



Guide to multi-instance scale in Atlassian Cloud

How Atlassian Cloud Enterprise enables you to unify and extend your organization.



Scale Dilemma

Adoption of Jira or Confluence often starts at the team level. But as organizations look to scale these products across the company, natural barriers such as geography, security and preference for specific workflows, Marketplace apps arise. It becomes critical to deftly balance the need for customizable solutions to meet the needs of individual teams while ensuring organization-wide governance and cross-team collaboration.

On one hand, front-line teams need the autonomy to work within environments tailored to meet their unique workflows, Marketplace apps and security needs. On the other hand, you need to make sure it isn't a wild west scenario with teams operating in silos, leading to duplication of effort, poor cross-team collaboration and worst-case scenario—security breaches or regulatory non-compliance.

So as you scale Jira or Confluence across your organization, you may run into challenges such as how to:

- 1 Support the need for customization while ensuring org-wide governance
- 2 Centralize user access management and enable granular permissions
- 3 Ensure compliance with company's security policies while customizing as needed
- 4 Enable effective cross-team collaboration and alignment
- 5 Scale across multiple teams without blowing your budget

In this guide, you'll learn how Atlassian Cloud Enterprise for Jira Software, Confluence and Jira Service Management addresses the above challenges and enables you to unify and extend your organization's collaboration with Atlassian tools and practices.

Contents

5	Challenge #1: Customization with organization wide governance
6	Standardize with an Atlassian Organization
7	Configure multiple instances to support custom needs
8	Challenge #2: Centralized user management with granular permissioning
9	Centralized administration hub
10	Granular permissioning with customized groups
11	Challenge #3: Custom security policies with enterprise controls
12	Flexible authentication policies
13	Security insights across the organization
14	Challenge #4: Foster cross-team collaboration and enterprise alignment
15	Navigate across instances
16	Find content across instances
17	Collaborate across instances
17	Sync information across instances
18	Data analytics and insights across instances
19	Challenge #5: Scale without blowing your budget
20	Centralized per-user licensing
20	Optimizing Marketplace app costs



CHALLENGE #1

Customization with org-wide governance

Independent departments or recently acquired entities may desire autonomy to manage their own Jira and Confluence environments. Similarly teams may desire a segregated environment for security reasons. You want to enable these teams with custom environments while also ensuring global control and oversight. Collaboration often happens across departments, lines of businesses and functions making it essential that you ensure the right users have access to the right environments. Also company-wide information needs to be easily accessible to any team on any device, which increases the number of security touchpoints and risks. That's why admins need centralized and scalable ways to manage user access, permissions as well as enable security policies to enforce appropriate governance.

Solution

Standardize with an Atlassian organization

The launch of Atlassian Cloud Enterprise for Jira and Confluence Cloud introduced the concept of **Atlassian organization** where you can manage your content and users across your company. Your Atlassian organization is your company's centralized admin hub, acting as a unifying layer for all of your company's users, sites and product instances in Atlassian cloud.

PRODUCT INSTANCE

A “product instance” refers to a single instance of each Atlassian product on a site. Each site can have its own set of users, permissions and security settings applied to the instances on it.

With an Atlassian organization, users are no longer tied to a specific instance and can now access multiple product instances across multiple sites. Significantly this unlocks the ability for admins to standardize governance across multiple cloud instances of a product – all from one central location.

