Setting up Single Sign On with ADFS

Last Modified on 18.04.2024

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.

In order to configure the Single Sign-On for Userlane, follow these steps below:

Setting up SSO with ADFS

Userlane can accept authentication via the SAML 2.0 Protocol.

Of the many implementations of this protocol, Microsoft Active Directory Federation Services (ADFS) is one of the most widespread. In this scenario, an ADFS server acts as the Identity Provider (IDP) and Userlane as the Service Provider (SP).

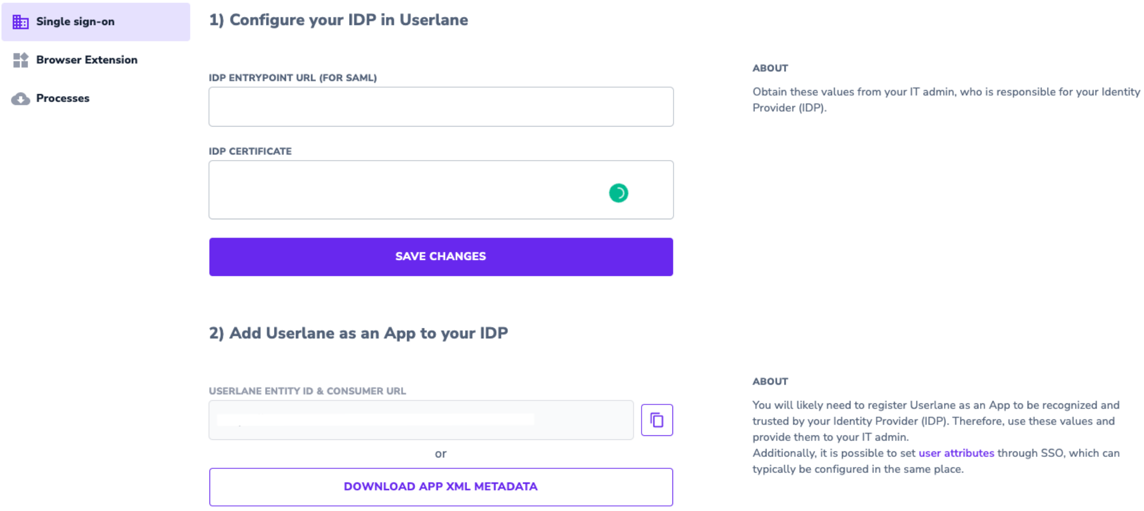
1.1. Adding the Identity Provider (IDP) details to Userlane

To register your IDP with Userlane, the IT Admin needs to provide the following info about the company IDP to the SA:

- Entry point/target URL that users will be redirected to for authentication
- X509 Certificate/Signatures so that Userlane can securely validate authentication claims

This information is often contained in a Metadata XML file.

Then, sign in to Userlane **Portal > Settings > Single Sign-on** and add the required information.



1) Configure your IDP in Userlane

IDP ENTRYPOINT URL (FOR SAML)

IDP CERTIFICATE

ABOUT

Obtain these values from your IT admin, who is responsible for your Identity Provider (IDP).

2) Add Userlane as an App to your IDP

USERLANE ENTITY ID & CONSUMER URL

or

ABOUT

You will likely need to register Userlane as an App to be recognized and trusted by your Identity Provider (IDP). Therefore, use these values and provide them to your IT admin.
Additionally, it is possible to set user attributes through SSO, which can typically be configured in the same place.

1.2. Adding Userlane as a Service Provider (SP) to your IDP

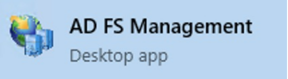
For the company's IDP to accept authentication requests by Userlane, the IT Admin must first register Userlane as a Service Provider (SP).

> ℹ The Userlane Service Provider Metadata differs for each customer. Your Userlane SA will provide you with a .xml file to import into your ADFS Server.

