Single Sign-On: Getting started with SSO

BY YANNICK MERCKX · NOVEMBER 10, 2022 · LAST UPDATED ON JULY 28, 2025

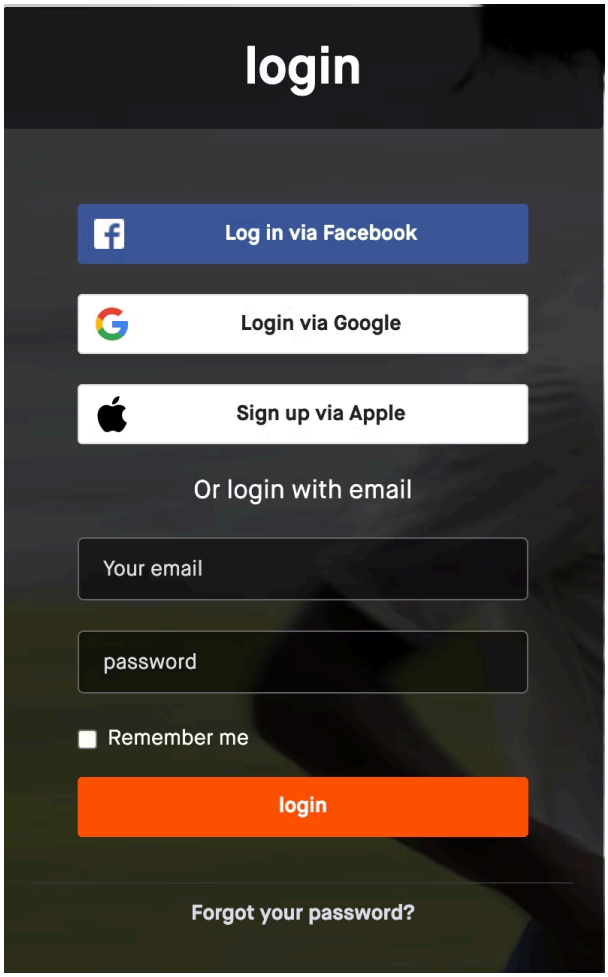
Single Sign-On: What is it? What does it do?

Single Sign-On (SSO) is a wonderful thing. As a user, it means no more handling hundreds of separate passwords or 2FA tokens. As a security professional, there's no more trying to enforce policies in different enterprise applications without the proper ability to do so.

For those of you who may not fully be up to speed with what SSO is and what it does, let's look into the definition as per the most popular online encyclopedia (you know which one):

> **""Single sign-on (SSO) is an authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.""**

While the above is technically true, it's often easier to refer to an example. The "Sign-in with..." button that is now found on most major web applications? That's SSO in action!



A classic example of SSO

Obviously, this works a little different in an enterprise context. To ensure the security of such systems, standards such as Secure Assertion Markup Language (SAML) and OpenID Connect exist. And for any of those standards, SSO is built around the concept of a so-called Identity Provider (IDP). This IDP, to refer to the example in the beginning, could be Google or Facebook, but for obvious reasons is often different in an enterprise context

How does SSO work?

When a user attempts to log in to a web application using SSO, the application performs a check with the IDP to confirm their identity. So, assuming you want to log into your favorite booking website and choose SSO, the website would recognize the request and then forward it to the chosen IDP, let's say Google. Google then asks the user for their credentials and possibly even multi-factor authentication, and responds to the website with: "That's the guy!".

Single Sign-On as implemented by Intigriti

The Intigriti implementation of SSO uses OpenID Connect as a framework and will therefore work with any IDP that allows the configuration of apps via OpenID Connect.

There are multiple reasons why we chose for OpenID Connect rather than SAML, but it was driven by the fact that OpenID Connect is new, lightweight and, most importantly, still actively evolving into the best iteration of itself.

So what does that mean? That mostly just means that the chosen Identity Provider should explicitly be able to support OpenID Connect. Of course, the most common ones do:

- Azure AD
- Okta
- Auth0
- OneLogin
- PingIdentity
- Google Identity

Configuring those largely depends on the chosen provider, but it doesn't work entirely without a bit of configuration in the Intigriti platform as well. We have dedicated some articles in our knowledge base for this purpose, but this can be summarized in two important steps:

1. Configure SSO in the Intigriti platform
1. Switch users over to SSO login

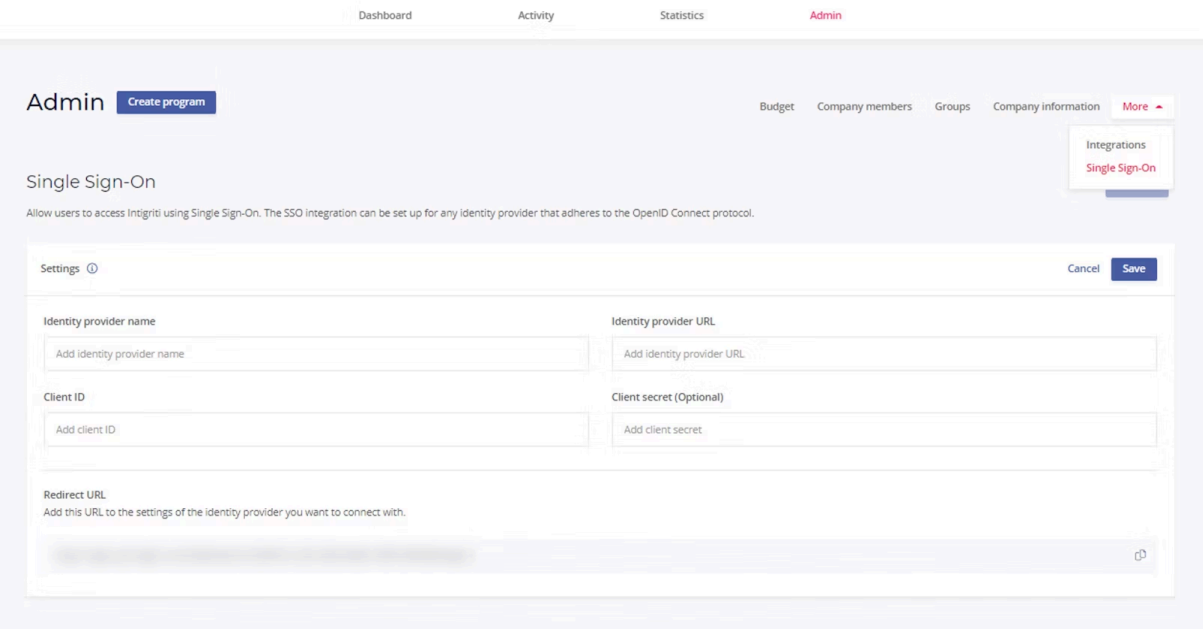
Configure SSO in the Intigriti platform

Setting up SSO in the Intigriti platform is generally quite straightforward, at least to the extent that configuration on the platform is concerned. No matter what IDP is supporting the SSO setup, the same three types of information always need to be provided in the Intigriti SSO admin panel:

- Identity Provider name
- Identity Provider URL
- Client ID and Client Secret (the latter is optional)

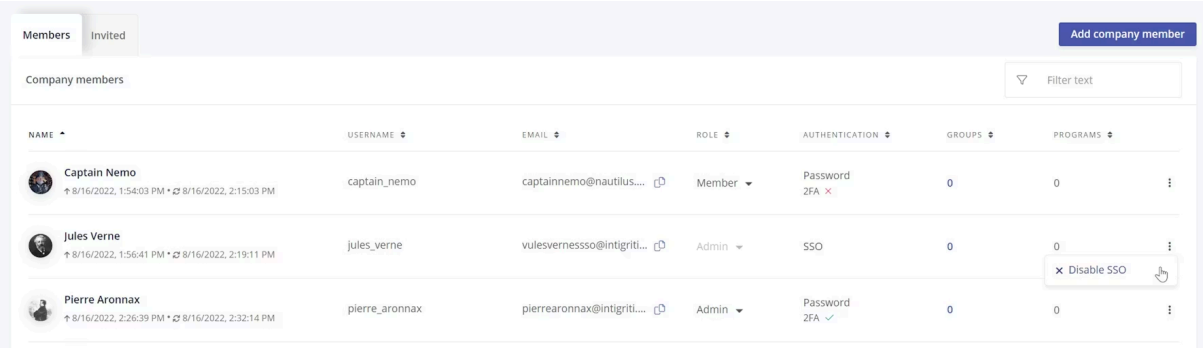
In addition, the Redirect URL from the field at the bottom of the screen needs to be shared with the IDP.

The above works differently for every IDP but but we have tried to make the setup process as quick and easy as possible. Good news, right?



Switch user over to SSO login

Exisiting company users don't have to worry. Once SSO is activated, you can easily transition from password-based authentication to SSO. In our knowledge base, you will find [a step-by-step guide on this transition]



What else have we got going on?

Visma's head of bug bounty is talking about what it takes to run a successful program and how valuable it is to them:

and they are organizing a live hacking event (LHE) soon!

> " #1337UP1122 alert!
> Visma (@HackersMother) just launched their second live hacking event with Intigriti!
> We can't wait to see all of these AMAZING hackers in Copenhagen next week! #HackWithIntigriti
> pic.twitter.com/8e2YOZeEv0
>
> — Intigriti (@intigriti) November 9, 2022"

We also did some considerable housekeeping on some of those smaller bugs and picked up some other small possible improvements.

If you notice any of these, we'd love to hear from you (your chance to make a Dev happy). Otherwise, we'll be quietly happy knowing that we contributed in some way to keeping everything nice and polished

Fun Fact

Last week, we had a small Halloween party at our HQ in Belgium. Who do you think was the scariest?

Does the idea of working in a promising, flexible and fulfilling environment inspire you? Discover careers at Intigriti by visiting our careers page or following us on LinkedIn. We look forward to your application!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com