Identity Automation
a Jamf company

K-12 MFA Guide

Make Districtwide Multi-Factor Authentication Not Only a Reality--- But a Success

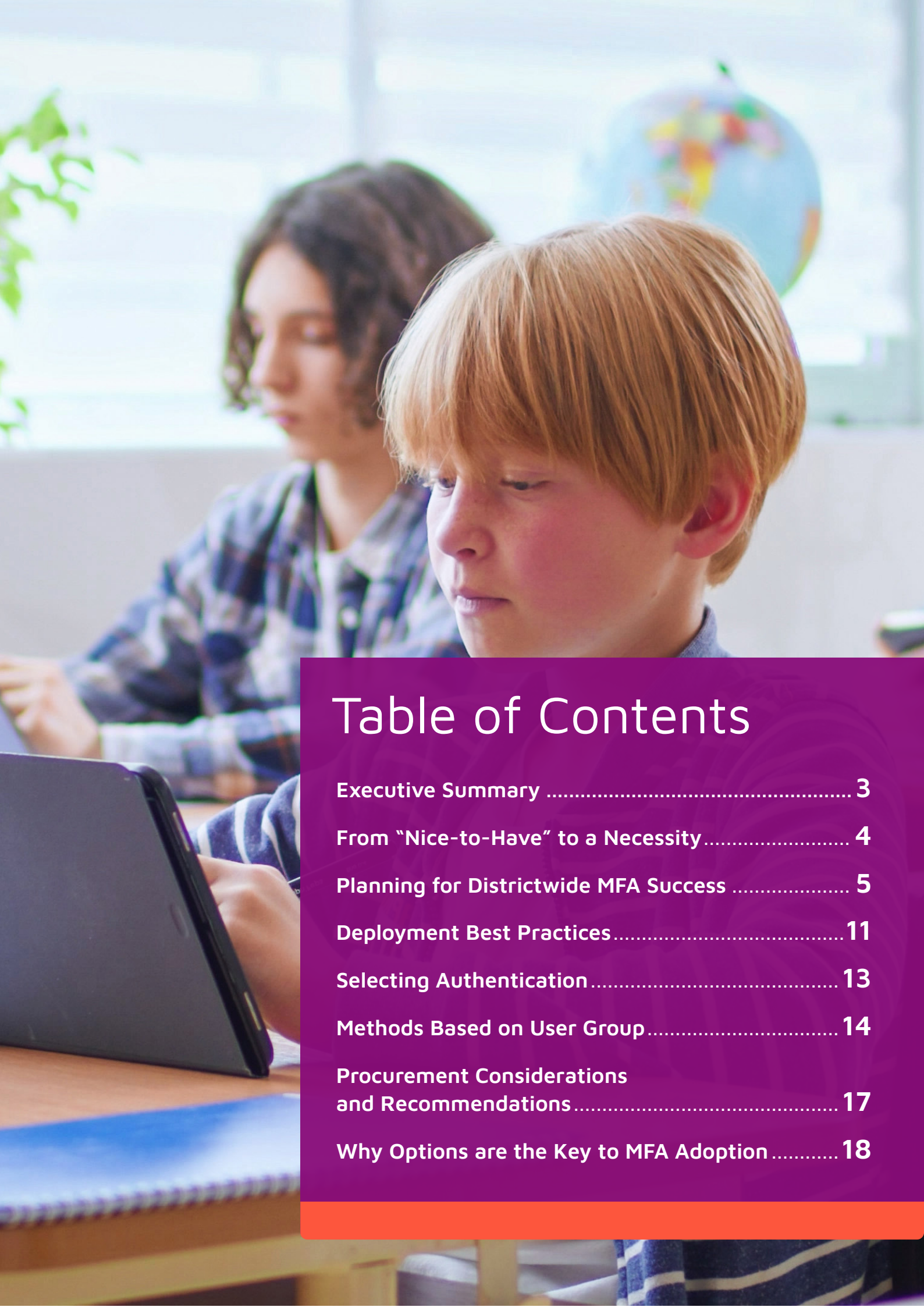


Table of Contents

Executive Summary

K-12 school districts have become a primary target for account takeover attacks (ATO)— especially ransomware— driving up cybersecurity insurance premiums and the bar for coverage. As these requirements become more stringent, districts must navigate how to stay compliant.