Registration steps:

1. Download the Metadata file onto your ADFS Server

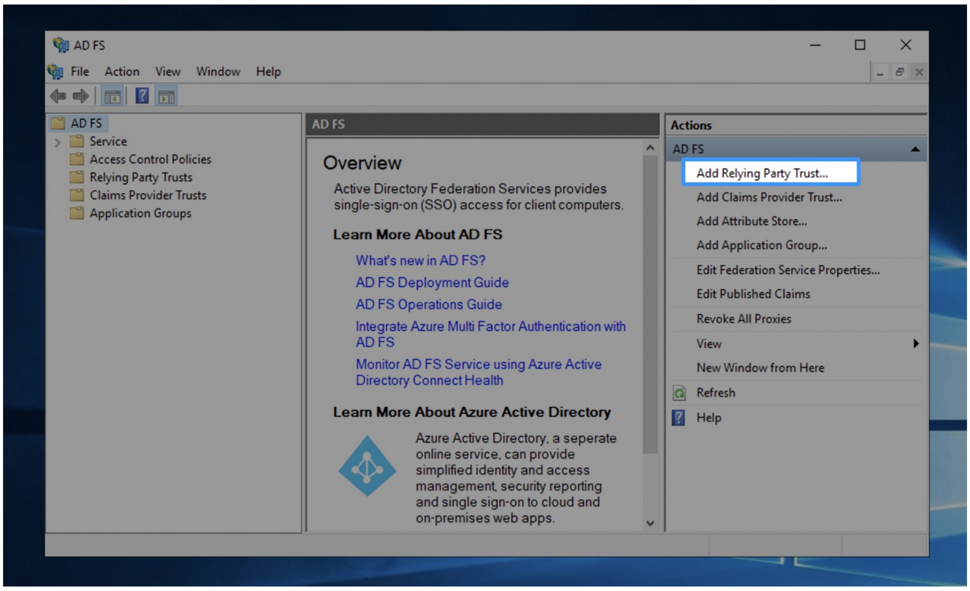
2. Open the “AD FS Management” app



AD FS Management

Desktop app

3. In the menu on the right, select “Add Relying Party Trust”



Overview

Active Directory Federation Services provides single-sign-on (SSO) access for client computers.

Learn More About AD FS

What's new in AD FS?

AD FS Deployment Guide

AD FS Operations Guide

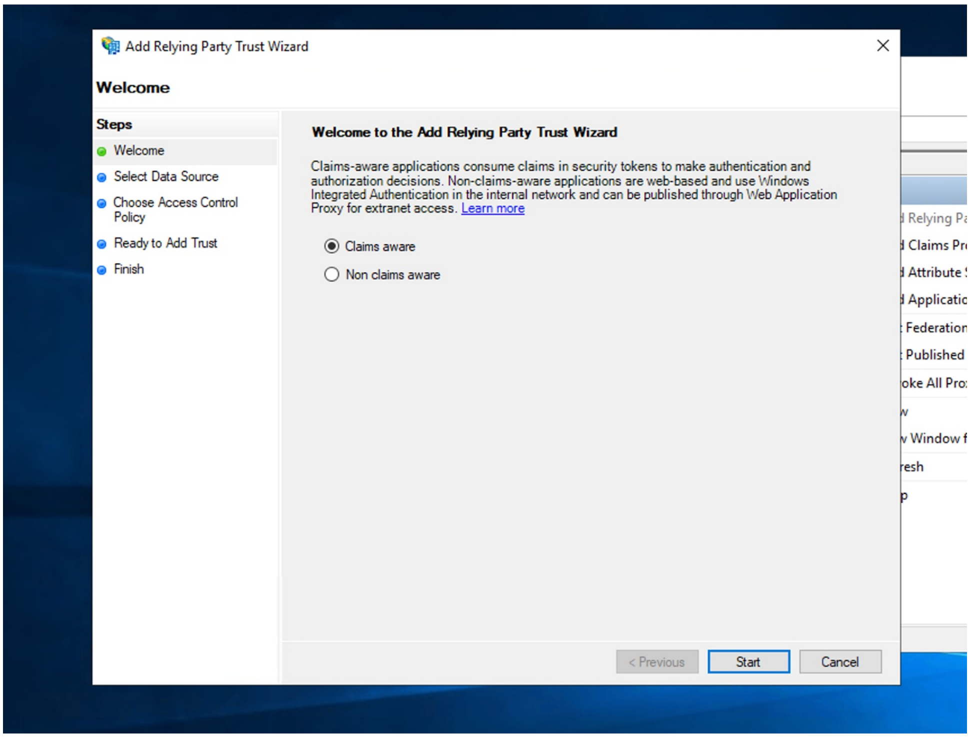
Integrate Azure Multi Factor Authentication with AD FS

Monitor AD FS Service using Azure Active Directory Connect Health

Learn More About Azure Active Directory

Azure Active Directory, a seperate online service, can provide simplified identity and access management, security reporting and single sign-on to cloud and on-premises web apps.

