evaluagent

Integrated User Management & Single Sign-On (SSO)

The dream...

Integrated User Management enables you to manage ALL user profiles across ALL your software applications in ONE place. Joiners, leavers, movers are updated in just one application, and all changes are then *automatically* replicated across all other applications.

Single sign-on (SSO) enables employees to enter their login credentials (*username & password*) into just ONE login screen to gain access to ALL their applications without having to repeat the process for every application they use.

Saves hours of effort and increases security

Instead of remembering *multiple* passwords (*or more likely writing them all down somewhere*) and then having to separately login into *multiple* applications, employees simply remember one strong password and log into one system which automatically logs them into everything.

Rather than having to manage the security controls of multiple applications, IT can now control security protocols using a single centralised Identity Provider application specifically designed for secure user management.

See next slide for more details

When employees join, leave, move, edit user details, their account profile only needs to be updated ONCE in ONE place - dramatically reducing admin effort & errors.

Step 1: Implement an Identity Provider application

An Identify Provider (IdP) application securely stores and manages software user profiles and acts as a *single* source of the truth. You'll first need to implement an IdP application for your business to benefit from *Integrated User Management* and *SSO*.

When browsing at home, you may be familiar with the Facebook IdP application which is used by many websites to enable users to "Sign in via Facebook".

More business-focused IdPs include: OKTA, OneLogin, Microsoft Azure Active Directory (AD), Google Suite and Ping Federate.

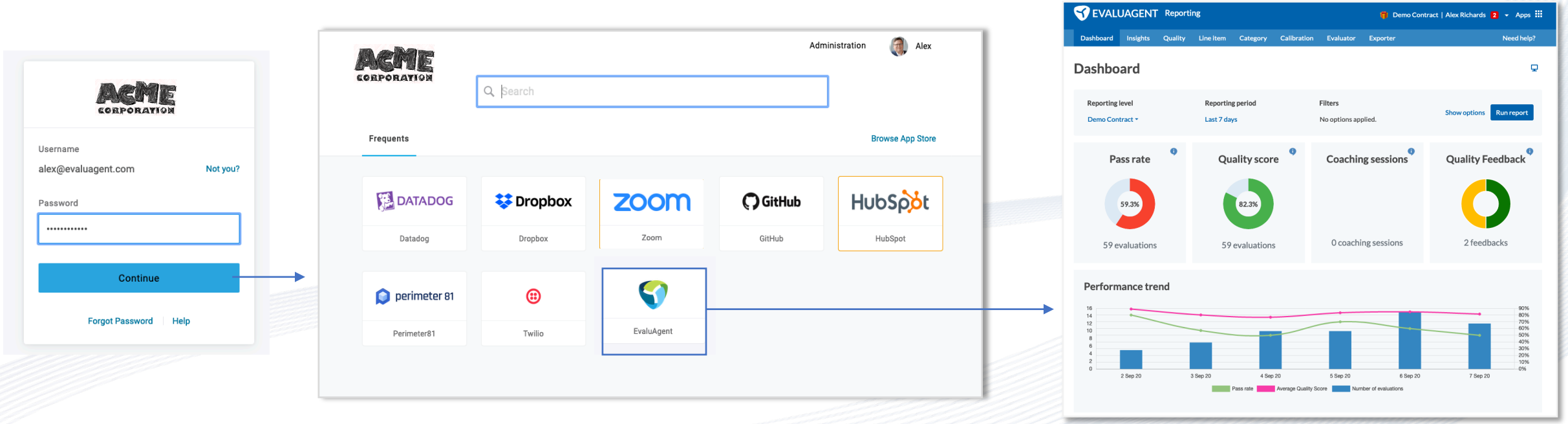
Step 2: Integrate your applications

Once you've implemented your IdP application, you'll need to connect each of your Service Provider (SP) applications (E.g. EvaluAgent) with your central IdP application.

Smooth integration is achieved based on all applications using a protocol known as Security Assertion Mark-up Language (SAML). This is simply, a standardised way of applications "talking" to one another - sending and receiving login and user profile data that is structured in the same way even when the individual applications are coded in different languages.

To integrate SP applications such as EvaluAgent with your IdP application, each SP application will need to support SSO and offer a System for Cross-domain Identity Management (SCIM) API.

SSO workflow for Users



Step 1

The user logs into the Identity Provider IdP application via the Internet.

