ATLASSIAN

Secure, but practical

Why organizations are embracing multiple authentication policies

Table of contents

For the 94 percent of organizations today that use the cloud, the ability to set and forget company-wide authentication policies can be a reassuring defense against data theft. And they're right to feel secure: according to Google, simply implementing two-factor authentication can protect individuals against 96 percent of bulk phishing attacks. But if an organization's policies are too strict–requiring users to use two-factor authentication every time they access their email, for instance–they can quickly bring down employee productivity.

While data security is a strong priority, it shouldn't be the only factor administrators consider when setting authentication policies. Some authentication settings are stricter than others, and not everything needs to be behind 18 dead-bolted doors. If you set just one policy for your whole organization, you could be forced to choose between slowing down your teams or leaving sensitive data unguarded. The solution? For large organizations, setting up multiple authentication policies allows you to keep data secure without putting hurdles in teams' way.

The benefits of multiple authentication policies

According to LastPass, the typical employee will reuse the same password an average of 13 times across separate applications. Considering that over 80 percent of security breaches today involve stolen and reused credentials, that's a scary thought. Compound that risky habit across the hundreds of employees at a company, and it's little wonder that over 30 billion credential stuffing attacks take place a year. Fortunately, by requiring users to independently confirm their identity, flexible authentication settings can block most credential stuffing attacks—while also keeping teams' to-do lists ticking along.

Credential stuffing attacks

Cyberattacks carried out by computers or people attempting to log in using stolen or generated credentials.

Setting up multiple authentication policies allows administrators to set up customized policies for specific subsets of users, including different teams, full-time employees, contractors, and outside partners. This allows organizations to take a Goldilocks approach to setting the right authentication policy for their users—rejecting an all-encompassing "too hot" or "too cold" authentication policy for multiple, unique policies that are "just right."

Authentication settings

There are a wide range of available authentication methods out there. When creating authentication policies, admins can mix and match multiple settings depending on their needs.

Username and password requirements dictate the minimum strength a user's password must meet, as well as how often their password will expire.

Single sign-on (SSO) allows users to use a single username and password to access various applications without having to re-enter authentication factors.

Multi-step verification requires that users confirm their identities using more than one 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.

Biometrics confirm a user's identity through one of their unique biological characteristics, such as a fingerprint, face, or retina. Most mobile phones today feature fingerprint and face scanners, which can be used to unlock phones or apps.

Risk-based authentication settings will prompt users for additional authentication depending on the risk level detected at login. A system might prompt a user to confirm their identity via email if they've entered their password incorrectly several times or if they're logging in from an unfamiliar IP address.

Session duration settings dictate how long a user can remain idle before they're automatically logged out of an app. This can protect organizations from data breaches in the event that a user steps away from their device.

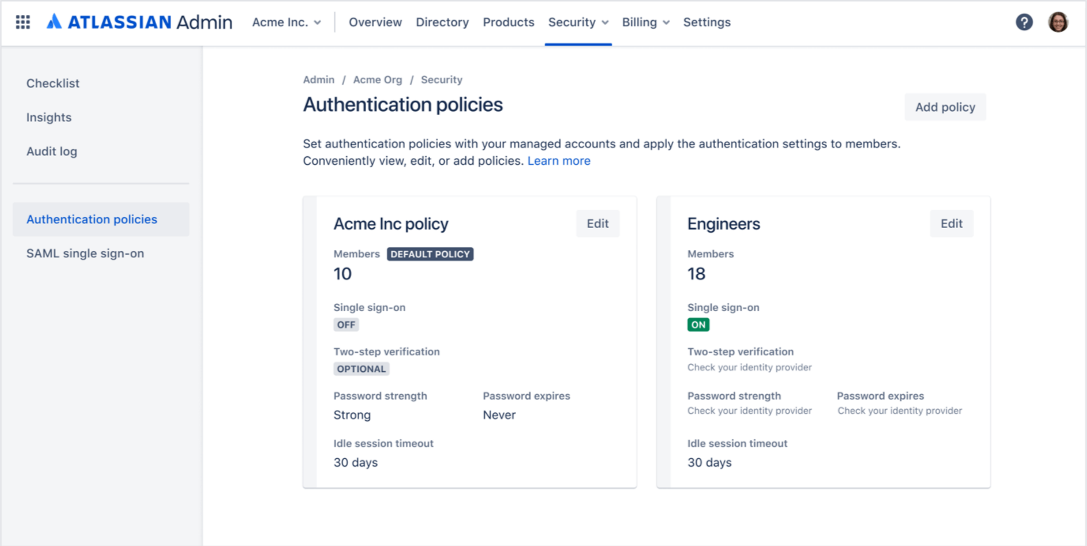
How to craft different authentication policies

There are three key factors to keep in mind when custom-building an authentication policy: the sensitivity of the data being accessed, who's accessing the data, and the lowest acceptable ease of use.

