






# The Atlassian Guide to Cloud Identity and Access Governance

# Contents

<b>03</b>	<b>Introduction</b>
<b>04</b>	<b>Cloud Identity and Access Management: A Primer</b> Benefits of Cloud Identity and Access Management Getting Started with Cloud IAM Understanding the Cloud IAM Landscape
<b>10</b>	<b>Implementing Your Atlassian Cloud IAM Strategy</b> Centralize for a Single Source of Truth Integrate Access with Your Identity Provider Enforce Security Policies Monitor User Permissions and Activities Next Steps to Implement Atlassian IAM



## Digital transformation is overtaking organizations—both large and small—expanding their capabilities and opening doors to new opportunities.



The key to taking full advantage of this new digital world is facilitating collaboration within an organization. In order to make good decisions, the right people need to be connected to the right information—and quickly. Plans need to be shared, critical issues need to be elevated, and decisions need to be documented, stored, and easily findable.


And increasingly, all of this activity (and the data it produces) is happening in the cloud.

Unlike the old world where on-premises software was behind a firewall and organizations worked in just a handful of centrally managed applications, individual teams now adopt cloud tools that solve for specific business problems. Often, they're integrating multiple applications via APIs and spreading valuable—and sometimes sensitive—data across multiple software vendors.

This brings about the biggest challenge of modern IT: keeping your organization's data secure across a growing number of applications and endpoints.

Moving your organization's sensitive assets to the cloud requires different—and greater—control over which employees can access those cloud apps and services. This aspect of IT governance—cloud identity and access management (IAM)—is the key to overcoming the biggest challenge in digital transformation.

**In this guide, we'll discuss the important changes in IAM as organizations have moved to the cloud, including:**

- 
- How the approach to cloud IAM has been reconceptualized from on-premises solutions, and from tools to processes
  - The benefits of cloud IAM in terms of automation, productivity, and security
  - How to get started with cloud IAM and build a plan for change
  - How Atlassian cloud products work with your cloud IAM approach



# Cloud Identity and Access Management: A Primer

# Cloud Identity and Access Management: A Primer

## What is cloud identity and access management?

Cloud IAM encompasses the tools and processes for managing user identities and controlling access to both on-premises and cloud applications. The best cloud IAM approach provides a central place to manage user identities and works within heterogeneous environments, allowing access to any IT resource regardless of the OS platform, authentication protocol, location, or vendor.

## How is cloud identity management different from managing identity on-premises?

Cloud identity management has been reconceptualized from the original solutions of twenty years ago. Then, most IT resources were managed on-premises, behind the firewall, using one vendor's systems and applications (most often, that vendor was Microsoft). These systems were designed to manage a few applications, not hundreds. Now, they simply can't keep up with current IT demands.

By contrast, today's cloud identity management systems:

- are offered as SaaS products, integrating with different types of systems.
- can be accessed by multiple types of devices.
- allow you to unify your identity and access policies.
- are designed to keep up with constantly changing access requirements.

But managing user identity in the cloud world is not as simple as just implementing new cloud IAM tools and then mapping the migration path from your old on-premises systems. Beyond the new tools, you'll need to create new policies, update existing policies, and—most importantly—look ahead to where your organization is going, to make sure you're set up to support ongoing growth.

## Benefits of Cloud Identity and Access Management

- **Centralized management for heterogeneous environments**  
Identity management in the cloud replaces the patchwork of on-premises identity systems and tools, and works seamlessly with whatever resources are in the IT organization: macOS, Linux, AWS, web applications, WiFi—anything the organization decides is best for them.
- **Automate user provisioning and enforce security policies**  
Modern IAM solutions help you centralize user access management across on-premises and cloud environments. You can automate provisioning to streamline onboarding and, as employees and contractors exit the company, you can close off access immediately, ensuring security policies are followed.
- **Enforce contextual access management**  
Automate dynamic access decisions based on assigned risk factors beyond the user's assigned role, including location, network, device restrictions, type of request, and timing.
- **Increased productivity for end users as well as IT**  
With a single sign-on (SSO) provider (which should be a key piece of your cloud IAM approach—more on that later), users can easily find and log in to all their company apps from a single dashboard.



