

Identity and Access Management in K-12 for Beginners

Every student is different. One might like math while another likes reading. One may learn best with an interactive game instead of verbal instruction. One may struggle with certain subjects due to a disability.

If devices are meant to enhance learning, they need to adapt to a learner's needs. If every student picks up a shared iPad that is a carbon copy of their friend's, despite being unique in their own way, are they getting the most from their device?

But how can schools make sure students are learning in a way that's best for them? Before you can customize a device, you must first know **who** is using the device — in other words, the student's identity.

School IT admins already do a lot behind the scenes. Adding identity and access management (IAM) to your plate can sound overwhelming. But with the right tools, IAM can simplify your workflows and improve security — while also enhancing students' experience in the classroom. We'll take a look at how this is done in the following pages.



In this e-book, we'll go over:



What Identity and Access Management (IAM) is



Identity challenges in K-12



Building your identity foundation



The benefits IAM brings to K-12



An IAM readiness checklist for your school

IAM can shape the classroom experience.

A classroom session can look very different, depending on your identity workflows.



Disruptions to learning caused by identity workflows can show up in several ways:



Students using (or forgetting) passwords for multiple accounts (like for specific apps or tools)



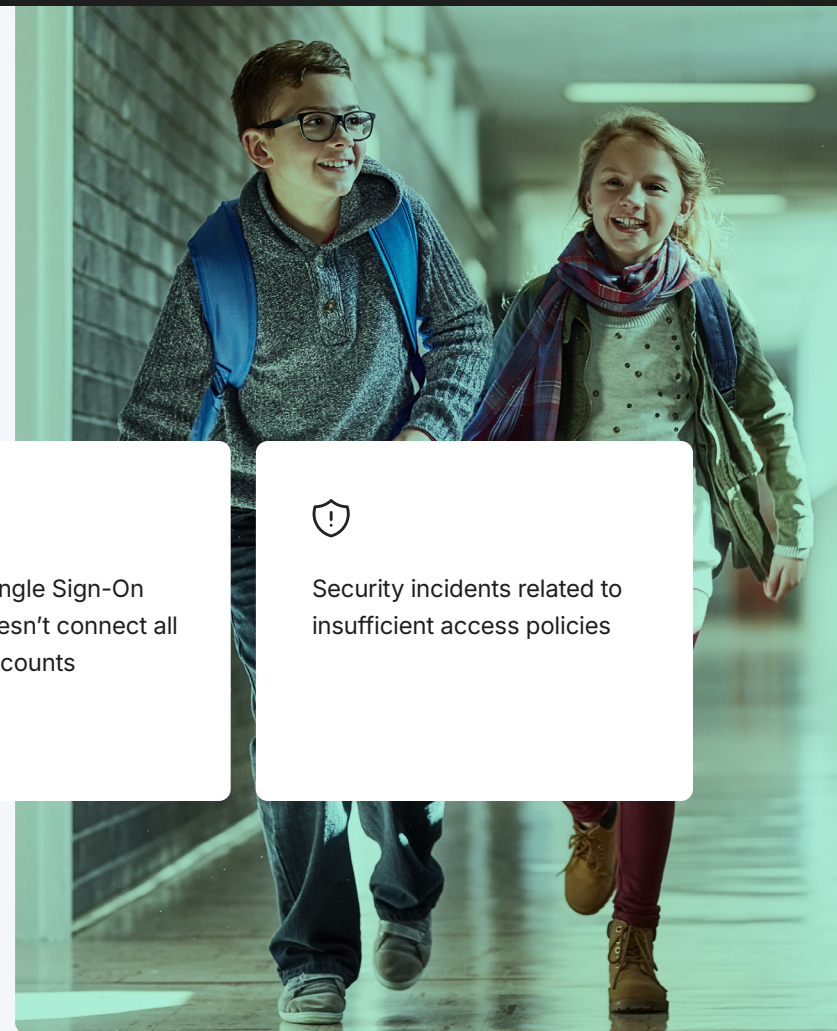
Students struggling to keep up with lessons due to device configuration



Incomplete Single Sign-On (SSO) that doesn't connect all a student's accounts



Security incidents related to insufficient access policies

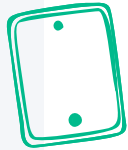


It doesn't have to be this way.





