

SSOJet Debuts AI-Native Enterprise SSO Platform Designed to Work Alongside Existing Auth Systems

AI-native platform adds enterprise SSO capabilities across 25+ identity providers to existing authentication infrastructure without migration

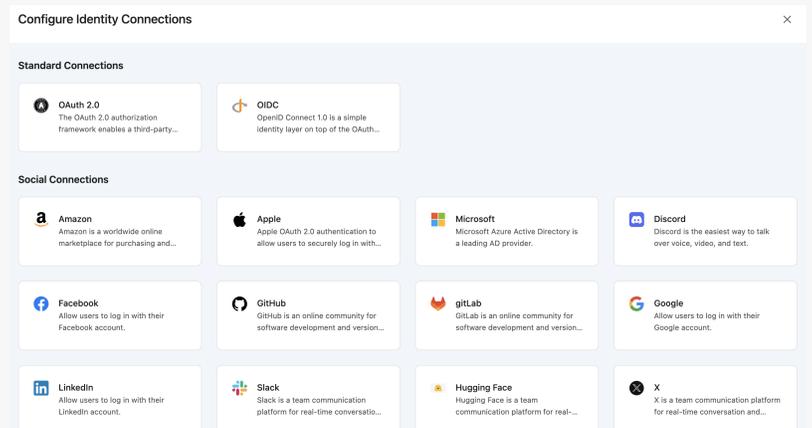
SAN FRANCISCO, CA, UNITED STATES, March 9, 2026 /EINPresswire.com/ -- SSOJet, an enterprise authentication infrastructure provider, today announced the general availability of its [Enterprise SSO platform](#) designed to solve one of the most persistent problems in B2B software: getting enterprise-ready without tearing out what already works.

For most B2B SaaS companies, the path to enterprise customers requires supporting Single Sign-On across a fragmented ecosystem of identity providers—Microsoft Entra ID, Okta, Google Workspace, Ping Identity, OneLogin, CyberArk, and dozens more. Historically, this has meant either building complex SSO integrations in-house, which can consume months of engineering time, or adopting a full authentication platform that requires migrating users and rearchitecting login flows.

SSOJet takes a fundamentally different approach. The platform operates as an enterprise SSO layer that sits on top of

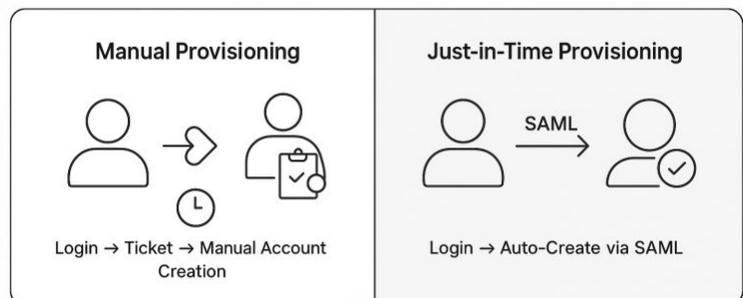


SSOJet Logo



SSOJet - External Identity Providers

**DON'T PROVISION USERS AFTER LOGIN.
PROVISION THEM WHILE THEY LOGIN.**



Powered by SSOJet – www.ssojet.com

SSOJet SCIM integration

a company's existing authentication infrastructure—whether that's Auth0, Firebase, Amazon Cognito, ForgeRock, or a custom-built solution. There is no user data migration, no workflow disruption, and no need to replace what engineering teams have already built and optimized.

[The Enterprise Readiness Gap](#)

Enterprise procurement processes increasingly gate deals on SSO compliance. Security questionnaires, vendor risk assessments, and IT policy requirements all demand that SaaS vendors integrate with the customer's workforce identity provider. For growing SaaS companies, this creates a painful choice: divert engineering resources to build SSO infrastructure, or lose enterprise deals to competitors who already support it.