4. Select “Claims aware”



Welcome

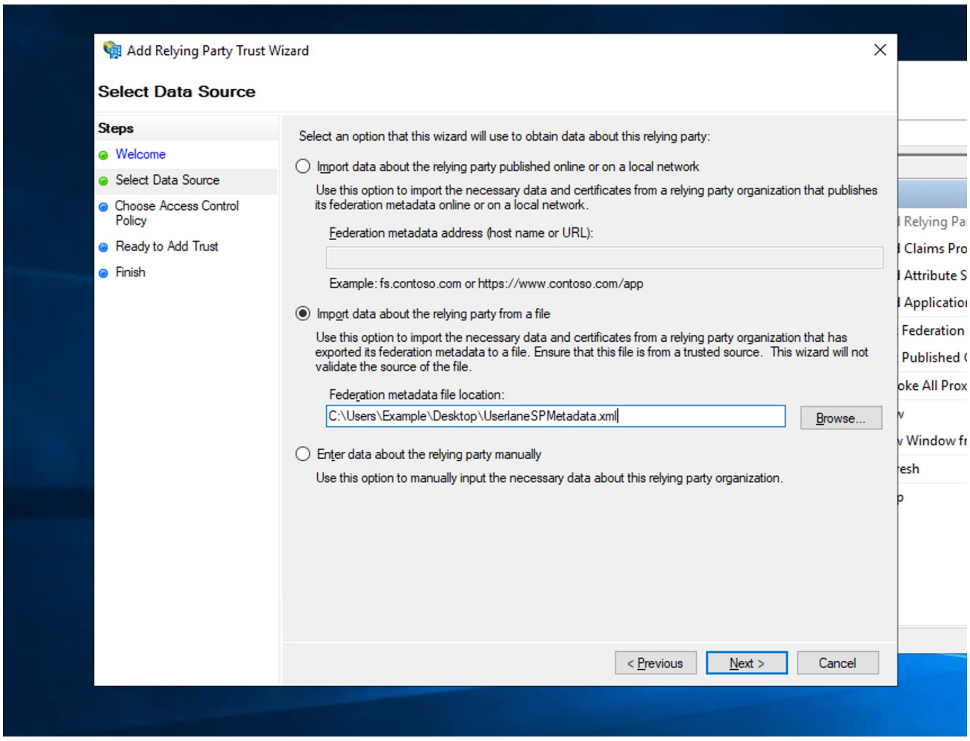
Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware

5. Select the Metadata file you’ve downloaded or follow the instructions for manual setup below



Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

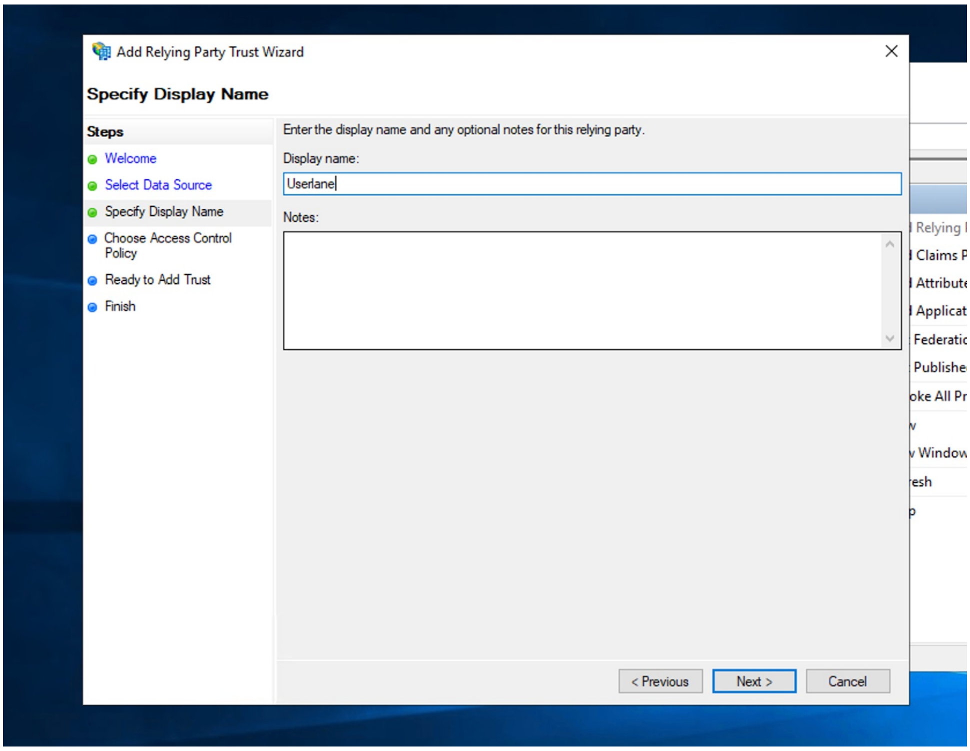
Federation metadata file location:

C:\Users\Example\Desktop\UserlaneSPMetadata.xml

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

6. Specify any display name or description you like



Specify Display Name

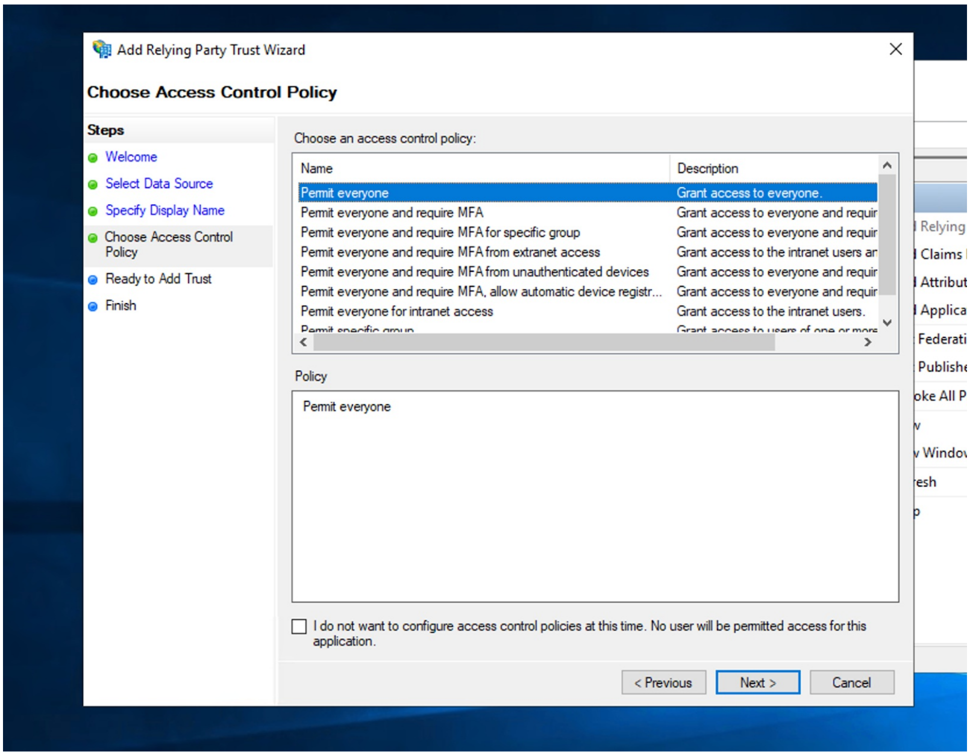
Enter the display name and any optional notes for this relying party.

Display name: Userlane

Notes:

7. It is essential to configure which employees are targeted for Userlane.
In general, any employee who has access to the connected application that uses Userlane for enablement purposes should also have access to the Userlane app. However, we recommend that App Owner confirms the target group after consulting with SA to avoid any misunderstanding.

Note: Do not configure MFA (Multi-factor Authentication) as a requirement in order to make the sign-in easier and seamless for your users.



Choose Access Control Policy

Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and requir
Permit everyone and require MFA for specific group	Grant access to everyone and requir
Permit everyone and require MFA from extranet access	Grant access to the intranet users ar
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and requir
Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and requir
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more