Organization

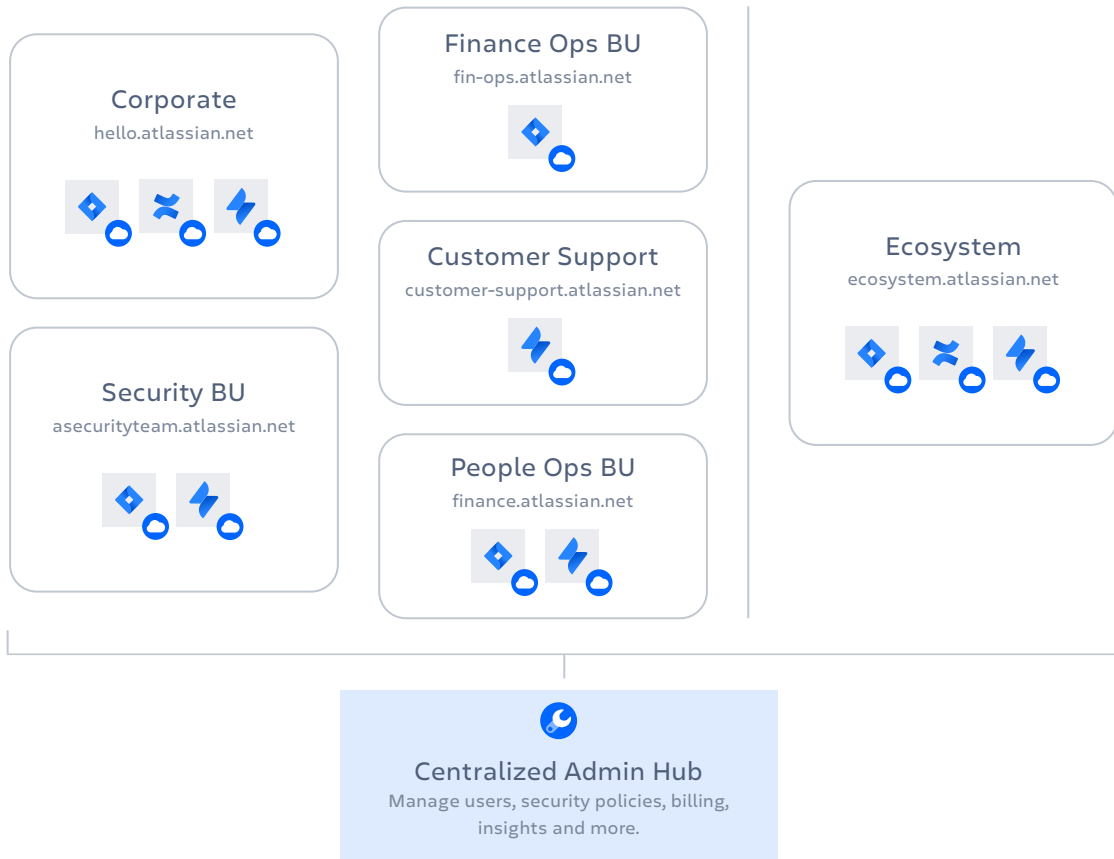


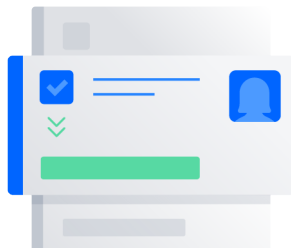
Configure multiple instances to support custom needs

Once you set up your Atlassian organization, you can create and configure as many instances as you need for all your Jira and Confluence products. Here are several reasons why a multi-instance model might work best for your organization:

- ✓ **AUTONOMY:** Multi-instance can support the needs of subsidiaries or independent business units who need the autonomy to manage their own ways of working. For instance, marketing teams may need their own instance so they can integrate CRMs and other SaaS marketing tools into custom workflows that they are able to manage. Also if you are frequently acquiring businesses, it may make sense to offer them the autonomy to manage their environments temporarily until the teams are fully integrated.
- ✓ **DATA SENSITIVITY:** Certain departments such as finance or HR who often deal with sensitive or proprietary information may benefit from a separate instance to keep sensitive data contained to a small group reducing the risk of a leak. Similarly separating content that requires external collaboration on its own instance can reduce the risk of external users getting access to sensitive company information.
- ✓ **DATA ISOLATION:** You might need to spin up an instance to isolate data to a single region to help comply with regulatory requirements such as data sovereignty laws.
- ✓ **BUDGETARY REASONS:** Some teams need specialized apps from the Marketplace in their workflows. By spinning up separate instances for users of those specific apps, you can avoid paying for additional seats for those apps than needed.

Atlassian itself utilizes multiple instances. They've set up dedicated cloud instances based on business needs, whether it's separate Jira Software instances for Atlassian's security and finance teams for data sensitivity reasons, a dedicated Confluence instance for the Ecosystem team for autonomy, or a highly customized Jira Service Management instance for their customer support team.





