1,000 devices, 1 IT admin:

How to scale Apple device management and security in education

Introduction: The ratio problem

Schools are investing in technology with clear intent — to personalize learning, expand access, and improve outcomes for every student. That investment is reflected in growing device fleets, expanding 1:1 initiatives, and a deepening commitment to digital tools that meet students where they are and support the way they learn best.

But as device counts rise, learning environments experience operational strain that compounds as deployments scale beyond the average EDU device-to-IT support ratio of 1000:1. When this occurs, educational operations sprawl, becoming difficult to sustain.

What is the result? An IT team that is constantly in "firefighting mode," that finds technical teams running from one problem to the next instead of focusing their skills on developing improvements that create value for all stakeholders.

When core device lifecycle management tasks, such as:

- Device provisioning
- Patch management
- Security monitoring
- Incident response
- Secure decommissioning

Are performed manually across thousands, or tens of thousands of endpoints with limited IT resources, even routine tasks that typically take only a few minutes to resolve, like:

- Resetting a password
- Installing an app
- Configuring Wi-Fi access

Sustain extraordinarily long wait times to resolve due to the sheer juxtaposition between the volume of requests and the number of personnel available to correct pending issues.

This is summed up in one word: imbalance.

Imbalance introduces interruptions

And this causes a ripple effect across the entire institution.

In classrooms, connectivity issues routinely prevent access to digital resources — and when they occur, educators often become the first line of support, shifting from teaching to troubleshooting mid-lesson.

For students, imbalance appears as friction. The technologies intended to enhance instruction instead frustrate learners when devices become unresponsive and apps crash, pulling attention away from the task at hand.

Over time, the pressures of imbalance compound. Alignment between students and teachers widens, leading to misalignment between educators and schools themselves. A common thread can be traced from students' inability to learn with failing technology to the institutions themselves, as negative impacts to educational goals and desired outcomes.

Each of these impacts is merely a symptom of the bigger problem yet they expose a broader, strategic issue: schools may successfully distribute devices — but without scalable management and support processes baked in as part of an overarching IT strategy — institutions will struggle to deliver the learning outcomes technology was designed to enable. Instead of bridging the digital divide, technology will instead create added barriers as reliability, usability and security fall out of alignment for students, teachers and schools.

The cost of manual processes

It takes an average of 2–4 hours to manually provision a single device. At the low end, that math looks like this:

1,000 DEVICES X **2** HOURS = **2,000** HOURS OF PROVISIONING WORK

Now compare that to what's actually available. Schools typically run 8-hour days, 5 days a week. Summer break — the primary window for annual refreshes — averages 10 weeks.

8 HOURS X **10** WEEKS = **400** HOURS PER IT STAFF MEMBER

400 hours to complete 2,000 hours of work. And that's before accounting for misconfigured devices, process fatigue or the inevitable variables that push provisioning time closer to that 4-hour ceiling.

Manual processes were never designed to match the economies of scale that modern K-12 device deployments require. The gap between what's needed and what's possible isn't a staffing problem — it's often an architecture problem.

Setting the stage

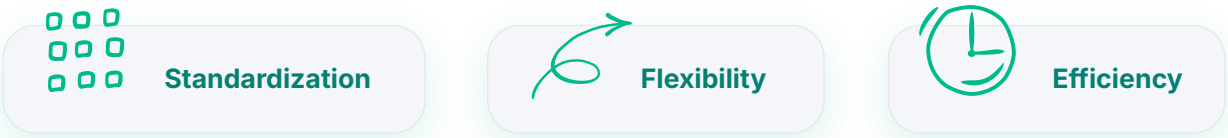
As it relates to device lifecycle management, scale is a critical aspect of effectively being able to provision ready-state devices into the hands of stakeholders with as minimal downtime as possible. It also holds another meaning that is similar in vein but slightly nuanced: in this secondary context, scaling refers to the ability to carry out deployments — including on-going device maintenance — with efficiency and minimal impact to educational operations.

While they are often considered as being synonymous with each other, they are at their core, very different concepts despite requiring the same solution to address.

Let's start with a basic understanding of what scaling refers to in IT:

"repeating the same steps on more devices."

With that in mind, there are three crucial considerations institutions must take into account when it comes to scaling, regardless of whether they're deploying new devices, keeping them compliant or both:



Inconsistency: The importance of standardization at scale

The criticality of establishing standards lies at the foundation of scalability, and whether scaling efforts will be successful or not. Why are standards so important? Because any variables introduced affect devices in different and unexpected ways.

When unaddressed or unaccounted for, their impact can range from minor inconveniences to impacts so severe that they require a complete redeployment of endpoints and/or the software, configurations and system settings that are necessary for learning to occur.

The first step in standardization is identifying a device state that translates to 'this device is ready for the stakeholder it's assigned to.' For students, consider this state "learning-ready," and it must include everything that is required for students at your school, grade and with the classes they're enrolled in, to best function in their capacity as a learner.

Given the scope of this paper, determining what learning-ready looks like from school to school, student to student may look similar but ultimately will vary based on many important distinctions, like student, educator, school, institution and regional needs. It is not the aim of this paper to provide every vast combination of potential standards that may exist, but rather to highlight the importance for school leaders and educators to define what learning-ready looks like and for IT to incorporate the standard into their provisioning workflows to ensure devices deployed meet the baselines necessary for that stakeholder each and every time.

