Seamless Access: A Complete Guide to SSO in K-12

Introduction

Every minute of instructional time matters.

Yet login friction continues to disrupt learning across K-12 environments. From delayed class starts to inequitable student access and increased IT workloads, authentication challenges create ripple effects that impact outcomes.

This guide explores how Single Sign-On (SSO) enables seamless learning access, reduces complexity and restores valuable learning time. For IT administrators, it provides a clear path to simplify identity management, strengthen security and better support educators and their institutional goals.

When learning has to wait

9:00 am: The classroom teacher just finished taking attendance as she looks up from her tablet to a sea of beaming smiles. The students are extra excited to learn about the solar system after having watched the Artemis II launch the night before. "Good morning, my fellow astronauts, this is your Command Pilot speaking. Time to grab your space gear because today... *we're* going to the moon!"

By "space gear", the teacher means for the Flight Specialists to take out their iPads and log on to their portal to access today's lesson titled, "Out of this world!"

Just as the teacher's about to begin, she's cut short by Johnny: "Miss, it says my password is invalid." Jane chimes in, "Me too. I can't log in either." Breathing out a slight sigh, Ms. Aldrin sets down her iPad before treading over to inspect their mission-critical equipment.

As she troubleshoots their login issues, some of the crew are "all systems go" for learning, while others remain in a space launch holding pattern because they forgot their login, used an incorrect password or can access the lesson just fine, but the solar system website linked to it won't launch.

What was T-30 seconds to learning at the top of the hour has become T+6 minutes (and still counting) of lost learning time.

The hidden cost of login friction

Each school year, various technology-related disruptions impact instructional time. Some of these include:

Budgets and funding | **Cybersecurity risk** | **Digital divide** | **Online distractions** | **Device health concerns**

While each of these undoubtedly affects institutions, an often-overlooked consideration that is equally impactful on learning outcomes are challenges that contribute to login friction.

For example, it takes a student approximately **30 seconds to three minutes** to log in to a device or website. Despite concrete statistics not generally being published publicly, this range represents a good rule of thumb to follow that accounts for variations, like typing ease, system familiarity, device performance and internet speed.

Though each instance takes only seconds to log in to a website or minutes to authenticate to your Mac, these delays compound over the course of a school year, adding up to a significant amount of learning time lost to authentication-related trouble.

Other important, time-sensitive averages to be aware of are:

- IT/Help Desk support ticket response times for non-critical issues: **1-2 days**
- Resetting a forgotten password or unlocking an account: **15-30 minutes**
- Receiving an authentication verification alert from MFA: **8 seconds**

30 seconds for a student to log in to one website x 4 classes:	**= 2 mins per day**
2 mins x 5 days a week:	**= 10 mins per week**
10 mins x 36 weeks:	**= 360 minutes**
360 mins / 60 mins:	**= 6 hours per school year**

Before we take a closer look at the math behind login friction, let's set some K-12 variables:

- Students typically have **4-8 classes per day**
- A typical school day lasts **7 hours**
- Schools are open **5 days a week**
- The average school year consists of **180 days** (or 36 weeks)
- Total learning time per school year is **1,260 hours**
- The average enrollment per elementary school (US) reached **470 students**
- **780.85 million** pupils in primary education worldwide in 2024

What do these numbers mean?

At just 30 seconds per login, each student loses about 6 hours of learning time per school year for just one website. Let that sink in.

This doesn't account for retrying authentication after mistyping a password or visiting multiple learning sites, each with their own unique credentials to remember. Because that could cost another 30 seconds for each mistake or additional website that requires a separate login.

It also doesn't account for forgotten passwords or locked accounts — which act as a force multiplier — resulting in compounding delays by an average of 15 minutes for the former to possibly 1 day for the latter, if a help desk support ticket is required.

30 seconds per website per student represents 2,820 cumulative hours of lost learning time per institution per school year in the US; or, 4,680,510,000 cumulative hours of lost learning time for K-12 students globally.

