Enhanced REST API Authentication

☑ Features ☑ Use Cases ☑ Advantages

REST API - Secure API Authentication for Jira: OAuth, JWT & API Keys

miniOrange's Enhanced API Authentication for Atlassian DC and Cloud with API Key/OAuth/JWT allows admins to securely integrate their Atlassian apps with external services using OAuth 2.0, JWT, and API tokens. This eliminates the need for passwords and significantly reduces security risks. The plugin ensures that your Jira, Confluence, and Bitbucket instances remain secure while enabling seamless integration with external services.

Using **the REST API plugin**, short-lived tokens can reduce the attack window by up to

80% significantly decreasing the risk of token replay attacks and un-authorized access.

Powerful Features to Simplify and Secure Your Atlassian Ecosystem

Integrated Client Credential Grant

Enables secure app-to-app communication without requiring user credentials.

Ideal for automating workflows between Atlassian apps and external services like CI/CD tools or monitoring systems.

JWT (JSON Web Token) Support

Uses digitally signed tokens to verify the authenticity of API requests, ensuring only trusted sources can access your data.

Simplifies integration with third-party systems that rely on JWT for authentication.

Enhanced OAuth Integration with PKCE Support

Protects against unauthorized access by adding an extra layer of security to OAuth 2.0 authentication.

Ensures secure communication between Atlassian suite and external apps.

User-Specific API Tokens

Allows individual users to generate their API tokens for personalized access to Atlassian apps.

Reduces risk by ensuring tokens are tied to specific users and can be revoked easily if needed.

IP-Based Restrictions

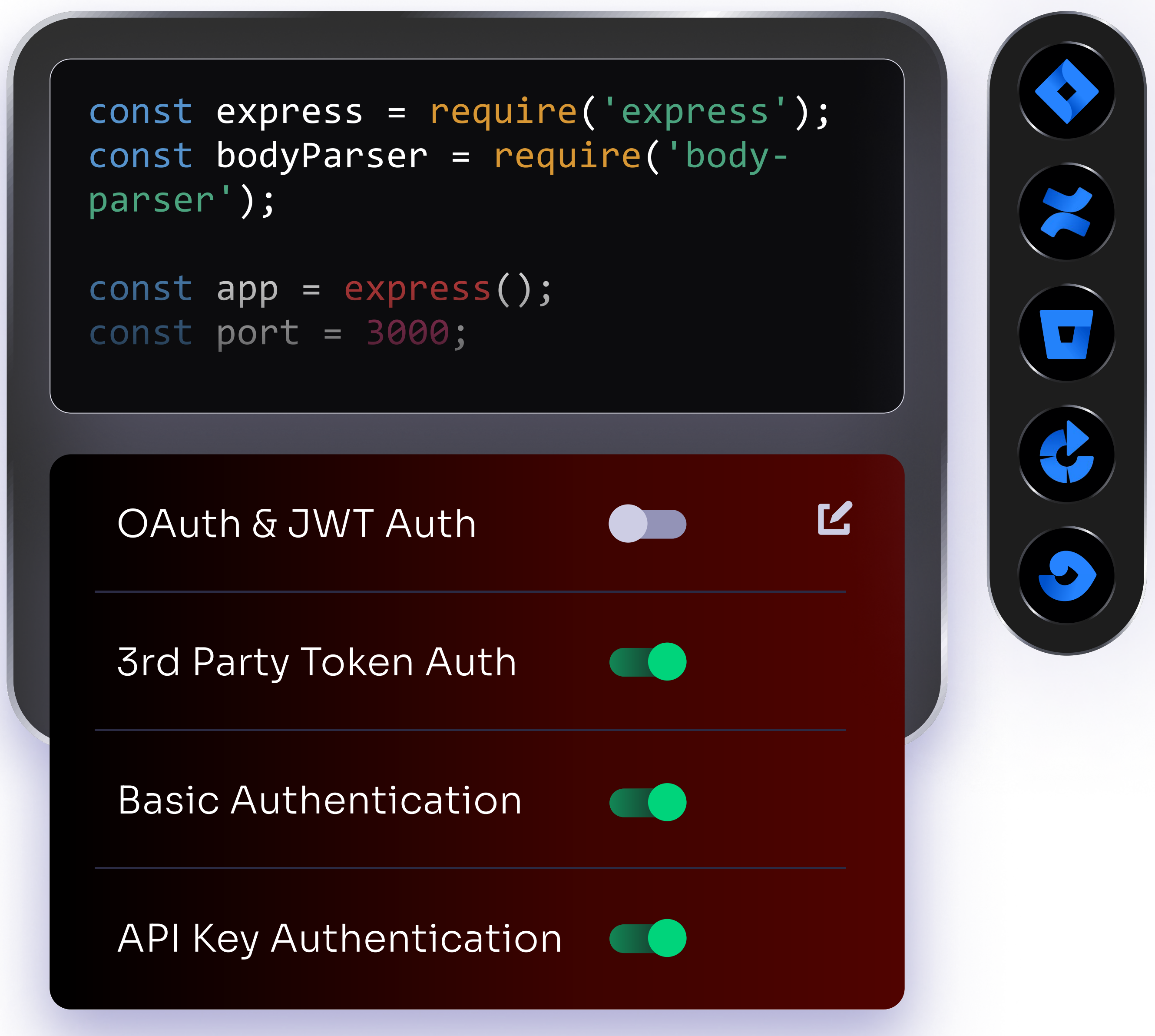
Limits API access to specific IP addresses or ranges, ensuring only trusted networks can interact with your Atlassian apps.