This guide provides best practices to create a step-by-step strategy for planning, selecting, and deploying Multi-Factor Authentication (MFA) districtwide.

Key Finding

- *K-12 districts struggle to implement enterprise-wide MFA, due to user population size and complexity (ex - young and special needs students), as well as the political and equity complications regarding use of cell phone.*
- *The key to successful districtwide MFA adoption is providing a broad array of authentication methods that can be tied to specific user groups, while being cognizant of the security, ease of use, and risks tied to each method.*

Recommendations

1. **Simplify Authentication with a Universal Login Point.** Fewer login points, means fewer access points to secure. Leverage a single universal identity provider that funnels all users to single point of entry where adaptive MFA is enforced.
2. **Create a Cross-Departmental Committee**. Foster districtwide buy-in for the project by developing champions who can explain the need for MFA and assist with adoption at each stage.
3. **Document an Inventory of Existing Resources**, including devices, systems, applications, access points, and more.
4. **Document Potential Cybersecurity Risks** to facilitate policies around mitigation and recourse.
5. **Tailor Authentication for User Experience and Risk-Level.** Different user groups have different needs and abilities. Providing end-users with authentication methods with which they are comfortable using increases adoption and ease of access, ultimately enhancing district security posture.

From “Nice-to-Have” to a Necessity

The pandemic was a catalyst for change in Education. Virtually overnight, almost every aspect of learning was turned on its head. However, through crisis, came innovation and the adoption of tools and technologies that enabled learning beyond classroom walls.

Millions of students who once lacked internet access and digital devices at home are now equipped to learn from anywhere. Our concept of where and when learning is done has changed. Digital learning is borderless— users can access online resources from anywhere, at any time.

District digital ecosystems have evolved into complex webs of systems, applications, and public networks that have become increasingly difficult to secure, making school districts prime targets for malicious actors. In fact, Education has become the most targeted industry for ransomware attacks, with Sophos reporting 63% of K-12 districts reporting attacks in 2024 and 80% in 2023.[7]

These mounting threats are not only driving an urgent need for greater cybersecurity, but also mandates from cybersecurity insurance providers. One of the most common insurance requirements is requiring multi-factor authentication (MFA) to secure access to district resources. District-wide MFA is no longer a “nice to have,” but a necessity.

Getting Started— The What, the Why, and the How

When faced with the predicament of evaluating a district-wide MFA strategy, the first questions that typically come to mind are:

- What is Needed?
- Why is now the time for MFA?
- And ultimately, how do we implement MFA successfully?!

In this guide...

We will not only break down the what, the why, and the how of implementing MFA— but we’ll also discuss the strategies successfully used by other K-12 districts for districtwide success.

Planning for Districtwide MFA Success

An MFA strategy in K-12 Education should accomplish four objectives:

1. Secure the entire digital ecosystem (not just EdTech or Enterprise systems)
2. Integrate seamlessly into the existing technology stack
3. Provide equitable deployment that caters to the individual needs of each user
4. Continuously evolve with a district's ever-changing and unique needs

However, for most districts, implementing MFA across such diverse user populations is daunting, especially with seemingly conflicting mandates that include:

- Enforce enhanced security measures
- Ensure frictionless access that doesn't disrupt the learning process
- Deploy a tool that is usable and equitable for all users

While balancing these requirements is a challenge, with the right planning, strategy, and solution, districtwide MFA is not only possible, but can even improve ease of access. With that said, let's get started!

What Is Needed?