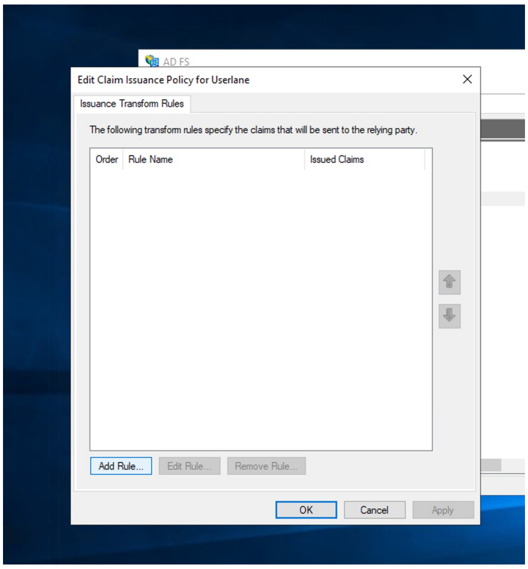
Policy

Permit everyone

☐ I do not want to configure access control policies at this time. No user will be permitted access for this application.

8. Confirm in order to add the Trust and continue with configuring a claims issuance policy for your application

8.1. Select “Add Rule”



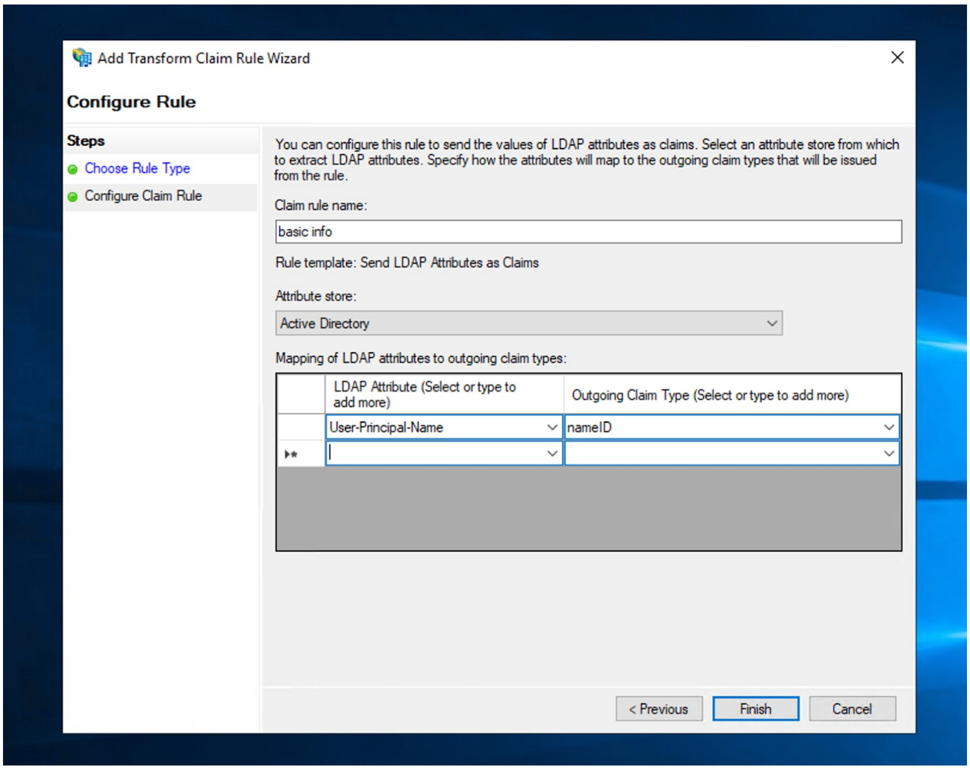
Edit Claim Issuance Policy for Userlane

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims

8.2. Userlane requires a “nameID” (**please keep the exact letter-case form**) in the Outgoing Claim Type. This will be the unique identifier on Userlane level and it is the only mandatory attribute required. This ID must be unique for each user and is not meant to be changed over time in order to keep historical information clean.



Add Transform Claim Rule Wizard

Configure Rule

Steps
- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
basic info

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

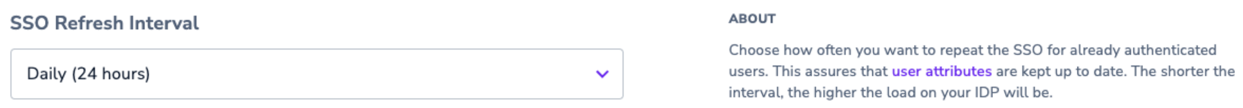
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	User-Principal-Name	nameID
▸*		

Additional user information required by App Owner for improved targeting is explained in the article Expanding the Settings

Save and apply the Claim Rule

Make sure to choose how often you want to repeat the SSO for already authenticated users. This assures that user attributes are kept up to date. For doing this: sign in to Userlane **Portal > Settings > Browser Extension** then in the dropdown SSO Refresh Interval choose one of the available options. Keep in mind that the shorter the interval, the higher the load on your IDP will be.



