ATLASSIAN

Taking a zero trust approach to IAM in Atlassian Cloud

Table of contents

Introduction

In a recent report, **51% of organizations increased security investments after a breach, with 32% citing increases in IAM security investments.**

Regardless of size or industry, your business must continually evolve its cloud identity and access management (IAM) strategy to keep pace with advanced threats and growing regulatory requirements. As your organization grows and expands in today's multi-cloud landscape, it is important that your IAM strategy is built on best practices that can scale.

Getting started with your IAM strategy doesn't have to be overly complex, you can take immediate actions to begin securing users in the cloud and continue to expand over time. Whether you're a global company starting a migration or a growing SMB with a cloud native footprint, we recommend taking a **zero trust** approach across your Atlassian cloud products with **Atlassian Access**. Extend your company-wide IAM policies and build a proactive defense strategy to protect your users and data in Atlassian Cloud.

Mapping out your IAM strategy in Atlassian Cloud

Because security threats are constantly evolving, there is no set it and forget it for your organization. Teams must constantly work together to shape and advance strategies and best practices. In this ebook, we'll cover common challenges our customers face based on their unique security needs, our recommended best practices, and how you can use tools in Atlassian Access to proactively defend against increasingly sophisticated attacks targeting your users and data. Atlassian Access is a single, organization-wide subscription that lets you enforce IAM security controls, like single sign-on (SSO), across all of your Atlassian Cloud products. Learn how admins have extended their visibility and created IAM policies to enable greater collaboration across their teams.

Scenario 1

Extending your IAM approach in the cloud

Complex enterprises are often on a multi-year cloud transformation journey. Piece by piece you're transforming your business and creating better processes to empower your teams. Setting stringent IAM requirements can sometimes feel like a blocker to this innovation, especially when time-constrained teams are responsible for quickly onboarding new applications and granting accurate access to users across numerous groups or departments. Starting a migration can also spark a lot of questions around parity in the cloud and whether or not your current IAM structure can be recreated.

To address these questions, it is important to have a clear understanding of your current footprint, your expected cloud IAM structure, and what your **shared responsibilities** will be in the cloud.

How we can address this

Empower user collaboration and improve processes for your administrators with Atlassian Access. All businesses have different security requirements, so we provide customizable IAM controls that can be paired with any cloud plan. With Access, you can accelerate your onboarding time and designate your IAM policies by user groups to meet your requirements.

Consolidate admin tasks in Atlassian Cloud with centralized user management through **admin.atlassian.com**.

To get the most out of Atlassian Administration, you can:

- Begin by **verifying your domain** and **claiming your users** to manage authentication settings.
- Gain additional visibility with **automatic product discovery**, this feature allows you to quickly scan and identify any unauthorized instances of Atlassian products across your organization. You can then bring these instances under centralized management to enforce consistent security policies.
- **Extend your current IAM policies** directly from your organization-wide identity provider (IdP) to give your users a secure, consistent log-in experience.
- Reduce the risk of compromised credentials by enforcing **single sign-on (SSO)** and **two-step verification** across all of your Atlassian Cloud products.

Once you've completed these steps, you can easily manage security policies, billing, and view audit logs all within Atlassian Administration.

> "Atlassian Access, coupled with Okta, has saved us so much onboarding and offboarding time. This was a painstaking process. Now, it's a dream. We never have to worry about access, the right groups syncing, or anything else. People just have access to Jira Software and Confluence on day one, and it works!

ERIC RAYMOND
Senior Manager of Business Technology, Castlight

Read the story:

How Castlight Health offloaded maintenance with Atlassian

Scenario 2

A more strategic approach to IAM for cloud native environments

For Atlassian customers starting in a cloud first environment, admins have the opportunity to evaluate their overall cloud security goals at the same time as they evaluate the Atlassian tools needed for their organization. Large, global organizations often accumulate a mixture of third-party and in-house applications. Over time it becomes difficult to manage secure access to all of these disparate applications, leaving the organization susceptible to attack due to inconsistent security controls and frequent password reuse. To reduce these risks, we recommend considering how users will interact with your data and each other across your cloud products. This will help you better map out authentication policies and processes that encourage collaboration in Atlassian Cloud.

How we can address this

Reduce the number of disparate processes and tools at your organization with Atlassian Access. From the centralized administration page, your organization can set authentication policies that apply to select groups of users across all Atlassian Cloud products. Further minimize risk with **SCIM provisioning and de-provisioning** to reduce overprivileged accounts and automate user lifecycle management. Connect Atlassian Access to your organization-wide directory so users who move to new departments or leave your company don't retain privileged access to your sensitive data.