What if login friction — inclusive of password resets and account unlocks —could be minimized to such a degree that students could authenticate once and access everything they need for learning instantly?

What this guide covers

In our foundational guide, **Identity and Access Management in K-12 for Beginners**, we explored what IAM is and why it matters. Now, we're going deeper into one of IAM's most powerful applications: **Seamless access through Single Sign-On (SSO**).

You'll learn:

- How login friction steals instructional time and creates inequity.
- What seamless access means in practice.
- Real-world impact: time reclaimed, tickets reduced and learning restored.
- How to assess if your school is ready for SSO.

Small disruptions, big losses

We've learned how login friction can impact the learning environment per class and per school at a global level. In this section, we highlight the different ways it shows up and affects student, teacher and IT team performance.

The real price of just one more.

Students

- Inequitable access (digital divide) limits their ability to engage with modern, blended learning.
- Loss of momentum during critical learning transitions, limiting "keeping up" with curriculums.
- Creates academic gaps, causing them to fall further behind peers in the classroom and during home learning.
- Lack of developing critical skills leads to frustration with technology and loss of attention.
- Disconnection from peers and teachers further hinders progress while increasing disengagement.

Teachers

- Classes start later than scheduled, significantly reducing instructional time.
- Personalized learning is impacted, due to the limited reliability of digital tools.
- Increased disruptions make it difficult to maintain classroom flow and engagement.
- Playing tech support and adapting lesson plans require inventing workarounds instead of teaching.
- Tech fatigue or burnout from the increasing mental stress of digital demands in the classroom.

IT teams

- Help desk ticket counts spike at the start of each school year, increasing workloads and stress.
- Manual provisioning delays leave students and teachers without access to learning tools.
- Password-related issues flood the help desk, significantly impacting productivity for all stakeholders.
- Security incidents increase in response to weak credentials and password sharing, alongside privacy risks.
- Spend time triaging and firefighting issues instead of focusing skills on strategic initiatives and better experiences.

A question of equity

Ask yourself: Are some students losing more time to login issues than others?

Before you answer, consider how the following points impact equity:

- Younger students (K-2) typically struggle more with password memorization than older students (3-12).
- Diverse learning preferences increase the cognitive effort required for students to process information.
- English Language Learners (ELL) must navigate both language and tech barriers simultaneously to succeed academically.
- Students in shared device environments often experience more friction from performing repetitive authentication.
- Higher student-to-device ratios experience compounding delays, such as slow performance and technical interruptions.

Now, recall your previous response — alongside the equity points above —answer the following question: **Are all students getting equal access to learning from technology?**

The IT burden nobody talks about

There's no question that a core IT function is to provide support that spans students, teachers and the school itself. From personalized issue resolution to empowering stakeholders to delivering exceptional digital experiences to infrastructure improvements – of which drive modern education environments.

And yet, there are aspects of support that often monopolize IT resources, causing a ripple-effect that limits the breadth and depth of support IT can provide to learners, educators, schools, districts and institutions.

Chief among these, hiding in plain sight, are password-related issues. Let's uncover the hidden costs:

- Research shows that up to **50% of all IT help desk tickets** are for password resets.
- A single password reset costs approximately $70, according to **Forrester Research**. This translates to significant time and money spent on password management throughout the school year.
- Resources that could be better spent on strategic initiatives, like aligning more closely with learning objectives.

The (unintentional) security risk: When technology becomes burdensome, stakeholders find workarounds. This also applies to passwords, with the results often compromising security:

- Creating easy to guess passwords: Nearly **6 out of 10 real-world passwords can be cracked** in less than an hour, nearly half in just a few seconds.
- Using the same password for every account: Threat actors **automate testing stolen credentials across hundreds of websites**; same password = more access.
- Writing down passwords on sticky notes: Everyone knows you keep **the password to your computer is kept on a yellow sticky** under the keyboard.
- Sharing accounts with other stakeholders: Research finds that **16% and 22% of respondents share passwords with friends and colleagues**, respectively.
- Never changing passwords: A data leak in 2025 **exposed 16 billion credentials** that were harvested from multiple breaches, ready for use in cyberattacks.

