ATLASSIAN

Guide to Multi-instance Model with Atlassian Cloud Enterprise

Learn how admins can tackle the challenges of flexibility and control in cloud by leveraging Atlassian Cloud's Enterprise plan.

Table of contents

Introduction

Your organization has made a major step forward by choosing Atlassian Cloud. While operating in cloud offers many benefits, **cloud adopters still report ongoing challenges** navigating business complexity and security and compliance requirements.

It's understandable that even in cloud, your organization faces unique challenges and needs to find a balance between customization and control. To combat these challenges, along with the high-change environment we all face, you need modern tools and advanced capabilities to stay ahead of the curve. Enter: Atlassian Cloud's Enterprise plan.

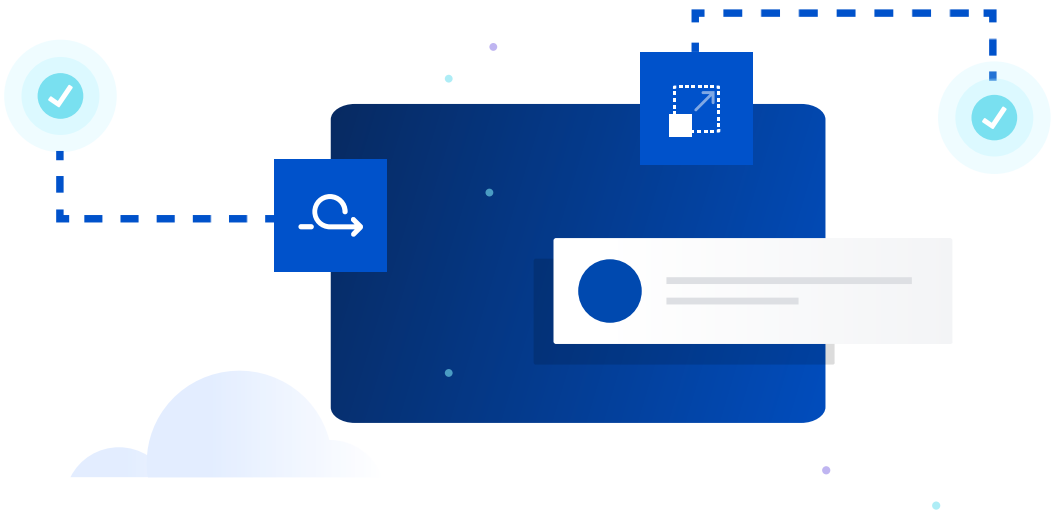
> Oh my gosh, where do I start? It's so flexible and easy to use (other than that filter thing I mentioned above). The integration between Jira and Confluence is really great. We have created workflows for so many different teams doing such different work, various boards and dashboards to track different things.

ATLASSIAN CUSTOMER EMPATHY REPORT
Q1 2023 CY

Scenario 1

Separate departments and governance

For complex enterprises, team autonomy is key. This means teams may need to work independently, yet utilize the same tools to achieve their goals. To solve this problem, an admin must assist each department to design best-fit workflows while maintaining visibility and control across their cloud footprint.



Solution:

By leveraging multiple instances with Atlassian's Cloud Enterprise plan, admins can create separate Jira or Confluence instances for their technical IT team, and their non-technical departments who work differently across Atlassian tools.

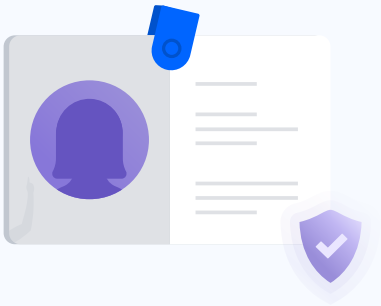
After configuring their environments, they can standardize controls through admin.atlassian.com. Identity and access management, security policies, billing, and utilization insights are all accessible via the Atlassian centralized admin view. Admins can also see the utilization numbers of each instance via **User Counts** - which provides near real-time numbers of how many users leverage each product.

In addition, when organizing different teams into respective product instances, admins are able to right-size their organization's app usage. Admins can therefore license a Marketplace app for users of a specific instance – rather than all the users in their organization. That means paying for just the users that need it – and no more.

