Security & Access Audits – Clovity AI Copilot for Jira

Conversational Security Audits

Run access and permission audits across Jira Cloud using a chat-first interface.

Natural Language Queries

Ask questions like:

- “Who has admin access in Project Alpha?”
- “Which users haven’t logged in for 90 days?”

Inactive User Detection

Automatically flags inactive accounts that still retain project or group permissions.

Project Role Insights

Provides a breakdown of user-to-role assignments within each Jira project.

Risk Alerts

Highlights excessive, overlapping, or misaligned permissions that may pose security risks.

Save & Share Audit Results

Download chat transcripts and audit findings as professional PDF reports.

Quick Access to Other Clovity Apps & Support

Use the in-app links to explore other Clovity Atlassian apps or contact support directly.

Installation

Step 1 – Open the App

- Navigate to the Atlassian Marketplace.
- Search for Clovity AI Copilot for Jira – Security & Access Audits.
- Click Install and grant the required permissions:
  - read:jira-work – Access project and issue metadata.
  - read:jira-user – Access user and group details.
  - manage:jira-configuration – Read project role mappings.
  - storage:app – Store audit history.

Step 2 – Launch in Jira

- Once installed, the app appears in Jira under Apps → AI Copilot – Security & Access Audits.

Getting Started with AI Copilot

First-Time Setup:

When you launch the app for the first time, the following happens:

- The **“Run Audit”** button will appear.

Clicking this will initiate the first-time scan of your Jira Cloud instance. The app will:

- Fetch all users, groups, and project roles.
- Flag inactive accounts with permissions.
- Build a baseline for access analysis.

Once the initial scan is complete:

- The Rescan and Analyze options become active for ongoing use.
- The interface also displays “Last Scanned: [Date/Time]” so you always know when the data was last refreshed.

Demonstrating Core Features

Conversational Queries

Ask natural language questions in the chat box. The assistant responds with direct answers and follow-up suggestions.

Risk Alerts

Examples include:

- Inactive users with elevated permissions.
- Users with both Admin and Developer roles.
- Groups with excessive project-wide access.

Audit History

- The interface shows “Last Scanned: [Date/Time]”.
- You can trigger Rescan anytime to refresh data.

Export Reports

After each audit or chat session:

- Click Download PDF.
- Generates a professional report including:
  - Audit summary.
  - Chat transcript with Q&A.
  - Risk alerts and recommendations.

Ideal for: Security reviews, compliance reporting, or sharing with IT leadership.

Best Practices

- **Run scans monthly** to ensure data freshness.
- **Check alerts first** to quickly mitigate security risks.
- **Export chat reports** for quarterly compliance reviews.
- **Restrict app access** to Jira admins for maximum security.

Troubleshooting

- **No Projects Found** → Ensure projects are active and not archived.
- **Audit Failed** → Retry or run during off-peak hours if your instance is large.

- **Missing Users** → Confirm admin-level permissions.
- **Chat Error** → Check internet connection or app configuration.

Support & Contact

- **Email:** support@clovity.com
- **Website:** https://clovity.com/contact
- **Documentation:** Atlassian Marketplace listing page