Why are risky password behaviors so impactful to K-12 cybersecurity?

Two words: **Compromised credentials.**

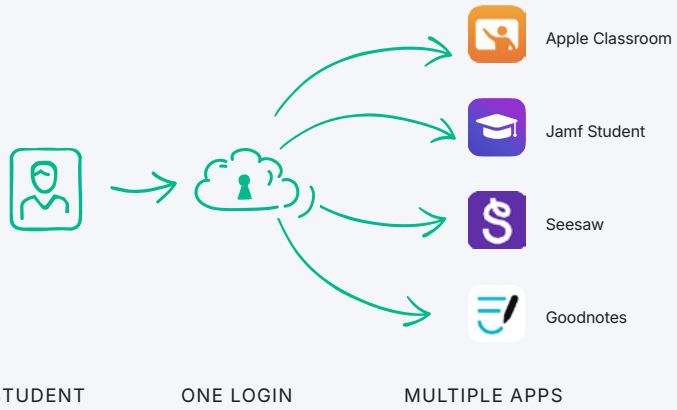
According to IBM, this root cause sits in third place — accounting for just over 10% of initial attack vectors globally. While 10% may seem like a minor percentage, especially compared to edu-centric threats like phishing and ransomware, know this:

- Most phishing campaigns act as precursors, often focusing on obtaining credentials from its victims prior to engaging in larger scale cyberattacks, like malware infections and data theft.
- Regulated industries, like K-12 education, are subject to local, state, federal and/or regional laws protecting sensitive and confidential information. PII and PHI are particularly attractive to threat actors, elevating education as a data-rich target for cyberattacks.
- The average financial cost of a single security incident from compromised credentials is estimated to be $4.67 million, according to research analyzed from the **Cost of a Data Breach Report 2025**.

What is seamless access?

One login. Endless learning.

Seamless access is the concept that educational stakeholders authenticate once at the start of their day. From there, they move effortlessly between digital tools, like apps, education websites and learning services without being required to enter their password again.



A day in the life of a student

Morning Arrival (8:15 AM):
Maya picks up a Shared iPad from the classroom cart. She taps her picture and enters a simple 4-digit passcode. She has access to her grade-appropriate apps, accessibility settings and personal files.

First Period - English (8:30 AM):
She navigates to the learning management system – no log in required, as she's already authenticated. She checks today's assignment, moves seamlessly to the digital textbook, highlights a passage and adds a note in Pages. All without entering any additional passwords.

Second Period - Math (9:30 AM):
Maya taps on the math app to practice fractions. Again, no login screen. She just jumps straight to learning, picking up right where she left off yesterday, because the app knows who she is.

Collaborative Project (10:30 AM):
When the time comes to work on a group presentation with three classmates, she opens Keynote. Because authentications are linked to Managed Apple Accounts, they're all able to work in the same file simultaneously. No password sharing, no access issues – just seamless collaboration.

End of Day (3:00 PM):
Before Maya returns the iPad to the cart, she signs out of her session. This syncs her data to iCloud, making the iPad ready for the next student by erasing the session. Tomorrow, she can authenticate on any iPad in the school and experience the exact same personalized session.

From the teacher's perspective

Before Class:
Review the lesson plan – no time wasted troubleshooting login or preparing iPads because SSO is in place.

During Class:
Students log in and are ready to learn within 30 seconds. The lesson starts on time, maintaining momentum and engagement.

After Class:
Focus shifts to providing feedback on student work — not playing tech support or submitting account-related requests to IT.

What makes it all work? The three pillars:

1. **Managed Apple Accounts:**
Integrated with your cloud-based identity provider (Google Workspace, Microsoft Entra ID or RapidID) for automatic provisioning and unified access to Apple services.

