Structure Cloud Security and Privacy FAQ

This document lists important security and privacy-related questions that you might have when evaluating the Structure app on your Jira Cloud instance. Should you have any additional questions, please let us know at support@almworks.com.

What kind of data is downloaded from Jira by Structure Cloud?

In order for Structure to display data on the Structure Board and perform calculations, the following data may be downloaded:

- Information about issues, such as issue field values and issue links.
- Information about the user's permissions (groups, roles in projects) – this information is used to validate the user's access to issues and structures.

Most of the data loaded from Jira is cached in memory, not stored in the Structure Cloud database. The expiration times of these caches vary from one minute to several hours, after which the data is removed and re-downloaded as needed.

What kind of data is stored by Structure Cloud?

The following data is stored on the Structure Cloud servers:

- Structure names, descriptions and permissions
- Hierarchies (referring to individual issues by their numeric IDs, without any field data)
- Folders
- Column configurations
- Generator configurations (link IDs, issue type IDs, field IDs, JQL and Text queries)

Where are the servers located?

- All the servers are running on AWS, U.S. East region (Ohio).

How is the data encrypted?

- We use TLS to protect information while in transit across the Internet and inside the cluster.
- We use AWS EBS encrypted disks to store data.

Who can get access to the data?

Only the on-call system engineers can access the production environment. Each employee of ALM Works has signed a strict confidentiality and non-disclosure agreement.

How does ALM Works audit access to the data?

- In order to access the database, one needs to request temporary credentials. All such requests are logged and reviewed.
- We are also working on an advanced audit process and data access mechanism, which will include:
    - Logging all data-related operations.
    - Automatic detection of unusually activity.
    - An approval workflow for getting access to the data.

How does ALM Works adhere to information security standards? Do you have any compliance certifications?

We do not hold any compliance certifications at the moment; however, we plan to obtain certification later this or next year.

Structure Cloud has been diligently built with security, privacy and informational security as a highest priority. We are also participating in a Bug Bounty program led by Atlassian.

What is your data privacy policy?

Please see the Privacy Policy published on our website.

Did you complete Atlassian's security self-assessment?

Atlassian's security self-assessment is a questionnaire that app vendors can go through to see if they adhere to the best practices offered by Atlassian. It is not regulated or verified by Atlassian, so it's on an individual vendor to decide how far they want to take it.

We approach security very seriously, and we'd like to pass this self-assessment at the highest possible level. This is why we are still working on finalizing some of the processes advised by Atlassian, even if some are optional. We expect to finish this rollout in a few months and rightfully claim that we passed the self-assessment at the highest standard.