# Getting Started with Cloud IAM

If you're ready to make the move to the cloud and centralize your identity and access management, choosing an identity provider (IdP) solution isn't quite as straightforward as your average software purchase. You'll need to consider several key factors as you start your search:

## 1 Look ahead to the future.

Know where your organization needs to go, in terms of growth and scale, so you can ensure that your new IAM system will support your goals.

## 2 Consider where you're starting.

This will help you prioritize potential vendors to research. In most cases, IT organizations that want to migrate to the cloud fall into one of three categories:

- Currently using an LDAP directory system on-premises and want to move to the cloud.
- Using an existing Microsoft Active Directory (AD) installation and want to move to the cloud, often in order to manage a heterogeneous environment.
- Not currently using any kind of user directory to manage user identity.

## 3 Take stock of your current IT environments.

Note all protocols, platforms, and networks in your infrastructure, to ensure interoperability with your systems.

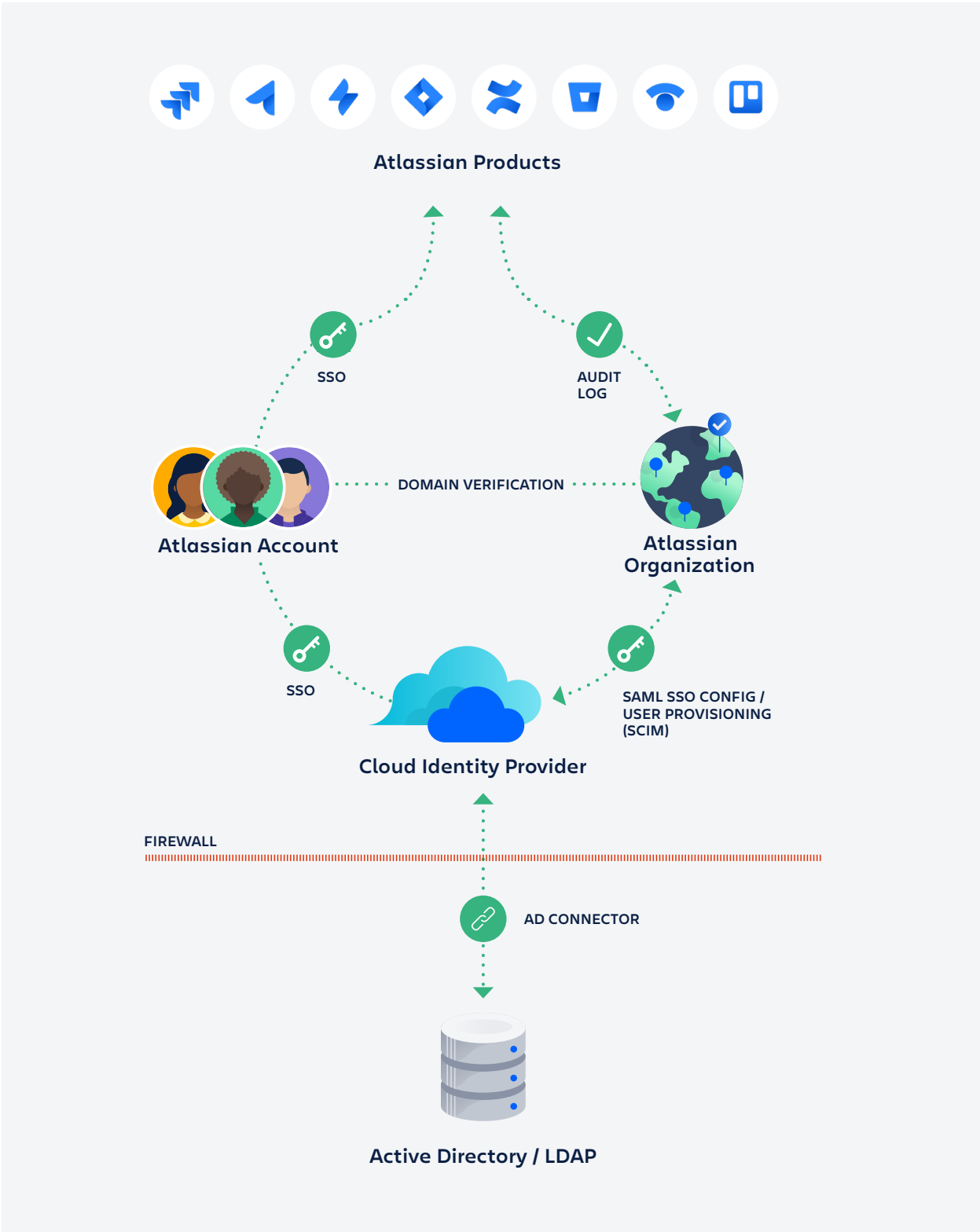
## 4 Inventory all vendor apps and SaaS tools, and determine which are critical to the business.