2. **Passwordless workflow:**
Tap-and-go authentication that increases efficiency and reduces cognitive load while maintaining security. Perfect for younger students or users with accessibility needs.

3. **Single Sign-On:**
One account, authenticated a single time, unlocks access to all federated applications – web-based and native apps alike.

The real-world impact of seamless access

Instructional time reclaimed

Instructional time is limited, and small disruptions quickly add up. Login friction is a consistent barrier that delays lessons and breaks classroom momentum. Reducing these interruptions helps teachers stay focused on instruction while enabling IT to support more effective, seamless learning experiences.

The research on lost time

If you recall in the first section, the average school year consists of 1,260 hours. In this section, this figure – which can differ depending on your region – will be used below to illustrate the criticality of reclaiming lost instructional time.

In 2024, researchers from Brown University found that nearly **25% of instructional time per school year is lost due to interruptions** and absences, among other disruptions. While some of the examples cited in the research may appear minor, like a 30-second intercom disruption, this is often followed by disruptions lasting several minutes of trying to regain students' focus.

Technology-specific time loss

During a similar study in 2021, researchers noted technology-related interruptions as one of several common types. Using both observational and survey data, they correlated the impact between how subsequent disruptions continue to negatively affect students' opportunities after even the smallest of interruptions occurs initially.

More than 50% of interruptions resulted in extended lost learning time, with researchers finding it "led to students being off task" and "the teacher having to pause the lesson."

Login friction occurs in every learning environment — on-campus and off. Prime examples of this happen each day, and at some point, to every student taking the form of:

- Delays from poorly designed user interfaces
- Slow loading times from inefficient authentication schemes
- Password fatigue from juggling multiple accounts
- Denied access from entering the wrong password
- Invalid passwords from varying complexity requirements
- Locked accounts from triggering a password policy

What SSO does

Simply put: SSO significantly reduces password-related friction and, in turn, technology-related disruptions. It's the conduit by which students securely authenticate once during initial log in and then move seamlessly between the applications, websites and services they use for learning.

Across every class period, every day and over the course of the school year, the time saved compounds and results in:

- Efficiency gains in classroom productivity and school operations.
- Reducing security risks and exposures while mitigating vulnerabilities.
- Systemically standardizing compliance and governance across institutions.
- Increased return on investment by reducing total cost of ownership.

What teachers can do with reclaimed time

Throughout this guide, we've covered some of the most common areas where teachers could benefit from additional time, such as:

- Start lessons immediately, maintaining energy and engagement.
- Spend more time on instruction and less on troubleshooting.
- Cover more material without rushing.
- Build in more time for student questions and differentiation.

But, rather than telling, we'd like to posit a question for Edu stakeholders to consider. If you recall back to the first section, we calculated that each student loses about 6 hours of instructional time per school year, based on the 30-second disruption of logging onto a website during each class.

During this time, teachers must stop their lesson and wait for the students to become ready so they may proceed with teaching. So, the question is this:

What are *your* teachers capable of achieving when the time from daily interruptions, disruptions and extended delays are reclaimed?

IT impact — From firefighting to strategizing

In addition to productivity gains and reducing potential password-related security vulnerabilities, implementing SSO simultaneously helps **cut down help desk costs by an average of 40%**.

Expected impact of SSO

After all, when half the support tickets are related to resolving account and password-type issues, a reduction of that magnitude means that IT is now able to address, more critical issues sooner. For example, for every 10 support tickets, the critical-to-non-critical-issue ratio shifts from 1:2 (without SSO) to 7:3 (with SSO).

Where IT can invest reclaimed time

Alongside workload impacts, time is positively affected as well. By way of automating, centralizing and streamlining authentication processes with SSO, time reclaimed by IT fuels strategic aims that:

- Enhance stakeholder experiences with technology.
- Develop better production and operational workflows.
- Modernize and improve K-12 computing infrastructures.
- Strengthen stakeholder skillsets through tech training initiatives.
- Achieve tighter alignment with desired learning outcomes.

