Effortless Jira Service Management Login with miniOrange SAML & OAuth SSO

☑ Use Cases ☑ Features ☑ Why Us

Secure and Simple Access to Jira Service Management

When customers, vendors, or partners reach out for support through Jira Service Management (JSM), the last thing you want is a compromised login putting your data at risk, or redundant spam ticket creation clogging your system. But with Atlassian's native SSO support, giving external users secure and seamless access usually means paying for high-end plans or sacrificing control. That's where miniOrange makes a difference.

Our SAML/OAuth SSO for JSM Customers solution allows users to authenticate via multiple IdPs, such as Entra ID, Keycloak, Okta, and more, without the need for Atlassian Guard or domain verification. Admins can also enable Multi-Factor Authentication and granular access controls easily, so every user gets a smooth, secure login experience tailored just for them.

Real-World Use Cases

OAuth-Based SSO for External Customers

> Atlassian natively supports only SAML for logging into JSM portals, which limits organizations that rely on OAuth or OIDC for authentication—such as Google, GitHub, or Entra ID (OIDC). miniOrange bridges this gap by enabling secure SSO with OAuth and OIDC-based IDPs. This helps prevent unauthorized access and spam ticket creation while eliminating the need for Atlassian Guard, significantly reducing licensing costs.

Use Multiple Identity Providers (IDPs)

> Large enterprises often collaborate with contractors, partners, or subsidiaries that use different IDPs. Atlassian supports only a single IDP configuration, which restricts operational flexibility. miniOrange removes this constraint by supporting multiple IDP configurations—whether SAML, OAuth, or OIDC-based. This allows organizations to unify external authentication under one system, without compromising on security.

Control Portal Access with IDP Groups

> By default, Atlassian doesn't allow fine-grained control over who can access specific portals after SSO based on their IDP groups or Jira organizations. With miniOrange, administrators can enforce portal access control by restricting it based on IDP groups or Jira organizations, ensuring users only see the support portals.

Automatically Assign Users to Jira Organizations

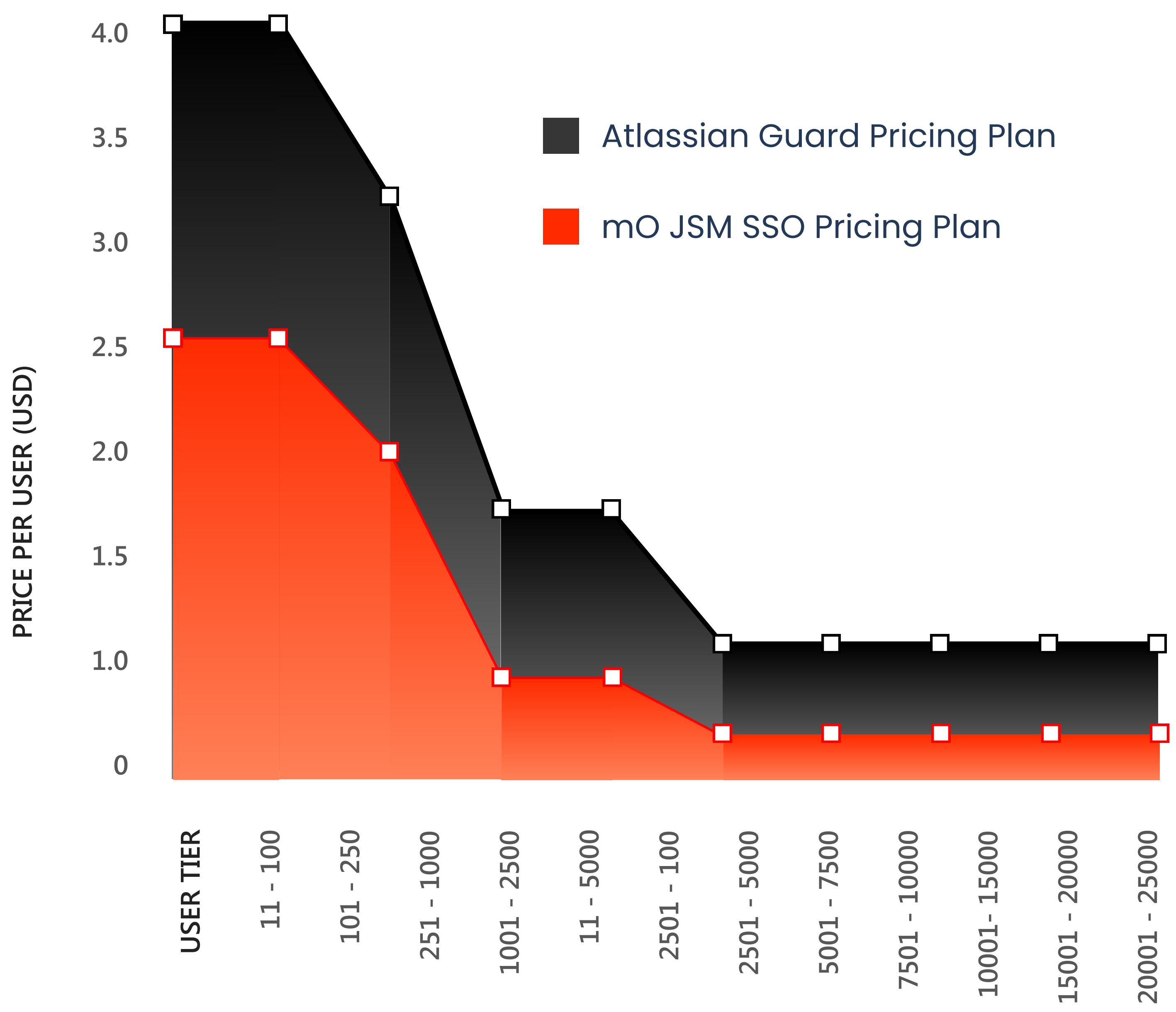
> Manually assigning users to Jira organizations can be tedious and prone to errors, especially for large teams with frequent onboarding or role changes. miniOrange automates this process by dynamically assigning users to organizations based on their email domain or IDP group. Assignments and removals happen in real time during login, ensuring users are always mapped correctly. You can bulk-import mappings via CSV or allow the solution to create new organizations on-the-fly based on incoming user data, streamlining administration and reducing overhead.