SSO Refresh Interval

Daily (24 hours)

ABOUT

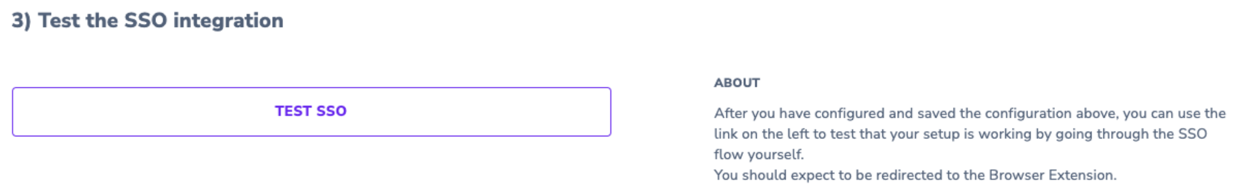
Choose how often you want to repeat the SSO for already authenticated users. This assures that user attributes are kept up to date. The shorter the interval, the higher the load on your IDP will be.

Test the single sign-on implementation

To test the integration after the setup has been completed, open the following URL in a browser:

https://sso-saml.userlane.com/c/USERLANE-COMPANY-ID/authenticate or you can do it within the Portal:

Then, sign in to Userlane **Portal > Settings > Single Sign-on** and click the Test SSO button.



3) Test the SSO integration

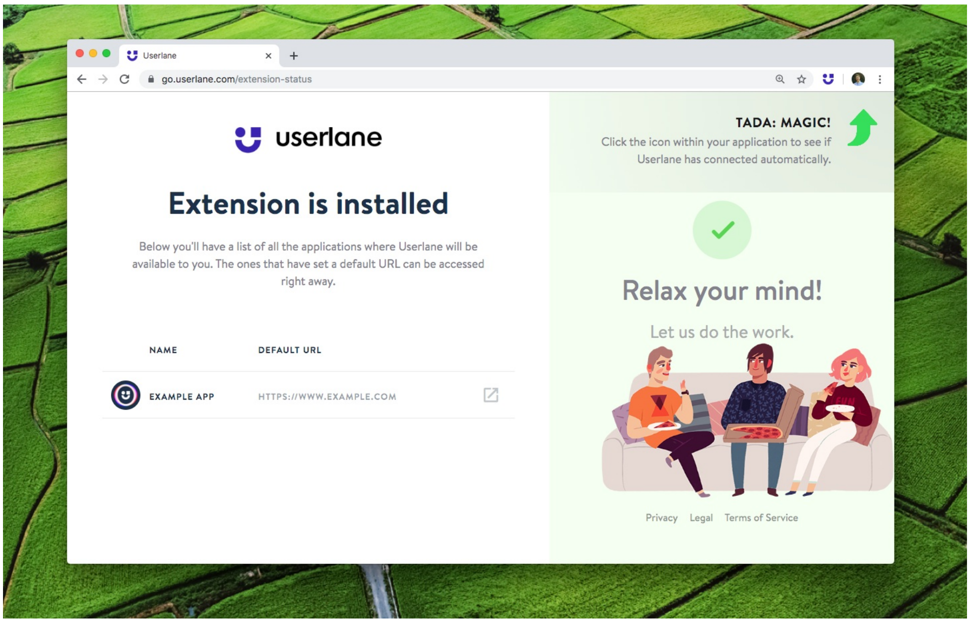
ABOUT

After you have configured and saved the configuration above, you can use the link on the left to test that your setup is working by going through the SSO flow yourself.
You should expect to be redirected to the Browser Extension.

The user will be redirected to the IDP.

After successful authentication, the user will be redirected back to Userlane and the Browser Extension will be authenticated.

Users with given permission will be authenticated and end up on the overview page:



Extension is installed

Below you'll have a list of all the applications where Userlane will be available to you. The ones that have set a default URL can be accessed right away.

NAME	DEFAULT URL
EXAMPLE APP	HTTPS://WWW.EXAMPLE.COM

TADA: MAGIC!

Click the icon within your application to see if Userlane has connected automatically.

Relax your mind!

Let us do the work.