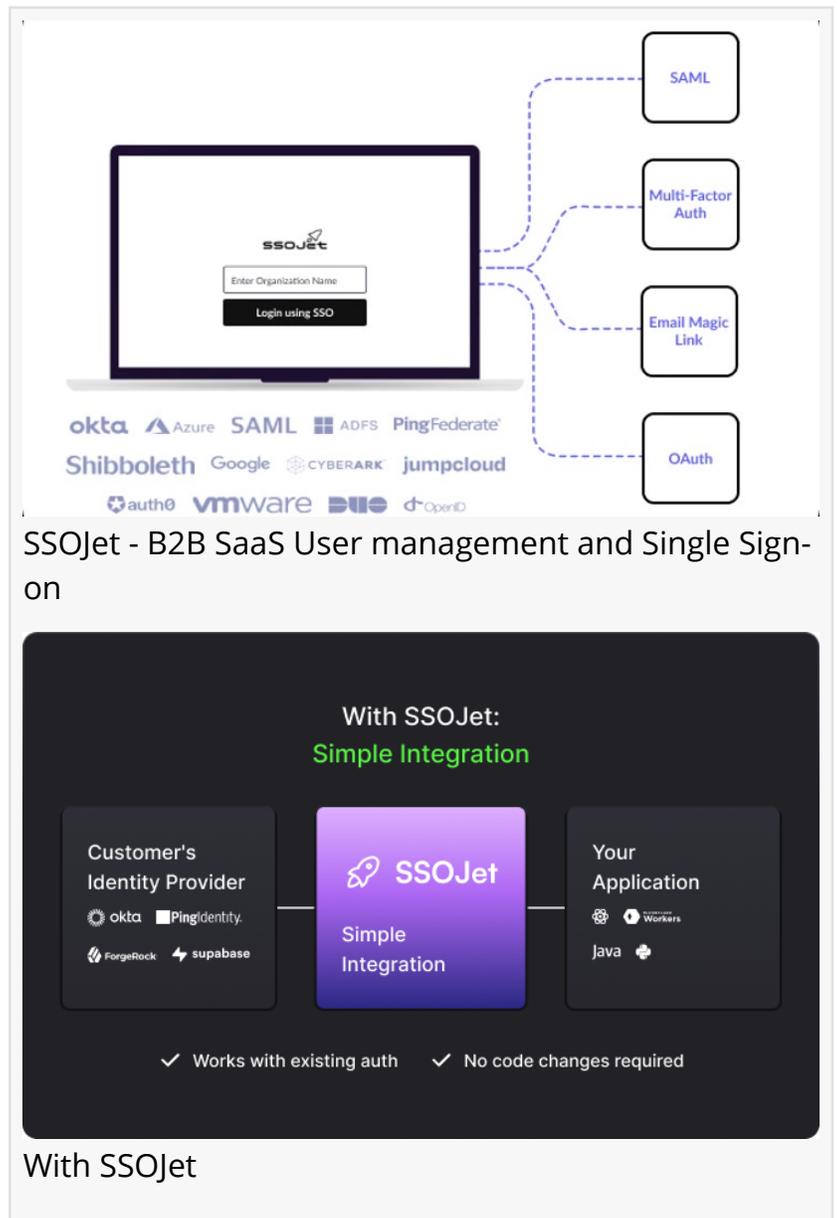
The complexity compounds quickly. Each enterprise customer may use a different identity provider. SAML 2.0 implementations vary between vendors. OIDC configurations require provider-specific handling. Certificate rotations, metadata management, and protocol edge cases all demand specialized expertise that most product engineering teams do not have in-house.

Industry estimates suggest that building production-grade SSO support for even a handful of identity providers can require 6–12 weeks of dedicated engineering work—time that directly competes with core product development.

Enterprise SSO as Infrastructure, Not Migration

SSOJet's architecture is built around a single principle: enterprise SSO should be additive, not disruptive. The platform provides a unified API and pre-built connectors for 25+ major identity providers, including Microsoft Entra ID (Azure AD), Okta, Google Workspace, Ping Identity, OneLogin, Salesforce Identity, IBM Security Verify, ForgeRock, JumpCloud, CyberArk, and others spanning enterprise, cloud, and specialized identity solutions.

The platform supports the [full spectrum of enterprise authentication protocols](#): SAML 2.0



(including Web Browser SSO Profile, Single Logout, Artifact Resolution, assertion encryption, and authentication request signing) and OpenID Connect (Authorization Code Flow, Hybrid Flow, Client Credentials, Dynamic Client Registration, session management, and front- and back-channel logout).

For SaaS companies whose enterprise customers use legacy or proprietary identity systems, SSOJet also supports custom SAML implementations through configurable metadata processing, as well as protocol translation for older identity management platforms.