In this scenario, Atlassian's Cloud Enterprise plan helps organization admins save time, and money, and facilitate team customization without compromising control.

Features to highlight:

- Multi-instances (support for up to 35k for Jira and 50k for Confluence on a single instance)
- Automatic user provisioning (Atlassian Guard)
- Unified billing
- User Counts
- Release Tracks
- Optimization of market place apps
- Centralized per-user licensing



Scenario 2

Growth through acquisition, collaboration with external stakeholders

Consolidation is all too-common in the market today. In healthcare, for example, consolidation has rapidly accelerated. In less than 25 years, there have been **1,887 hospital mergers (1998-2021), according to the American Hospital Association. Those mergers reduced the number of hospitals by 25%.** This isn't unique to healthcare either - it's present in media, retail, and technology services.

For Atlassian customers who are growing through mergers or acquisitions, their admins have to manage this growth with the need to ensure security and compliance as a non-negotiable. Challenges like who has access to what, how tooling comes together, and how leaders and administrators can track progress from one subsidiary to another present complication and hindrances to the cost-savings that consolidations offer.

Solution:

In this scenario, the flexible scale that comes with Atlassian's Cloud Enterprise plan provides immediate relief to an admin. Firstly, an admin could leverage the **Multiple Identity Providers (IdP)** feature - which gives an organization engaging in M&A time to marry different identity providers. In this case, an admin can continue to manage separate organizations as they slowly merge into one.

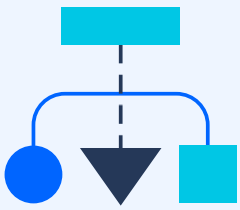
Additionally, an admin can set up a separate instance for a newly acquired organization, via the multi-instance model, as to not disrupt current work in flight. With the help of admins and cloud architects, enterprises can be confident when determining the best-suited configurations going forward.

When it comes to M&A, there are typically consultants and outside partners evolved. Many customers utilize Confluence as a common source-of-truth, and take advantage of **External User Security** and **External Collaboration** to subject these collaborators to strict authentication controls and restrict access to only correct spaces.

Change takes time, but with the right tools, Atlassian customers growing through acquisition, or simply acting with many external collaborators, can find peace of mind that they could maintain consistent tooling and control.

Features to highlight:

- Multiple Identity Providers
- Multi-instances (support for up to 35k for Jira and 50k for Confluence on a single instance)
- External User Security
- External collaboration in Confluence



Scenario 3

Highly sensitive intellectual property

Regardless of the size or maturity of an organization - one of its most valuable assets is its data. As such, data management and protection is paramount. For Atlassian customers with extremely sensitive data and confidential projects across the organization, a partitioned environment may be necessary. This design allows an admin to control each project's identity and access management strategy and ensure their sensitive projects are on a need-to-know basis.

Solution:

Due to the fact that security and control are the top priority for many organizations, admins need access to centralized, detailed information about user access and behavior within Atlassian Cloud products

With Atlassian's Cloud Enterprise plan, which includes an **Atlassian Guard** subscription, admins can implement different authentication policies across multi-instances, as well as enforce two-factor authorization and single sign-on.

In addition to custom authentication policies and enforceable controls, admins can utilize user-activity logs, also known as **advanced audit logs**, for Jira and Confluence.

In addition, Atlassian's bring-your-own-key (**BYOK**) program is coming soon (2023), which will empower admins to encrypt Cloud product data with keys hosted in their own AWS account. BYOK will grant admins more control by giving them the ability to revoke access at any time, both for the organization's end-users and for Atlassian systems.

Features to highlight:

