ATLASSIAN | Gold Marketplace Partner

miniOrange

Securing and Streamlining the Atlassian Ecosystem with miniOrange

Secure | Simplify | Scale

Author: Akshay Kedari & Aditya Kekre

Table Of Contents

Executive Summary

miniOrange provides cutting-edge security and user management solutions for the Atlassian ecosystem, addressing identity security vulnerabilities and streamlining user access. This whitepaper highlights how miniOrange's suite of security and automation apps helps businesses enhance security, simplify authentication, and optimize user workflows across Jira, Confluence, and other Atlassian applications.

Introduction

Organizations worldwide rely on Atlassian products like Jira, Confluence, and Bitbucket to manage projects and collaborate efficiently. However, managing access security and user provisioning across multiple platforms can be complex and prone to security risks.

Problem Statement

Security Gaps : Weak authentication and external integrations pose threats to Atlassian environments.

User Management Overhead : Manual user provisioning and de-provisioning lead to inefficiencies and compliance issues.

Access Control Challenges : Lack of streamlined governance results in unmonitored resource access and security risks.

License Overhead : Overpaying for inactive users or outdated accounts leading to huge license costs.

Purpose and Scope

This whitepaper explores how miniOrange's security and convenience-focused solutions empower businesses to secure their Atlassian ecosystem while streamlining processes for better efficiency and cost savings.

Challenges In Atlassian Security & Workflow Management

As businesses scale their use of Atlassian tools like Jira, Confluence, and Bitbucket, they face growing challenges in securing access, managing users, and ensuring governance due to authentication gaps and external collaboration risks.

Authentication Risks: Weak Authentication and Credential Management

Without a centralized authentication mechanism, organizations often rely on multiple, disjointed login credentials for different Atlassian applications. This increases security risks such as:

Password fatigue : Employees struggle to remember multiple credentials, leading to the reuse of weak passwords.

Phishing and brute-force attacks : Without robust authentication layers like Multi-Factor Authentication (MFA), user credentials are susceptible to attacks.

Session hijacking and unauthorized access : Attackers can exploit open sessions and insufficient session management controls.

Why it matters: Organizations need a secure, seamless authentication mechanism like Single Sign-On (SSO) and MFA to reduce the risk of credential theft and unauthorized access.

User Access Management: Inefficient Onboarding, Offboarding & Permissions Handling

Manually managing users across Atlassian tools results in administrative **inefficiencies and security loopholes:**

IT administrators spend **excessive time manually provisioning and de-provisioning users,** leading to onboarding delays.

Orphaned accounts (inactive users still having access) increase the risk of insider threats.

Lack of **automated role-based access control (RBAC)** results in employees gaining incorrect permissions, leading to **privilege escalation attacks.**

Why it matters: Organizations need automated provisioning and de-provisioning to maintain a secure, up-to-date user directory across all Atlassian applications.

External Sharing Risks: Unsecure Collaboration with External Users

Atlassian applications play a crucial role in interdepartmental and external collaboration. However, without secure access control mechanisms, organizations face:

Data leaks: Sensitive Jira issues and Confluence pages may be inadvertently exposed to unauthorized users.

Unmonitored external user access: Granting long-term access to external contractors increases security risks.

Compliance violations: Industries subject to GDPR, HIPAA, or SOC 2 require controlled external data sharing.

Why it matters: Businesses require secure external collaboration tools that allow controlled access with expiration dates and audit trails.

Compliance & Governance Issues: Poor Access Controls & Auditability

Security compliance mandates require organizations to maintain a transparent access control and governance framework. However, businesses struggle with:

Lack of visibility into user access history

Inability to enforce periodic access reviews

Weak approval workflows for application access requests

Why it matters: Organizations need a centralized governance model to enforce compliance, track access requests, and automate audit trails across Atlassian tools.

