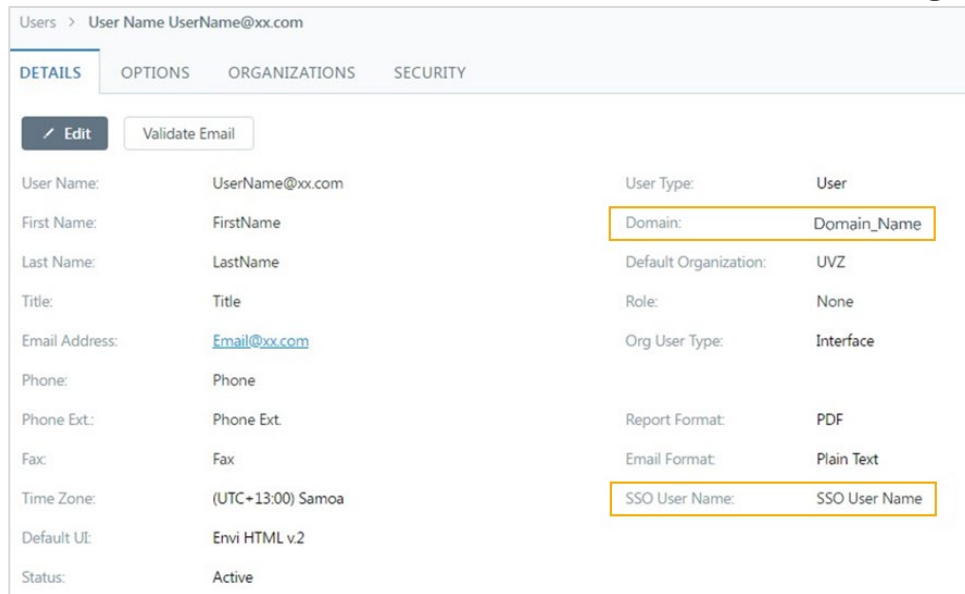
SSO Message: Please provide your SSO credentials for further logins

Do not require force authentication.  
 Do not require device registration.  
 Do not restrict IP Addresses



**Note:** While creating a user, perform the following steps:

- a. Select the needed domain with **HTTP Redirect** type of authentication.
- b. In the **SSO User Name** field, enter the username from the **OneLogin** application.



Users > User Name UserName@xx.com

DETAILS OPTIONS ORGANIZATIONS SECURITY

[Edit](#) [Validate Email](#)

User Name:	UserName@xx.com	User Type:	User
First Name:	FirstName	Domain:	Domain_Name
Last Name:	LastName	Default Organization:	UVZ
Title:	Title	Role:	None
Email Address:	<a href="#">Email@xx.com</a>	Org User Type:	Interface
Phone:	Phone	Report Format:	PDF
Phone Ext.:	Phone Ext.	Email Format:	Plain Text
Fax:	Fax	SSO User Name:	SSO User Name
Time Zone:	(UTC+13:00) Samoa		
Default UI:	Envi HTML v.2		
Status:	Active		

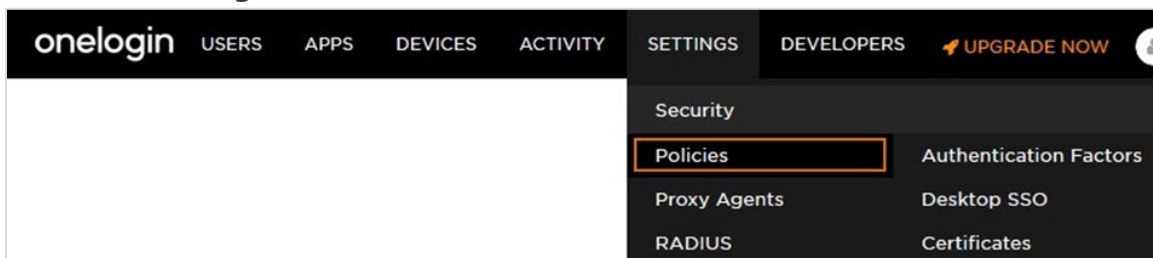
Now, you can sign in to the **Envi** application using **OneLogin SSO**.