When defining your MFA strategy, start by examining your users' points of access. The fewer login points that exist, the fewer access points you have to worry about securing.

Ideally, your users will be provided with a universal login point that they are funneled to—regardless of which systems they access. At this login point, the user authenticates once, and then, gains access to their relevant applications with security tokens as a part of a **federated trust** (think: SAML, OAUTH, WS-FED, etc).

This should apply to controlling devices, applications, and remote access. The near-term goal should be to have a **single identity provider that can enforce adaptive MFA**. Following this strategy can serve as a general 'catch-all' to secure the authentication of all users, to all systems.

Authentication Built on Identity Management

At its core, authentication is the end user action that is built on top of a foundation of access management and authorization policies. Without those foundational elements squared away, authentication of a user logging in is not a viable security measure in and of itself.

So, how can your district ensure learning workflows are efficient, yet secure? The answer is simple: by putting the digital identities of each person within your organization's community at the center of your technology strategy.

Most districts today still think about identity management as simply automated provisioning of accounts that provides users with access to the tools they need. However, there is so much more to it! True identity management offers far more than simple login syncing, which is more of a user experience than security benefit. Digital identity management provides automated enforcement of access control policies and seamless execution of your cybersecurity strategy across the entire digital ecosystem.

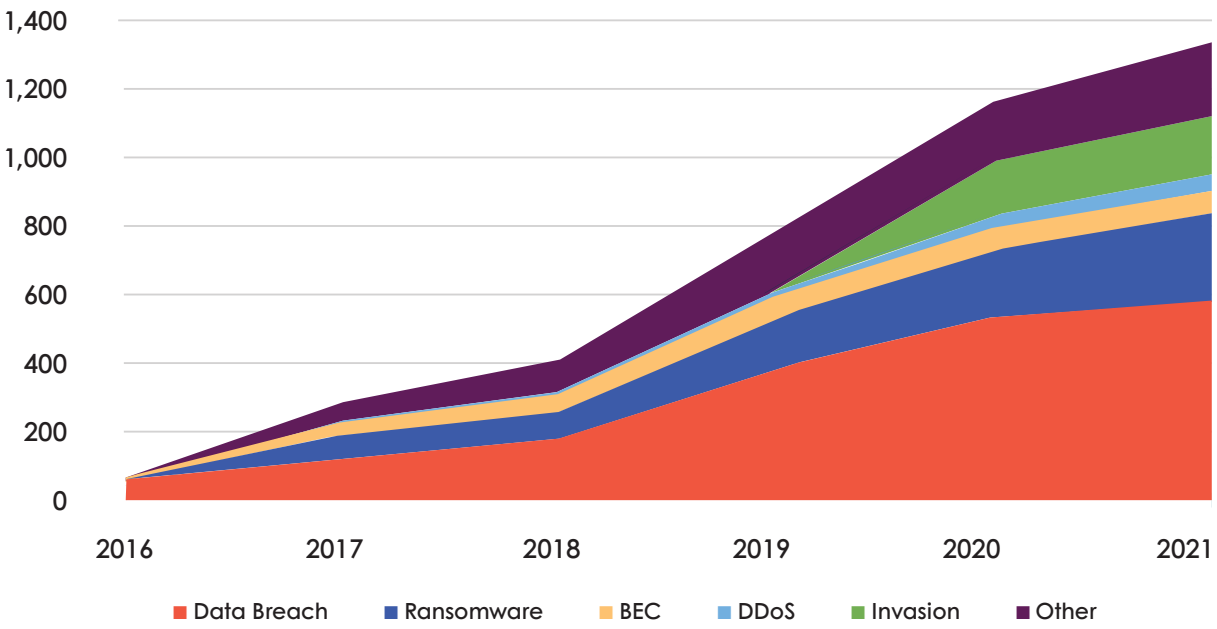
Simply put: Identity-driven policy enforcement enables secure, but flexible, authentication across ALL users, applications, and devices without impacting classroom experience. To learn more, download the full eBook here.