Choose Single Sign-On, Multi-Factor Authentication, or Both

Every organization has different security needs. Some prefer the simplicity of SSO, while others require an added layer of protection with MFA. With miniOrange's in-house MFA solution, you're in control. You can enable just SSO for quick access, only MFA for extra security, or combine both, asking users to log in with their IDP first and then verify with a second step. Unlike Atlassian Guard, miniOrange gives you the flexibility to secure your portal on your terms, without complicating the user experience.

Pricing Comparison mO JSM SSO vs Atlassian Guard

Avoid high licensing costs with Atlassian Guard. The graph below highlights how miniOrange offers a significantly lower price point for SSO in Jira Service Management. With in-house Multi-Factor Authentication, Multiple IdP Support, Portal Access Mapping, and Attribute Mapping, you get enterprise grade security without the enterprise-grade price.



Easy-to-Understand Feature Table

No Atlassian Guard Needed	Enable SSO, MFA, group-based access, and auto-organization mapping for external users—without needing Atlassian Guard or an Enterprise plan.
SAML & OAuth SSO Support	Enable Single Sign-On (SSO) for external users using trusted Identity Providers (IdPs) that support SAML or OAuth/OpenID Connect protocols—such as Google Workspace, Entra ID, GitHub, Okta, and more.
Multiple Identity Providers (IdPs)	Integrate and authenticate users from multiple IdPs simultaneously—perfect for organizations with distributed teams, subsidiaries, or external partners.
MFA Enforcement After SSO	Add an additional authentication layer post-SSO using methods like SMS/email OTP, or hardware tokens, even when the IdP itself does not support MFA.
Role-Based Portal Access Using IDP Groups	Restrict access to specific Jira Service Management portals or request types based on group membership retrieved from the connected IdP.
Automated Organization Assignment	Dynamically assign or remove users from Jira organizations during SSO based on their email domain or group attributes—eliminating manual intervention.

Bulk Organization Mapping via CSV	Configure multiple organization-to-IDP group or domain mappings at once by importing a structured CSV file—streamlining admin setup for large environments.
Dynamic Organization Provisioning	Automatically create new Jira organizations during login based on user attributes from the IdP when a corresponding organization does not already exist.

Why Choose miniOrange

Built for Flexibility

Use SAML or OAuth, connect multiple IDPs, and manage external users with ease, whatever your setup is.

Security Access

Implement strong authentication and precise access control to guard your support portals against unauthorized entry.

No Extra Cost or Lock-In

Enable SSO for your external customers using multiple Identity Providers—without needing an Atlassian Guard subscription or Enterprise plan, thereby saving costs.

Trusted by Industry Leaders Worldwide

BAJAJ Allianz | ARCADIA | CTM CONSORCITRANSPORTSMALLORCA | TRAX GROUP | MRAS

illum | XOPS | Qarbon Technologies | Smarkia | WebBank

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