Proposed Solutions: miniOrange Apps for Security & Convenience

miniOrange addresses these challenges with a suite of security and workflow automation solutions tailored for the Atlassian ecosystem. These apps enhance identity security, streamline user management, and provide centralized governance.

Security-Focused Apps : Strengthening Atlassian Security

Single Sign-On (SSO) (SAML, OAuth) for Atlassian Applications

Enables seamless authentication across Jira, Confluence, Bitbucket, Crowd, Bamboo, and Fisheye.

Supports 20+ identity providers (IDPs), including Okta, Microsoft Entra ID (Azure AD), Google Workspace, ADFS, and many more.

Reduces password-related risks by allowing users to log in once and access all Atlassian applications securely.

Key Benefits : Reduced password fatigue, enhanced security, and improved user experience.

Multi-Factor Authentication (MFA) for Atlassian

Enforces an additional layer of security using OTP, push notifications, and hardware-based authentication.

Supports adaptive MFA policies (e.g., requiring MFA only for specific roles, devices, or locations).

Ensures only verified users access sensitive data in Jira, Confluence, Bitbucket, Bamboo, and Crowd.

Key Benefits : Eliminates password-based vulnerabilities, prevents unauthorized access, and enhances compliance.

Enhanced API Authentication

Protects REST API and external integrations by enforcing secure authentication mechanisms like API tokens, OAuth, and JWT.

Controls API access with granular permissions to prevent unauthorized data exposure.

Key Benefits : Strengthened API security, reduced risk of unauthorized integrations, and controlled data flow.

Enhanced SSO & MFA for JSM Customers

Enables secure authentication for Jira Service Management (JSM) customers using their existing enterprise identity providers (IdPs).

Ensures seamless MFA integration, enforcing strong authentication for support portals.

Key Benefits : Strengthened customer authentication security, improved user experience, and compliance with security mandates.

Convenience-Focused Apps: Streamlining Atlassian Workflows

Automated User Management

Bulk user actions: Automates deactivation, activation, and deletion of Atlassian users.

Syncs users, groups, and attributes between Atlassian and identity directories (LDAP, AD, SCIM, etc.).

Key Benefits : Saves IT time, prevents security gaps from inactive users, and ensures up-to-date user records.

SCIM Provisioning for Atlassian

Automates user provisioning & de-provisioning for Atlassian Cloud & Data Center.

Ensures real-time updates when employees join, leave, or change roles.

Key Benefits : Reduces manual provisioning efforts, improves compliance, and enhances security.

Active Directory (AD) Integration for Atlassian Cloud

Bridges Active Directory with Atlassian Cloud, enabling seamless SSO login for AD users.

Provides real-time user synchronization with Azure AD and other LDAP-based directories.

Key Benefits : Simplifies authentication for AD users, enhances security, and improves user management efficiency.

Secure Share for Jira & Confluence

Allows organizations to securely share Jira issues & Confluence pages externally.

Features include password protection, expirable links, and controlled permissions.

Key Benefits : Enables secure collaboration with vendors/clients without extra licensing costs.

Application Access & Governance Workflow for Atlassian DC

Enables role-based access requests through Jira Service Management (JSM).

Allows admins to review and approve access requests before granting permissions.

Key Benefits : Reduces unauthorized access, enhances compliance, and centralizes access governance.

Implementation & Use Cases

A leading global insurance and financial services company needed to improve authentication security for its Atlassian applications while maintaining a seamless user experience. Their challenge included :

Use Case: Securing Jira & Confluence Authentication with SSO & MFA

The Challenge: Enhancing Security with SSO & MFA for Internal and External Users

A leading global insurance and financial services company needed to improve authentication security for its Atlassian applications while maintaining a seamless user experience. Their challenge included :

Managing authentication for different user types internal employees and external partners while maintaining security.

Implementing Single Sign-On (SSO) for internal users to delegate authentication to an Identity Provider (IdP).

Enforcing Multi-Factor Authentication (MFA) for external users who log in with application credentials.