Why is Now the Time for MFA?

So, why are cybersecurity insurance providers declaring premiums will double for districts without MFA in place?

This push is directly tied to the staggering rise in ransomware attacks on educational institutions. In 2020, ransomware attacks affected 1,681 school districts, colleges, and universities in the United States.3 In the first half of 2021 alone, these attacks nearly doubled as 1,097 organizations reported they were hit by ransomware.[4] Although a small decline has been observed in 2024 attacks for ransomware, 2023 proved to be the worst year on record with Sophos reporting almost 80% of school districts having some form of attempted ransomware attack.[4]

Number of Publicly-Disclosed K-12 Cyber Incidents by Incident Type: 2016-2023.



Source: K12 SIX, The State of K-12 Cybersecurity: Year in Review

This research, combined with the Joint Cyber security advisory releasing **Weak Security Controls and Practices Routinely Exploited for Initial Access** in May 2022, has led cybersecurity insurance companies to set forth mandates to retain coverage.

MFA is a critical component to curbing the epidemic of account compromise attacks plaguing Education, and it's not a new concept. Verizon's 2020 Data Breach Investigations Report stated that **"MFA can block over 99.9 percent of account compromise attacks**, and with MFA implemented, knowing or obtaining a password alone will not be enough to gain access to a system." [5]

The strategic goal of IT teams should always be to harden the attack surface. The harder it is for a bad actor to gain access, the safer our students, faculty, and ultimately, our data sets are.

How Do We Actually Implement MFA Successfully?

The "how" of implementing MFA is easily one of the biggest challenges faced by technology teams, regardless of industry— disparate user groups, devices, and remote locations must all be considered.

However, this challenge is exponentially more difficult in K-12, due to the lack of institutional control over users and their devices, the need for equitable enforcement, and the importance of not adding friction to the learning process. All of these issues have only been exacerbated over the past few years, as the learning landscape has permanently shifted to include a diversity of identities, devices, and locations that will only continue to grow in number and complexity.

The steps below outline an approach that other school districts have successfully used to deploy MFA at scale and across all users. Following this strategy has allowed these districts to not only harden their attack surface and mitigate rising cybersecurity insurance premiums, but actually enhance ease of access for users.

Step 1: Create a Committee

Instead of asking yourself "How do I implement MFA?," re-angle your thought process to: "How do WE implement MFA?" While implementing MFA may be the responsibility of the technology team, successful adoption requires buy-in across the organization.

In her address to Congress in May 2022, Amy McLaughlin, Cybersecurity Project Director for CoSN, highlighted the importance of this mindset:

> *Cybersecurity is not only an unmet technology need; it is an organizational culture challenge. K-12 schools and districts experience significant challenges in protecting themselves from cyberattacks...It is an issue that requires everybody in an organization to understand and be part of the solution.* [6]

Amy's message rings true going into, and out of every school year. Your greatest tool in deploying MFA is to engage leaders from impacted departments.

By design, MFA increases the amount of steps taken to authenticate to your resources. However, having "boots on the ground" in respective departments helps ensure there are champions to explain the need and assist with adoption at each stage. Controlling change management is crucial to the successful adoption of any new technology initiative.

Step 2: Call Out Weak Points

The first item the committee should assemble on is documenting an inventory of existing resources: "What do we have today?", "What do we use it for?", and "What can we use it for?" are all questions that help determine what is missing in terms of security posture and assess your level of risk. This inventory can include devices, systems, applications, access points, and more.

Step 3: Create a Plan

The committee should be aware of the potential risks and create a plan to address them. While not every cybersecurity risk needs to be completely mitigated by the plan, it's imperative to document all known risks, as well as a potential recourse for each.
For example, consider scenarios, such as:

- What happens if someone guesses the SIS administrator's password?
- What about a student's password and gaining access to their accounts?
- What happens if we lose power in our on-premises data center?
- What do we do if we suffer a ransomware attack?