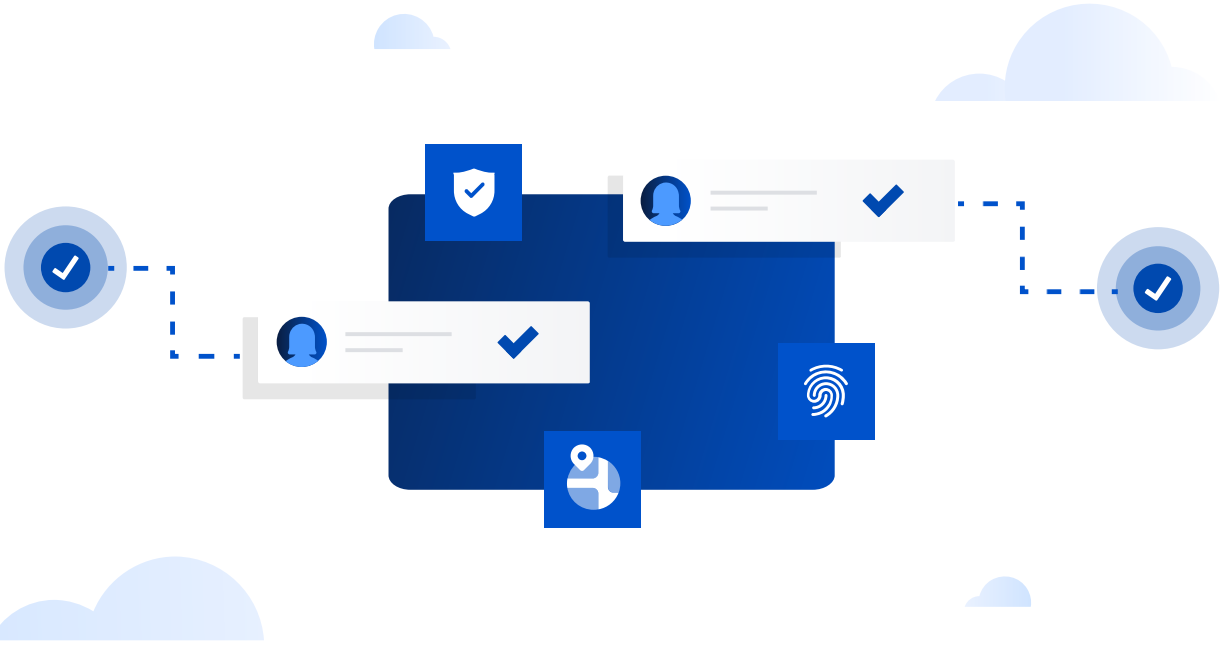
- Atlassian Guard for 2FA, SSO, and custom authentication policies across instances
- IP Allowlisting
- Multi-instances (support for up to 35k for Jira and 50k for Confluence on a single instance)
- User activity audit logs
- BYOK
- Content policies for Confluence

Scenario 4

Data Isolation for geo-dispersed teams

With more team distribution and the rise of remote-work - organizations' geographical footprints are getting bigger. With this, there is a critical need to not only facilitate connection, but comply with with evolving requirements depending on local, state, or federal regulations.

For global organizations, the ability to separate instances and manage the security and compliance of their data differently isn't just a nice to have, it's a necessity.



Solution:

Geo-distributed organizations are tasked with keeping their teams connected all while working across different departments, projects, and time zones. It's not easy for an admin, who needs to keep work as standardized and centralized as possible, to navigate this. For admins operating in highly regulated and complex environments, compliance requirements, especially those related to industry or geography, are top of mind. Thankfully, Atlassian's Cloud Enterprise plan offers the **most advanced compliance certifications** to help customers stay ahead of the curve. In addition, Atlassian offers **Data Residency** for specific regions and countries - North America, EU, Australia, Germany, Ireland and Singapore - with more coming soon.

Similar to customers with highly sensitive data, an admin facing this scenario can leverage administrative controls and information protection features - segregating out instances and customizing authentication of users based on location. In addition, **advanced audit logging** provides historical records of user activity for any compliance audits required. Admins can feel relief that with Atlassian's Cloud Enterprise plan, compliance and customization go hand-in-hand.

Features to highlight:

- Advanced compliance for industries and geographies
- Data Residency
- Atlassian Guard for 2FA, SSO, and custom authentication policies across instances
- Multi-instances (support for up to 35k for Jira and 50k for Confluence on a single instance)
- User activity audit logs

With the move to cloud, admins need connection, customization, security and control.

Contact ByteSource, your local Atlassian Solution Partner, for a full feature dive into Atlassian ’ s Cloud Enterprise plan.

ByteSource Technology Consulting GmbH

Damböckgasse 4/3, 1060 Vienna, Austria

contact@bytesource.net

+43 1 904 32 400

https://bytesource.net/

ATLASSIAN