Scaling devices ≠ scaling deployments

An important consideration when developing standards is their capability for flexibility. If standards are too rigid, whenever an issue arises (and they will) the standard will not fit the need, resulting in added downtime because IT must manually configure the device to ensure they meet the unique needs of the use case. However, if standards are too lax, they will fail in their aim to provide the access to the necessary tools the intended stakeholder needs as well as lacking in foundational management capabilities and security protections at scale. Both extremes result in IT manually configuring devices to meet varying stakeholder needs.

The key to flexibility is balance. The more hardware and software configurations encompassed, the more universal standards will be, however, the caveat is they will also be less secure. Imagine deploying an iPad to a student that includes the app teacher's use to input grades; or a teacher being assigned a laptop that doubles as a shared student laptop from a cart. When the teacher tries to save a lesson plan, they're prompted with an error message because the storage space is maxed out from all the student data saved on the device.

The message regarding flexibility isn't that devices cannot serve dual purpose. Instead, the takeaway is to factor intent when establishing standards. This will not only reflect your school's unique needs more accurately but also the realities of available hardware and software resources for use by stakeholders. By doing so, flexibility is baked in so that devices can be deployed or reprovisioned effortlessly while seamlessly getting that stakeholder learning or teaching with secure access to the tools and resources they need to successfully perform in their role.

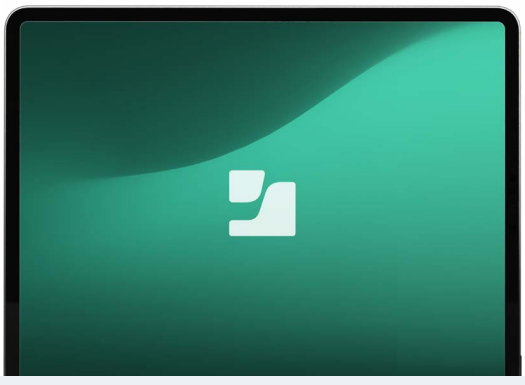
Where scaling breaks down in practice

To recap thus far, standards provide a foundational framework for configuring devices to a learning-ready state each time they're deployed. Flexibility gauges the ability for standards to adapt to changing stakeholder needs, with the aim being to be as seamless as possible to minimize disruption to educational or IT operations.

Efficiency, in this scenario, is determined by how time-consuming it is for IT to implement standards flexibly across device fleets. Because device fleets vary depending on institution, efficiency isn't measured by a quantifiable number of devices. Instead, it is measured by how seamlessly your existing workflows provision devices, deploy them to stakeholders and/or perform on-going maintenance throughout a device's lifecycle — regardless of whether it's a class set of shared iPads or a 1:1 MacBook program across multiple grade levels and sites for a regional deployment.

When attempting to scale, schools still relying on manual workflows often get tripped up by efficiency. While misconfigured devices or missing essential software are the most common issues encountered during provisioning, the fact remains that even armed with a strong understanding of stakeholder needs (standards) and accounting for the variables that affect your institution's plan (flexibility) — the entire deployment process implodes because manual processes become exponentially more unstable as device count grow.

The truest measure of an efficient, scalable workflow is in its ability to consistently handle deployment of 1,000 (or 10,000 devices for that matter) just as easily as 1, 10 or 100 without interrupting stakeholders, impacting operations or burning out IT in the process.



To quote Apple's design philosophy,

"it just works."

The pivot: Repeatability is the key to scaling without burning out

When it comes to scaling K-12 device programs, the term that resonates most is **repeatability**. The ability to repeat the same steps across multiple devices in your fleet – without being affected by changing variables – leads to minimized operational burdens.

> **But what is the driver that enables the change from reactive to proactive, uncoordinated to agile and manual to orchestrated?**

It's automation. Specifically, integrating multiple tools into a single, seamless architecture synergizes device management, identity and access and endpoint security workflows to meet the following three objectives that serve as the hallmarks of achieving repeatability to scale without burning out IT or technical teams:

Resources

Standardize hardware and software provisioning that supports educational goals through consistent stakeholder experiences.

Efficacy

Minimize teaching and learning disruptions by developing **flexible** workflows that streamline access to learning tools.

Financial

Repurpose EDU dollars by leveraging technological **efficiencies** that eliminate manual toil, delivering significant ROI for institutions.

A core consideration when developing deployment strategies is not to automate everything in one go, but rather to focus on the most crucial aspects of deployment and device management after assessing the unique needs of your school, institution and/or region, to reap the greatest benefits from automation first.

> **ProTip: Just because something can be automated doesn't mean that it should be automated (or that stakeholders will benefit from doing so).**

The clear goal with automation is to transform repetitive manual tasks into a predictable operation using comprehensive and holistic workflows that can be reused to meet scaling requirements with thoughtfully designed architecture (automated consistency through repeatable workflows) – not by force (adding headcount to keep up with manual demands).