# Browser Extension

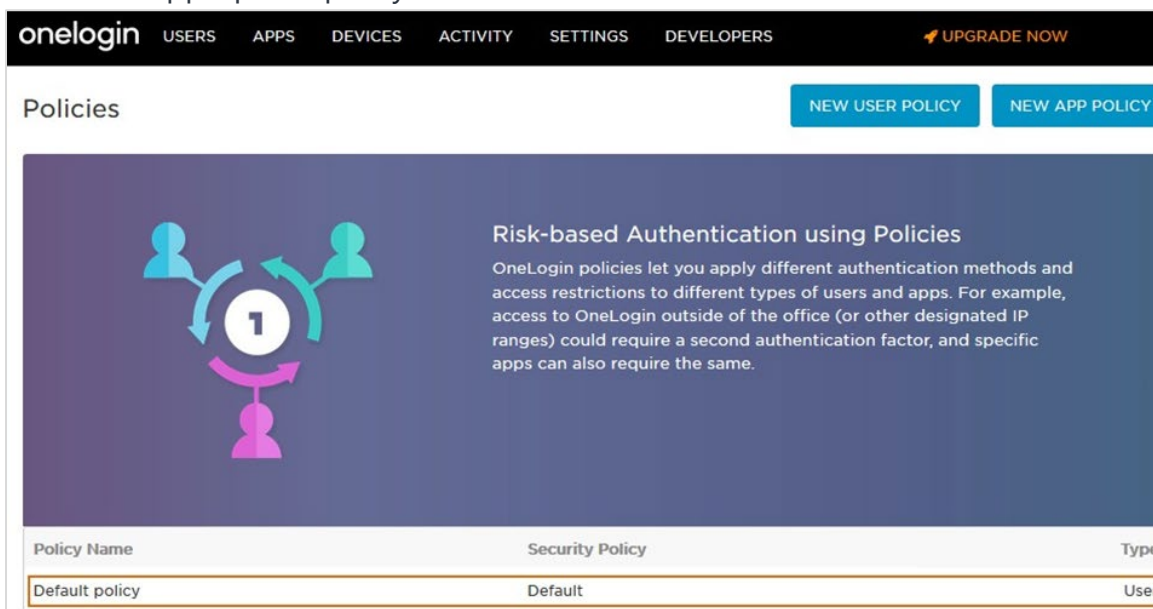
The **OneLogin** browser extension provides a convenient toolbar shortcut to your **OneLogin** dashboard.

To enable users to use browser extensions, make appropriate changes in the policy assigned to this user. To do this, do the following steps:

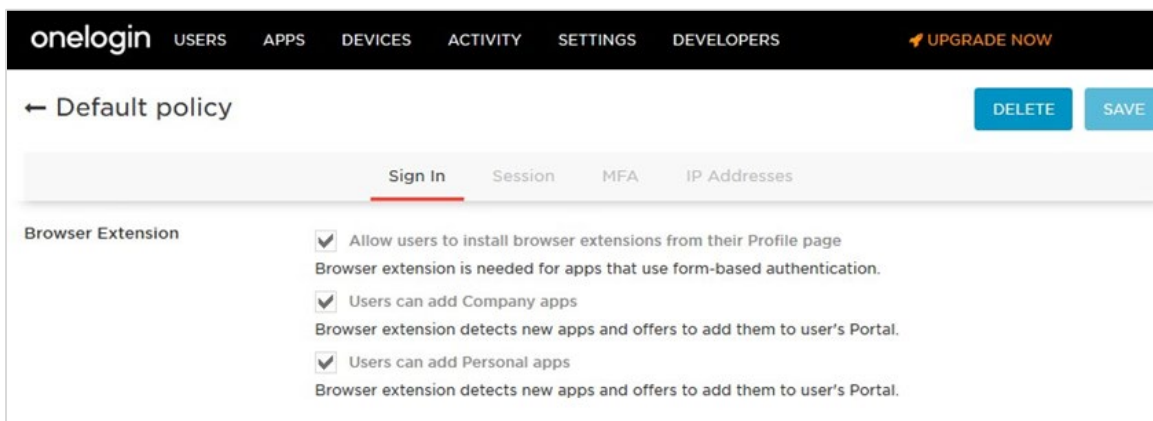
1. Go to the **Settings** tab and select **Policies**.



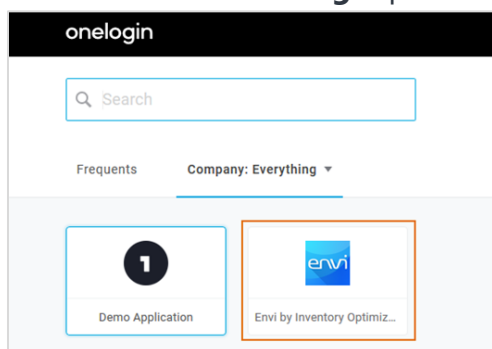
2. Select the appropriate policy.



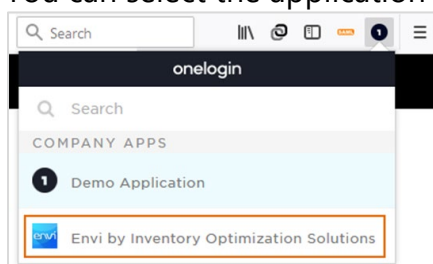
3. On the **Sign In** tab, in the **Browser Extension** section, select needed checkboxes, and then select **Save**.



When you do all configurations and install the extension, your application will be available in the list of the **OneLogin** portal.



**Note:** You can select the application directly from the browser extension.



Now, the browser extension is added for a needed user.