Use these documented risks to facilitate policies around mitigation and/or recourse by asking questions, such as:

- Can a product or human resource mitigate this risk?
- Can our own policies and user-behavior reduce this risk?

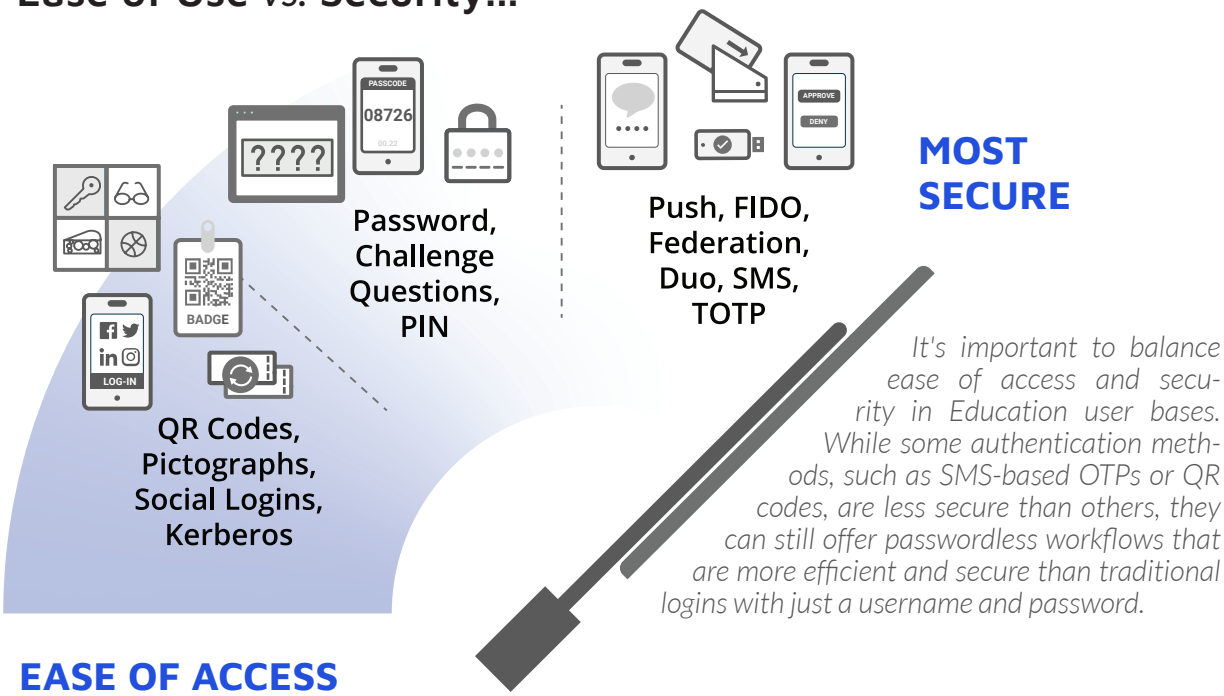
Step 4: Procure Necessary Resources

If it is determined that new resources are required after calling out the weak points and creating a plan, remember the impacted user base. This is critical, particularly in Education, because many two-factor authentication (2FA) and MFA products were designed for enterprise users.

These products were designed with only the corporate employee in mind— subject to one function that values security above all else.

However, in Education, teachers and students are subject to the decisions of the committee, so the right balance between security and ease of use must be highly-considered for each individual.

Ease of Use *vs.* Security...



EASE OF ACCESS

If only one authentication workflow is permitted for all users, it leads to issues with administration, equity of access, user adoption, and ultimately, negates the success of an MFA program, resulting in wasted budget.