The latter road leads to never-ending hurdles. As IT attempts to align manual workflows with educational objectives, technical teams remain in "*firefighting* mode" as they attempt to:

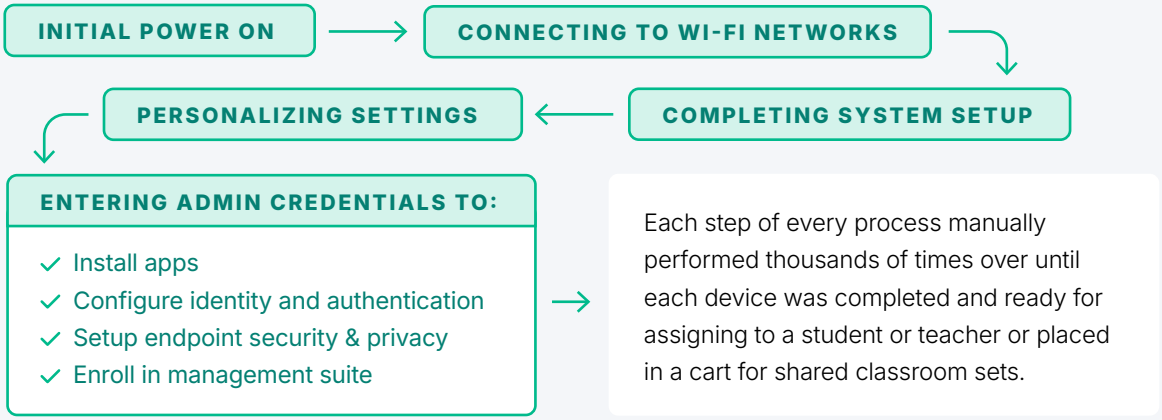
- **Maintain accurate inventory lists** of hardware and software resources, including device and licensing assignments.
- **Actively monitor fleets** and apply OS, software and security updates to mitigate risk from vulnerable devices.
- **Configure device fleets** for students and teachers across different grades and sites while meeting varying requirements for each.
- **Enforce baseline compliance** across multiple platforms and device types, while providing unified reporting and auditable proof.
- **Ensure endpoints are secured** against evolving cyber threats and stakeholder privacy is upheld in accordance with regulatory requirements.
- **Perform service calls and equipment repairs**, as well as off-boarding and disposal of devices meeting EOL.

Conversely, the former "seamlessly converts dream workflows into operational reality" through sophisticated technologies (that we'll cover throughout the chapters of this paper) that combine to form a unified solution. The result is a single, cohesive strategy for device lifecycle management that:

- **Scales alongside growing device programs efficiently.**
- **Delivers consistency and compliance across ready-for-learning devices.**
- **Supports learning goals and educational outcomes.**
- **Shifts focus from manual setup to aligning with instruction.**
- **Adopts repeatable, automated deployment models.**
- **Empowers IT teams – small and large – with reusable workflows.**

Enrollment and provisioning at scale

IT has spent the better part of summer break unboxing new devices, laying them out in a production line and physically touching each device:



However, it's the first day of a new school year. Teachers can't teach and students aren't learning because:

- Devices can't connect to Wi-Fi
- Stakeholders can't login
- Necessary apps aren't installed
- Security settings are misconfigured
- Teacher devices are personalized for students (and vice-versa)
- Not all devices are communicating with the MDM

The above is a real-life example of a problem that has been impacting schools globally since the dawn of technology adoption in K-12.

The problem isn't "IT's not working hard enough" – it's that manual provisioning processes were never intended to match the economies of scale required to successfully deploy large device fleets within narrow time frames. From human limitations to process fatigue, and a healthy sprinkling of Murphy's Law, the higher the volume of devices, the more evident cracks in manual processes become from increased pressure and uncontrolled variables.

You don't have to be a wizard like Harry Potter to achieve this because it isn't magic – it's architecture. And while there's certainly something magical about watching 1,000+ devices enrolling in your MDM and automatically getting provisioned for the intended stakeholder right out of the box – arguably the best part is that IT doesn't have to lay a finger on it. The device merely needs to be unboxed and powered on for the workflow to kick in. And because devices can be used while remaining workflows are executed, stakeholders can dive right into teaching and learning sooner rather than later.

The average time spent manually configuring a device is 2-4 hours, depending on configuration needs. Switching from reactive (manual) to proactive (automated) workflows, that delay can be reduced to approximately **15 minutes for Mac and shaved down further to 5-7 minutes for iPad**.

The strategy: Work smarter, not harder

Scaling begins at enrollment. After all, device fleets without centralized management, identity and security are like a house without a solid foundation.

With that in mind, our recipe for scalability relies on three essential technologies, working hand-in-glove, to deliver a fully automated enrollment and provisioning workflow. One that it does seamlessly across a classroom, grade level, school, multiple sites or an entire region.

Automated enrollment via Apple School Manager (ASM)

Apple hardware procured directly from Apple or authorized resellers, think Mac computers, iPad and Apple TV devices are linked to your ASM account. Also, linked to ASM is your Jamf instance, creating a pass-through where current and future equipment purchases automatically appear within Jamf streamlining the enrollment process. Additionally, obtaining access to student and employee information is made easy when integrating Student Information System (SIS) data with ASM, saving countless hours of manually creating credentials for each student and faculty member to access device resources.

Simply put: no manual entry or toil required to enroll devices or create managed Apple IDs with MDM – that's already taken care of.

Evolve core management as needs grow with Jamf

Jamf is a single, purpose-built solution that minimizes complexity and acts as a single source of truth when managing devices. Equally important, it significantly reduces administrative overhead across device lifecycles for K-12 fleets by integrating device management, identity and access management and endpoint security by design. Alongside support for common tooling used in K-12 environments, like digital signage, Learning Management Systems (LMS) and unified reporting, it sets the stage with enrollment and serves as the central touchpoint for each subsequent phase. Implement baseline security postures? Yes. Perform active monitoring and trigger policy-based remediation? Check. Maintain up-to-date inventory lists and execute secure decommissioning workflows? Handled, all within Jamf.

