Bulk Clone Professional for Jira

Security Overview - Encryption, Logging, Data Transmission & Residency

Bulk Clone Professional for Jira is a Forge app that runs entirely on Atlassian's cloud infrastructure. This means the app inherits Atlassian's platform-level security controls. The following summarizes how encryption at rest, logging, data in transit, and data residency are handled.

1. Encryption at Rest

All data the app stores (e.g. clone logs, templates, and presets) is held in Forge hosted storage and encrypted at rest using **AES-256**, applied automatically under Atlassian's cloud encryption policies and backed by AWS KMS. Backups are encrypted to the same standard.

Encryption keys are Atlassian-managed by default and held in secure key-management systems with strict access controls and regular rotation. Customers on eligible Atlassian Cloud Enterprise plans may optionally enroll their own AWS KMS keys (CMK/BYOK), which then also encrypt this app's stored data, giving the customer full control over key lifecycle and access.

The app stores no data outside Atlassian's infrastructure, and each customer's data is logically isolated per installation.

2. Logging, Audit Logs & Monitoring

Bulk Clone Professional for Jira maintains an operational audit trail of all cloning activity. Each clone operation is recorded at issue level - including successes, errors, and warnings - and is viewable in the app's **Log** tab, alongside an organization-wide **Dashboard** summarizing cloning activity (issues cloned, active users, sessions, and top projects).

Log records can be exported/downloaded for review or for ingestion into your own monitoring tools. Jira Administrators can also manage retention directly by bulk-deleting log history by age or date range; this affects log records only and never the cloned issues, comments, or attachments.

As a Forge app, platform-level monitoring and log-access controls are operated by Atlassian, which restricts log access based on organization permissions and proactively monitors the platform for performance, security, and abuse events. Application telemetry is captured via the Atlassian Developer Console, and the app stores no end-user identifiable information (EUII) beyond the error/operational logging described above.

3. Data in Transit

All data transmission is TLS-encrypted and enforced at the platform level. The Forge shared responsibility model commits Atlassian to use TLS to encrypt all traffic, including HSTS. Across Atlassian Cloud, TLS 1.2+ is enforced for all interactions with Jira Cloud and Forge apps (TLS 1.3 where available).

A particular strength is Forge's handling of credentials: the app never handles user credentials directly. Through Forge's managed APIs, third-party code is never trusted with user credentials, and API calls are automatically authenticated on behalf of the app. Long-lived secrets are kept

inside Atlassian's infrastructure and are not accessible externally.

The only data flow that leaves Atlassian's infrastructure is the call to the Xray Cloud API, which occurs only when the optional Xray integration is enabled. The app then calls Xray's API (authenticated with the API token you configure) to clone test cases. This call is made over HTTPS/TLS. As this is the only external data flow, it is documented explicitly, and the receiving side is governed by Xray's security measures rather than Atlassian's.

4. Data Residency

Bulk Clone Professional for Jira stores its data in Forge hosted storage, which automatically inherits Atlassian's data residency. The app's data is therefore stored in the same region as your Jira instance and moves with it if you migrate to another region.

Because all data is stored exclusively in Forge hosted storage, the app qualifies for Atlassian's **PINNED** status without additional configuration, which can be verified in admin.atlassian.com. Atlassian's regions include EU, US, Australia, Germany, the United Kingdom, Japan, and Switzerland, among others. The app stores no data outside Atlassian's infrastructure.
