

Single Sign-On (SSO)



Mitigate risks, reduce password fatigue, lower the number of support calls, & reduce IT costs.

Highlights

Provides comprehensive support for the **SAML 2.0** and **Open ID Connect (OIDC)** federated single sign-on protocols. Use both **Service Provider (SP)** and **Identity Provider (IdP)** initiated sign-on flows: enter your username in Enterprise and be guided through the authentication or go to your company application portal (such as Microsoft 365®) to sign into Enterprise.

Pricing

- Service charged annually at **\$1,000 per aircraft.**
- **Discounts available** based on fleet size.
- SSO will be billed as a **separate line item.**
- Consolidated billing option.

For more information, contact us at learnmore@atp.com or call 1-800-747-4560.

Frequently Asked Questions

Q: What is SP-initiated SSO?

A: This is when users enter their username in Enterprise and Enterprise redirects them to the IdP sign-in page.

Q: What is IdP-initiated SSO?

A: This is when users go to their company portal and click the Enterprise app there to access it without additional signing in.

Q: What do I need to set up SSO?

A: An IdP, such as Microsoft® Active Directory, Azure AD, or LDAP, that supports either SAML 2.0 or OIDC protocols.

Q: Is there a process to enable new users to be automatically provisioned?

A: No. All user accounts must be created in Enterprise before a user can sign in with SSO.

Q: Do you require artifact-based federation?

A: No. We support artifact, but do not require it. We also support http post and http redirect.

Q: Do you require encryption in sign-in flows?

A: We support but do not require encryption. We utilize HTTPS URLs for all posts and redirects on both sides but it is not a requirement.

Q: Do all Enterprise users have the same access?

A: No. Permissions are 100% managed inside of Enterprise. The IdP will be responsible for identifying users and granting them access through perimeter security.

Q: How are users mapped or linked between Enterprise and the IdP?

A: There is flexibility in how mapping is achieved. The ideal mapping configuration is established through a collaboration between Flightdocs and you. To establish an initial mapping, the first time a user signs in, we map from the IdP name identifier attribute to Enterprise username. The attribute we map to is configurable per customer.

Q: Do you provide a non-production environment for SSO testing?

A: Yes. We provide a sandbox environment in which SSO can be tested and validated.

Q: Do you support SSO in your native iOS and Android apps?

A: Yes. We support SP-initiated SSO in the mobile apps. The IdP-hosted web interface facilitates the SSO process.

Q: Do you support SAML token encryption?

A: Yes. We support all modern and secure Microsoft.net encryption protocols.

For more information, contact us at learnmore@atp.com or call 1-800-747-4560.