Streamline device provisioning with Zero-Touch

The seamless integration between ASM and Jamf delivers zero-touch deployments across your entire K-12 infrastructure. Whether scaling across grade levels, multiples buildings – on-campus or off – devices are deployed consistently regardless of whether they are new equipment assignments or require resetting to resolve an issue. Devices provision automatically and according to the stakeholder's needs with consistency and in a fraction of the time – reducing interruptions and help desk ticket requests – enabling stakeholders to be productive sooner while freeing IT teams to focus on delivering better experiences.

Configuration consistency across schools

In this paper, "inconsistency" is used in reference to the problem of variability. Specifically, it's the leading cause of device misconfigurations — also referred to as configuration drift — and contributes to unsuccessful deployments.

Generally speaking, drift occurs as an inevitable result of tech usage over time. Consider something as necessary as apps being installed or OS updates performed as being enough to cause changes in existing configurations. That said, it's important to acknowledge that drift is also a byproduct of negligence, introduced when performing repetitive tasks. A missed step or slight misconfiguration, requiring a 30-second manual fix per device, adds up to over 8 hours of educational time lost to manual corrections for every 1,000 devices.

1,000
DEVICES
X
30s
PER DEVICE
=
>8
HOURS LOST TIME

And that's just one resource during one instance. Imagine what teachers, students, IT, leadership and institutions could accomplish with that amount of time (or the equivalent financial impact it represents) at their disposal?

The answer underscores precisely why consistency matters — and highlights the criticality of consistency-driven workflows at scale.

How can schools achieve consistency and efficiency through provisioning and deployment workflows? Before you can deploy a workflow, it must first be designed to carry out specific tasks. Those tasks define what the "ready for learning" state for a device will look like. While this state can differ from school to school, the road to consistency for K-12 institutions begins with identifying what apps, settings, configurations – basically everything a student or teacher needs to learn or teach – and document what ready for learning looks like for your site.

The approach: Plan for resilience

> **"An hour of planning can save you 10 hours of doing."**
>
> **– Dale Carnegie**

Defining what a 'ready for learning' looks like sits at the intersection of enrollment and scalability. Once armed with this crucial information, there are tools and technologies baked into Jamf to help IT streamline consistency for each stakeholder persona – ensuring deployments are standardized while mitigating drift at scale.

Apply templated configurations with Jamf blueprints

Once instructional technology teams decide what ready for learning looks like, institution-specific requirements alongside necessary apps, settings and SSO configurations can be stored as a blueprint. During the provisioning phase, each device is automatically configured according to the blueprint assigned, matching the ready for learning state consistently.

Managing multiple personas, such as student, teacher or staff member is as easy as creating a blueprint as unique as the needs for each use case. This ensures that devices earmarked for specific stakeholders apply the blueprint mapped out to meet their specific needs every time.

Prevent drift automatically with modern management

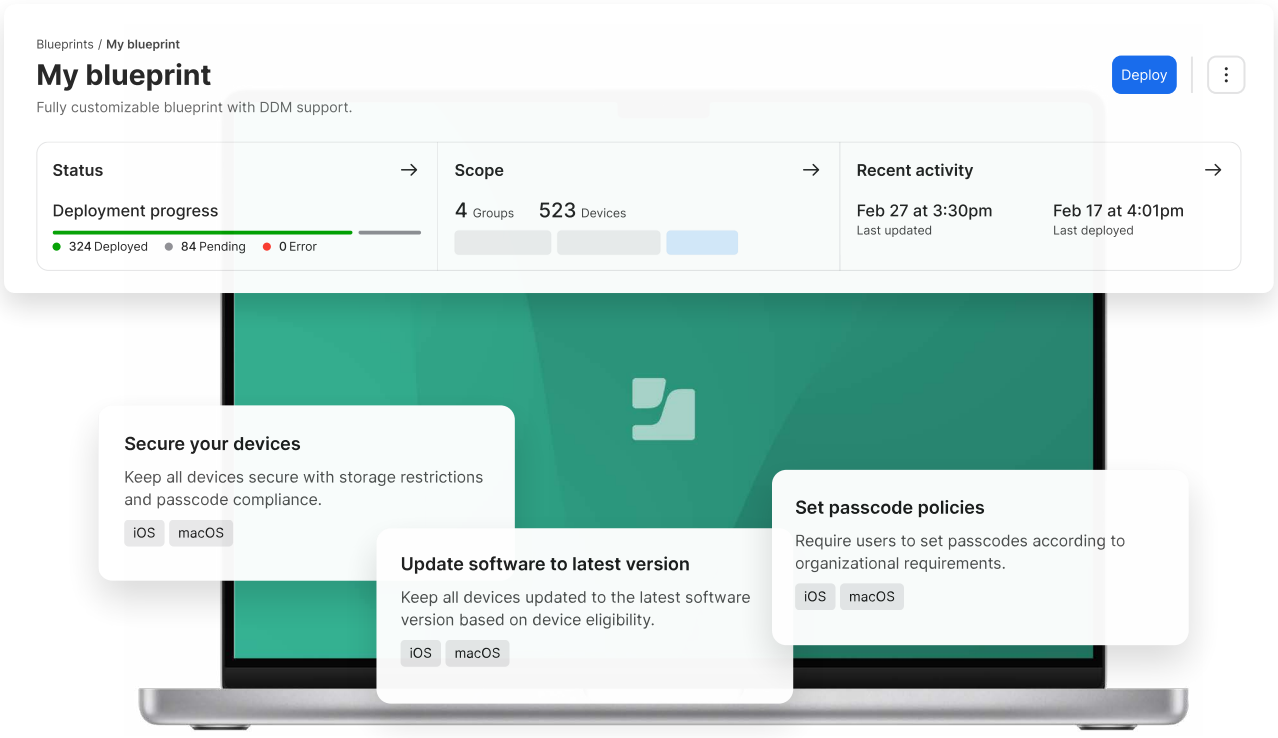
Declarative Device Management (DDM), or the modern protocol for managing devices is designed by Apple. DDM ensures that devices are configured and enforces configurations with performance and scalability in mind and is the engine behind blueprints. Asynchronous communications shift to proactive device health reporting by keeping a copy of required settings stored on devices themselves, ensuring endpoints remain consistent, even without internet connectivity.