CHALLENGE #2

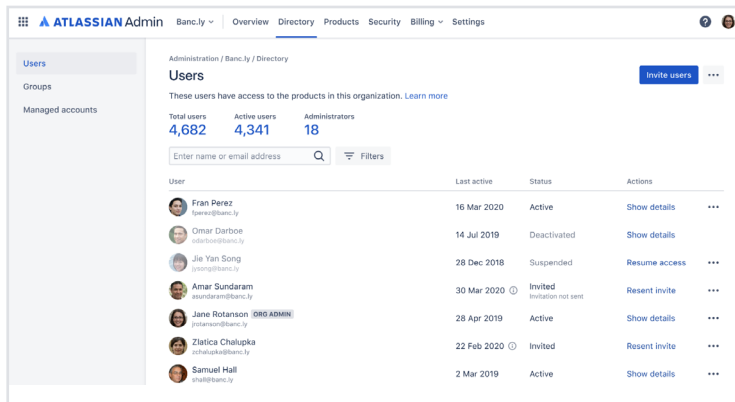
Centralized user management with granular permissioning

For IT admins at organizations with multiple Atlassian product instances, managing user access across hundreds – if not thousands – of employees can quickly become a full-time job. Yet, admins need to carefully balance the need for scalable ways to define access policies across multiple instances with the flexibility to allow granular permissions based on employees' roles. Cross-team collaboration is a central tenet of many enterprises' cultures and strategies today but admins need to ensure that the right users have access to the right product instances with the right permissions or else it could lead to costly data leaks.

Solution

Centralized admin hub

Fortunately, with Atlassian Cloud Enterprise, admins can manage all users' access and permissions through a centralized admin controls hub while ensuring granular permissions by role, instance and more.

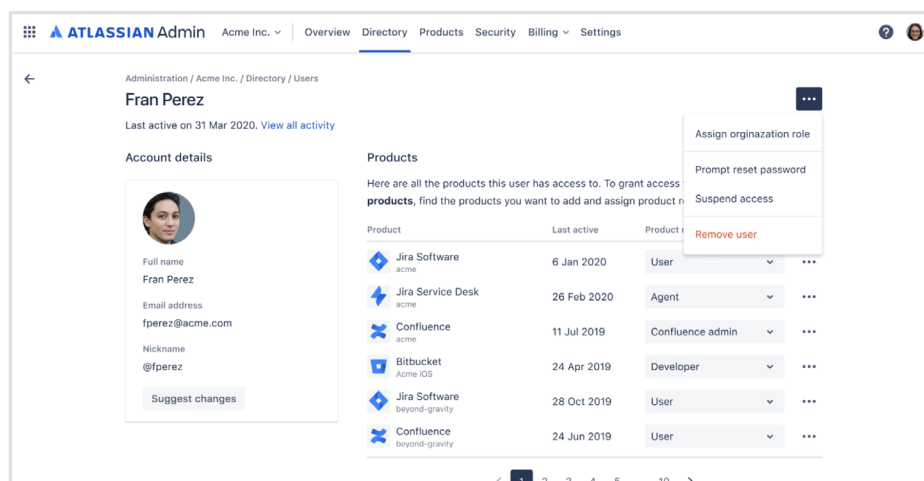


By navigating to managed accounts under **Directory** tab, admins can see all users of Atlassian products with an account associated with their company email. The account capture system ensures admins have

full visibility into all internal users, and which Atlassian products and instances they are using.

COMING SOON Admins will be able to see both internal and external users – that have access to the Atlassian Cloud products and instances within your organization in one location. Admins can invite new users to multiple product instances in one click.