Explore the questions below to ensure authentication policies strike the right balance of safe yet practical.

1. **The sensitivity of the data being accessed**: How confidential is the data? Does it contain intellectual property, confidential personnel information, or customers' personally identifiable information?
2. **The risk introduced by the users accessing the data**: Are the users full-time employees working out of the office or contractors who may be working from a coffee shop? Are they working on corporate-issued devices or their personal laptops?
3. **The lowest acceptable ease of use**: How frequently are these users accessing this app? Do they use it hourly, daily, weekly, or monthly? How will potential authentication settings impact their day-to-day workflow?

An organization may choose to assign policies by team or by employee type (such as full-time employees, contractors, or outside partners). Other businesses may choose to mix and match, depending on their needs.



Admin / Acme Org / Security

Authentication policies

Set authentication policies with your managed accounts and apply the authentication settings to members. Conveniently view, edit, or add policies. Learn more

Acme Inc policy

Members DEFAULT POLICY
10

Single sign-on
OFF

Two-step verification
OPTIONAL

Password strength
Strong

Password expires
Never

Idle session timeout
30 days

Engineers

Members
18

Single sign-on
ON

Two-step verification
Check your identity provider

Password strength
Check your identity provider

Password expires
Check your identity provider

Idle session timeout
30 days

An online retailer’s HR team, for instance, likely deals with confidential employee information (highly sensitive data). They may occasionally work remotely, but they’re mainly office-based and work solely on corporate devices (low user risk). And since they’re managing current employees and reaching out to new prospects daily, they constantly rely on their multiple tools to get their work done (high app use).

In this case, it would make sense to assign the HR team to an authentication policy that relies on strong password requirements, single sign-on, and a shorter idle session duration. The stringent password requirements would keep data safe from virtual attacks, and a shorter idle session duration would ensure sensitive data wouldn’t be exposed if employees stepped away from their desks. Single sign-on capabilities, on the other hand, would allow HR employees to easily log back into their myriad tools by logging in just once.

The marketing team at that same online retailer, however, might have different authentication requirements. A core group of in-house employees may use corporate devices, while remote contractors work on their own devices. Both, however, rely on a wide variety of tools daily and work on a mix of less sensitive and more confidential projects.

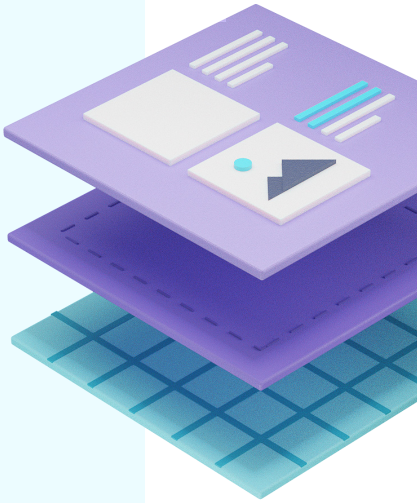
In the marketing team’s case, it might make sense to create two authentication policies: one for in-house employees and one for contractors. The authentication policy for employees could include strong password requirements and single sign-on, allowing users to move through their daily workflow unhindered. However, since contractors work on personal devices outside of the office, their policy would likely also include two-factor authentication, adding an extra layer of security as they access the organization’s system externally.

How Canva manages cloud security for its global team

With a team of over 1,000 employees and contractors spread over multiple offices, Canva relies on Atlassian Access to keep its data safe while ensuring everyone has access to the information they need.

Canva uses external identity provider Okta to sync different groups of users to Atlassian cloud. HR teams are subject to a stringent set of security measures to protect confidential employee information. New employees are given permission to view a restricted set of systems and documents a few days before they start at Canva, and the company uses Access to enforce SAML SSO to give contractors secure access to their systems.

“They aren’t able to see anything but the documents we send them because access is restricted through user group access mapping,” says Jeff Lai, Canva’s Internal Infrastructure guru. “There’s a high level of security measures in place.”



Test authentication settings before rolling them out

Of course, as companies grow and evolve, so do their security needs. With multiple authentication policies, you don’t have to change the whole company’s access at once. Test new security settings in small groups before rolling them out to everyone else.