Increasing device counts creates additional network traffic which bogs down communications. But DDM was developed to minimize polling between your MDM server and device fleet, side-stepping connectivity issues and efficiently handling updates, allowing learning to occur at school, from home or anywhere else.

Smart Groups enables flexible management combinations

Jamf's scoping technology, and the secret sauce behind automation at scale, dynamically groups devices together to deliver customizations, settings, applications and among many others, blueprints to devices based on targeted personas. For example, when students change grades, removing those devices from the former grade level and adding to the new one automatically deploys and configures those devices to the designated ready to learn state for the appropriate grade level.

From a security perspective (more on this topic later), Smart Groups can be paired with policies to detect non-compliant devices, triggering the linked policy to automatically execute, remediating the endpoint in the background without interrupting the stakeholder or requiring a help desk ticket to resolve.



App and update management

In this section, the term "software" is used to refer to any code base that is used to perform a function on a device. Examples include an app that facilitates student creativity, a service used by teachers to take attendance or an update to security or the underlying OS. The distinction is necessary since, at a micro view, application management refers not just to keeping apps up to date, but highlights K-12's dependence on apps also being present on the right devices at the right time for digital learning and teaching to occur without interruption.

At a macro level, app lifecycle management is a crucial part of the software ecosystem. Considerations like volume and policies add to variability, making it both markedly difficult to manually manage software as it scales and significantly riskier as unpatched vulnerabilities increase exponentially as device counts and variability sprawl.

In short, when software management breaks down, learning breaks down.

But what exactly causes this in K-12?

- **Varying software tools needed across different grade levels**
- **Access permissions and configurations that change depending on stakeholder roles**
- **Apps deployed to the wrong devices (or not deployed at all)**
- **Incompatibilities due to missing software updates**
- **Increased risk from insecure and/or misconfigured apps**

On their own, each point represents an inconvenience that may only take minutes to resolve on one device. But when multiplied by hundreds, thousands or tens of thousands of devices, this burden increases to days, potentially weeks, worth of work for IT to resolve, and leaves institutions without access to the very tools necessary to drive desired learning outcomes. And while there's never a good time for problems of this scale, it's especially troubling just before or during high-stakes testing windows where all stakeholders already feel the pressure to succeed.

What does successful software management at scale look like?

- Student devices can access the learning tools they need, when they need them.
- Teachers can introduce new tools without submitting a help desk request.
- Patch management occurs automatically in the background – no stakeholder intervention necessary.
- Managed apps are configured with security and privacy by default.
- Policy-based management ensures devices remain compliant.
- IT implements changes once while the architecture handles delivery.
- Changes are logged and easily retrievable to prove compliance to auditors.

CHAPTER 3

The process: Resolve breakdowns *before* they occur

Accounting for blockers by implementing processes to prevent them causing breakdowns shifts IT from reactive to proactive. Now, the team can turn their attention and skills to tightening alignment with educational operations to deliver stellar stakeholder experiences instead of scrambling to fix problem after problem or worse still, be the "reason" why stakeholders couldn't complete a task or objective.

Automate Patch Management to maintain security postures

Unfortunately, Edu remains a high-value target for data breaches and misconfiguration (including missing updates), accounts for 30% of risk from miscellaneous errors according to the Verizon 2025 Data Breach Investigation Report. Automating patches leverages architecture to scale as needed while closing gaps in security across device fleets while being mindful of K-12 schedules (i.e., deferring updates to a suitable time vs mid-lesson).

Optimize the learning environment with Jamf Teacher

Teachers gain a specialized app that augments digital instruction by providing them the capability to securely deploy managed apps to their classes. Simple and easy to use, this reduces lag between "we need this tool" and "students have this tool," without requiring access to Jamf's management console or an IT degree to make it happen.

Eliminate app management overhead with App Installers

A curated, and growing, list of applications sourced securely from their developers and expertly packaged by Jamf. Not only do App Installers uphold baseline security postures, but they eliminate manual distribution of macOS apps. When combined with Smart Groups, it automates delivery of the right apps to the right devices – scoped by grade, role, group membership, or any other attribute customized to meet your school's unique needs.