Equity outcomes

Access gaps

Students do not refocus all at the same time from everyday disruptions. In 2025, researchers corroborated this, when **their findings determined** that "*the average student loses 25 percent of instructional time to these many interruptions.*" Interruptions like:

- Students being tardy
- Teacher absences
- Intercom announcements
- Classroom visits

Are common in K-12 schools around the world. Recalling our 7-hour school day average, 25% (1.75 hours) reduces instructional time to 5.25-hour school days.

Correspondingly, login friction not only impacts instructional times, but the similarities extend to how long disruptions last before students readjust their attention back to learning.

Students do not experience technology barriers equally. Some equity considerations that further impact instructional time loss are struggles with:

- Memorization
- Cognitive load
- Language barriers
- Physical disability

How SSO helps

All students experience equitable access, empowering them to learn wherever learning takes place, regardless of tech skill. SSO is designed with the following in mind:

- Students only need to remember one account – that's it.
- Security is built-in, so passwords can be complex (but easy to use passcodes may be configured as well), while remaining secure.
- Authentication workflows are streamlined so it looks and responds the same way for everyone, every single time.
- Credentials are maintained centrally and easily managed by self-service, or with teacher or IT assistance (if needed).

The "dignity factor"

When a student can't log in while their classmates can, it's not just a tech problem – it's an emotional one. SSO removes this source of frustration and embarrassment, creating a more inclusive classroom environment.

Security improvements

Did you know that "*passwords are the root cause of more than 80 percent of data breaches*"? According to the Fast Identity Online (FIDO) Alliance, this is an exploit of choice for threat actors due to **easily being phished, intercepted or otherwise uncovered.**

SSO security benefits

Chief among the benefits is centralizing password policies at the IdP level. This not only aids compliance (which we'll cover in the next section) but hardens passwords holistically by standardizing security across educational infrastructures – extending the same level of access protection to every app, website and service. Additionally, SSO provides the following security benefits for K-12 environments:

- Eliminate creating and remembering multiple, unique passwords.
- Establish a single policy for using strong passwords – not many complex schemes.
- Simplify defining access permissions by role, not individually or manually.
- Reduce account sharing (a common practice when stakeholders can't log in).
- Automate pruning inactive accounts when stakeholders leave.
- Enhance account security, pairing MFA, to minimize unauthorized access.

Compliance confidence

Implementing protections are only one aspect of security. Another equally critical one is ensuring that layered controls are functioning as configured. Additionally, each function occurs in support of your K-12 operational strategy. That means enforcing compliance and providing IT a standardized means to:

- Enable centralized monitoring of all access attempts.
- Document access controls for policy reviews.
- Establish clear evidence of appropriate safeguards.
- Maintain detailed audit trails for regulatory compliance.

Total cost of ownership (TCO)

The full picture

Technology costs in education go beyond the sticker price of the hardware itself. When adding up backend costs — including software licensing, warranty and support, training, maintenance, and decommissioning — TCO balloons to several thousands of dollars per device over the course of its usable lifetime. Depending on the size of your institution, thousands of devices can easily scale TCO well beyond **initial procurement expenditures**.

Consider the following basic formula to calculate TCO using industry averages:

Cost of an Apple iPad (128GB):	$329
AppleCare+ for Schools (3-year):	$79
iPad Case (Rugged):	$20
$329 + $79 + $20	= $428 (per device)

Number of students (1:1):	1,000
$428 x 1,000	= $428,000

TCO estimate per device (3-years):	$194
$194 x 1,000	= $194,000

Total cost of ownership (hardware and warranty only):	
$428,000 + $194,000	= $622,000
$194,000 / $428,000	= 0.45
0.45 x 100	= 45%

Costs related to software licensing, training, maintenance and decommission vary widely by school needs making them difficult to quantify. Moreover, variables drift by institution and/or governance potentially affecting cost deltas further.

