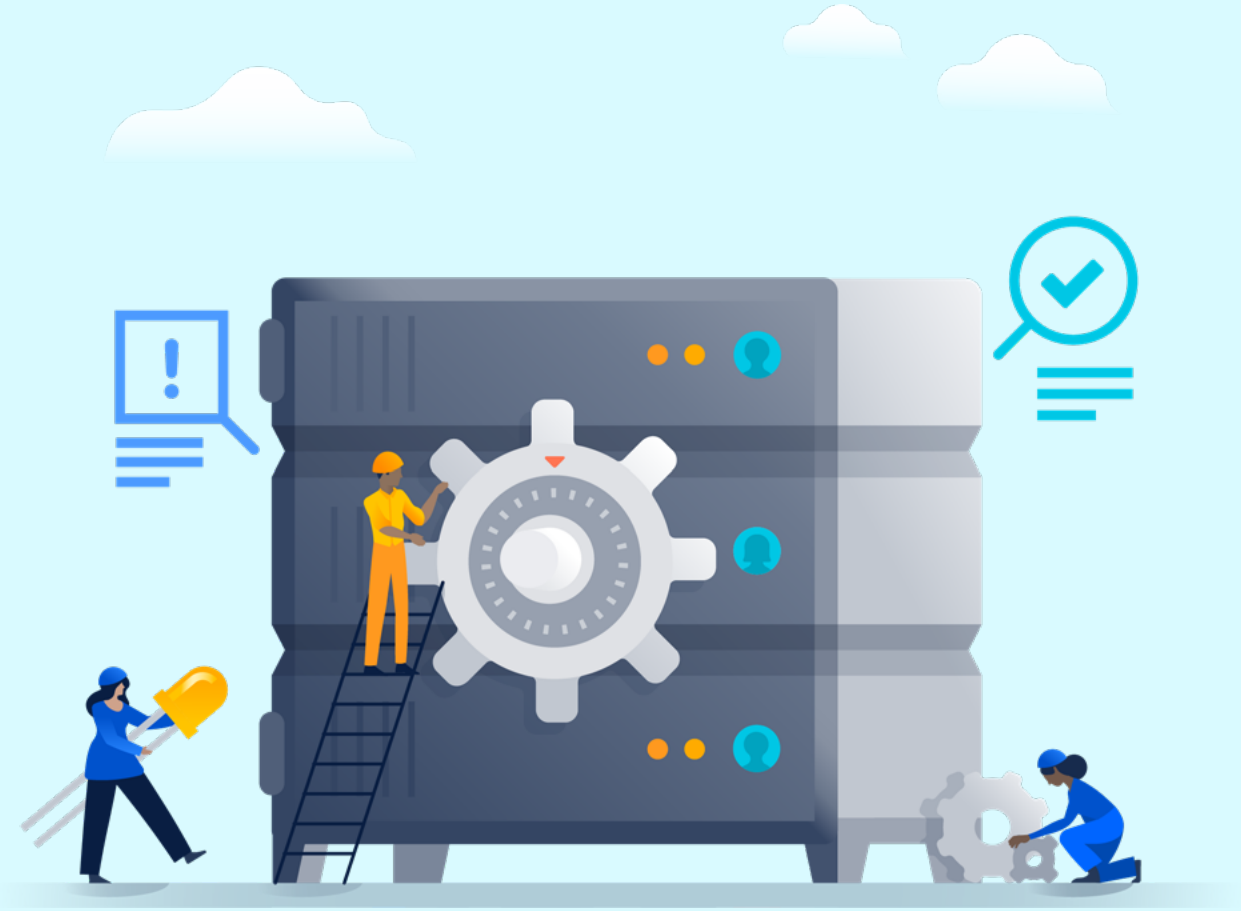
ATLASSIAN



Enterprise security and compliance for self-managed environments

A guide to how Atlassian Data Center protects people and data at scale

Contents

Executive summary

An enterprise edition for security and compliance at scale in self-managed environments.

While ensuring a secure environment is at the top of any organization's priority list, this objective is often more nuanced for an enterprise. Enterprise security and compliance leaders often oversee an inherently decentralized business, with a broad range of teams and tools spanning functions, regions, and (in most cases) subsidiaries.

Modern enterprises need more. They need the peace of mind that the right controls are built into the very fabric of the everyday tools used across their organization.

While these values have always been core to the Data Center offering, newer capabilities like support for leading security and compliance standards, expanded audit capabilities, and an advanced Confluence permissions framework in Data Center help deliver the security and compliance enterprise organizations need.

Regardless of an enterprise's particular goals, it's imperative that the products they deploy provide capabilities that make it easy to protect their people, intellectual property, and data proactively rather than reactively.

This handbook will focus on providing advice to security and compliance for organizations that manage their Atlassian suite of products on-premise, including a deep dive into how product capabilities available in Atlassian Data Center can help meet evolving enterprise security and compliance needs.

Introduction

There is more change than ever before in the modern workplace. Not only is there an ongoing evolution of IT capabilities and practices, but as an organization grows, the amount of tools and complexity of the systems that support them increases as well. Teams are collaborating in real-time, switching between different types of tools, and the sheer volume of data being created and transferred is staggering. As a result, the number of applications with access to sensitive information increases by the day, and the cost of not meeting security and compliance standards has never been more significant.

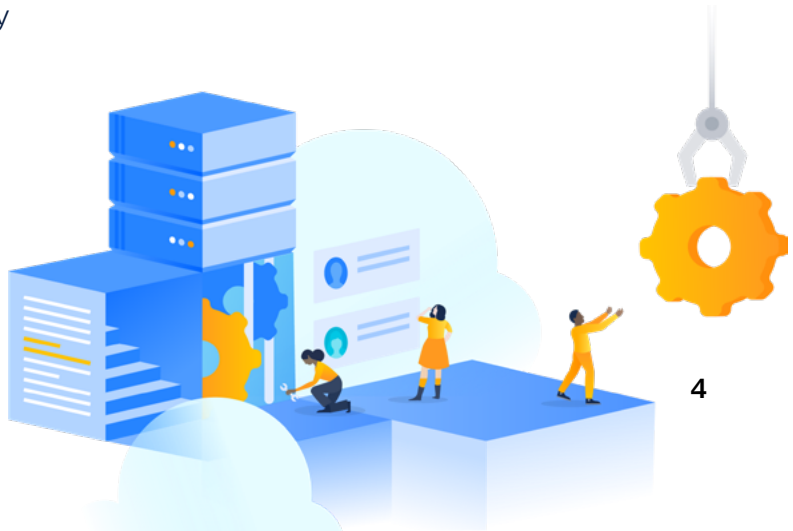
In 2017, organizations spent an annual average of USD 11.7 million on cybersecurity incidents and recovery, with the number reaching as high as USD 17 million for organizations in the financial industry (Accenture/Ponemon Institute, Cost of Cyber Crime Study, 2017). However, the reality is that the cost of losing identity or proprietary information has implications beyond monetary loss.