Reduce IT requests and empower stakeholders via Self Service

Imagine being able to visit an app store with curated software, settings and common configurations, customized to your site. Say 'hello' to Self Service from Jamf. Students, teachers and staff gain access to IT-approved tools that they can download and install without submitting a service ticket or experiencing delays. Think of it as stakeholders getting access to what they need, when they need it, or flexibility with guardrails.

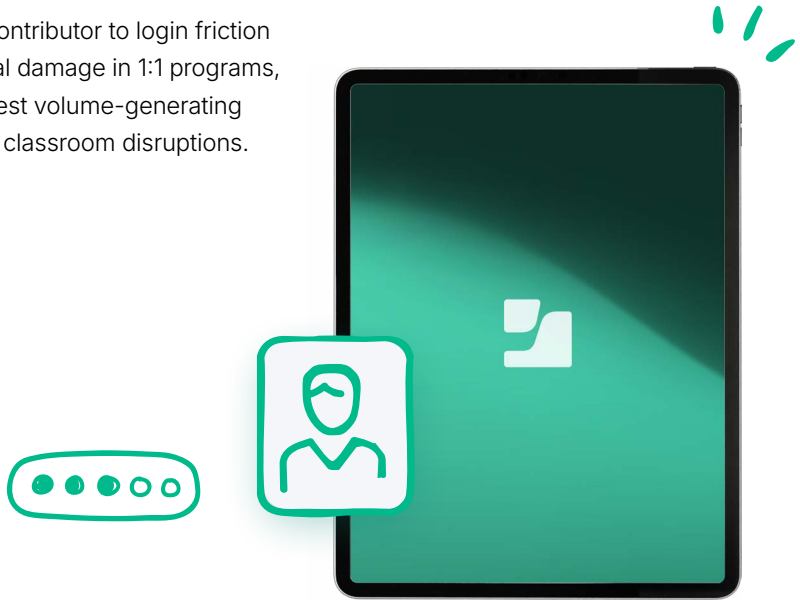
Jamf Student keeps learners on-task and distraction-free

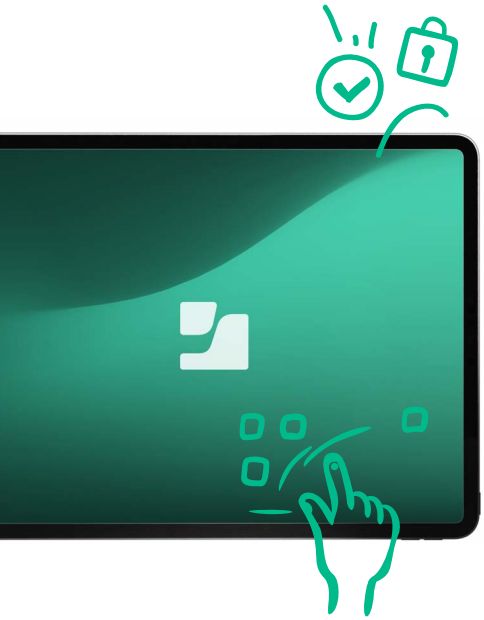
Keeping students motivated to learn while on the internet is difficult enough. App-related issues can easily turn from disruption to distraction. This is why Jamf Student was designed: to extend real-time control over what's accessible on student devices (and when) to keep instruction time at the forefront of learning.

Identity and login friction

Identity is synonymous with authentication. The term ***'login friction'*** is often used to describe both — but it leans too heavily on the latter while providing too little context on the former. For the purpose of this paper, ***login friction*** refers to authentication issues, like password resets and manual toil associated with login fatigue (too many passwords) whereas identity refers to the security-oriented concept of provisioning credentials and securing access to K-12 resources.

To say managing passwords at scale is a main contributor to login friction is no minor statement. Sitting just behind physical damage in 1:1 programs, password resets and access issues are the highest volume-generating sources for IT support tickets and subsequently, classroom disruptions.





Unlike devices, which are limited in number to the hardware on hand, identity is much more unbounded when considering one account per stakeholder, non-human identities (NHI), commonly known as service accounts, and the permissions and/or privileges designated to each account type. These don't just represent a potential pain point for IT at one time or another, but when managed manually, the constant stream of tickets doesn't just slow down the stakeholder requesting support – it creates a queue that grows more unwieldy with each device, stakeholder and app/service that requires a unique login.

When multiplying a single support issue by 1,000-10,000 stakeholders, login friction doesn't just slow down individual stakeholders — it grinds the gears of learning, teaching and daily operations. Left unaddressed, what starts as minor slowdowns compounds into something that brings everything to a halt.

CHAPTER 4

The framework: Structuring authentication and authorization

This scenario above underscores the criticality of identity at scale. For teachers, when accessing educational resources securely, like lesson plans stored in the cloud without requiring three different passwords. For learners, it's seamlessly moving from one app to the other when changing classes without reauthenticating. Below we discuss how modernized identity integrations eliminate manual, repetitive tasks to reduce friction that compounds at scale while streamlining digital stakeholder safety, operational security and continuity of education.

Seamlessly access apps with Single Sign-On (SSO)

SSO enables stakeholders to gain access to all protected apps, platforms and services by authenticating only once. Cut down on forgotten credentials or security concerns, like weak or repeated passwords by enabling stakeholders to focus on school-related tasks after initially authenticating to the device or portal.