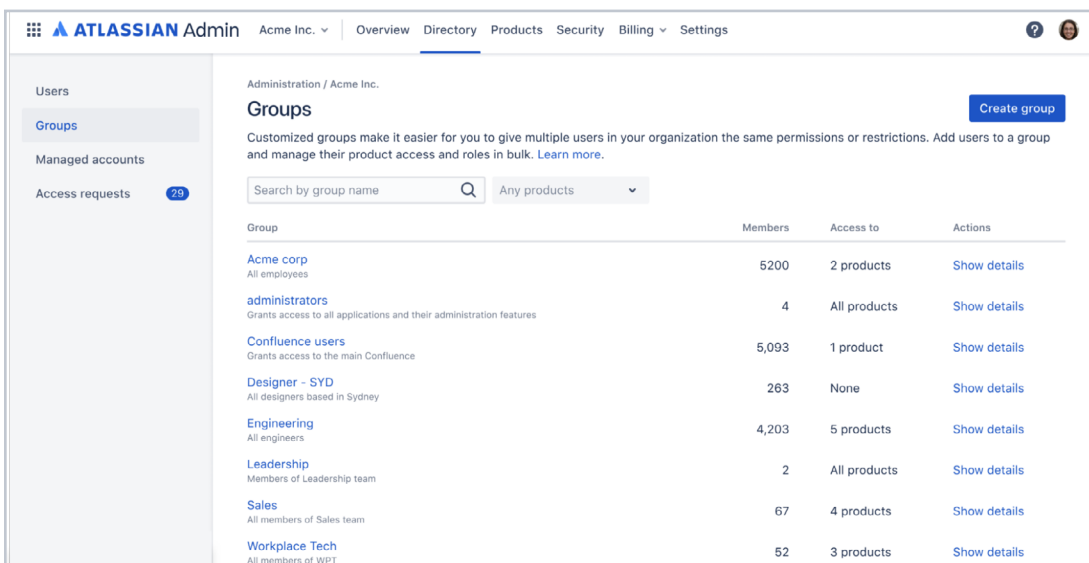
You can then drill into a specific user and assign roles and grant different permissions at the instance level. You can suspend access for a product instance or completely remove the user from your organization.



Granular permissions with customized groups

To manage user access at scale while enabling granular permissions, you can create custom groups within your admin directory. By creating custom groups – such as “Leadership,” “Engineering,” “Sales,” or “Confluence users” – you can grant groups of users spread across multiple Jira and Confluence instances the same permissions and restrictions with just a click.

Individual users can be added to specific groups from either the admin directory or [an external directory](#), such as Okta, Google Cloud, Azure AD, or OneLogin. So for instance, when an incoming employee is classified within the “Engineering” group in your external identity provider, they’ll automatically be granted access to the Jira and Confluence instances permitted for the “Engineering” group within Atlassian Directory.



The screenshot shows the Atlassian Admin interface for 'Acme Inc.'. The left sidebar has a 'Groups' link. The main content area is titled 'Groups' and includes a 'Create group' button. Below this is a search bar and a table of groups.

Group	Members	Access to	Actions
Acme corp All employees	5200	2 products	Show details
administrators Grants access to all applications and their administration features	4	All products	Show details
Confluence users Grants access to the main Confluence	5,093	1 product	Show details
Designer - SYD All designers based in Sydney	263	None	Show details
Engineering All engineers	4,203	5 products	Show details
Leadership Members of Leadership team	2	All products	Show details
Sales All members of Sales team	67	4 products	Show details
Workplace Tech All members of WPT	52	3 products	Show details

COMING SOON At the moment, users and groups still need to be defined separately for each instance, unless you’re syncing from an external directory. Atlassian plans to soon rollout [organization-level user and group directory](#) that allows you to use a single set of users and groups across multiple cloud products and instances.



CHALLENGE #3

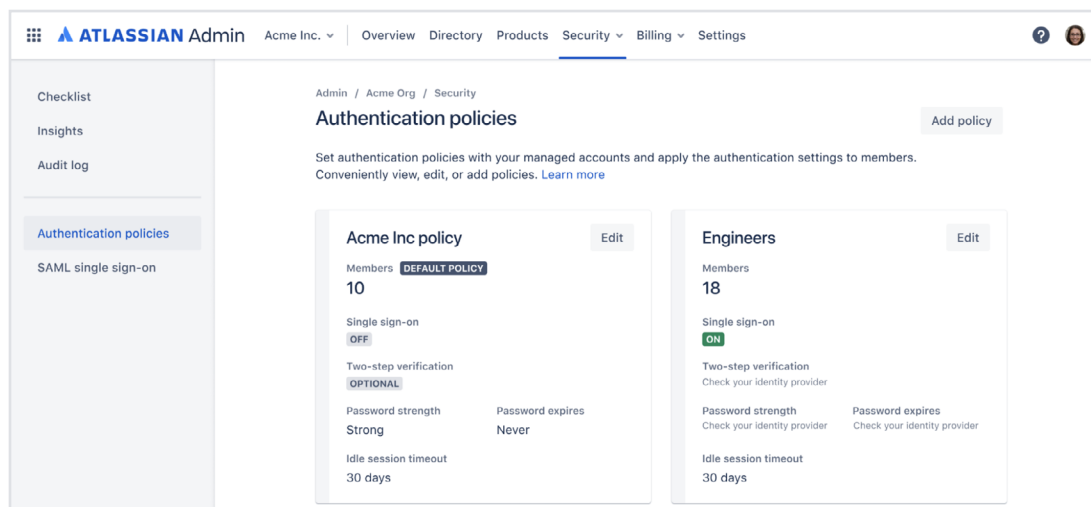
Custom security policies with enterprise controls

