Simplify Atlassian Authentication with SAML SSO

Use Cases Features Why Us

Single Sign On SAML SSO for Atlassian Suite

Managing user authentication across multiple Atlassian apps shouldn't be a constant struggle. Yet, many organizations find themselves tangled in a web of passwords, manual user provisioning, and inconsistent access controls. Every new user added—or removed—brings a risk of security gaps.

The miniOrange SAML Single Sign-On (SSO) with SCIM solution simplifies this complexity by enabling secure, seamless access to Jira, Confluence, Bitbucket, and more. By integrating with your identity provider, it eliminates password fatigue and automates user provisioning. Whether your organization operates on Atlassian Cloud or Data Center, this solution delivers a streamlined login experience without compromising security.

34.5% of executives report that their organizations' accounting and financial data were targeted by cyber adversaries in the past year. [1]

Use Cases: Real-World Applications for Every Organization

Handling Multiple Departments with Different Login Systems

> In a global organization, employees, contractors, and partners may each use different IdPs to log in. Instead of creating separate configurations for each group, you can connect all IdPs at once. This way, everyone logs in securely and smoothly, without IT needing to manage them separately.

Automatically Directing Users to the Right Login Page

> When users try to sign in, the system can recognize their email domain (like @company.com or @partner.org) and automatically redirect them to the correct login page. This removes the confusion of "which login do I use?" and prevents unnecessary support requests.

Scaling User Access in High-Growth Environments

> As your team grows quickly, manually setting up accounts for every new hire or removing access when someone leaves becomes impossible to manage. Automated provisioning and deprovisioning ensure users get access instantly when they join and are removed immediately when they leave.

Regaining Access During Lockouts or Downtime

> If your single sign-on (SSO) system goes down or is misconfigured, it could lock everyone out. But with a secure backup login method for admins, you can still get in and fix the issue, keeping your teams up and running.

1. Source: Bennett, S. (2025, March 23). Single sign on Software Statistics 2025. LLCBuddy.

Protecting Confidential Projects with Role-Based Restrictions

> Some projects or documents, like executive plans or HR files, need to be accessed only by specific teams. SCIM can automatically sync user roles (like "HR" or "Finance") from your identity provider, ensuring only the right people see sensitive content.

SAML Single Sign-On + SCIM Key Features: Secure and Seamless Access

Signed SAML requests and encrypted responses	Protect sensitive data with end-to-end encryption and signed SAML assertions. Such measures secure communication between your IdP and Atlassian applications, safeguarding against data breaches.
IdP Certificate Rotation	Automatically update IdP certificates without downtime, ensuring continuous security and compliance. This feature eliminates manual certificate management and reduces the risk of service interruptions.
Single Logout (SLO)	Enable users to log out of all applications with a single click. Hence, you can reduce the risk of unauthorized access and enhance overall security across your ecosystem.
Custom login, logout, and error pages	Personalize the login experience to reflect your brand's identity. Custom pages create a seamless and professional user journey, enhancing trust and engagement.
SCIM User Provisioning	Automate user creation, updates, and deprovisioning based on IdP data. The feature reduces manual processes, reduces errors, and ensures your user base is always accurate and up-to-date.

Why Choose miniOrange: Advantages of Streamlined Access and Security

Seamless Access

Enable seamless logins across Atlassian apps, reducing authentication delays and keeping teams focused on work.

Reduce Admin Overload

Automate user provisioning and password management, freeing IT teams from repetitive administrative tasks.

Multiple Customization Options

Tailor authentication policies, role mappings, and security settings to fit your organization's unique requirements.

Trusted by Industry Leaders Worldwide

About Us

miniOrange's security experts are trusted by 25,000+ organizations across the world. Standing at the forefront of Atlassian security, we deliver Single Sign-On (SSO), Multi-Factor Authentication (MFA), and User Management solutions. Be it Data Center or Cloud, our apps secure Atlassian with seamless SAML and OAuth integration for ease of use and top-tier security.

www.miniorange.com

+91 97178 45845 (India) | +1 978 658 9387 (US) | info@xecurify.com