Reduce IT's password reset burden

In a case of "less is more," fewer credentials mean fewer passwords to reset because stakeholders aren't experiencing cognitive overload from trying to memorize dozens of accounts. This translates to two things for IT: fewer tickets from account-related failures, which equals more time to focus on higher-skill work, like improved stakeholder experiences and driving value from greater alignment with educational objectives.

Extend identity with Jamf + Identity providers (IdP) you use

Move away from manual account maintenance to centralized identity management when integrating the IdP your institution already uses with Jamf to extend management and security workflows. Configure and enforce consistent access policies tied to stakeholder credentials – not specific devices – so permissions follow stakeholders from K-12 without manually reconfiguring per-app, per-device or per-grade.

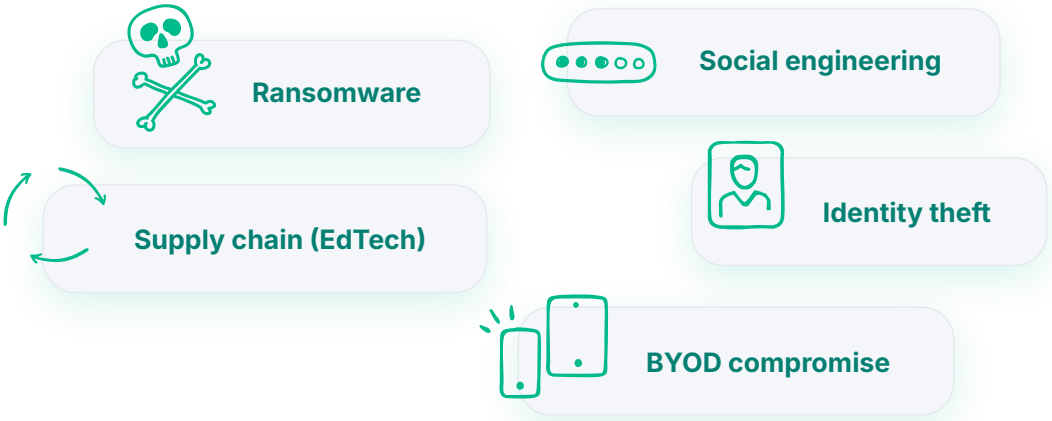
Set account provisioning and access permissions correctly each time

Automated account provisioning for new students, faculty and staff places the right tools in the hands of stakeholders from day one. No help desk tickets necessary or waiting on IT to perform on-boarding – just authenticate and access to the apps, sites and services you need are already configured. What about grade level or staffing changes? Pairing Jamf + your IdP + Smart Groups ensures access automatically updates based on grade level or role requirements.

Security without added burden

Securing stakeholders, devices and data while upholding privacy and maintaining lockstep with compliance requirements is difficult enough without the added challenge of hybrid use cases. 1:1 initiatives, computer labs, shared devices contained in COWS (computers on wheels) – a percentage of devices on-premises and protected by perimeter controls, the rest move freely from home to school, after-school activities and so forth. The gist here is that apart from annual refresh cycles, these devices spend the majority of the time off campus.

Pair this "moving target" scenario with the modern threat landscape actively targeting K-12 globally with sophisticated attacks, like:



And the complexity increases significantly as it mixes with the volume multiplier from growing device fleets to add a security layer to the scaling challenges we've been discussing throughout this paper.

IT is tasked with directly overseeing each device, app and connection while mitigating risk from vulnerabilities, threat actors and stakeholder behaviors. At scale, this represents potentially thousands of data points to assess daily. The 2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience, found that during an 18-month period between July 2023-December 2024, there were 9,300 confirmed cybersecurity incidents. To quantify this further, this amounts to nearly 17 cyberattacks occurring each day during the 548-day period.

In other words, threat actors don't keep school hours, so K-12 cybersecurity protections need to be automatic, contextual and holistic – regardless of whether devices are in the classroom, at the family dinner table or on holiday. When threat protection never turns off and policies adapt to where devices are and when they're there, that's not just better security – it's the only model that works dynamically and scales across K-12 infrastructures with efficacy and consistency.

The model: Defense in depth (DiD)

DiD is a concept that blends multiple security controls and processes under one umbrella, effectively layering protections in a manner that provides stakeholders, devices and institutions alike many levels of protection against sophisticated attacks. If a threat manages to evade one layer, the layers above and below it provides added safety nets to mitigate the risk before it becomes something worse. Where modern environments see different device types (computers, tablets, and media connectors) running on multiple platforms (macOS, iPadOS, tvOS, Android and Windows) – all are being used by education stakeholders to learn, teach and perform daily operational tasks – less complexity and better, dynamic protections are the best model for scaling security while minimizing interruptions.

Prevent network-based threats, cross-platform

Attacks like phishing, eavesdropping and cryptojacking are all seeing record growth in targeting K-12 institutions. Across desktop and mobile devices alike – anywhere where there's an active network connection – Jamf security acts as the bouncer that keeps the door is proverbially open learning and closed for attack vectors that place school data at risk. Paired with visibility into device health data, IT gains detailed information regarding which devices are being targeted and why, to mitigate risk factors appropriately.

Keep students safe from harmful content with Jamf Safe Internet (JSI)

K-12 students range in age and maturity, making a "one size fits all" approach not very conducive to learning or requiring constant manual adjustments to meet the needs of older groups at the cost of younger groups. JSI not only blocks inappropriate content (and distractions) but offers granular controls, like age-appropriate filtering and policies to automate access to internet resources outside of school, say on weekends, without compromising student online safety.