Imagine this experience:



1.

A student picks up a Shared iPad from their classroom cart.

2.

They tap on their picture and enter a passcode.



3.

The iPad is configured to that student's individual apps and settings, based on their grade level, classes and more.



4.

With a Managed Apple Account and identity provider, the student can log in to any of their resources, without having to remember a variety of passwords.



5.

When the student is done, their session is erased from the iPad.



This integrates devices smoothly into a teacher's lesson plan. And with passwordless authentication, there are fewer passwords to remember (or steal).

Overview of modern IAM

We're getting ahead of ourselves here. Before we get to these streamlined workflows, we have to understand what IAM actually means and how it applies to your school.

It's built on two key concepts:

1.

Authentication



confirming **who** a student or teacher is

2.

Authorization



controlling **what** they can access

First, we need to keep track of all of our users and offer a way for them to prove their identity, like a username and password. Then, we need to associate permissions with that identity, like what apps, data and resources they can access.

To achieve this, we need a directory to name each user. This might contain users':

- First and last name
- Username
- Email address
- Attributes like class, grade level or school name
- Authentication information, like hashes

With this information, we can start to establish permissions. For instance, if you know a user is a fifth grader in a certain teacher's math class, you can give them access to a math games app that teacher likes to use.

So what does IAM do?

IAM is more than a directory that holds a list of student identities. It contains account information — users' access permissions to various applications — meaning it can dictate what users can access and how they can access it.

IAM is dynamic, adapting to the context around a user's account. If they change classes and need a new set of apps, IAM can provision the right apps and revoke permission to those no longer needed. A third grader and a twelfth grader may both have access to the internet, but the twelfth grader may get less restrictive content filters. If an eleventh grader drops a science class, IAM removes their license to expensive lab software used only in that class.

In other words, IAM is like your class roster — but smarter. It's key to making sure your user accounts and data are secure. And it makes the classroom experience better for both students and teachers; more on that later.

Glossary of IAM terms for schools

Identity Provider (IdP)

Your “digital directory” that verifies users and their permissions, like Google Workspace, Microsoft Entra ID or Okta

Single Sign-On (SSO)

One login for all resources, including Apple, Google, your learning management system and more

Multi-factor authentication

An additional layer of account security that requires multiple factors to log in, like a password *and* a biometric or one-time password

Identity orchestration

Control center for identity, integrating directories and identity workflows, enabling features like SSO

Why K-12 schools need IAM

Something is always happening at schools. Students change grades, classes or buildings every year. Young students forget their passwords. Devices change hands, get lost or go home with students.

Few departments are immune from at least some chaos, especially IT. You might find yourself trying to make the most of tools you didn't choose or wrestling with mixed systems, like a combo of Apple, Google, Microsoft and your student information system (SIS).