Know all the applications that you'll have to manage access to, especially as you start to develop a prioritized integration plan.

### A note of good news

When you're clear on your requirements and priorities, your search for the right mix of IAM vendor tools has a better chance of proceeding smoothly. What's more, since you're taking this IAM process to the cloud, you won't need to make significant long-term investments in new hardware or internal resources for managing security or patches. That work will be done for you by your cloud vendors.

# Understanding the Cloud IAM Landscape





Once you've selected your cloud identity provider (IdP), it's important to understand how it fits into the overall landscape of your on-premises and cloud applications. Here are some of the elements of that cloud identity landscape to consider:

- **Identify your profile master**

First, identify your profile master, the application that will be your single source of truth for users and groups. One option is to master your users and groups directly in your cloud IdP. Another option is to have users and groups mastered in your HR information system, like Workday.

- **Connect your cloud IdP to your on-premises directory**

In this diagram, we've defined the source of truth for profile masters as an on-premises Active Directory or LDAP database. In this case, you need to be able to connect your cloud-based IdP to your directory service hosted on your network.

All the major cloud IdPs provide agents or connectors that work within your corporate network to facilitate syncing between the cloud IdP and the users and groups in your Active Directory or LDAP server, your single source of truth. If you have Active Directory or LDAP in your on-premises system, you can still use it to manage identity and access with your on-premises applications.

- **Authenticate to cloud apps via your cloud IdP**

For applications that are in the cloud, you can connect them to your cloud IdP, and your users can access and authenticate to those applications from the public internet, via protocols like SAML single sign-on (SSO).

- **Manage user access to Atlassian applications via your cloud IdP and SSO**

Your cloud IdP can also provide SSO authentication between Atlassian Organizations and the IdP via SAML SSO using their Atlassian account. When users access Atlassian applications, like Jira Software Cloud, via their Atlassian account, they are redirected to your IdP to log in.

- **Provision new Atlassian users via your cloud IdP**

Similarly, you can provision users and groups that exist in your cloud IdP (that originally synced from your local on-premises Active Directory) to your Atlassian Organization. Then, those groups are passed downstream to the applications that you've linked to your Atlassian Organization, keeping identities in sync.



# Implementing Your Atlassian Cloud IAM Strategy

# Implementing Your Atlassian Cloud IAM Strategy

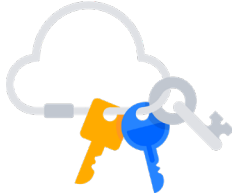
Here at Atlassian, we went through our own digital transformation, so we understand all the likely pain points your organization may encounter as you make this transition.

We've set up a framework of best practices that helped us—and our customers—overcome some of the issues IT teams face when it comes to collaborating across an organization at scale—while keeping all the right security protocols in place.

In this framework, we've set up guidelines that help you:



**Centralize**  
your user identity management in a single source of truth.



**Integrate**  
your applications with your primary identity provider for greater security and efficiency.



**Enforce**  
2FA or password policies if you don't have an identity provider already doing so.



**Monitor**  
user access, permission, and audit logs regularly.

# Centralize for a Single Source of Truth



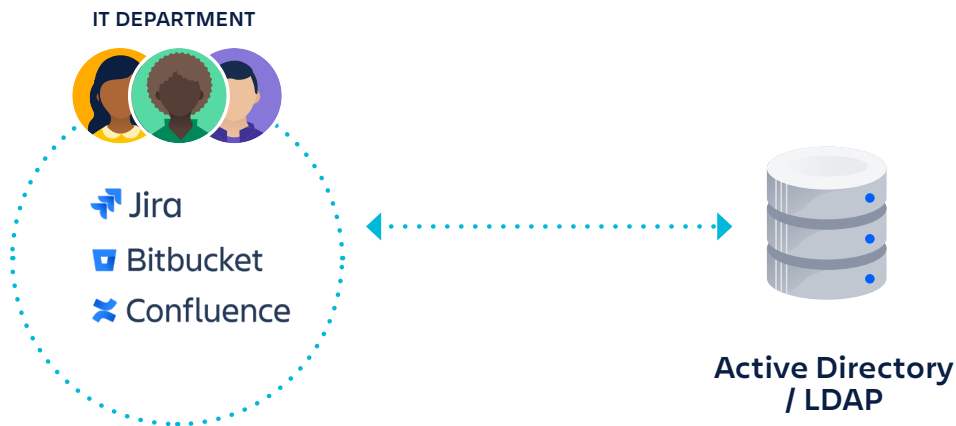
## Enforce policies and control costs with centralized identity management and access