Adds an extra layer of protection against unauthorized access from unknown locations.

Group-Based Restrictions

Controls API access based on user groups, ensuring only authorized teams or departments can perform specific actions.

Simplifies permission management by aligning API access with existing group structures.



```
const express = require('express');
const bodyParser = require('body-
parser');

const app = express();
const port = 3000;
```

OAuth & JWT Auth ○

3rd Party Token Auth ●

Basic Authentication ●

API Key Authentication ●

Enhanced API Authentication

Authenticate third-party APIs with secure OAuth tokens, and JWT authentication to gain granular access control to your Atlassian environment.

Token Rate Limiting

Prevents API overload by limiting the number of requests a single token can make within a specific time frame.

Ensures fair usage and protects your Jira instance from being overwhelmed by excessive API calls.

Read-Only Access

Allows you to grant read-only access to specific tokens, preventing unauthorized modifications to your data.

Ideal for sharing data with external partners or tools without risking accidental or malicious changes.

User-Specific API Tokens

Allows individual users to generate their own API tokens for personalized access to Jira.

Reduces risk by ensuring tokens are tied to specific users and can be revoked easily if needed.

Audit Logging

Tracks all API activity, providing a detailed record of who accessed what and when.

Helps with compliance audits and identifying suspicious behaviour in real-time.

On-Demand Feature Support

Offers customizable solutions to meet unique organizational needs, ensuring the plugin adapts to your workflows.

Provides dedicated support to help you configure and optimize the plugin for your specific use cases.

IP-Based Restrictions

Limits API access to specific IP addresses or ranges, ensuring only trusted networks can interact with your Jira instance.

Adds an extra layer of protection against unauthorized access from unknown locations.

Solving Real Challenges: Use Cases for Secure Integrations

Secure Integration with External Applications

- Allow external applications to interact with Atlassian products securely without exposing user credentials.
- Use Authorization Grant, Client Credentials Grant, or JWT methods to authenticate external applications.

Enforce IP-Based Access Restrictions

- Restrict REST API access to specific IP addresses or ranges to enhance security.
- Reduce potential attack vectors by allowing only trusted networks to access APIs.

Implement Group-Based Access Control

- Limit REST API access based on user groups to ensure only authorized personnel can perform specific actions.
- Enable fine-grained control over API endpoints.

Integrate with Third-Party OAuth/OIDC Providers

- Authenticate REST API requests using tokens issued by external providers like Azure AD, Okta, or Keycloak.
- Simplify integration with external identity providers.

Monitor and Audit API Usage

- Track and analyze REST API usage to detect anomalies and ensure compliance.
- Use detailed logs for security reviews and audits.

Why Choose miniOrange?

The Advantages of Enhanced API Authentication

Precise Access Control

- Granular resource accessibility ensures sensitive data is protected from unauthorized access.

Effortless Integration

- Seamlessly connect external services to Jira, Confluence, and Bitbucket while maintaining strict security standards.

Centralized Authentication

- Simplify authentication management across your Atlassian ecosystem and third-party applications.

Recognized for Innovation & Excellence

Trusted by Industry Leaders Worldwide

JPMorganChase

T Mobile

Radisys

STARBUCKS

GRDF GAZ RÉSEAU DISTRIBUTION FRANCE

bpifrance

BNY MELLON

sopra hr SOFTWARE

SIEMENS energy

IBM

About Us

miniOrange is a cybersecurity company offering advanced security solutions for workforce and customer identities, backed by 24/7 global support. We serve over 25000 businesses with IAM, CIAM, PAM, CASB, MDM, and DLP solutions, featuring 6000+ pre-built app integrations. Our tailored solutions are available on leading marketplaces, including Atlassian, WordPress, Shopify, Drupal, and BigCommerce.

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

www.miniorange.com