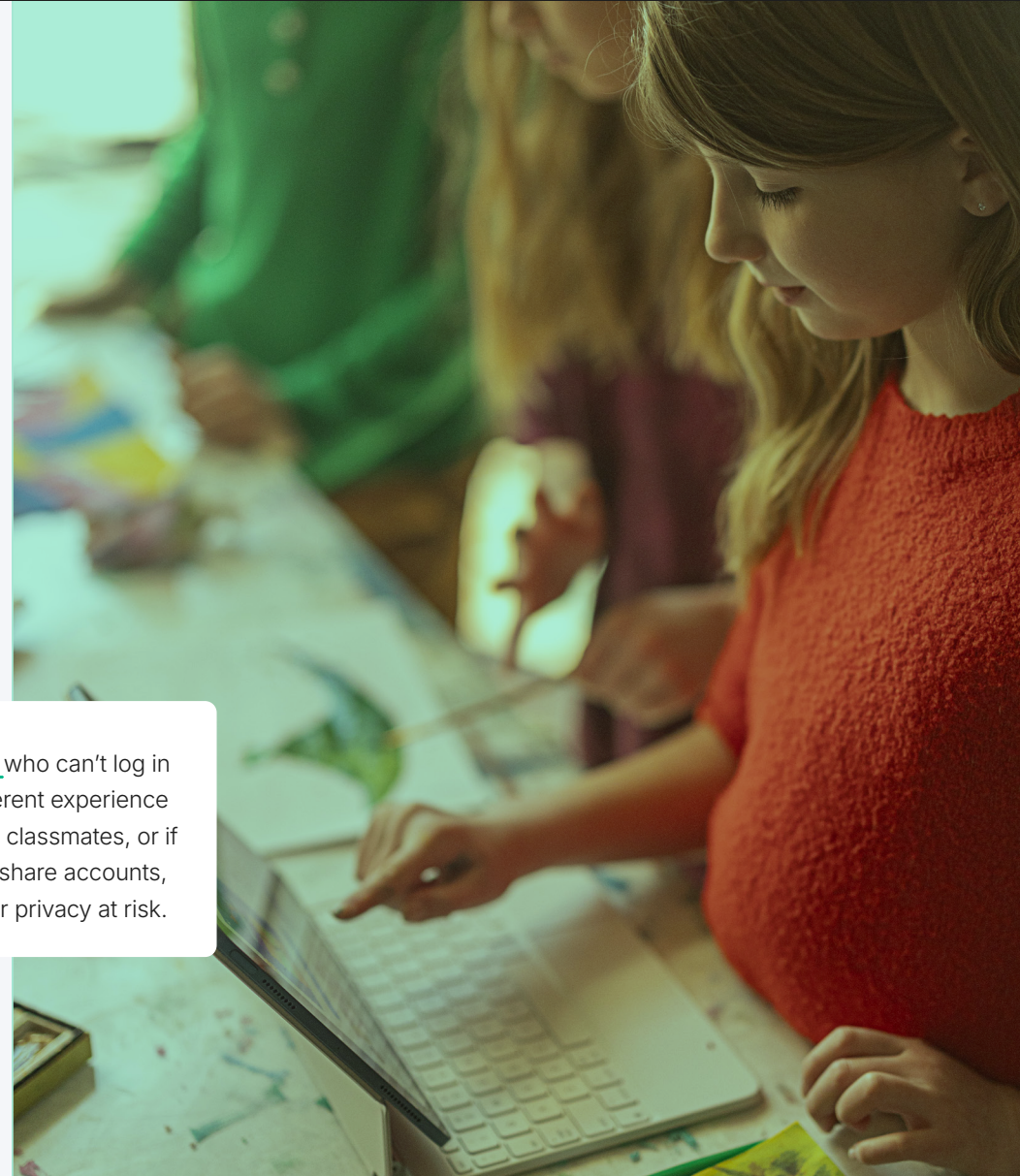


**Without IAM, authentication is more difficult.
This impacts everyone:**

IT teams have to deal with chaotic logins, more support tickets and provisioning delays.

Teachers lose instructional time, leading to frustration and potential changes to curricula.

Students who can't log in get a different experience from their classmates, or if forced to share accounts, place their privacy at risk.



With and without IAM in Apple environments

With IAM, student and staff identities become the foundation of your Apple environment. Connecting your IdP, Apple School Manager and mobile device management (MDM) help you deliver simple, secure and personalized learning experiences.



With IAM

- 🔑 **One** login for all resources
- ⚙️ **Automated** provisioning and access
- 👤 **Personalized** experience on shared iPads
- 🛡️ **Stronger security** with SSO and MFA



Without IAM

- 🔑 **Multiple** logins per student
- 💬 **Manual** account set up and intervention
- 🕒 Lost class time and increase in help desk tickets
- 🔒 **Inconsistent security** and access



Building your identity foundation

Okay, so you want to begin the journey of IAM at your school. How do you begin?

1.