Atlassian cloud products—like Jira Software, Jira Service Desk, Confluence, Bitbucket, Trello, and Opsgenie—typically see a “bottoms-up” adoption within companies, just like many other SaaS apps. Subscriptions are purchased by departments, bypassing IT procurement—and the security and privacy vetting process. In order to control costs and enforce policies, IT administrators need to centralize the management of all of these cloud applications in one system.

## Atlassian server world vs. cloud world: Different concepts in identity and access management

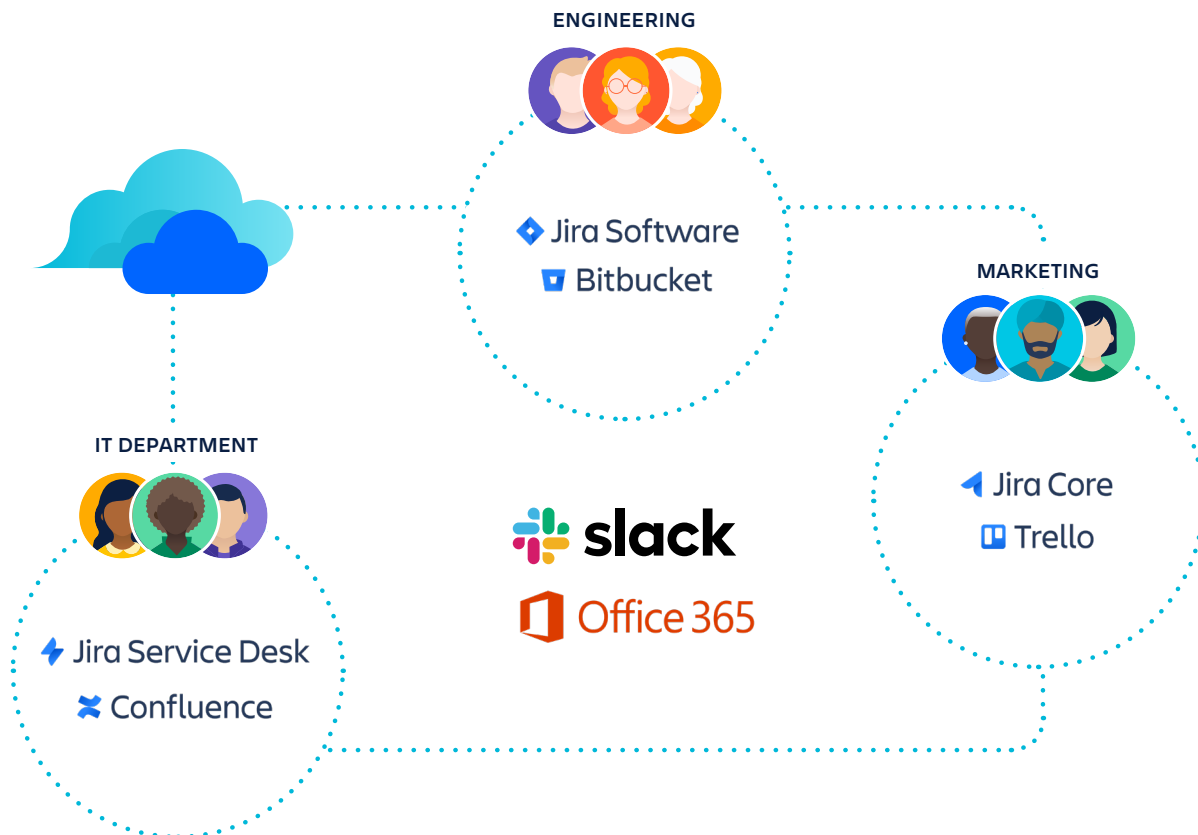
Here’s a comparison of what identity and access management look like in a typical on-premises Atlassian server world, and in an Atlassian cloud world. You’ll notice the data integrations among the applications look different in the server world compared to the cloud world, and the concept of identity management differs, too.