Microsoft's Active Directory IdP application can be linked to a PC's security so that the process of logging into the PC triggers the process

Step 2

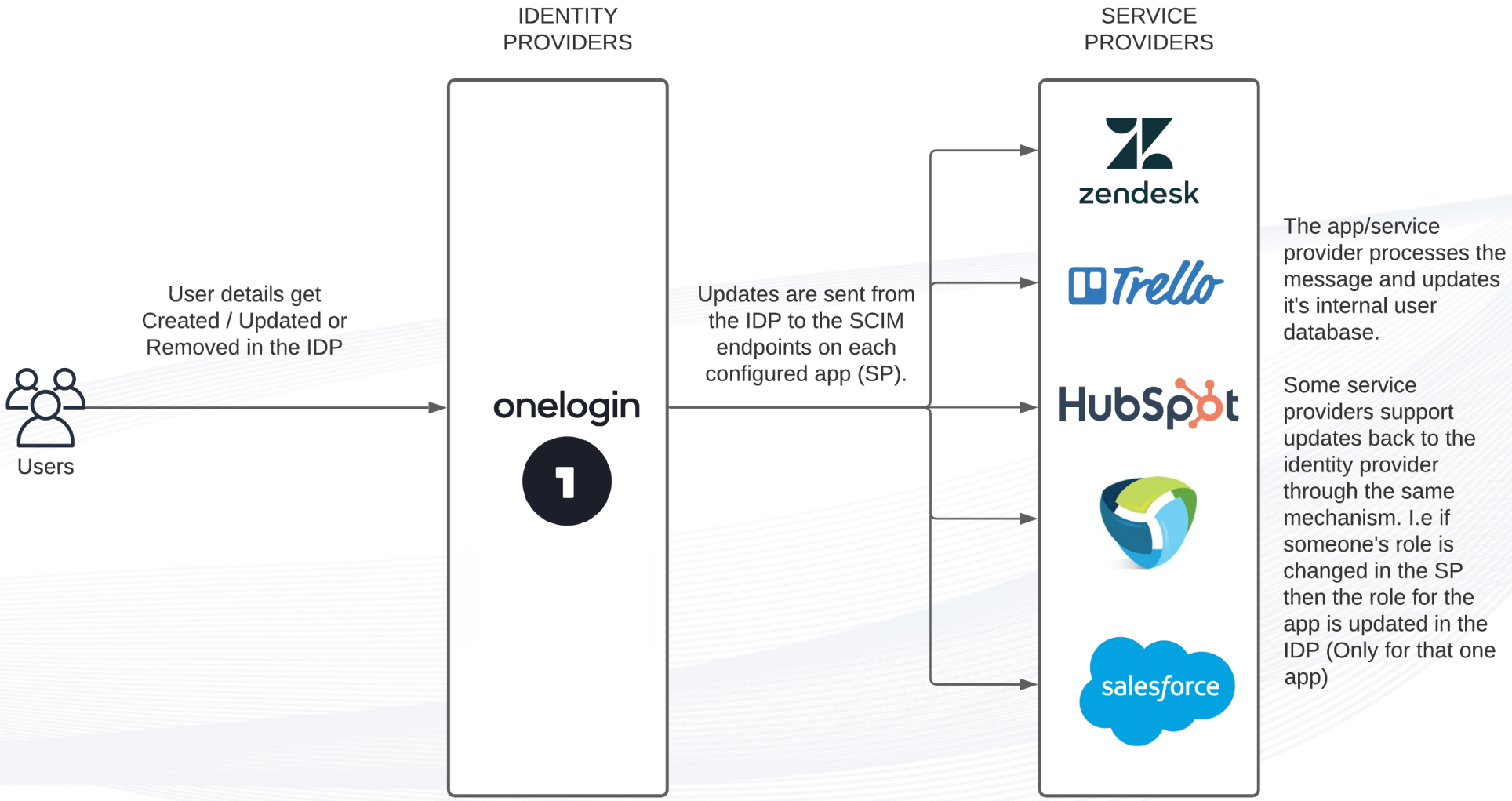
The User is directed to a screen which shows all of the service provider applications he has access to. He can access any one of the platforms by clicking the relevant icon.

Step 3

The user is automatically verified when a SAML request sent over the Internet from the IdP application to the service provider application is verified

The User is seamlessly transferred into his account in the service provider application without any further action required on the part of the User.

Integrated User Management for Administrators



The app/service provider processes the message and updates it's internal user database.

Some service providers support updates back to the identity provider through the same mechanism. I.e if someone's role is changed in the SP then the role for the app is updated in the IDP (Only for that one app)