Typically Jira and Confluence are accessed by a broad set of users in an organization ranging from C-suite to entry level hires as well as full-time employees to alternate workforce and more. Hence admins need the flexibility to manage the diverse security needs of the various user tiers. At the same time, they need scalable ways to configure and manage these policies across the organization and avoid costly errors associated with manual workflows. They also need a centralized way to audit and monitor user activities across multiple instances for compliance reasons and for reducing security risks.

SOLUTION

Flexible authentication policies with centralized control

With Atlassian Access (included for users on Enterprise plan or as an add-on for lower plans), admins can set custom authentication policies for specific user groups and even control these settings from a centralized location. Depending on the sensitivity of the information accessed by each group and the risk level associated, admins can decide what kind of authentication policies should apply to the users in a particular group.



The authentication policies that you can configure for each user group include:

- **SINGLE SIGN-ON (SSO)** allows users to use a single username and password to access various applications without having to re-enter authentication factors. This can be configured using an external identity provider.
- **ENFORCED TWO-STEP VERIFICATION (2SV)** requires that users confirm their identities using a second login step. For instance, after authenticating with their username and password, they may need to provide a token (a four to eight digit code) that's been sent to their mobile phone.
- **PASSWORD POLICIES** dictate the minimum strength a user's password must meet, as well as how often their password will need to be reset.
- **SESSION DURATION** settings dictate how long a user can remain idle before they're automatically logged out of an app. This helps protect organizations from data breaches in the event that a user steps away from their device.

To meet regulatory data privacy requirements and for additional security, admins can leverage [data residency](#) controls to isolate data on a per-instance basis by pinning it to a geographic realm such as the United States or European Union. Admins can also [configure IP allowlists](#) on a per-instance basis, restricting access to certain instances to a limited number of IP addresses. Allowlists can contain up to 100 IP addresses or network blocks per allowlist, helping bring an extra layer of security to instances that contain sensitive data.

Security insights across the organization

Of course, while strong access controls are half the battle in ensuring enterprise security, the other half often takes place after those settings are in place – using tools that allow you to monitor security and track suspicious activity across multiple Jira and Confluence instances.

Thanks to the organization insights feature in Atlassian Access, admins can track the number of active daily or monthly users accessing Jira or Confluence cloud instances. This allows admins to see things like which users have access to certain products but don't use them – meaning their access could be revoked to save the company both licensing costs and unnecessary security risks. Admins can also monitor how many users have SSO or 2SV enabled and prevent security lapses.

The [Organization audit log](#), on the other hand, logs all key activities carried out by admins – whether that's changing permission settings, creating new groups, or altering a group's membership. That way, any access or security setting changes are logged for posterity and can easily be monitored for suspicious activity on a regular basis.

COMING SOON By the end of 2021, Atlassian also plans to roll out a [User Activity Log](#) to enable admins to get a detailed log of all the users that viewed a piece of content such as a Jira issue or Confluence page. This not only helps triage suspicious activity for sensitive pieces of content but also helps meet regulatory compliance for specific regions and industries.



CHALLENGE #4

Foster cross-team collaboration and enterprise alignment

According to the [Beezy 2021 Digital Workplace Report](#), sixty-five percent of remote employees say it's challenging to collaborate across teams, and 41 percent are overwhelmed by the number of tools they're required to use at work. In a multi-instance environment, this problem could get magnified. End-users of Jira and Confluence require a centralized way to access and search for data residing across multiple instances. They need seamless cross-team collaboration workflows whether it's being able to easily switch context from one instance to another or getting important updates from other teams.