If Atlassian products are being used on premises, the landscape looks like this:



You have one “company” instance of each product, managed by the IT department, and all are connected to your corporate Active Directory or LDAP directory, two of the most common means of managing user identity.

With the cloud, achieving the same level of governance becomes complicated. You may have multiple departments using their own instances of cloud products. The IT department may have its own Jira Service Desk and Confluence applications, and the engineering department has its own instance of Jira Software and a Bitbucket repository.



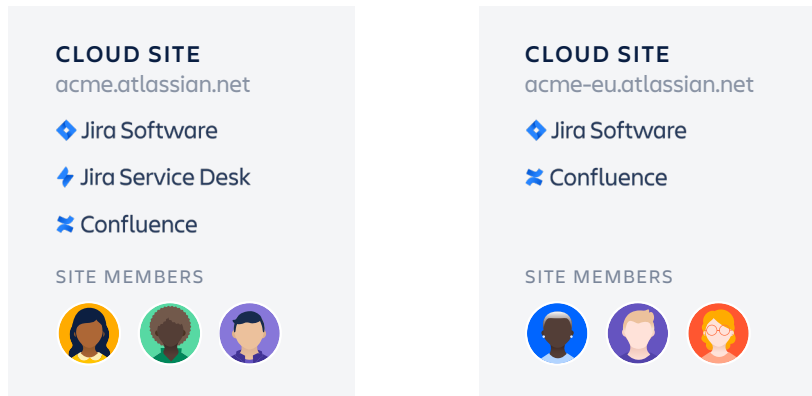
Meanwhile, you discover that folks over in the marketing department have adopted Trello. And the whole time, you’ve also got teams using tools like Slack and Office 365.

Just who are all these people and what do they have access to? When you have so many unmanaged applications in use, it’s impossible to know.

Additionally, in the Atlassian cloud world, users have a single account, one per email address. Each user has one company identity and one password—and only has to set up 2FA once, whether it’s for a Jira Cloud instance or a partner’s Confluence instance. This means an administrator has to manage only one set of credentials per user, and each user can access all Atlassian cloud products with one set of credentials, greatly simplifying identity management for everyone.

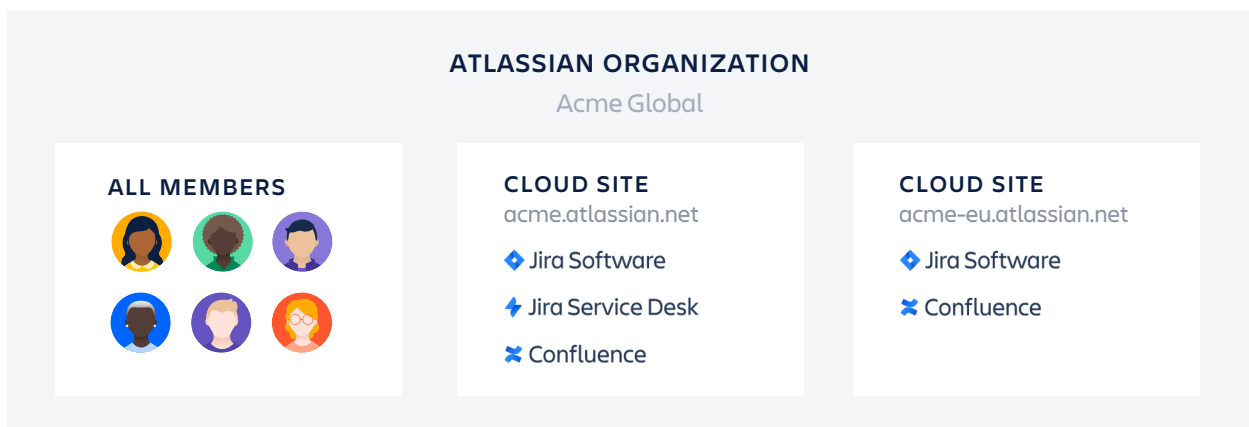
## View and manage all users across your company with Organizations and domain verification

You might be familiar with **Sites**, a concept that we use for the Jira and Confluence family of products that allows you to manage access to the different products and share groups and other settings across the site. When you set up your Jira or Confluence instance, you can name your site, and that generates the URL that you use to access your instance.