Establish a single source of truth

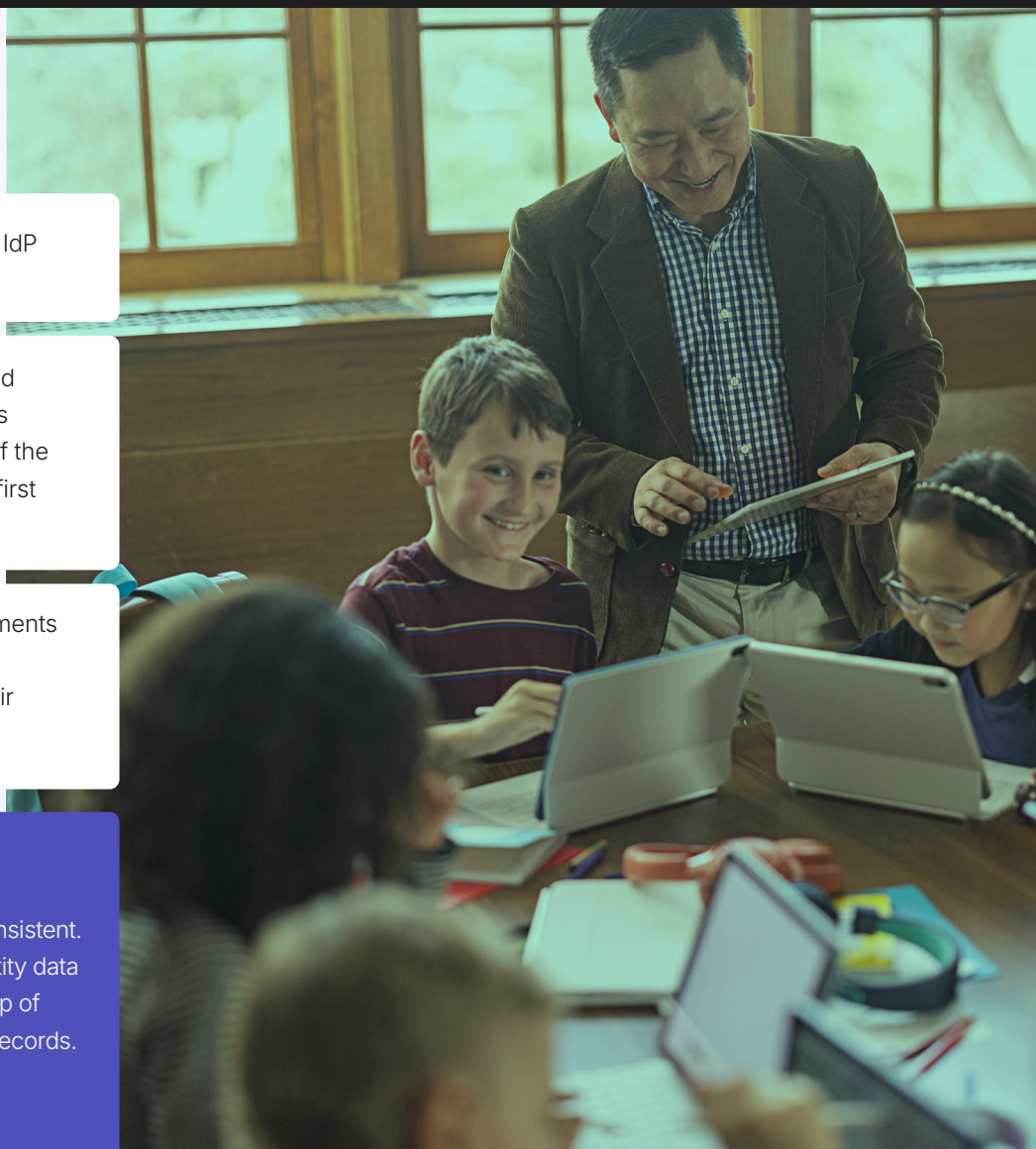
Integrate your systems: Connect your SIS with your IdP for real-time data continuity.

Automate account provisioning: Create, manage and remove user accounts based on data in your SIS. This helps prevent bottlenecks at the beginning and end of the school year and ensures students get access on the first day of school.

Stay in sync: Keep your class rosters, device assignments and app access consistent and in sync. Students can be placed in their appropriate classes and access their assigned apps based on that information.

How consistent is your data?