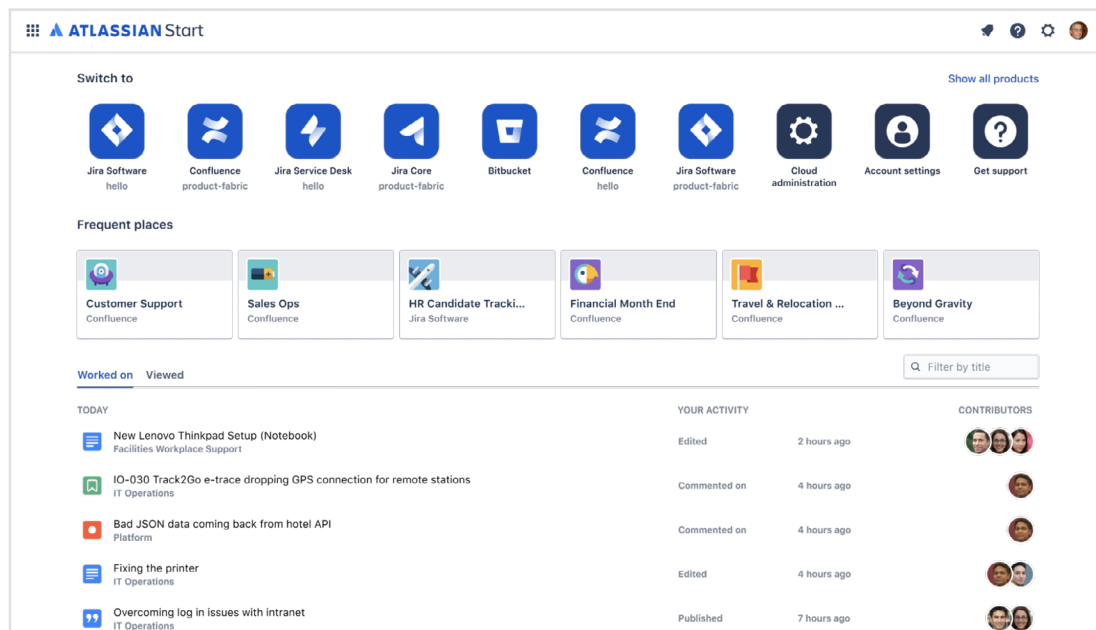
And, when it comes to running an effective organization at scale, it's critical for leadership to be able to see how projects are progressing across individual departments, teams, and instances. After all, you can't execute on a company-wide strategy if you can't access the data and analytics that show how projects, initiatives, and day-to-day tasks align to that larger strategy.

SOLUTION

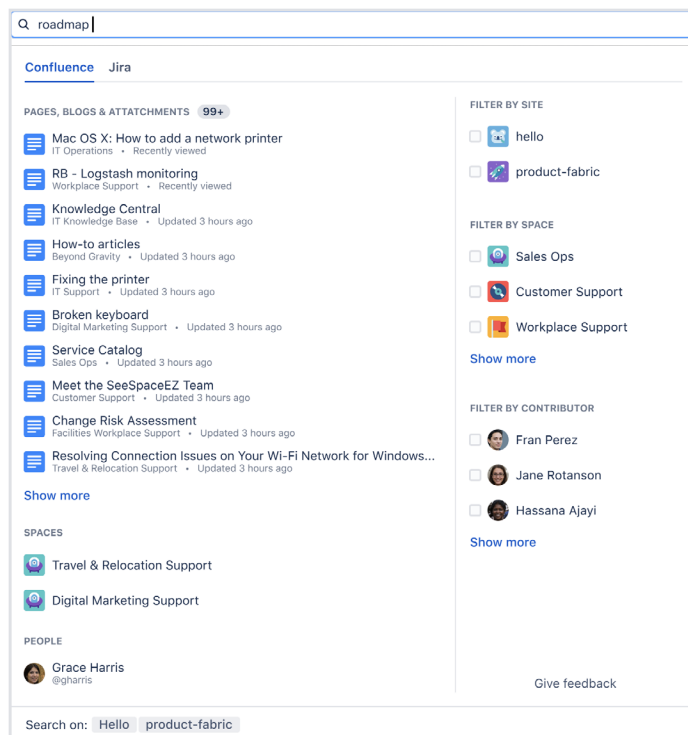
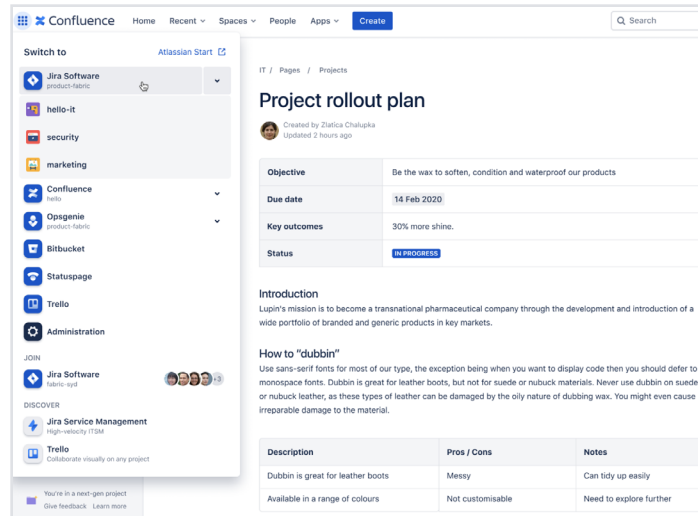
Atlassian Cloud Enterprise is home to several features that help make collaboration across instances effective and seamless. In fact, Atlassian uses a multi-setup internally, and frequently trials new capabilities and features related to the multi-instance experience before it's ready for the world. Atlassian continues to invest in offering advanced data insights and visualization capabilities across instances to help you effectively align technical initiatives to larger business goals.