Within a single organization, different teams could be using multiple Atlassian cloud products and sites. A team in San Francisco could be using Jira Software on one site, while the team in the New York office could be using Jira Service Desk on a different site. And engineers across the globe could be using their individual Bitbucket accounts to store their code. As an administrator, you need one place where they can see all the Atlassian cloud users across their organization, regardless of site or product.

To enable managing multiple Atlassian cloud products and sites in one place, we've created a new global administration layer for Atlassian cloud products called **Organizations**.



Organizations give you a unified view of all the users of Atlassian cloud apps in use at your company.

And since you might have more than one site, we created a new destination that brings Organizations together, called Atlassian Admin Hub, or [admin.atlassian.com](https://admin.atlassian.com).

Under the umbrella of an Organization you can begin managing all of the users in your organization across the cloud versions of Jira Software, Jira Service Desk, Jira Core, Confluence, and Bitbucket through a process called **domain verification**.

Once you verify the ownership of your domain, you'll begin managing every single user with an email address at your domain that Atlassian knows about. We call these managed accounts. As an Organization admin, you'll be able to export, change, deactivate, and delete these managed accounts. You'll also be able to enforce **Atlassian Access** security policies across your managed accounts.



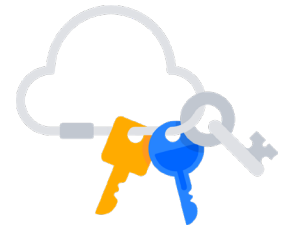
#### **INSIDE ORGANIZATIONS: CENTRALIZED USER MANAGEMENT FOR YOUR CLOUD PRODUCTS**

Once you set up your organization, you will find tools that can help you manage products and users:

- **Directory:** Includes a list of accounts you manage, assuming you've [verified your domains](#). It's also where you can connect your identity provider for user provisioning. [Learn more](#)
- **Security:** Get more control and security features when you [subscribe to Atlassian Access](#), giving you the full benefit of organizations. [Learn more](#)
- **Settings:** Update your details, make a user an organization admin, add another domain, and create an API key. [Learn more](#)
- **Sites and products:** See all the products you use and their sites, where you can administer users and update groups and product access. [Learn more](#)

In addition to administering your Organization from the admin site, you can use the [Organization REST API](#) to retrieve details about your organization, such as all of its users and domains.

# Integrate Atlassian with your Identity Provider



## Enable SSO for increased security and simplified login for end users

The single most important thing you can do to secure user accounts is to set up SAML single sign-on, or SSO. You can make sure that every user is logging in and meeting your requirements for strong passwords and multiple standards of authentication, and you can ensure they're logging in from approved locations and devices—all via your SSO provider.

When you use a cloud IdP for SSO, you can go further than just controlling authentication. You can also control who has access to which data. You can assign levels of permissions to individual users, not only for your Atlassian cloud products, but for all of your SaaS applications.

## Support for top identity providers, with more to come

Atlassian cloud products, with a subscription to Atlassian Access, supports five of the most common identity providers, as well as setting up a custom SAML connection with any identity provider not listed below. With an IdP, you can ensure that all Atlassian product usage is going through an authentication endpoint that you control, and it takes you one step closer to achieving your security requirements.



### GET STARTED WITH SAML SINGLE SIGN-ON

To set up SAML single sign-on for Atlassian cloud products, create your Organization, verify your domain, and then start your trial of [Atlassian Access](#). You can then follow these instructions for setting up [SAML single sign-on](#).



## Automate user lifecycle management with user provisioning (SCIM)

As your company grows and you have more people in your systems, it makes sense to move from manual provisioning to automated, policy-driven access management via your IdP. This gives IT a centralized view into the permissions assigned to each user, and it allows you to automate user provisioning and de-activation, and automatically assign rules based on user or group attributes that determine who has access to which applications.

To facilitate this user provisioning, we use a protocol known as SCIM. It allows you to manage user identities with an IdP like Okta, Azure AD, or Onelogin, and then sync those details to your Atlassian products. For example, you can assign a user to Atlassian applications in Okta, and Access will automatically detect changes and sync them to Jira or Confluence instances that you choose.