IAM works best when the data between systems is consistent. But actually getting to this point isn't always easy. Identity data management tools add a data orchestration layer on top of IAM to transform your data into clean and normalized records. Consider this if your data is giving you grief.





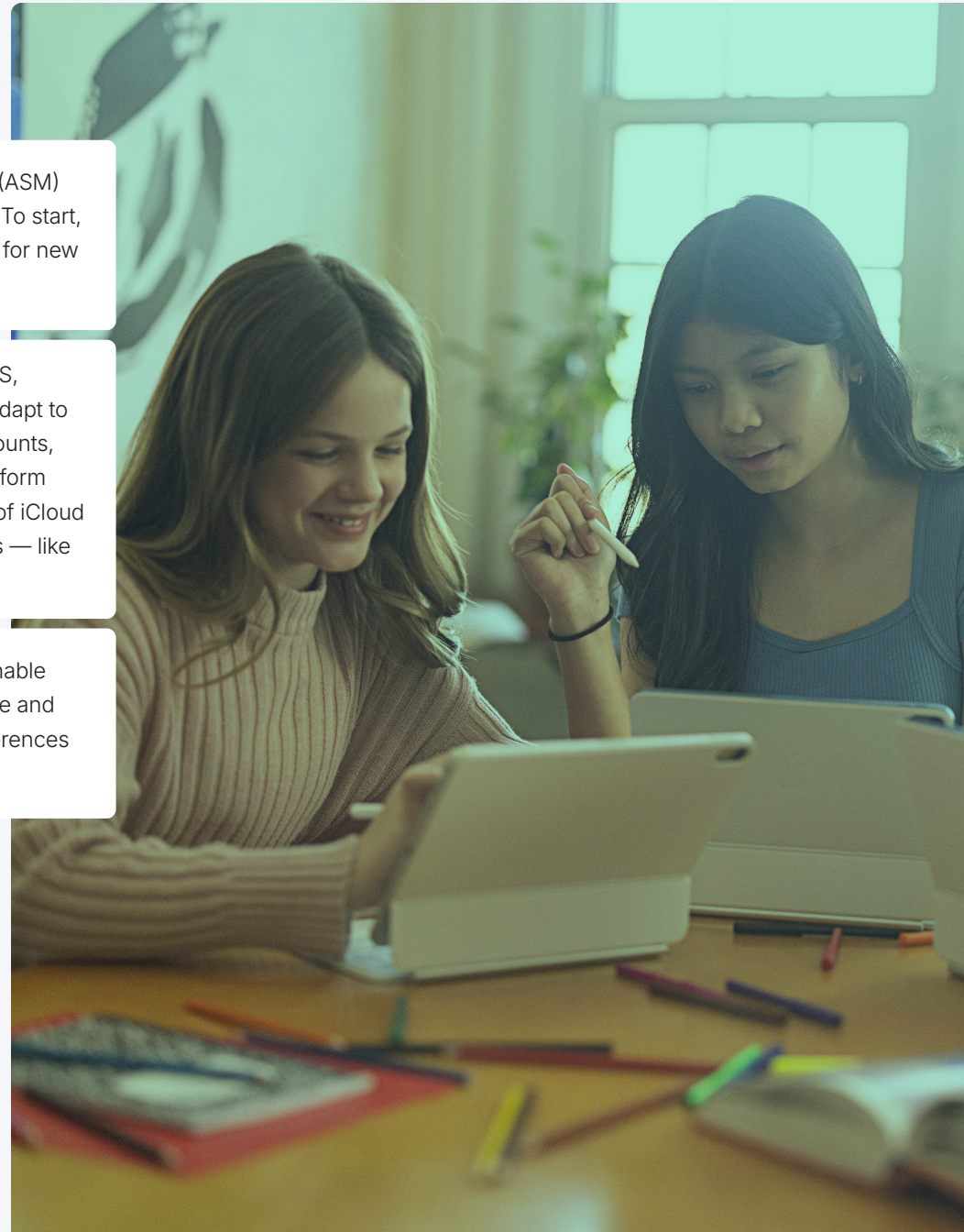
2.