Navigate across instances

Any user that belongs to an Atlassian organization can access their own Atlassian Start homepage, found at start.atlassian.com, where they can easily navigate across cloud products and instances, view their most frequently visited places and access pages and tickets that they recently worked on.



Project switching isn't limited to Atlassian Start. While within any Atlassian Cloud product, users can also use the Atlassian App Switcher—found in the menu bar of each app—to jump to other Atlassian Cloud products and their associated instances. In a “Join” pane, users can also see which instances they've been invited to but have yet to join, while a “Discover” pane allows users to find and explore products that they don't yet have but might be interested in.

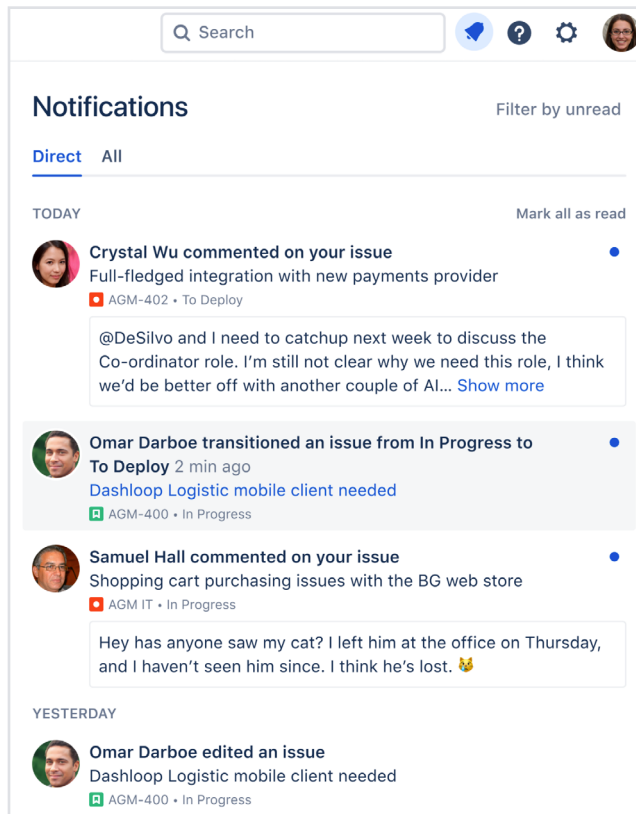


Find content across instances

Using the search bar within Atlassian Start, a user can use basic text searches to find resources across any Jira or Confluence instances that they have access to. (At the moment, Jira Query Language searches can only be carried out within single instances.) Atlassian also plans to make basic **multi-site searches** available within Jira Software, Jira Service Management, and Confluence by 2022.

Collaborate across instances:

Jira and Confluence Smart Links reveal important information about links (such as a Confluence page or Jira ticket) without leaving the page. You can get a preview of the type of content as well as richer details about the content—all without switching your current context.



With multi-site notifications, users working across teams don't have to worry about missing important project updates. An in-app drawer in Atlassian Start displays notifications from all instances, and users can sign up to receive separate email notifications with important updates from each of the instances they belong to. Those working with Slack or Microsoft Teams can get notifications delivered in-app, and Atlassian's mobile apps also support multi-site push notifications – allowing users to stay updated no matter where they're working.