IT organizations are under tremendous pressure to meet business requirements and ensure the security of their corporate data and employees. They need comprehensive systems in place that will give them the flexibility to keep up with an ever-evolving security and compliance landscape.

130

The average number of security breaches per organization each year.

Source: Accenture/Ponemon Institute, Cost of Cyber Crime Study, 2017



The value of security and compliance in self-managed enterprises

Modern enterprises rely on a multitude of specialized systems, and as they grow and evolve, these systems become that much more intricate. Furthermore, some enterprises are held to more intensive compliance standards than others. For example, they may operate in a highly regulated industry, and In some of these cases, organizations may choose to host their tools on-premise.

Atlassian's Data Center edition of products is explicitly built with these enterprise organizations in mind. Data Center provides a number of security and compliance capabilities and focuses on providing these organizations with protection, assurance, and predictability across the entire business.

60%

Number of executives who rank cybersecurity as one of their organization's top five risks.

Source: The Cyber Risk Perception Survey, 2018

Protection

Protection of people and data is the underlying need of any security measure put into place, and ensuring security at scale is a broad and continuous effort. Nearly 60% of executives rank cybersecurity as one of their organization's top five risks. (Marsh & McLennan Agency, Managing Cybersecurity: The Cyber Risk Perception Survey, 2018) From user authentication and permissions to audit visibility and security event coverage, Data Center provides the capabilities to protect an organization's people and data through improved security mechanisms.

Assurance

In 2015, corporations paid USD 59 billion for U.S. regulatory infractions. This number grew more than five times between 2010 and 2015, and has continued to do so. (McKinsey & Company, "Are You Prepared for a Corporate Crisis?," 2017 April). Organizations need the assurance that they are set up to meet compliance as both internal and external mandates continue to increase. Atlassian Data Center editions make it as easy as possible to abide by and adapt to the increasingly evolving regulatory landscape, mitigating the concern of potential roadblocks and giving an organization peace of mind

Predictability

Perhaps the biggest fear of security and compliance leaders is not knowing what could happen next, and not knowing how to be prepared. 87% of organizations see tech risk management as a siloed, reactive process rather than "an organization-wide function for proactive risk management." (KPMG / Forbes Insights, Disruption Is the New Norm: Tech Risk Management Survey Report, 2018). By automating processes and establishing a culture of predictability, Data Center helps turn responses to potential threats from reactive to proactive.

User management

Advanced user management capabilities

Atlassian's advanced user management capabilities help ensure simple and secure authorization, flexible authentication with support for the leading standards, and a streamlined user provisioning process that gives admins valuable time back.

Identity security has always been an important consideration for IT admins. Ensuring secure authentication and authorization of their users and the tools they need access to is paramount to the safety and success of any business, but managing this at the enterprise-scale can present its fair share of difficulty. Additionally, many of the products that admins choose to deploy are often decided by the security standards they satisfy.

As a system administrator, it can be overwhelming to find how disparate and inconsistent processes are across the business. Different teams often follow different authentication standards or employ different identity providers (IdPs). While consistency is important, flexibility is just as critical to achieve effective user management at scale.

Admins usually don't have enough time to effectively oversee all user-related activity because of monotonous tasks that could otherwise be streamlined or automated.

For these reasons, Atlassian has built enterprise-grade user management capabilities into Data Center products to help administrators easily achieve consistent, yet flexible, authorization, authentication, and user provisioning processes.

Support for OAuth 2.0

Support for OpenID Connect (OIDC) and Security Assertion Markup Language (SAML)

Multiple identity providers (IdPs)

Just-in-time (JIT) user provisioning

Support for System for cross-domain identity management (SCIM)

Support for OAuth 2.0

The OAuth 2.0 authorization framework is known as the most secure data sharing standard on the market, and for good reason. It limits access to user data and allows platforms to block attackers from logging into accounts even if they've somehow retrieved user credentials. On top of providing a strong base layer for authentication, it is also easier to implement. As most admins will recognize, there are multiple reasons why an organization might require their systems to support OAuth 2.0.

Microsoft Exchange and Gmail end-of-support for Basic Authentication

Across 2020–21, both Microsoft and Google are ending support for Basic Authentication, meaning that any integrations with their mail servers must support the OAuth 2.0 authorization framework as a measure to increase security. (Microsoft's Exchange ends support in October 2020, while Google's Gmail ends support incrementally, with users who try to connect to an LSA for the first time ending in June 2020, and access to LSAs turned off completely in February 2021).

Flexible authentication policies

Support for SAML, OIDC, and multiple IdPs

When it comes to providing secure authentication protocols, Atlassian supports two of the most common authentication protocols, SAML and OIDC. Admins can connect Atlassian Data Center products with their infrastructure by delegating authentication to the SAML or OIDC IdP of their choice.

> **Want to get started with SAML or OIDC?**
> Contact your local Atlassian Solution Partner to help get you set up with SSO.

Many organizations require flexibility in how these standards are applied. For example, organizations that own subsidiaries or have an external-facing website or portal for their employees to interact with customers or 3rd party vendors, often want to set authentication policies based on these separate domains to avoid inappropriate access.

But the buck doesn't stop at providing support for leading authentication standards. There's also the question of flexibility when it comes to using multiple identity IdPs. Data Center's support of multiple IdPs allows users to authenticate with different IdPs based on the domain name in their email address. .