### Benefits of user provisioning

- **Automates employee on-boarding and off-boarding**  
With direct sync to your identity provider, you no longer need to manually create user accounts when someone joins the company.
- **Manage access and permissions**  
You can control an individual's access to Jira projects and their ability to see certain dashboards or filters. You can also view and edit Confluence pages with groups synced from your identity provider.
- **Manage costs with automatic de-provisioning**  
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.
- **Reduces risk of information breaches**  
With automated de-provisioning, ex-employees' access is automatically removed when they leave the company.

## Sync users and groups to your Organization

This diagram illustrates how users and groups sync once you set up user provisioning. After you connect your IdP to your Organization, the users and groups within your IdP are synced to your Atlassian cloud products.

- Users and groups sync from your IdP to your Organization, creating a directory of your provisioned users.
- Your company's directory syncs to all associated sites, providing access to your provisioned users and groups.
- Groups are assigned to products, granting users within each group default product access.



### GET STARTED WITH USER PROVISIONING AND LIFECYCLE MANAGEMENT

To set up user provisioning for Atlassian cloud products, create your Organization, verify your domain, and then [start your trial of Atlassian Access](#). You can then follow these instructions for setting up [user provisioning](#).

# Enforce Security Policies

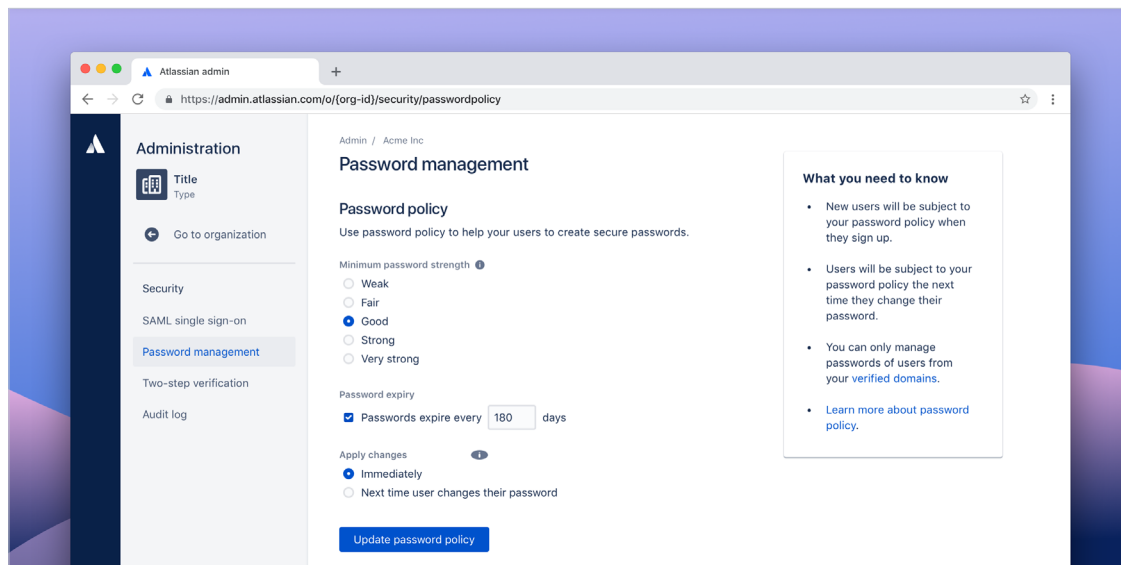


## Secure your account with two-step verification

Most major identity providers manage two-factor authentication (2FA). But if you don't have a cloud IdP, you can use Atlassian Access to set this up and manage users with an Atlassian Organization. Two-step verification adds a second login step to your managed users' Atlassian accounts, requiring them to enter a 6-digit code in addition to their password when they log in. The second step helps keep their account secure even if the password is compromised. When account logins are secure, your organization's products and resources are safer.

## Enforce strong password policies across all users

In the case that you're not using an IdP to enable SSO, Atlassian Access can also help you enforce stronger password requirements across all of your users. Password policies help ensure that the people accessing your Atlassian cloud products are using best practices when creating passwords. This helps reduce the risk of security breaches.