Eliminating usability issues where internal users were required to complete 2FA twice—once via the IdP and again within Atlassian applications.

The Solution: Implementing miniOrange's Crowd SAML SSO & MFA

To address these security and usability concerns, miniOrange implemented:

Crowd SAML SSO

Functions as a SAML Service Provider, connecting Atlassian applications to the company's Identity and Access Management (IAM) system.

Enables SSO login across Jira and Confluence, ensuring seamless authentication for internal users.

Retains existing user permissions and group structures while providing centralized access control.

SSO Connectors for Jira & Confluence

Extends SAML authentication to individual Atlassian applications, enabling secure login without separate credentials.

Jira Two-Factor Authentication (2FA) Add-on

Enforces MFA for external users, who authenticate using application credentials.

Bypasses MFA for internal users already authenticated via SSO, preventing duplicate authentication requests.

How It Works

Internal Users (SSO via IdP)

Employees authenticate via SSO, with authentication handled by the company's IAM system.

2FA is enforced at the IdP level, allowing internal users to bypass additional 2FA prompts in Jira and Confluence.

External Users (Atlassian Login + 2FA)

External partners log in directly to Atlassian applications using their credentials.

miniOrange's 2FA add-on applies an additional authentication layer, strengthening security for non-SSO users.

Key Benefits

Centralized Access Control

Authentication is managed via Crowd SAML SSO, integrating Atlassian applications with the organization's Identity Provider (IdP) while maintaining role-based access control.

Improved User Experience

Internal users experience a seamless login process without repeated MFA prompts.

Strong Security & Compliance

Selective MFA enforcement—required for external users but skipped for internal users already secured by the IdP.

SAML-based authentication ensures compliance with security policies and regulatory requirements.

Scalability & Future-Readiness

The solution easily scales, allowing the organization to integrate additional applications without managing multiple login credentials.

Conclusion

By integrating Crowd SAML SSO and 2FA, the company achieved a secure and streamlined authentication process across Jira and Confluence. Internal users now enjoy seamless, passwordless access, while external users benefit from enhanced security through enforced multi-factor authentication. Additionally, the solution simplified user management, reducing administrative overhead while ensuring compliance with security regulations.

This use case demonstrates how miniOrange enables enterprises to strike the perfect balance between security, usability, and operational efficiency in complex authentication environments.

Use Case: Automating User and Group Management with SCIM Provisioning

The Challenge: Enhancing Security with SSO & MFA for Internal and External Users

A leading telecommunications provider needed to streamline user and group management within Jira. As a company operating at scale, they faced challenges in :

Manually provisioning and deprovisioning users, leading to administrative inefficiencies.

Synchronizing users and groups across Microsoft Entra ID (formerly Azure AD) and Jira.

Ensuring compatibility with Atlassian's SSO, so authentication and authorization remained centralized.

Managing license costs effectively by automating user deactivation based on account status.

With thousands of employees and dynamic role changes, the company needed a scalable, automated solution to handle user provisioning, deprovisioning, and permission management efficiently.

The Solution: Implementing miniOrange SCIM User & Group Provisioning.

To address these challenges, miniOrange deployed its Jira SCIM User and Group Management App, which:

Established a SCIM connection between Microsoft Entra ID and Jira

Enabled real-time user and group synchronization, ensuring that all user updates in Microsoft Entra ID were reflected in Jira.

Automated provisioning of new employees and deprovisioning of departed employees, maintaining an up-to-date user directory.

Seamlessly Integrated with Atlassian's SSO

Ensured that authentication and authorization were centrally managed via the organization's existing identity provider (IdP).

Allowed users to log in seamlessly while ensuring that their access was controlled based on their group memberships.

Reduced Administrative Overhead

Enabled automatic, manual, and login-triggered syncs, providing flexibility in user management.

Eliminated the need for IT administrators to manually update user roles and permissions, saving significant time and effort.

Optimized License Cost Management

Automatically revoked access for deactivated users in Microsoft Entra ID, preventing unnecessary Jira license consumption.