Atlassian Data Center products support the following providers out of the box

Microsoft Azure

Microsoft Active Directory Federation Services

onelogin

okta

PingIdentity

BITIUM

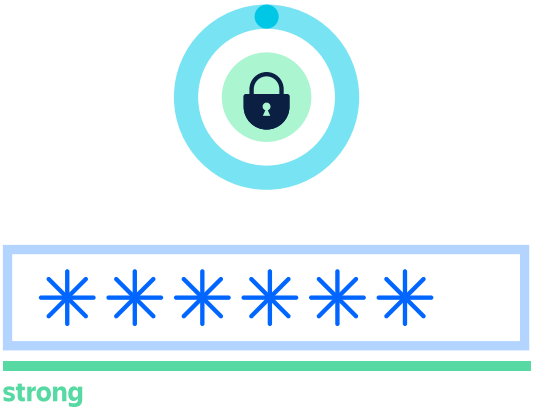
Don't see your IdP in the list? Don't worry, you can also set up a custom SAML or OIDC connection.

With the extended range of supported authentication options, as well as the ability to authenticate with different IdPs, you have more flexibility to achieve seamless authentication for all of your users across the entire organization.

Enterprise-grade single sign-on

Delegate authentication to the SAML or OIDC IdP of choice.

As an organization grows, so does the number of users, products, and instances of those products. Some of our customers manage as many as fifty instances of a single product! Whether it's triggered by a merger, an acquisition, organizational changes, or normal user growth, user management at scale calls for an enterprise-grade single sign-on (SSO) solution.



Most people understand the benefits of SSO at its most basic function - simplifying and centralizing the identity verification process. But not everyone fully understands the security benefits of SSO.

Usernames and passwords are the primary targets of cybercriminals. Every time a user signs in to an application, there's an opportunity for a hacker to collect verified credentials. Furthermore, without SSO, employees often use the same or similar passwords for the majority of their accounts, meaning that if a hacker finds access through a poorly secured application, they are more than likely to find access to other corporate systems. Minimizing the number of logins or sets of credentials helps mitigate the potential of a cyber attack.

Atlassian Data Center editions automatically come with SSO support using the SAML or OIDC IdP of choice. As mentioned earlier in the handbook, both SAML and OIDC provide additional security capabilities that make it increasingly difficult for hackers to steal login credentials.

User provisioning

Automate user lifecycle management with the next level of user provisioning

As an organization grows and has more people in their systems, it makes sense to move from manual provisioning to automated, policy-driven access management using an IdP. This gives IT a centralized view into the permissions assigned to each user, and it allows admins to automatically provision and deactivate users using pre-established rules based on user or group attributes.

As a means of facilitating this process, we use a protocol known as SCIM, which manages user identities with an IdP and then syncs those identities with Atlassian products. For example, an admin can assign a user to Atlassian applications in Okta, and the Data Center product will automatically detect the changes.

Another way to can take advantage of automation to streamline the user provisioning process is by enabling JIT user provisioning. JIT helps reduce friction for admins provisioning new users by automatically creating an account when a new user authenticates into an application for the first time using SSO.

Executive summary of user management capabilities

Data Center provides several user management capabilities, built with the enterprise environment in mind. Their purpose is to make processes like authorization, authentication, SSO, and user provisioning easier to achieve at scale, while also ensuring that regulatory requirements - both internal and external - are met without friction. With Data Center's advanced user management capabilities, organizations are able to:

Ensure compliance with flexibility for authorization and authentication

OAUTH 2.0 | OIDC/SAML | MULTIPLE IDPS

Support for OAuth 2.0, SAML, OIDC, and multiple IdPs gives you flexibility and makes it easier to comply with requirements set by your organization, all the while eliminating the need to pursue costly workarounds.

Automate employee on-boarding and off-boarding

JUST-IN-TIME PROVISIONING

With direct sync to your identity provider, you no longer need to manually create new user accounts when someone joins the company.

Manage costs with automatic de-provisioning

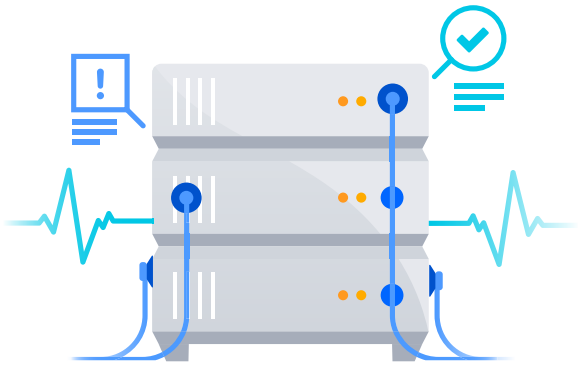
SCIM

By automating the de-provisioning process when people leave the company, you can ensure you're not billed for subscription licenses you don't need.

Reduce the risk of information breaches

SCIM

With automated de-provisioning, ex-employees' access is automatically removed when they leave the company.



Advanced auditing

Advanced auditing

Atlassian's advanced auditing capabilities give an organization the security-relevant digital record to demonstrate compliance, improve security, and better manage risk while enabling admins to have the level of visibility they need to monitor the state of the business.

The ability to audit has always been a staple for security and compliance teams. We've talked about the complexity that is inherent in enterprise systems, and how the larger the organization, the more intricate these systems will be. From a security standpoint, this means there are that many more points of vulnerability to monitor, maintain, and if necessary, cauterize. But it's not limited to security vulnerabilities; it's just as critical to align with potential business regulations, whether these are internal or externally mandated.

