onelogin

SOLUTION DATASHEET

Single Sign-On with Trusted IdP

Secure access across multiple applications with a single, shared identity

In order to accelerate time-to-market and support business growth, modern organizations today need to provide anytime, anywhere access not only for their own employees, but also for their partners and end customers. This, however, poses additional challenges for IT and Security teams on how to efficiently manage diverse user groups, which includes 3rd party identities, provide adequate security controls to protect critical data, and ensure end users enjoy a consistent and familiar experience no matter what application or service they need to access.

Single Sign-On with Trusted IdP

The Trusted Identity Provider (TIdP) feature of OneLogin's Single Sign-On (SSO) solution allows administrators to configure multiple identity providers to securely sign in users, such as customers and partners, into various applications via OneLogin. Automatically pass information from 3rd party identity providers to OneLogin without having to manage the identities themselves, thereby improving overall efficiency and security through easy and cost-effective management of external identities.

KEY BENEFITS OF ONELOGIN SSO WITH TRUSTED IDP

Enhance the user experience with identity federation

Allow end users to leverage their local or existing credentials, such as social accounts (e.g. Facebook, Google, LinkedIn), without having to create an additional username and password for each application–all while keeping the authentication experience between identity providers consistent and transparent to the end user.

Enforce additional security controls

Increase security and visibility by layering MFA on top of your applications to protect sensitive data. Provide consistent user-based security policies for managing access to all your on-premises and cloud applications. Optionally add risk-based MFA to balance security with the end user experience. Stream event data to SIEM tools, like SumoLogic and Splunk, to better detect potential security threats.

Leverage automated, real-time provisioning

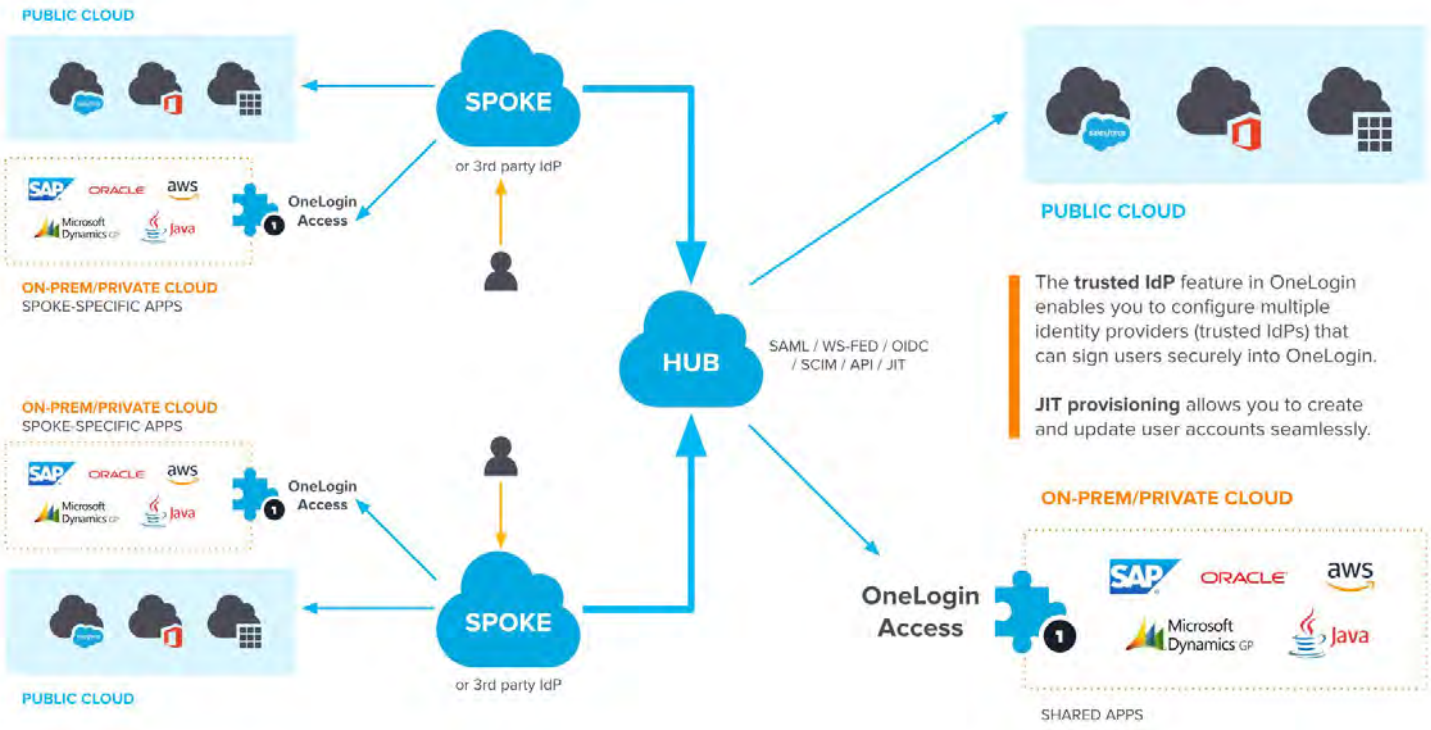
Eliminate manual user onboarding and offboarding with Just-in-Time (JIT) provisioning. Automatically create user accounts when a new user logs in for the first time and update the account during subsequent logins so that OneLogin has the most up-to-date user information asserted by the IdP at the time of authentication. Utilize fine-grained entitlement mappings based on user attributes to consistently provision and deprovision users across multiple applications and services.

Simplify management & reduce TCO

Control how users access corporate apps without having to manage their identities in-house. Improve overall business agility by eliminating the need for costly and time-consuming directory integrations. Reduce unnecessary license costs for on-prem directories and applications, while extending business services to your different partners and end users.

"Our member firms continue using their local identity providers but we can be confident about secure access to commonly used resources. We have aligned our security controls using OneLogin."

HELDER SANTOS | Director of Digital & IT, CMS Legal Services



How OneLogin SSO with Trusted IdP Works

OneLogin's TIdP feature with SSO follows a "hub and spoke" model, where the identity provider, which could be another OneLogin tenant or any 3rd party IdP utilizing SAML, OIDC or OAuth, represents the "spoke". The OneLogin tenant, where the target application resides, represents the "hub". You can have multiple identity providers, or "spokes", that feed into the hub. The spoke is where the user signs in and where the authentication for the TIdP flow happens.

With OneLogin's Reseller model, the hub administrator can spin up additional OneLogin tenants on behalf of their partners for those that don't have an existing IdP.

Trusted IdP supports several different flows for logging into a new application via the hub with SSO. This can be as simple as a single click from the user's home IdP portal with IdP-initiated scenarios, to a variety of more complex flows to support SP-initiated scenarios.

Providing support for different user flows ensures that users gain the SSO access they desire in the way that suits them best.

Regardless of the specific flow, the user's identity is transferred to the OneLogin hub via the chosen standards-based protocol (SAML, OIDC or OAuth). This inbound identity is either matched to a local account where one exists, or created on the fly using JIT provisioning.

Automated mappings ensure that users are assigned access and provisioned into the relevant services and downstream applications. Depending upon security policies in place, which may dictate the need for a step-up MFA authentication, the end user enjoys a seamless sign in experience into the hub via TIdP as well as the requested applications integrated with the hub.

Over 2,500 enterprise customers globally secure their applications with OneLogin

AAA AIRBUS pandora Steelcase STITCH FIX