Ensured that only active employees had Jira access, optimizing licensing costs and reducing waste.

How It Works

SCIM Connection Setup

miniOrange's SCIM provisioning app establishes a secure connection between Microsoft Entra ID and Jira.

User & Group Synchronization

The app automatically syncs users, roles, and group memberships, reflecting any changes from Microsoft Entra ID in Jira.

Seamless Authentication & Authorization

Users log in via SSO, and their permissions are dynamically assigned based on their groups in Microsoft Entra ID.

License Optimization & Deprovisioning

If a user is disabled or removed from Microsoft Entra ID, the SCIM integration automatically revokes their Jira access, preventing inactive accounts from consuming licenses.

Key Benefits

Automated User and Group Management

Eliminates manual user provisioning, ensuring efficient and accurate user updates in Jira.

Reduced Administrative Burden & Improved Accuracy

Saves IT teams significant time by automating user updates and access management.

Optimized License Costs

Automatically deactivates inactive users, reducing unnecessary Jira license consumption.

Seamless Integration with Atlassian SSO

Ensures authentication and authorization are centrally managed, enhancing security and user experience.

Conclusion

By integrating SCIM provisioning with Microsoft Entra ID and Atlassian SSO, the company achieved seamless user management, reduced administrative overhead, and optimized license costs. This solution ensured that only active users had access, preventing security risks associated with orphaned accounts while simplifying IT operations.

Use Case: Automating External Customer Authentication & Access Management in JSM

The Challenge: Streamlining External Customer Authentication & Portal Access

A global insurance provider needed to enhance authentication and access control for external customers accessing their Jira Service Management (JSM) portals. Their key challenges included:

Ensuring seamless Single Sign-On (SSO) for external customers using Microsoft Entra ID (formerly Azure AD).

Automatically mapping customers to JSM organizations upon login, eliminating manual admin tasks.

Restricting portal access based on an organization's permissions to ensure data security.

Reducing administrative workload associated with manually adding, managing, and removing customers from JSM organizations.

With **hundreds of JSM portals and numerous external customers,** automating authentication and access management was critical for improving security, efficiency, and user experience.

The Solution: Implementing miniOrange's SAML/OAuth SSO for JSM Customers

To address these challenges, miniOrange provided a comprehensive authentication and access management solution that included:

Enforcing SSO for JSM Customer Portals

Implemented SAML/OAuth SSO for JSM Customers, allowing external users to authenticate via Microsoft Entra ID before accessing JSM portals.

Ensured seamless, passwordless authentication while maintaining strong security protocols.

Automated Organization Mapping

Introduced the Organization Mapping feature, enabling automatic customer-to-organization assignments based on the user's domain or IDP group.

Eliminated the need for administrators to manually add or remove customers from JSM organizations.

Portal Access Management via Organization & IDP Groups

Enabled Portal Access Mapping, allowing admins to link portals to JSM organizations and IDP groups.

Ensured that only authorized customers could access designated JSM portals, preventing unauthorized access to sensitive data.

How It Works

User Authentication via SSO

Customers access JSM using a substitute link provided by miniOrange.

Users are redirected to the Microsoft Entra ID login page for authentication.

Automatic Organization Mapping

Upon successful authentication, miniOrange receives user attributes like domain and IDP groups.

The system automatically assigns or removes users from JSM organizations based on pre-configured mappings.

Controlled Portal Access

The Portal Access Mapping service checks the user’s organization and IDP group.

The system grants or denies access to specific JSM portals based on predefined access rules.

Key Benefits

Seamless Customer Authentication

Enabled secure, hassle-free login for external customers via Microsoft Entra ID.

Automated User & Organization Management

Eliminated manual tasks by automating customer-to-organization mapping based on domain or IDP groups.

Enhanced Access Control & Security

Ensured that only authorized customers could access specific portals, improving data protection and compliance.