Cost reduction areas

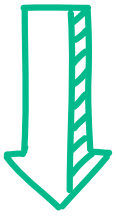
It's no surprise that, given the costs associated with procuring, managing and securing technology, institutions are interested in finding areas to lower TCO — and potentially raise Return on Investment (ROI).

In 2023, Forrester Consulting conducted a study titled **The Economic Impact of Microsoft Entra** to assess ROI using Microsoft's IdP solution compared to using multiple-point solutions. The end result yielded two interesting findings:

- Modernizing device management, identity and security means reducing complexity and centralizing tools.
- An ROI of 240% was realized by moving away from the "patchwork approach" (more on this in the next section) of multiple-point solutions, simultaneously increasing security while lowering costs.

Other costs SSO helps to reduce include:

- IT labor: Standardizing account management and provisioning substantially lowers costs in proportion to password-related tickets and resets.
- Instructional time: Reclaiming even a portion of 25% lost instructional time per student translates to significant educational value for all stakeholders.
- License optimization: Automated deprovisioning reclaims unused licenses for reassignment



SSO for non-techies

Understanding the technology without the complexity

"Complexity is the enemy of security."
– Bruce Schneier

You don't need to be a cybersecurity expert to understand how SSO doesn't just protect access to K-12 devices and resources – it safeguards learning time by:

- Minimizing technology complexity
- Increasing authentication visibility
- Mitigating hidden vulnerabilities
- Enhancing security postures
- Reducing human error
- Automating account management
- Simplifying login processes
- Consolidating IT tools

Theory aside, let's review a practical example drawn from a real-world K-12 use case involving Apple iPad.

The bell rings and it's time for class to start. Like clockwork, the students take out their iPads and log in to their devices using one flavor of SSO as the teacher readies the lesson. After a few minutes, the class is logged in to the device.

Pause.

The students need a few minutes to log into their portal, the one that uses a second SSO solution. Finally, at the portal, the students follow the teacher until the lesson concludes. Now, students open their word processor app to begin writing.

Stop again.

There's a third SSO product used exclusively for that app. Let's pause again until everyone authenticates for a third time.

Good, we're now in the word processor app and starting to work on our group project.

Oh no, not again! Yes again. In order to work together in real-time, we need the students to access the collaboration app which – you guessed it – uses another instance of SSO. The students need to stop what they're doing for a few more minutes to login for a fifth time.

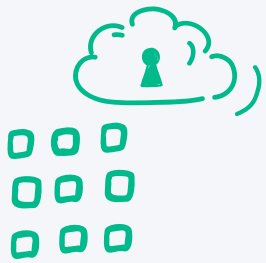
Sadly, by the time the students get back on track, the hour-long period is nearly over, and they've spent approx. 15 minutes, or 25% of instructional time authenticating to various SSO versions strung together in a patchwork approach to emulate Single Sign-On.

While some products may even go so far as to claim single sign-on capability for iPadOS, the hallmark of SSO is a truly Seamless Learning Access solution that allows stakeholders to authenticate just once during their initial iPad login. From there, regardless of whether they access:

- Institutional portals
- School resources
- Educational websites
- Cloud-based services
- On-device apps

The initial authentication steps forward to automatically log in seamlessly in the background, granting stakeholders access to the requested resource without manual intervention or delay.

Core concept



One Login, Many Apps:
SSO works like a backstage pass at a concert. Show your credentials once at the entrance, and you can access all the different areas without showing your pass again. Your identity provider (Google Workspace, Microsoft Entra ID, or Okta) is the security checkpoint that vouches for you to every app you need.

Security without barriers

SSO doesn't compromise security – it enhances it. Follow along below for a brief walkthrough of how SSO secures identity by design:

1. Stakeholders authenticate once to the IdP using their credentials. (This typically occurs when initially logging onto their device).

2. Upon validating the credentials, the IdP issues a digital token that cryptographically secures the stakeholder's identity.

3. When the stakeholder navigates to a service provider (SP), like a protected resource, the IdP sends the digital token to the SP.