In smaller trial groups, admins can easily test:

- Single sign-on for admin test accounts, allowing admins to log in and troubleshoot any configuration errors
- Idle session duration in order to new meet company or industry regulations
- Two-step verification on a test group of users to ensure it’s set up correctly

Customer use case

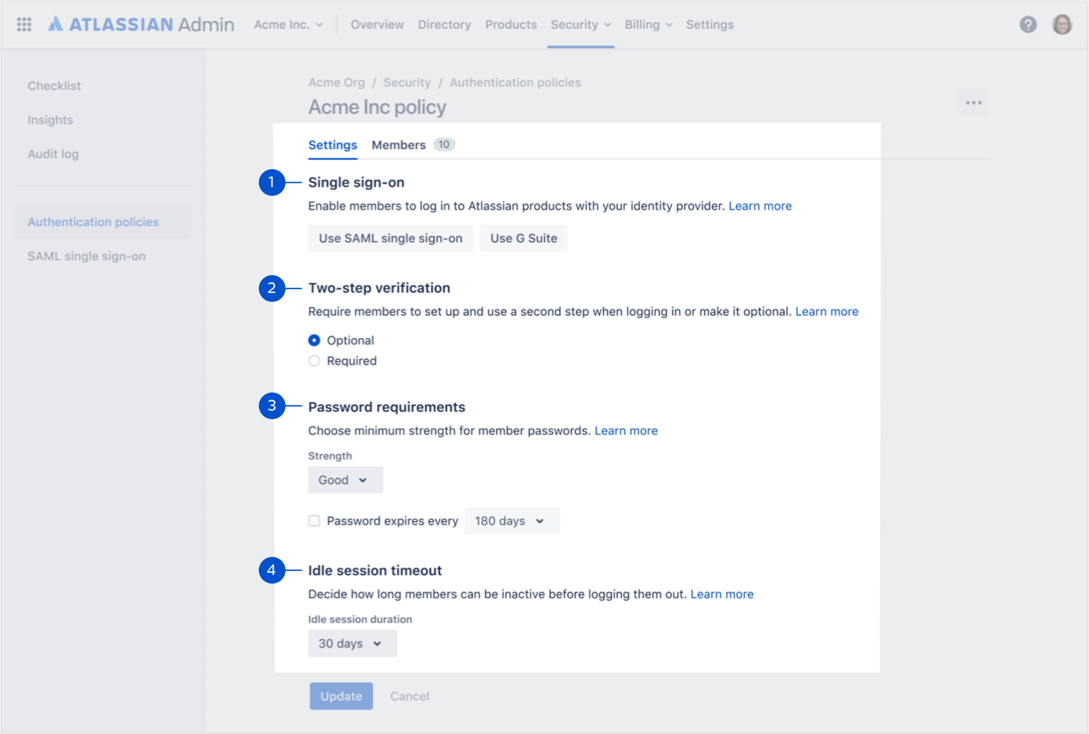
One global enterprise technology company created a separate authentication policy in Atlassian Access to test and enable single sign-on company-wide. This not only allowed admins to try out the process ahead of time, but ensured they had a simple rollback plan if it was configured incorrectly.

Custom-build unique authentication policies with Atlassian Access

With Atlassian Access, admins can set up to 20 unique authentication policies for their organization. For organizations that use multiple Atlassian cloud products, Access's user-based authentication policies allow admins to set policies by user so that their policy remains the same regardless of the product they're using.

> Wow! This is fantastic. It's going to save me–and you–a lot of time and give me much greater control over access to the system. It works a treat.
>
> **ORGANIZATION ADMIN**
> at an enterprise financial company

When you get started with Atlassian Access, you can sync your external identity provider to Access to automatically add all users from your managed accounts to your default policy. Then, as you build out policies for different subsets of users, you can reassign users to their respective groups.



Acme Inc policy

1 Single sign-on

Enable members to log in to Atlassian products with your identity provider. Learn more

Use SAML single sign-on | Use G Suite

2 Two-step verification

Require members to set up and use a second step when logging in or make it optional. Learn more

● Optional
○ Required

3 Password requirements

Choose minimum strength for member passwords. Learn more

Strength: Good

□ Password expires every 180 days

4 Idle session timeout

Decide how long members can be inactive before logging them out. Learn more

Idle session duration: 30 days

Within Access, you can set the following authentication settings:

1. Security Assertion Markup Language (SAML) single sign-on: Allow users to authenticate into Atlassian cloud products using your organization's existing identity provider. Don't have one currently? Access customers can use Okta's leading cloud identity management software with Atlassian products at no cost.

2. Two-step verification: Require that users use two-step verification to access Atlassian cloud products.

3. Password requirements: Set password strength and expiration requirements.

4. Idle session timeout: Set the amount of time a user can remain inactive before Atlassian automatically logs them out.

Get started with Atlassian Access

Operating in the cloud does bring unique security challenges with it. However, with the right solution, organizations can improve not only their security but their overall operations–keeping teams productive, collaborative, and secure. To learn more about Atlassian Access and how it can boost your organization's security, contact us. If you're ready to give Atlassian Access a test run, start a free 30 day trial today.

> We've been able to improve our level of security with the integration of our SAML/SSO provider (Okta) and Atlassian Access.
>
> **JOSH COSTELLA**
>
> Senior Atlassian Solutions Specialist at Nextiva

ATLASSIAN