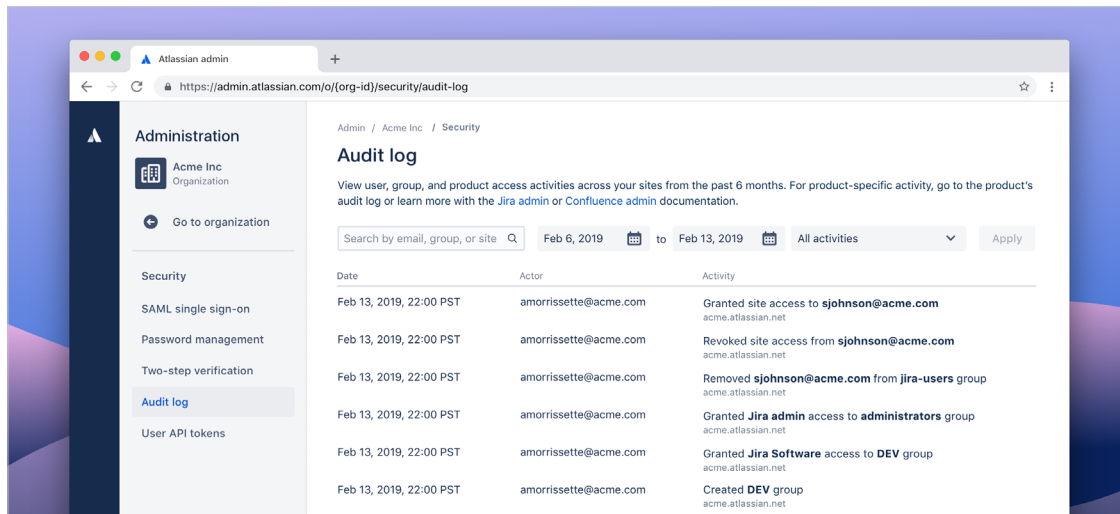


### GET STARTED WITH BEST PRACTICES FOR SECURING YOUR ACCOUNTS

To begin enforcing two-step verification and password policies across your Atlassian cloud products, create your Organization, verify your domain, and then [start your trial of Atlassian Access](#). You can then follow these instructions for setting up [enforced two-step verification](#) and [password policies](#).



# Monitor User Permissions and Activities



## Track memberships, activity, and permissions in one place with audit logs

Audit logs are a primary means of proving compliance with various regulations and internal policies. With Atlassian Access, you can now get Organization-wide audit logs for increased visibility into user and group changes across your Jira and Confluence products. These audit logs allow you to view details, including who made changes, user and group memberships, who granted access to these different groups, and more.

With an Atlassian Organization, admins can also view who has access to API tokens, including who created the token, the number of tokens created, and the last access to a token. Administrators also have the ability to revoke a token.

With these insights inside your Atlassian Organization, you have a comprehensive and documented view of who has access to your data, which can simplify investigations into changes and help prove compliance.



### GET VISIBILITY INTO WHO HAS ACCESS TO YOUR DATA

To view audit logs across your Atlassian cloud products, create your Organization, verify your domain, and then [start your trial of Atlassian Access](#).

## Next Steps to Implement Atlassian IAM

- 1 **Create** a plan that outlines your organization's goals for growth, so you can prioritize requirements for your new IAM system.
- 2 **Investigate** IdPs and the identity and access landscape, and determine the types of tools you'll need.
- 3 **Identify** new or updated policies you'll need to implement.
- 4 **Choose** your IdP and accompanying cloud applications to complete your IAM plan.
- 5 **Create** an Organization for your Atlassian cloud products and claim your domain.
- 6 **Subscribe** to Atlassian Access to apply security policies.
- 7 **Integrate** Atlassian Access with your identity provider for SSO and user provisioning.

Learn more about how [Atlassian Access](#) gives you company-wide visibility into your Atlassian cloud applications, plus unified user and policy management, enhanced security, and simplified user lifecycle management. [Start your 30-day free trial.](#)

### ADDITIONAL RESOURCES

#### [Webinar: Secure and scale Atlassian in the cloud](#)

Empower your team with collaborative tools and enhance the security of your company data. In this webinar, you'll walk away with a clear understanding of the Atlassian cloud identity and security landscape and learn key strategies to enhance security and streamline processes for user management.

#### [Blog: 7 non-negotiable practices for any cloud product](#)

Implementing security best practices for your cloud products might feel like you're playing a game of chess against a chess grandmaster. You think you need to know the most complex strategies and plan ten moves in advance, but in reality, you're playing against a 3rd-grade checkers player.

#### [Documentation: Follow cloud security best practices](#)

Use these best practices to create a strong foundation for securing your company's most important work.