Sync information across instances

At the moment, Jira Software boards can only contain issues from one instance. However, there are several Marketplace apps that can be used to sync issues across multiple Jira instances. [Backbone Issue Sync for Jira](#), for instance, allows users to bi-directionally and automatically sync issues across Jira instances – whether they're found within Jira Software, Jira Service Management, or Jira Work Management. You can be rest assured that information is always up to date, regardless of which instance it's being accessed from.

For those that need to migrate projects or native issues between instances, Atlassian is currently working on cloud-to-cloud project migration solutions.

Currently, Atlassian is actively developing the [Jira cloud-to-cloud migration feature](#), with existing Atlassian Cloud customers involved in an early access program for the feature. Using the cloud-to-cloud migration feature, you can select Jira Core or Jira Software Classic projects to migrate from one source instance to another new (or existing) instance, with the ability to:

- Migrate all of a project's data, including its related issues
- Migrate all attachments related to a project
- Migrate configurations related to a project
- Migrate all users related to a project

DUPLICATING CONFIGURATION OBJECTS ACROSS INSTANCES

At the moment, configuration objects – such as workflows, custom fields, and schemes – can't be easily moved between Atlassian Cloud instances. Users can [reuse existing workflows](#) by exporting them from an existing instance and importing them into a new one, but at the moment, there's no centralized way to duplicate certain configurations across instances.

COMING SOON DATA ANALYTICS AND INSIGHTS

Atlassian is working hard to help enterprises get visibility across all product instances at the enterprise level down to project and even task level so they can better align technical initiatives to broader business goals. To support this, in March 2022, Atlassian plans to launch [Data Lake](#) (available with Enterprise plan), a tool that allows you to connect data from across all your Jira Software instances to your external business intelligence (BI) tool. You can even ETL (extract, transform and load) the data into your data warehouse to then layer BI tools on top. With Data Lake, you can access a structured data set that's easy to both query and plug into external BI tools, including Tableau, PowerBI, Looker, Qlik, Databricks, Mulesoft, and SQL. This will allow users to interpret any data pulled from Jira Software – such as teams' average sprint times, resolution time, and workloads – in whatever platform works best for them. In the future, Atlassian is also aiming to integrate Data Lake into more Atlassian Cloud products.

The recent acquisition of Chartio will bring data visualization and analytics capabilities to Atlassian Cloud Enterprise, allowing users to pull insights from across Atlassian products and instances.



CHALLENGE #5

Scale without blowing your budget

Purchasing a separate license for each additional Cloud instance a user needs access to can quickly bring up costs, so scaling teams on a single Cloud instance may seem cost-efficient. However, this can greatly restrict the ability to meet custom needs of today's global and distributed workforce, leading to a highly complex instance with a lot of technical debt that becomes costly to maintain over time. Also you could end up with dozens of specialized Marketplace apps that are licensed for all users but only a few end up using them leading to poor use of budget resources.

SOLUTION

Centralized per-user licensing

For companies that need to spin up multiple instances, the Enterprise plan for Jira and Confluence offers the flexibility needed to do so while keeping costs down with centralized per-user licensing. This lets you pay for a user just once while granting them access to as many instances as they need. This can lead to significant cost savings especially when the majority of users need to access multiple instances. For instance, you can create a corporate instance for all users with general settings while allowing the same users to be part of specialized instances with custom workflows, Marketplace apps or security settings without incurring additional costs.

Optimize Marketplace app costs

Operating with multiple instances can also allow admins to bring down the cost of customization. Teams that need to customize their workflows with specialized **Marketplace apps** can be grouped into a separate instance, allowing you to license the app only for users of that instance – rather than all the users in your organization. For instance, if your Design team wants to add the design tool **Canva for Jira** to their workflow, you can easily create a separate instance that includes just the Design team and install the Canva for Jira Marketplace app there. That means paying for just the users that need it – and no more.

Scale confidently across multiple instances with Atlassian Cloud Enterprise

With Atlassian Cloud Enterprise for Jira Software, Confluence and Jira Service Management, you can easily balance your organization's need to support customized environments while still ensuring centralized governance and cross-team collaboration at scale.