For example, a teacher may decline to use their personal cell phone for work-related purposes or a student may forget their username over the summer. In these instances, if there is a single mandated authentication workflow, then these users have no ability to access the resources they need. Unfortunately, a single function or workflow for all users in Education cannot exist. It is simply not practical.

Hands down, the best piece of advice for **making districtwide MFA a reality AND a success** is to remember that: **options equal adoption.** Providing end-users with methods that they are comfortable using not only increases enrollment (and ultimately, security posture!), but actually makes it easier for the individual to gain access to the resources they need.

This approach has proven crucial to keeping students and faculty secure, while enabling remote learning. Otherwise, how can a student request their password to be reset when they are trying to access a Chromebook at home? How can a teacher securely access their email from their iPad?

For the committee and IT teams— this means evaluating a product with multiple modalities or multiple products in combination. Whether it's one platform or multiple products, the key is to provide a broad array of options, while being cognizant of the security, ease of use, and risks tied to each.

For example, authentication methods, such as QR code, Pictograph, and challenge questions are great for ease of access and can be combined with other factors to provide a form of 2FA. However, these options are not as secure as other methods, such as FIDO tokens.

Deployment Best Practice

For all of the options to turn into true adoption, context is queen. Who should use which methods? When should they use them? These are policies that should be a part of the committee's plan.

With Education's diverse and constantly changing user base, ease of access can be leveraged to get end-users comfortable with a passwordless environment, and they can grow from there— literally. As a student progresses through grades, they gain more user access and subsequent risk.

A student's educational journey could begin with authentication methods that focus on ease of access, such as QR code or Pictograph, and evolve over time to more secure methods, like TOTP or FIDO Tokens based on grade level or whether they are logging in from a campus IP address or not. These are just two examples of contextual policies that should be thought through.

Guiding Principles

Consider the following guiding principles as best practice standards when implementing MFA districtwide:

1. ALL privileged accounts must have MFA—this is non-negotiable.
2. When possible, go passwordless.
3. Keep user experience top of mind when selecting authentication methods for each user group.

Access Points

At a minimum, your MFA deployment should be enforceable at the following points of access:

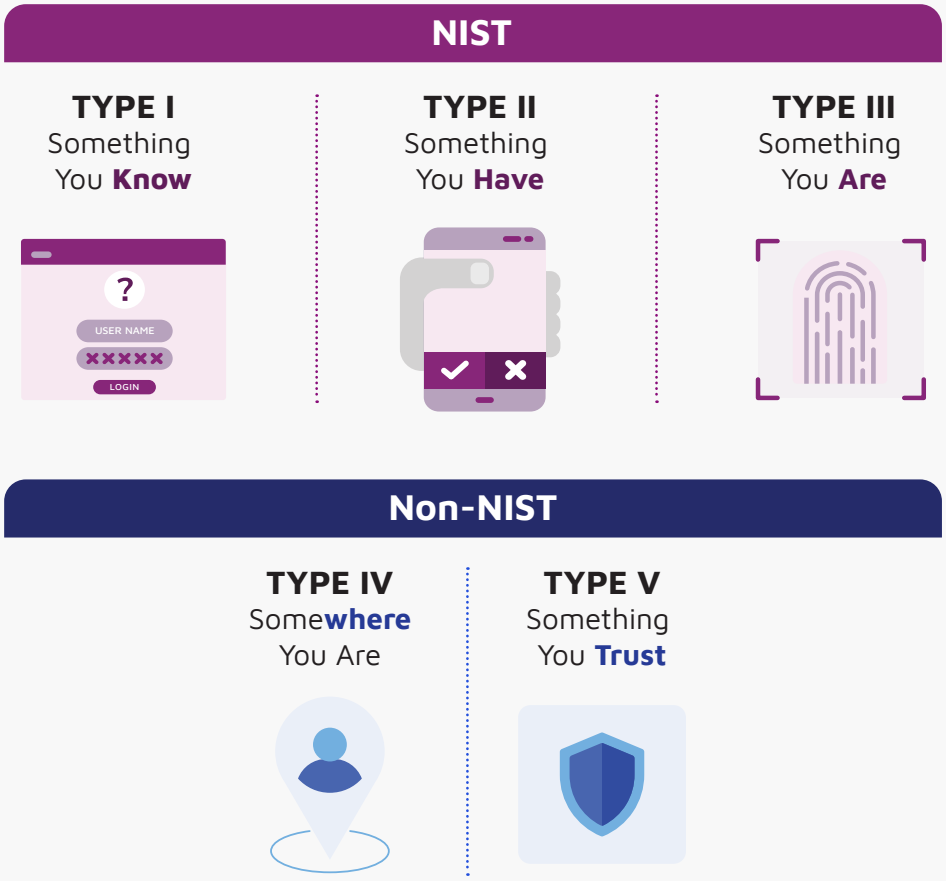
1. Device-level login
2. Federated SSO portal login to access cloud applications
3. Remote access points, like RDP, VPN, etc.