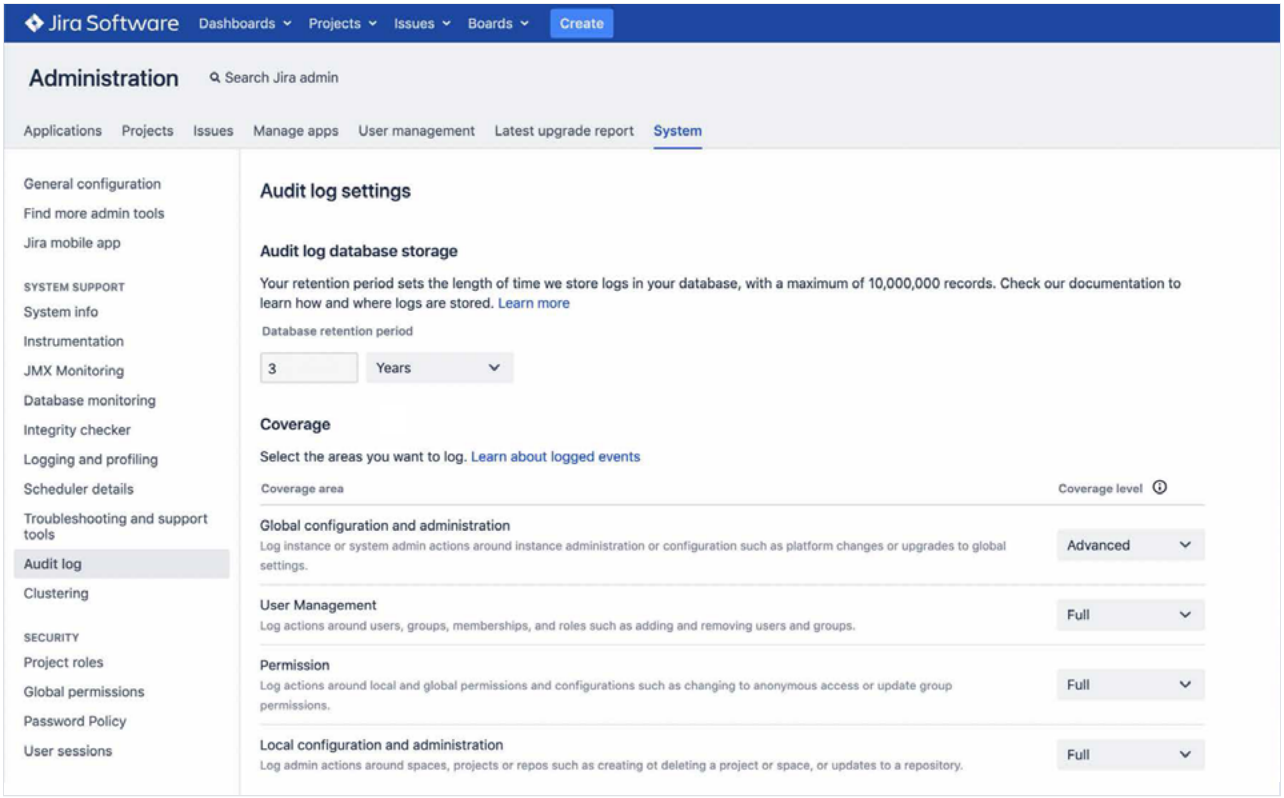
Atlassian Data Center's advanced auditing provides organizations with a security-relevant digital record to help increase security, demonstrate compliance, and improve visibility and workflow. Advanced auditing includes three primary components: extended auditing coverage, audit delegation, and file externalization. But how do these collectively improve the auditing process for enterprises?

Extended audit coverage

Increasing the range and volume of trackable events

With advanced auditing, we have revamped the breadth of audit coverage by increasing the range and volume of trackable events. These events vary slightly from product to product; however, there are a few key areas across core Data Center products.

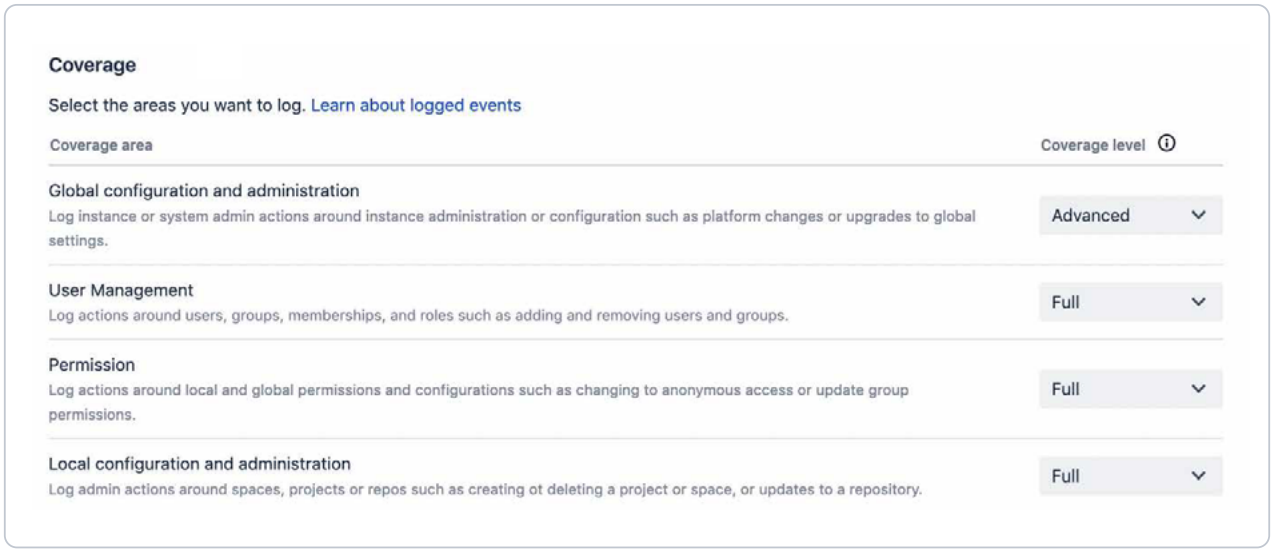
- **Global configuration/administration**
- **Security**
- **User management**
- **End user activity**
- **Permissions**
- **Apps**
- **Local configuration/administration**



Configurable log level

Customizable levels of trackable event coverage

Tracking every security and compliance-related event can be overwhelming, or even detrimental. To meet the varying workloads and needs of different enterprise organizations, admins can choose to opt-in to the following different levels of coverage:



To meet needs of different enterprise organizations, admins can choose to opt-in to the following levels of coverage

Off
Turns off logging events from this area.