Integrate with Apple School Manager

Optimize your deployment: Apple School Manager (ASM) helps you get the most out of your iPad deployment. To start, it enables features like Automated Device Enrollment for new devices and lets you purchase apps and books.

Automate identities: ASM can integrate with your SIS, automatically create Managed Apple Accounts and adapt to changes throughout the school year. With these accounts, IT admins can also perform password resets and perform other administrative functions. Students get 200 GB of iCloud storage and access to other Apple apps and services — like collaborating on a Keynote with their classmates.

Personalized learning: Managed Apple Accounts enable Shared iPad features. Students can tap on their profile and enter their pin to get an iPad configured to their preferences and needs.



3.

Connect to your MDM



Leverage your IdP: Integrating your MDM with your IdP allows you to drive enrollment, profiles and access policies to your devices.

Automate provisioning: Automatically provision apps and settings based on a user's role.

Streamline setup: Assign devices based on identities and have devices ready for action on the first day of school.





Implement identity best practices

Use SSO: SSO makes it easier for students and teachers to login to their apps. With fewer passwords to remember, password fatigue and resets decrease, and attackers have fewer opportunities for account compromise.

Enforce MFA: Multi-factor authentication adds another layer of security for staff and admin accounts.

Automate provisioning and deprovisioning: When you integrate your MDM, IdP and other systems, you can automate user provisioning and deprovisioning. This closes security gaps without time-consuming and delayed manual intervention.

Conduct regular audits: Ideally, setting up access based on a user's role or other attributes only grants them access to what they need. But things can change — regularly review that access policies are granting the least privilege.



5.



Pilot, then scale

Start small: Consider starting with one grade level or a building. You'll be able to smooth out kinks in your process and tools before a large-scale implementation.

Adapt and optimize: Gather feedback from teachers — are there fewer disruptions? Is it easy for students to log in to their accounts? With this feedback, you can address any concerns and make sure learning is enhanced, not hindered, by technology.

Emphasize collaboration: Technology is most impactful when it's not siloed into IT. Working with school administrators and curriculum leaders makes sure everyone is getting the most out of the experience. And in turn, students will too.



IAM enhances IT workflows, security and the classroom experience.

Once you build this foundation, you reap the benefits.



Streamline IT operations:

When you combine your systems with central IAM, you unlock powerful automations that simplify processes.



Automate the identity lifecycle:

With the right setup, you can automatically manage identities throughout the entire school year (and beyond). With IAM that autonomously adapts to changes to rosters, roles, buildings, classes and other attributes, access permissions are assigned with minimal IT intervention.



Enhance cybersecurity and compliance:

SSO and automation close security gaps before they become a problem. IAM reduces password fatigue, autonomously manages permissions, prevents unauthorized access and saves IT time — all features that boost security and compliance in some way or another.



Improve the user experience:

As we've already mentioned, the fewer passwords students need to remember, the better. And since access is based on a user's role, they get access to all the apps they need from the get-go. This means less disruption during class time with fewer password resets, help desk tickets and teacher headaches.

IAM is a journey: start simple.

There's a lot to learn. If you're starting from scratch, implementing IAM can sound insurmountable. Thankfully, it's not an all-or-nothing deal. Start with the components that are in your reach. Maybe that means ensuring your data is consistent across your tech stack. Or integrating Apple School Manager with your MDM. You'll likely find that small steps still benefit your school, with fewer headaches, faster logins and safer students.





Checklist: Is my school ready for IAM?

Use this quick checklist to see if your school is ready to add IAM to your tech stack.



Know your current setup

☐

I know how student and staff accounts are created and removed.

☐

Our data is consistent across systems (SIS, Google, Microsoft, etc.)



Establish a foundation

☐

We have or are planning to have a cloud IdP like Google Workspace, Microsoft Entra ID or Okta.

☐

ASM and our MDM (like Jamf School or Jamf Pro) are set up and connected.



Follow best practices

☐

We use SSO for core learning tools.

☐

We protect staff and admin accounts with MFA.

☐

We automate user provisioning and review access regularly.

If you checked most of these boxes, you're ready to simplify logins, strengthen security and enhance the learning experience with IAM.



Try Jamf