ATLASSIAN

# User Management Feature Guide

Easily manage users at scale and keep your products secure with Atlassian Data Center

# 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 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**

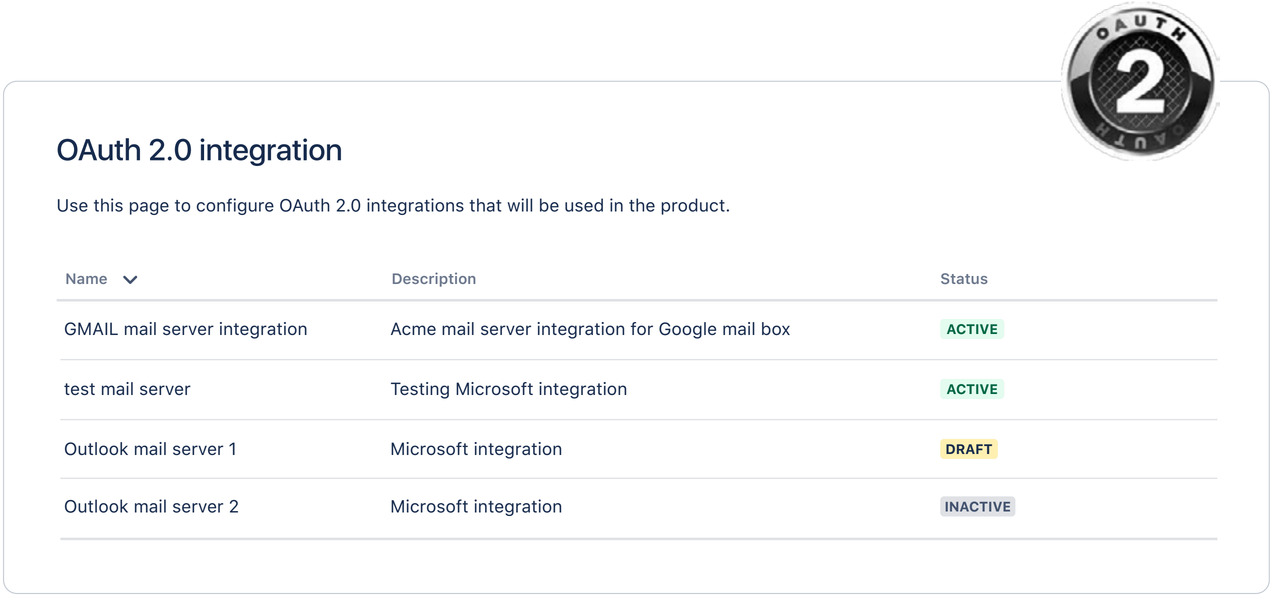
**Support for System for cross-domain identity management (SCIM)**

# 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).



OAuth 2.0 integration

Use this page to configure OAuth 2.0 integrations that will be used in the product.

| Name | Description | Status |
|---|---|---|
| GMAIL mail server integration | Acme mail server integration for Google mail box | ACTIVE |
| test mail server | Testing Microsoft integration | ACTIVE |
| Outlook mail server 1 | Microsoft integration | DRAFT |
| Outlook mail server 2 | Microsoft integration | INACTIVE |

# 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

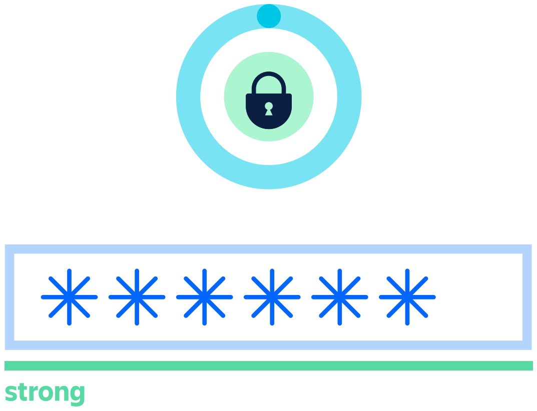
**Don't see your IdP in the list? Don't worry, you can also set up a custom SAML or OIDC connection.**

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.

## Ready to chat about if Data Center is the right fit for your organization?

## Contact your local Atlassian Solution Partner for a custom consultation.

ATLASSIAN