4. The SP validates the token and grants the stakeholder's request to access the resource securely – no password needed!

It works everywhere

For Web-Based Apps:
Learning management systems, Canvas, Khan Academy, BrainPOP – students click and they're in.

For Native iPad Apps:
Pages, Keynote, GarageBand, and educational apps like Seesaw and Goodnotes, all recognize the student's Managed Apple Account for automatic sign-in.

For Shared iPads:
Each student gets their personalized experience on any device in the school. When they log out, the session is temporary, but their work remains safely stored in iCloud.

IT control layer

Great SSO means students and educators experience frictionless access while IT retains manageability over security and compliance behind the scenes. As part of a broader defense-in-depth strategy — one that integrates device management, identity and access management, and endpoint security — SSO functions as a control layer protecting K-12 stakeholders, devices and sensitive data. This gives IT:

Real-time visibility into who's accessing what resources.

Policy-based access controls (by grade level, role or deployment model).

Systematic provisioning when students enroll or change grades.

Automatic deprovisioning when students graduate or transfer.

Robust **security protocols** ensure secure, cross-platform communications.

Is your school ready for SSO?

SSO readiness assessment

Use this checklist to evaluate where you are today and what steps you need to take to implement Seamless Learning Access.

Identity infrastructure

- ☐ Cloud-based IdP (Google Workspace, Microsoft Entra ID, RapidID)
- ☐ SIS integrated with IdP
- ☐ Identity data is consistent across systems
- ☐ Apple School Manager set up
- ☐ Managed Apple Accounts are (or can be) created for students and staff

Device management

- ☐ MDM solution set up (Jamf School or Jamf Pro)
- ☐ MDM integrated with IdP
- ☐ Shared iPad, 1:1 devices or a hybrid model in place
- ☐ Devices enrolled in Apple School Manager

Application readiness

- ☐ 10 most-used learning applications identified
- ☐ Apps supporting SAML, OAuth (or other SSO protocols) identified
- ☐ Plan for apps that don't support SSO created
- ☐ Understand current app licensing and usage

Organizational readiness

- ☐ Leadership understands learning time and equity case for SSO
- ☐ Stakeholder buy-in (IT, administrators, teachers) achieved
- ☐ Ready to pilot with a test group before scaling
- ☐ Essential resources (time and budget) allocated for implementation
- ☐ Training plan for teachers and students established

Baseline metrics

- ☐ Identified how much instructional time is lost to login issues
- ☐ Tracked password reset tickets and IT support time performance indicators
- ☐ Teacher feedback on current access challenges provided
- ☐ Student populations facing the most barriers identified

Scoring:

12-15 boxes checked: You're ready to implement SSO now. The data shows clear ROI and you have the technological foundation in place.

8-11 boxes checked: You're close. Focus on filling the gaps in your identity infrastructure before moving forward with a pilot program.

4-7 boxes checked: You have foundational work to do. Start with our Identity and Access Management in K-12 for Beginners guide to understand the critical components, then return to SSO planning.

0-3 boxes checked: Begin with the basics. Establish your identity infrastructure and Apple School Manager before pursuing SSO.

jamf

Conclusion

Login friction quietly erodes instructional time, creates inequitable access for students and increases IT burden. Each delay disrupts momentum, limits engagement and compounds learning gaps across diverse classrooms.

And it adds up. Thirty seconds per login, multiplied across every class, every student, every school day — thousands of hours of learning time that never comes back.

Single Sign-On is what drives Seamless Learning Access — and Seamless Learning Access changes that equation. By simplifying authentication, strengthening security and restoring instructional time across every class period, SSO transforms access from a daily obstacle into something students and teachers stop noticing entirely — because it just works.

When that happens, teachers focus on instruction instead of troubleshooting. Lessons start on time. IT moves from firefighting to building — enabling better experiences, streamlining operations and aligning technology more closely with what learning actually requires.

jamf

With Jamf, IT delivers the secure, scalable access that keeps every student learning.

www.jamf.com

Discover How