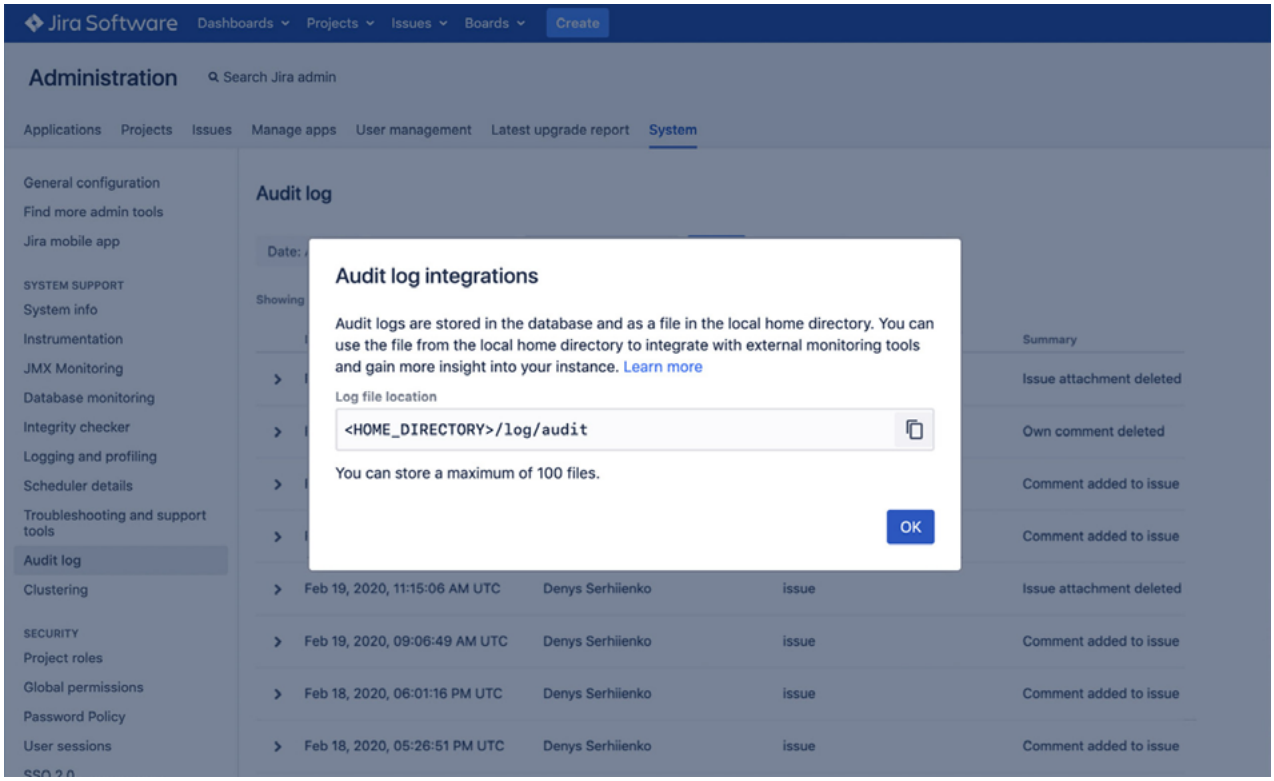
Base
Logs only the least frequent events to learn what's noteworthy.

Advanced
Logs the events that happen with medium frequency for an optimal amount of data.

Full
Logs all the events for a comprehensive audit.

Wondering about how this may impact your audit log storage and performance? You can also customize your database retention period. The database is intended for short term storage of audit logs and allows your admins the ability to quickly diagnose what's changed recently within their instance or projects. The database storage is limited by the retention period and is capped at 10 million records to ensure it does not cause any performance issues.

File externalization



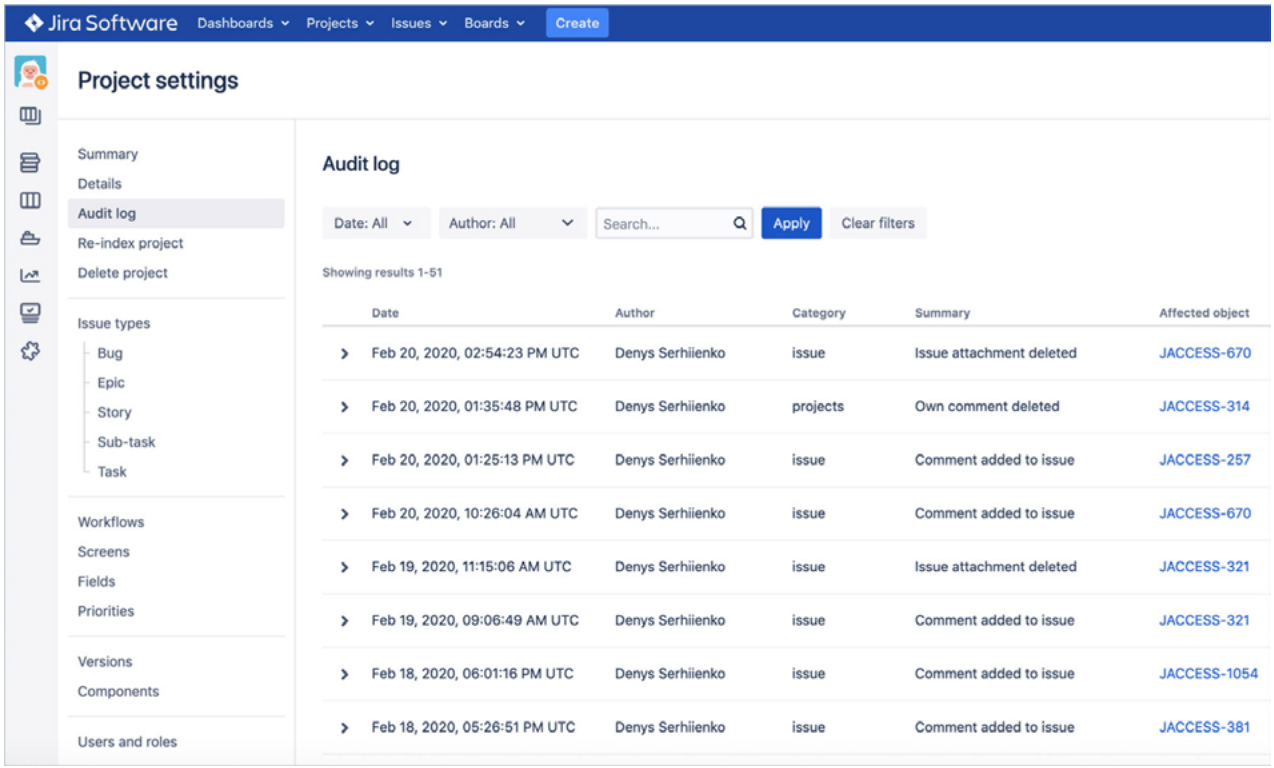
We think of the database as perfect for short-term storage. Depending on the product and the activity of the instance, database storage can last anywhere from a week to a few years. But what if there's the need for a long-term storage option?