Reduced Administrative Burden

Saved IT teams significant time and effort by automating customer onboarding and access management.

Improved User Experience

Streamlined the ticket creation process, making support interactions faster and more efficient.

Conclusion

By integrating SAML/OAuth SSO for JSM Customers, the company successfully:

Automated customer authentication & organization mapping, eliminating manual user management.

Enhanced security by ensuring only authorized customers accessed JSM portals.

Streamlined IT operations, reducing administrative overhead and improving service efficiency.

Use Case: Secure External Content Sharing in Atlassian Without Additional Licenses

The Challenge: Reducing Licensing Costs While Maintaining Secure Access

A university migrating to Atlassian Cloud faced a significant challenge:

High licensing costs – Moving to the Atlassian Cloud required converting all users into paid licenses, significantly increasing expenses.

Limited content access requirements – Many users only needed read-only access, making full licenses unnecessary.

Security & access control concerns – The university could not enable anonymous access due to sensitive information being stored in Confluence.

Granular access restrictions – Users from different departments (e.g., HR, Finance) needed access only to relevant pages, controlled via Active Directory (AD) groups.

Password fatigue – The university wanted to avoid requiring users to manage yet another set of login credentials.

With **hundreds of JSM portals and numerous external customers,** automating authentication and access management was critical for improving security, efficiency, and user experience.

The Solution: Implementing miniOrange's Secure Share for Confluence

To address these concerns, miniOrange implemented Secure Share for Confluence, enabling:

Single Sign-On (SSO) for Shared Links

Enforced SSO authentication on shared Confluence links, allowing users to log in with their existing credentials instead of creating new ones.

Granular Access Control via IDP Groups

Implemented IDP Group-based Authorization, allowing link creators to restrict page access based on Active Directory (AD) groups.

Ensured that

1. HR team members could only access HR pages
2. Finance members could only access Finance pages

Secure External Sharing Without Extra Licenses

Allowed users to share Confluence pages externally without requiring additional Atlassian licenses.

Prevented unauthorized access by requiring SSO authentication before viewing shared content.

How It Works

Admin Enables Secure Share

Administrators configure SSO enforcement and IDP-based access control within the Secure Share settings.

User Creates a Secure Link

Users generate a shareable Confluence link with restricted access based on IDP groups.

Access is Verified via SSO & IDP Groups

When a recipient accesses the link:

1. They are redirected to their Identity Provider (IdP) for authentication.
2. Their AD group membership is checked to confirm authorization.
3. Only authorized users are granted access.

Key Benefits

Significant Cost Savings

Eliminated the need for additional paid Atlassian licenses by enabling secure external content sharing.

Seamless User Experience with SSO

Allowed users to access shared content using their existing credentials, reducing password fatigue.

Granular Access Control & Compliance

Ensured that only authorized users from specific IDP groups could access sensitive content.

Prevented unauthorized access to confidential HR, Finance, and administrative documents.

Enhanced Security for Shared Content

Enforced SSO authentication on shared links to prevent unauthorized access.

Conclusion

By implementing Secure Share for Confluence, the university successfully:

Reduced licensing costs by enabling external content sharing without requiring additional Atlassian licenses.

Enhanced security by ensuring only authenticated users could access shared content.

Improved user experience by enabling SSO-based access control and removing the need for additional passwords.

Conclusion

miniOrange empowers organizations to secure, automate, and optimize their Atlassian ecosystem with best-in-class security and workflow management apps. Try miniOrange today to enhance security and efficiency in your Atlassian environment.

Contact Information

Author: miniOrange

Email: info@xecurify.com | aditya.kekre@xecurify.com

Website: www.miniorange.com/atlassian

This whitepaper provides a comprehensive overview of how miniOrange enhances the security and efficiency of the Atlassian ecosystem. By implementing miniOrange's security-focused and workflow-automation applications, businesses can mitigate security risks, simplify authentication, and streamline user management across Jira, Confluence, and other Atlassian products.