Enhancing Atlassian Data Center Security with Two-Factor Authentication

☑ Use Cases ☑ Features ☑ Why Us

Two-Factor Authentication

Atlassian tools often contain sensitive business data, proprietary project information, and internal communications. As teams increasingly adopt remote and hybrid work models, the risk of unauthorized access to critical systems continues to grow. Weak or stolen credentials have become a leading cause of data breaches. To address this challenge, miniOrange offers a dedicated Two-Factor Authentication (2FA) for the Atlassian suite. This solution is designed to improve access security through an additional verification step, ensuring that only authorized users can access your systems.

99.9% Microsoft states that Multi-Factor Authentication can prevent over 99.9 percent of account compromise attempts.

Use Cases: How the Plugin Adds Value

Blocking Automated Intrusion Attempts

Brute force attacks are a common tactic used by hackers to guess passwords through automated scripts. The Two Factor Authentication (2FA) for Atlassian Suite detects repeated failed login attempts and temporarily blocks suspicious activity. It offers an automatic layer of defense, reducing the need for manual oversight during high-risk events.

Location-Based Access Control

Not every login attempt should be treated equally. The plugin's IP Whitelisting and Blocking feature allows administrators to allow or deny access based on geographic or network-specific criteria.
Users working from trusted environments can be allowed in, while unrecognized access points are blocked by default.

Role-Based Security Enforcement

Not all users in your organization face the same level of risk. With the ability to enable 2FA individually or based on groups, IT teams can apply stricter controls to users handling sensitive data or administrative tasks.
Security is applied where it's needed most, without causing unnecessary friction for other users.

Custom Authentication Per Department

Different departments may have different workflows and risk profiles. With the ability to restrict 2FA methods to specific groups, teams can use authentication methods that work best for them—whether it's hardware tokens, biometrics, or app-based verification.
It provides customization without compromising overall security.

Seamless Experience for SSO Users

> For organizations using a native Crowd connection for authentication through the common login page, the plugin allows administrators to bypass 2FA for trusted SSO-based logins.
> This avoids redundant authentication steps, improving the login experience for verified users.

Delegated Access for Department Leads

> Large organizations often need to distribute some administrative control. With group-based access for non-admins, team leads can manage 2FA settings for their own groups without having global admin rights.
> It balances control and efficiency, allowing scale without compromising governance.

Key Features of the Plugin

Brute Force Protection	Automatically blocks repeated failed login attempts, helping prevent credential-stuffing and other automated attacks.
Multiple Authentication Methods	Supports a wide range of authentication options, including TOTP-based apps (such as Google Authenticator, Microsoft Authenticator, Authy, and others), OTP via SMS or email, Yubikey hardware tokens, WebAuthn (FIDO2), Duo Push notifications, security questions (KBA), and backup codes.
2FA as a Choice	Let users enable 2FA voluntarily for added personal account security.
Device Remembering	Users can mark trusted devices to avoid repeated 2FA prompts, enhancing usability without compromising security.
IP Whitelisting and Blocking	Control access based on IP addresses to ensure only approved networks can access your Atlassian environment.
Backup Options	Allows users to configure multiple methods and use them as backups during emergencies.
Customizable Interface	Organizations can modify the look and feel of end-user login pages to align with their brand or user experience guidelines.
Authentication and Configuration Logging	The plugin provides detailed audit logs that track both user and administrator activities related to authentication.
Multilingual Support	End-user interfaces are available in multiple languages to accommodate global teams.

Why Choose miniOrange

Flexible and Granular Control Over Security

Apply 2FA settings specified to different users and groups, customize authentication methods, and manage access precisely as your organization requires.

Reliable Support and Enterprise-Ready Features

From multilingual support to audit logs and delegated admin access, miniOrange offers the depth and stability needed for large teams.

Fast, Responsive Assistance When You Need It

Our support team helps with setup, troubleshooting, and customization—so your team can stay secure without delays.

Recognized for Innovation & Excellence

> Your customer support is excellent. The app updates are also quick, making the app more robust. I am satisfied with the features and am using it. Thank you.

Hyojun Choi

> Lots of configuration options such as ip whitelisting or ip blocking lists. It is doing what is supposed to do, good job. We are using it for Crowd/Jira/Confluence.

Sylvain Leduc

Trusted by Industry Leaders Worldwide

YES BANK | البنك العربي ARAB BANK | Peraton | comet | CGI

Informations Technik Zentrum Bund | sopra hr SOFTWARE | NetBrain | verizon wireless | Allianz Technology

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