Advanced auditing includes a capability, file externalization, which allows admins to integrate with third-party tools such as Splunk, Elk, SumoLogic, and Amazon CloudWatch. They can securely log events to a database and to a file in the local home directory, where they have the opportunity to sort, customize, and create reports; however they see fit.

This helps ensure a secure and tamper-proof record along with a long-term storage mechanism, and – depending on the tool – a solution that can help detect security anomaly patterns.

Audit delegation and visibility

The other capability, audit delegation, gives admins the ability to enable select users within an instance to view and analyze the audit log. With the ability to delegate auditing tasks, admins can reduce the time spent on simple requests, and unblock teams by giving them the visibility and agility needed to get their work done.



Use Case

Think about how frequent brute-force attacks are, or at the very least attempts. Repeated unsuccessful login attempts often can be an indicator that someone is trying to brute-force access your site. Now with advanced auditing, you can review security-related events, and identify threats. Being able to identify this in your logs allows you to prevent further attacks and take any necessary action.

Executive summary of advanced auditing capabilities

Data Center's advanced auditing provides a number of capabilities that help bolster the effectiveness of auditing for security and compliance purposes. It begins with extended coverage; widening the field of vision for potential vulnerabilities and giving admins the assurance that no stone is left unturned. This is supported by additional capabilities like configurable log level, file externalization, and audit delegation, so that the functionality does not exceed necessity, impede on performance, or take up the majority of the admin's time. With Data Center's advanced auditing capabilities, organizations are able to:

Speed up security processes with a more expansive forensic log

EXTENDED AUDIT COVERAGE

With increased audit coverage, organizations will have an improved forensic log to reference if there happens to be any security issue, increasing the speed for security breach investigations and helping them prevent them from happening in the future.

Help demonstrate compliance by tracking scheme changes

ADVANCED AUDITING

If an organization needs to ensure that schemes adhere to business rules or other standards, it's essential to be able to monitor changes to these schemes. The audit log can record changes to scheme related tracking and roles related tracking so it's easy to track down how someone got access to something.

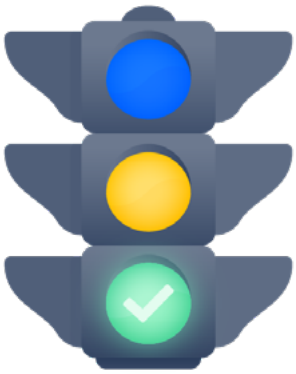
Keep security as a primary focus while not blocking teams

AUDIT DELEGATION

With the ability to delegate audit visibility, admins can allowlist or blocklist certain groups from seeing certain information, saving time, while also ensuring enterprise-grade security.

What is allowlist/blocklist?

Allowlist is the practice of explicitly allowing an identified entity or entities access to a service, mobility, access or recognition. Blocklist is the practice of explicitly denying an identified entity or entities access to a service, mobility, access or recognition.



Permissions

Permissions improvements

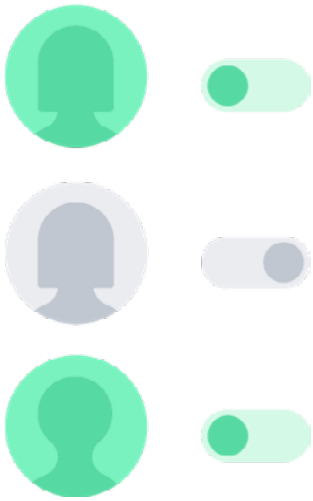
As more and more teams across an enterprise use Confluence as their single source of truth, there is a wealth of sensitive information that relies on the right permissions to be set in place for security to be effective.

We know many teams rely on Confluence to get their work done, too. We've had customers tell us of various use cases of Confluence, where they've customized their instance to serve as their organization's main workspace, a knowledge management tool, an internal intranet or wiki, or even for customer-facing documentation.

Regardless of how Confluence is being used, we know that the information that teams store in the Confluence instance can often be proprietary and highly confidential. Organizations need to be able to trust that the content stored in Confluence is secure and that the correct people have access to view or edit that information.