An AI-Native Approach to Authentication Infrastructure

SSOJet distinguishes itself from traditional SSO vendors through its AI-native architecture. The platform includes an AI-powered implementation assistant that scans existing authentication frameworks to identify optimal integration points, generates framework-specific code tailored to a company's codebase, provides real-time troubleshooting during setup, and automatically creates customer-facing onboarding documentation.

The company has also built integrations optimized for modern AI development workflows. SSOJet's documentation is structured for AI code editors such as Cursor, Windsurf, and GitHub Copilot, enabling developers to implement enterprise SSO through natural language prompts rather than manual documentation parsing. An open-source LLM integration guide and agent-ready skill repository allow AI coding assistants to implement SSOJet authentication correctly and securely across multiple environments.

Additionally, SSOJet supports the Model Context Protocol (MCP), the open standard for connecting AI agents to enterprise tools. As AI agent deployments move into production, the authentication layer between agents and enterprise identity providers becomes critical infrastructure. SSOJet's MCP authentication support enables B2B SaaS companies to extend their SSO infrastructure to AI agent connections—ensuring enterprise identity providers maintain visibility and policy control over automated access.

A Different Model for a Different Market

The enterprise SSO market includes established players such as Auth0 (Okta), WorkOS and Stytych (Twilio), each with their own approach to B2B authentication. Most of these platforms operate as full authentication systems—requiring companies to adopt a new auth stack or commit to a per-user pricing model that scales with customer growth.

SSOJet's model diverges in two key ways. First, the platform is designed exclusively as an enterprise SSO layer rather than a full identity replacement. Companies keep their existing authentication solution intact and add SSOJet specifically for enterprise SSO capabilities. This means there is no user migration, no database transfer, and no disruption to current login workflows.

Second, SSOJet uses connection-based pricing rather than per-user fees. Each SSO connection

represents a link to one enterprise customer's identity provider. The company's Business plan starts at \$99 per month for two SSO connections with unlimited users per connection. This pricing structure means costs remain predictable as enterprise customers scale their user base—a meaningful distinction for B2B SaaS companies whose enterprise clients may have thousands or tens of thousands of employees.

Built for Modern Engineering Teams

SSOJet provides native SDKs and quickstart guides across a broad range of frameworks and platforms: Next.js, React, Vue, Angular, Node.js, Go, .NET, Java Spring Boot, Python, PHP, Laravel, ASP.NET Core, iOS, and Android. The API-first architecture supports automated provisioning and deprovisioning through SCIM 2.0 directory sync with major providers including Okta, Microsoft Entra ID, OneLogin, JumpCloud, and CyberArk.

For enterprise customers' IT administrators, SSOJet provides a self-service admin portal with step-by-step configuration guides, diagnostic tools for troubleshooting, and sandbox testing environments to validate integrations before production deployment. The company also offers a downloadable IdP integration guide with setup instructions and templates for each supported identity provider.

Security and Compliance

The platform is built on a zero-knowledge architecture with enterprise-grade audit logging for every authentication event. SSOJet supports multi-factor authentication integration, role-based access control, just-in-time user provisioning, and conditional access policies. The company maintains compliance documentation for SOC 2, ISO 27001, GDPR, HIPAA, and CCPA requirements.

Availability

SSOJet's Enterprise SSO platform is available immediately. The company offers a 30-day free trial for B2B SaaS companies evaluating enterprise SSO requirements. More information, documentation, and integration guides are available at ssojet.com.

About SSOJet

SSOJet provides turnkey enterprise Single Sign-On infrastructure for B2B SaaS companies. The platform enables companies to add enterprise authentication capabilities—including SAML 2.0, OIDC, SCIM directory sync, and Model Context Protocol support—on top of their existing auth stack, without migration or replacement. SSOJet serves companies across the B2B SaaS ecosystem who sell to mid-market and enterprise customers with mandatory SSO requirements. The company is headquartered in San Francisco.

Product: <http://ssojet.com>

Documentation: <https://docs.ssojet.com/en/getting-started/>

Case Studies: <https://ssojet.com/case-studies/>

Community: <https://ssojet.com/community>

Media Team

SSOJet

media@ssojet.com

Visit us on social media:

[LinkedIn](#)

[Bluesky](#)

[YouTube](#)

[X](#)

[Other](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/897897942>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.