Single sign-on (SSO) and Journyx

What is single sign-on (SSO)?

Simply put, single sign on is a way for your employees to use Journyx and all the other applications they need without having to sign into each application separately. A single corporate login screen gives your employees immediate access to all the apps they need throughout the day without having to remember or type a separate password for each application.

What is federated identity?

A federated identity management system connects different departments and organizations so that a person's account, password and other identity attributes can be used seamlessly across the whole enterprise. Identity federation allows for easier administration, better IT security practices, and a more consistent user experience through single sign-on.

Why would I want single sign-on?

Organizations are rapidly moving towards federated identities and single sign-on for a number of reasons, including convenience, flexibility, and perhaps most importantly, security. Passwords are one of the biggest sources of security risk and cyberattack in the enterprise. Your workforce needs secure access to a wide array of applications. A single enterprise-wide sign-on is not only more convenient for your users, but helps protect them and your organization from numerous password-related vulnerabilities.

What types of SSO are there?

There's a bewildering array of different identity and authentication products out there; too many to list here. The Security Assertion Markup Language (SAML) has emerged as a standard protocol for connecting applications with identity providers. Most federated identity products including Microsoft's Active Directory Federation Services (ADFS), PingFederate, Shibboleth, and Okta support SAML in some form. All of these products offer password-based login screens, but many of them support two-factor authentication (2FA), biometrics, and other features like account lockout control and recovery.

How does SSO work with Journyx?

Journyx version 9.5 and higher supports SAML single sign-on through the optional PSAuth module. In SAML lingo, Journyx is a service provider (SP) that connects to your corporate identity provider (IdP). That means your users never see the Journyx login screen or type a password directly into Journyx. Being signed into the central identity server means you are automatically signed into Journyx and any other SSO-enabled applications.

How this works in practice is that when your users access Journyx they are automatically redirected to your enterprise login screen as needed. Once they have signed in there they are redirected back to their Journyx time entry screen. If they have already signed in that day from another SSO-enabled app, this will be a seamless process. Depending on your exact settings they may not have to type their password a second time.

How is SSO more flexible for my organization?

Having a single identity or account across the enterprise allows you to set policies that affect all SSO-enabled applications. For example, you can set password quality requirements, enforce selective or temporary lock-outs, and so on. The exact capabilities depend on the identity provider solution. Most SSO products allow you to combine account or identity sources from many different departments or organizations, a process known as identity federation. This also makes it easier to on-board new users to your organization.

How does SSO make life easier for my users?

Most workers need to use several different applications throughout their workday. Users appreciate the convenience of only having to enter a single password to gain access to all their apps. They only have to learn one standard process for resetting a lost or forgotten password. Having a familiar, standard enterprise-wide login screen also helps to assure users that their password won't be intercepted or hijacked.

How does SSO improve security?

Aside from the benefits mentioned above, SSO helps protect your organization by giving centralized control over authorization and access to applications. Different applications can have very different standards for things like password aging and quality requirements. When users don't have to remember a long list of passwords for different services, it makes it less likely that they will write them down insecurely or share them inappropriately. SSO makes it easier to deploy two-factor authentication (2FA), which supplements password security (a knowledge factor) with physical factors like the possession of a hardware token or a mobile phone, or biometric factors such as fingerprints.

What about logging out? (Single Logout or SLO)

Journyx supports single logout or SLO. Because signing in gives your users access to all of their applications, signing out should likewise remove access to all SSO apps until the next time they sign in. The SLO process is not as standardized as sign-on, but Journyx can work with your IT department to ensure that your users have the workflow they need. The Logout button inside Journyx can be hidden, or we can make it start a "service provider initiated single logout" with your identity provider that signs them out of all relevant apps.

What about mobile devices and the iPhone and Android apps?

The Journyx web application is exactly the same when used on an iPad and other mobile devices, including any single sign-on features. Journyx also provides a "native" mobile app for Apple and Android devices. The current version of the native mobile app does not support SSO. Your users can still access this app with the built-in Journyx password option, which can be used alongside SSO, or with LDAP-based password checking integration. Future versions of the native app may support SAML-based SSO login screens. The web app fully supports SSO on mobile devices right now.

How is SSO different from LDAP or Active Directory password integration?

With single sign-on your users only see a single enterprise login screen for all SSO-enabled apps. Journyx also supports a separate LDAP or Active Directory integration where the user types their password into the Journyx login screen and we check it against your corporate directory instead of the internal Journyx password database. This type of backend password integration can be useful, but SSO has numerous other benefits that make it worth considering. SSO is the best option when Journyx hosts your application instance (known as SaaS).

What if my users sometimes share a device to enter their time?

Users may need to share a single physical device to enter their time in some cases, especially at job sites. This can include both desktop web browsers and mobile browsers like a phone or tablet. Single sign-on with the single logout (SLO) option is perfect for this scenario. Users sign in, enter their time and expense information, then click the Logout button to get signed out everywhere. They are put on a login screen that is ready for the next user to type his or her credentials and start entering time. The Journyx mobile app for iPhone and Android doesn't currently support SSO login screens, but does support switching user accounts on the fly.

How do I get started with SSO?

If you would like to use single sign-on in your organization but don't yet have a SAML identity provider service, Journyx can work with you to find an optimal solution. If you do already have an existing SSO solution, or have one in mind, talk to your Journyx sales associate to learn more about activing single sign-on in your Journyx application.