AI-based threat protection that evolves

Threat actors are leveraging AI to augment attack sophistication. This makes them harder to identify and protect against, which is why Jamf complements in-network controls with on-device protection that incorporates Machine Learning (ML) to assess AI-risks, like zero-day phishing and stop them – even if stakeholders mistakenly click malicious links. Moreover, on-device means security is enabled and working regardless of third-party VPNs, proxy or DNS settings used, this eliminates bypassing protections and gaps in coverage.

Automatically apply policies based on contextual needs

It used to be that using a device at school offered access to all the resources and protection stakeholders needed while using it away from school offered little, if any. K-12 stakeholders increasingly rely on technology off-campus in the same capacity as they do on-campus, but the context change often requires changes to settings. This is where schedule-based policy adaption shines, by automating policy shifts based on contextual information, such as time of day or school calendars (like weekends or holidays). IT defines the rules once and Jamf handles every context shift moving forward – no more interruptions or manual configurations necessary.

Conclusion

Throughout this paper, we discussed the average K-12 ratio of 1,000 devices for every member of IT. Compared to enterprise organizations where ratios hover around 70:1, budget constraints make it nearly impossible for K-12 institutions to close that gap by adding headcount. **In fact, in some regions, this ratio grows ever closer to (or already sits at) 10,000:1**.

This only makes the already heavy burden of supporting students, teachers and staff in K-12 environments even more grueling at scale, including the many variabilities, such as:

- Provisioning diverse and growing device fleets
- Age-appropriate considerations across institutions
- Identity and authentication friction, on-premises/cloud-based
- Multi-site/building and institutional deployments
- Grade-level requirements across schools
- On-campus and off-campus security parity
- Cross-platform support and compliance enforcement

THE PROBLEM: Manual processes are broken

There simply aren't enough hours in a day, days in a week, or weeks during annual refreshes to perform each and every task at scale when facing down 1,000 devices.

THE SOLUTION: Better architecture not more hands

Once again, we circle back to the key term that bears repeating (no pun intended): Repeatability at scale beats manual effort every time.

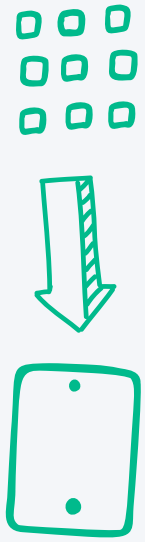
"The ability to repeat the same steps across multiple devices in your fleet – and to do so without being affecting by changing variables – leads to minimized operational burdens."

Across the device lifecycle, from:

- **Procurement** — PLANNING AND ENROLLMENT
- **Maintenance** — SECURITY AND VULNERABILITY MANAGEMENT
- **Deployment** — CONFIGURATION AND APP MANAGEMENT
- **Decommissioning** — INVENTORY AND SECURE DISPOSAL
- **Monitoring** — IDENTITY AND ACCESS REPORTING

Standardization, flexibility and efficiency are the central themes of automation. Across each chapter, the central thread of automating tasks and processes resonates as the keys to "achieving repeatability to scale without burning out IT."

THE VISION: **Shift from reactive to proactive**



Through automation, manual, repetitive tasks are transformed into predictable operations that enable comprehensive and holistic workflows that are reused again and again to scale consistently, effectively and efficiently each time new devices are added or existing devices require provisioning.

More importantly, is that this occurs without interrupting learning environments and without requiring IT to step in to perform the task every. single. time. In fact, because the architecture is thoughtfully designed with stakeholders of all skill levels in mind, teachers are able to quickly return to lesson exploration after deferring an update if prompted during teaching. Or optimizing student engagement, when an unavailable app is needed, learners can simply access Self Service and install the pre-approved software to continue learning.

Neither of these common scenarios required a help desk support ticket or IT intervention – and most importantly – none of them prevented the stakeholder from performing in their role or delayed them until someone with admin privileges could attend to the problem.

Takeaways for IT and technical teams

As device counts increase, manual workloads quickly become unsustainable and educational performance — not just IT's ability to provide timely support — suffers exponentially.

Automate to break device count bottlenecks

Replace manual provisioning with automated workflows, cutting provisioning time from hours to minutes.

Standardize "learning ready" devices at scale

Use templated configurations to ensure every student and teacher device is consistently setup from day one.

Eliminate IT toil with zero-touch deployments

Enable devices to automatically enroll and configure out of the box, promoting first-day readiness.

Shift from reactive support to proactive operations

Unify device, identity and security management through automation to focus on improving learning outcomes – not firefighting.

Resource delivery at the right time without friction

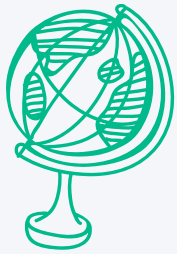
Dynamically assign apps and resources based on role or grade, giving stakeholders immediate access without delays.

Eliminate login friction and password fatigue

Implement SSO and automated identity workflows to reduce password resets and maintain secure access.

Scale security without disrupting learning

Apply layered protections that dynamically adapt enforcement on- and off-campus seamlessly.



Experience how Jamf lifts K-12 operational burdens by empowering stakeholders to resolve everyday issues without taking focus away from the task at hand and shifts IT mindsets from fighting fires to contributing to learning outcomes.

jamf

www.jamf.com