Atlassian Access can address many of these challenges with features that support a comprehensive IAM security strategy. We recommend all admins evaluate these topics as part of their IAM planning:

- Determine how users within your organization will collaborate with external users in your cloud environment. Global organizations often need the flexibility to work with agencies, partners, and contractors that may be external to your managed users. Ensure secure interactions with your data by enforcing **external user security** settings on these collaborators.
- Evaluate Atlassian's Cloud Enterprise plan to see if it better suits the needs of your organization. **The Cloud Enterprise** plan includes Atlassian Access at no additional cost and unlocks additional IAM capabilities like our **multiple identity providers (MIdP)** feature - which gives an organization with several acquisitions or a complex identity footprint the flexibility to manage users across different identity providers. In addition to Access, Cloud Enterprise offers organizations Atlassian Analytics, multiple instances, and advanced admin controls.
- Assess how users will interact with your cloud products, including whether or not you'll allow them to access your data from their own devices and distributed locations to support flexible work. We believe collaboration helps teams be successful, empower your teams with the flexibility to securely access your cloud products using **mobile app management (MAM)**. MAM allows you to create and manage security policies across managed and personal devices without requiring any additional software downloads. This feature allows you to block screenshots, restrict data export, and require device encryption.

> "Atlassian Access is, for us, a mandatory required component. Otherwise, my employees will need separate access and entry points for each tool. That would reduce usability and cause security issues.

GARY CHAN
Head of IT Infrastructure and Employee Services, Zoom

Read the story:

Zoom surpasses growth goals with Atlassian cloud products

Scenario 3

Proactively defend against growing threats

Growing businesses need scalable, flexible security controls that can adequately protect them without adding to an already long list of administrative tasks. In a recent study, **59% of IT professionals reported SaaS sprawl challenging to manage**. Attackers are pinpointing scaling organizations as prime targets for attacks. Attackers often exploit vulnerabilities as organizations grow without advanced security controls aiming to capture overprivileged credentials. Once they have this information, they can easily navigate through your internal systems undetected. Proactively defend your growing business with advanced IAM controls that can be applied across your organization to simplify user management and security in Atlassian Cloud.

How we can address this

Many factors contribute to an organization's security requirements, as a result, businesses can be at different points of the security maturity journey. Atlassian Cloud is designed to grow with you as your organization builds its security maturity. Out of the box, we offer foundational security and visibility with **domain verification** and **user claim**. Verifying your domain proves you own it and allows you to manage users and products within the organization. Claiming users with your email domain gives you the flexibility to manage **authentication policy** settings like password requirements, session duration, and more.

As your organization's security requirements expand, you can designate multiple policies with varying levels of security controls based on the groups of users and the data they must access to complete their job tasks. Integrate directly with your organization's existing IdP to quickly onboard new Atlassian products, reduce manual user management tasks, and scale with your user base.

> "Atlassian Access is, for us, a mandatory required component. Otherwise, my employees will need separate access and entry points for each tool. That would reduce usability and cause security issues.

GARY CHAN
Head of IT Infrastructure and Employee Services, Zoom

Read the story:

Zoom surpasses growth goals with Atlassian cloud products

Scenario 4

Building processes to protect your highly regulated organization

Businesses across highly regulated industries and geographies, like healthcare, financial services, and government agencies, must take a look at their security approach through a different lens. Security isn't a nice to have, it is a requirements and failure to meet these requirements could have a significant impact on their reputation or finances. In fact, based on the size of your organization you may have different requirements to meet based off of geographical location, consumer rights, or sensitive data classification. To protect your business from threats and address your compliance requirements, you must take an approach to IAM that keeps your data secure, allows you to accurately report for compliance, and empowers your users with positive user experiences.

How we can address this

Manage access across all of your Atlassian Cloud products with Atlassian Access. You can customize **authentication policies** for managed and external users so each group of users is only given access to the products and data needed to complete their job tasks. This flexibility means your organization can work collaboratively across departments or agencies while adhering to IAM related compliance requirements.

74% of all breaches include the human element, either through error, privilege misuse, use of stolen credentials or social engineering. There's no question that a compromised account is a significant vulnerability for your organization. Proactively defend against the human element by implementing additional controls like customizing session duration to minimize an attacker's lateral movements with compromised credentials. Once the session duration limit is met, a user will need to re-authenticate to access your Atlassian cloud products. Your admins can add another layer of protection with API token management to control if a user is able to access your products with API Tokens and understand which users are currently using API Tokens across your Atlassian products. Finally, ensure accurate compliance reporting and gain reassurance that any risky behavior will be captured in your organization's audit logs. You can feed these logs into your organization-wide CASB or keep them for your records in accordance to your compliance requirements.

> Atlassian Access is a crucial component in ensuring enterprise-wide, regulated access management in the cloud. It's a significant advantage over our previous on-premise instances as we are able to apply security policies in a simplified way.

TIM BRUTSCHER
Enterprise IT Architect, Software AG

Read the story:

Germany's Software AG strengthens security and fosters innovation with Atlassian Cloud products

Rethinking IAM in the cloud

Securing access to your Atlassian Cloud products offers the opportunity to rethink how you structure identity to enable smoother processes, reduce manual tasks, and address compliance in the cloud. With Atlassian Access, you can take an approach to cloud IAM that addresses your IAM security requirements while enabling efficiency and collaboration. Learn more about Atlassian Access and how to improve IAM across your Atlassian Cloud products today.

Atlassian Access Setup Guide

ATLASSIAN