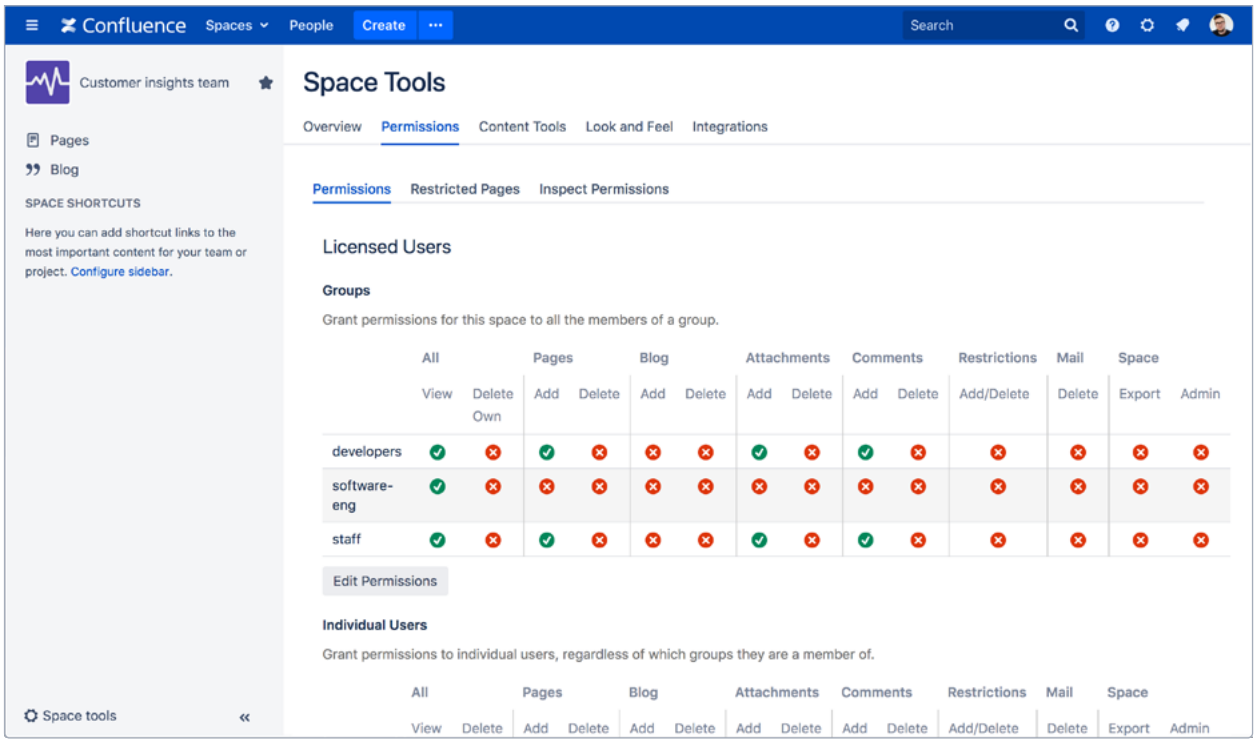
As we mentioned earlier in the handbook, enterprise teams are usually managing a long list of priorities, so keeping administrative overhead to a minimum is essential. Across industries, for admins of large Confluence instances, investigating permissions and creating audits for compliance reporting can be manual, time-consuming processes. With these advanced permissions capabilities in Confluence Data Center, teams can meet the security and compliance requirements that their enterprise organization demands in a more efficient manner.

Let's look at exactly how permissions is improving for Confluence.



Troubleshooting delegation

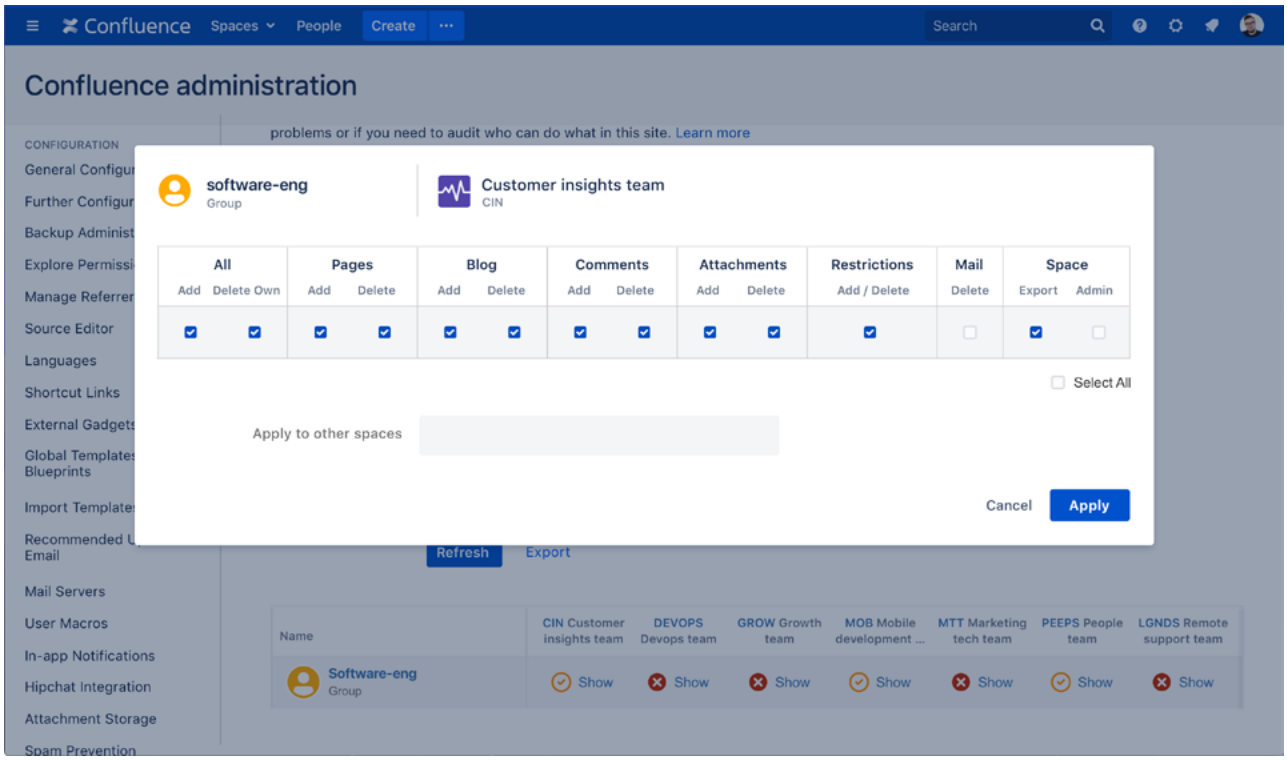
Troubleshooting can eat up a lot of a system admin or Confluence admin's time - which is why admins have the ability to delegate some of this administrative overhead. Space admins can investigate permissions, without having to rely on Confluence admins, giving them more control over their own processes while reducing requests on the other end. And this can be done on an individual or group basis.



As you can see, within the tool you are able to quickly and easily view permissions for groups (or individuals), making it a lot easier and efficient to troubleshoot.

Bulk editing

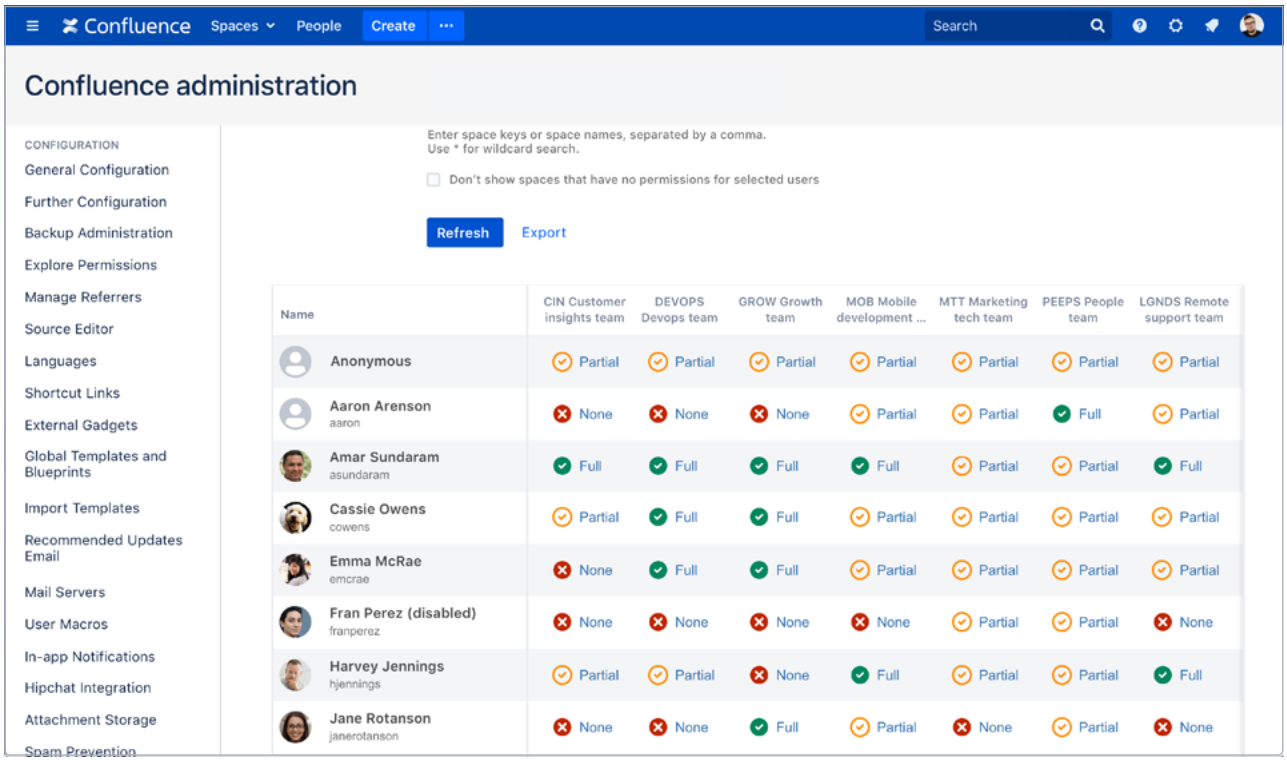
For enterprise organizations, we understand that certain processes can take longer because of the sheer quantity of actions involved. Permissions capabilities need to be scalable, which is why admins can bulk edit. Making bulk changes reduces the amount of time spent manually updating permissions in the future, and reduces potential errors in permissions management.



With bulk editing you can quickly and easily update permissions with a couple clicks of a button, and you can make these changes individually or at the group level. So you can go to and an individual user or a certain group, and simply edit and grant the permissions that individual or group requires.

Auditing permissions

Troubleshooting and bulk editing are great for when you need to identify or make changes to permissions – but what about when you need to provide a snapshot of access to your leadership or compliance teams or even an industry regulator?



The auditing permissions capability makes getting such a snapshot is a breeze. The permissions levels are all displayed in a table, as shown above.

- **Full** means the person has every permission, including the space admin.
- **Partial** means that the person has permission to view, and may have a number of other permissions.
- **None** means that they cannot see the space.

From this table, admins can verify that this information is what's needed and export these permissions as a .csv file for record-keeping purposes or for compliance reporting. This means no manual auditing and reporting! Admins can create, customize, and export these permissions reports whenever they need them.

As a reminder, all of these features are available in Confluence Data Center 7.3 and above.

Conclusion

Data Center can help you safeguard your people and information, meet or demonstrate compliance, and eliminate any potential friction through features that enable predictability.

Protection

There is a significant amount of sensitive information that flows through your Atlassian products every second of every day, and we can no longer limit this flow of information to strictly dev teams. As Atlassian usage in your organization grows, we've seen non-software teams adopt Jira or Confluence as a means to track, manage, and collaborate on their business goals. Company-wide objectives and sensitive projects need to be protected not only from external actors but within the organization to an extent by leveraging authorization and permissions; in 2018, more than a third of breaches involved an internal actor (Source: 2019 Data Breach Investigations Report, Verizon).

The bottom line is that managing security at scale is not a straightforward or static task – it's layered and always changing – and you need to have the confidence and capabilities to keep your products safe. Whether it's protecting valuable IP or the personal information of your employees, Data Center helps you uphold the security of your Atlassian products with capabilities that protect your people and data from harm.

Assurance

Adhering to compliance policies – whether they are internal or external – is something every organization is subject to, however, these regulations are often more strict for enterprise organizations. Complying with

such regulations can often come at a cost, whether it's from paying for specialized tools to achieve a workaround or paying regulatory fines. This is why our core Data Center products (Jira Software, Jira Service Management, Confluence, and Bitbucket) not only offer support for leading security standards but provide auditing capabilities that help make it easier to demonstrate compliance in other areas too.

Proof of compliance doesn't need to just be a "check the box" activity. These standards are established for a reason, and we all know that proof of compliance doesn't merely exist as an activity to mark as "done". Ensuring that your organization's IT tools are compliant and flexible in the event of future regulations can help prevent lost revenue, market opportunity, stock value, and give you the confidence that your systems are as safe as they can be.

Predictability

Change management encompasses a broad range of practices and processes to ensure that data is protected in the frequent event of change - such as people turnover, the deployment of new tools, or changes made to the instance. No organization is static, and this is compounded for enterprises who oversee a decentralized business, with a range of teams and tools spanning function, region, and even subsidiary.

All of these reasons make it complex to proactively and confidently manage change across the board and establish a system of predictability. However, with Data Center, you have access to features and support for your Atlassian products that make it easy to streamline your change management processes and enable a culture of foresight.

Ready to chat about whether Data center is the right fit for your organization?

Contact your local Atlassian Solution Partner for a custom consultation.

ATLASSIAN