Defining Multi-Factor Authentication

While MFA can be defined a number of ways, one trusted source for public and private educational institutions alike are the published standards by the National Institute of Standards and Technology (NIST).

As defined by NIST, *"MFA, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence— your credentials— when logging in to an account. Your credentials fall into any of these three categories: something you know (like a password or PIN), something you have (like a smart card), or something you are (like your fingerprint). Your credentials must come from two different categories to enhance security— so entering two different passwords would not be considered multi-factor."*[2]

MFA Requires at Least Two Authentication Factors



*Your cedentials **must come from two different categories** to enhance security. Entering two different passwords would not be considered multi-factor.*

-NIST

Selecting Authentication Methods Based on User Group

Authentication methods can be joined together in any combination.
For example:

- **Password + Pictograph**
- **Pictograph + QR Code**
- **QR Code + Social + TOTP**

However, in order to deploy NIST-compliant two-factor authentication, something you have (Token) or something you are (FaceID), should be combined with something you know, such as a Password or Challenge Questions.

It is especially important to be cognizant of ease of access vs security in Education user bases. While some authentication methods, like SMS-based one time passwords (OTP) or QR Codes are not as secure as FIDO tokens or mobile device enrolled push notifications, they can still provide passwordless workflows that are more efficient and secure than a traditional login with username and password.

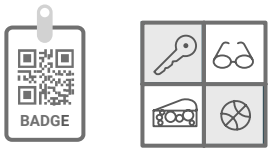
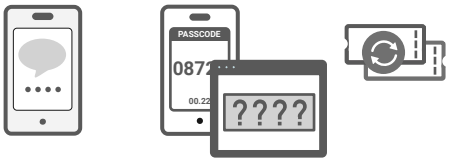
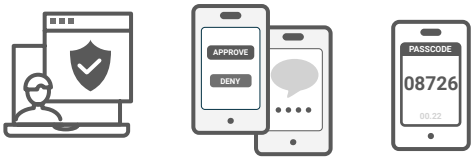
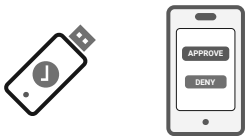
The chart on the following page gives a breakdown of available authentication methods, including level of assurance provided, recommended user groups, deployment examples, as well as pros and cons.

Authentication Methods from Highest Level of Assurance

	FACTOR	ASSURANCE	USER GROUP
WebAuthn/			
	II or III	HIGHEST	Faculty, Staff
Examples: **FIDO 2.0,Windows Hello, Face ID, etc.**			
PRO: Most Secure		**CON:** Requires devices/hardware	
Push Authentication			
	II	HIGH	HS Faculty, Staff
Examples: **RapidIdentity Mobile**			
PRO: User convenience, low cost, Easy, More Secure devices are enrolled		**CON:** Requires a smart phone, Hardware-based, devices can be lost	
Duo Authentication			
	II	MEDIUM	Faculty, Staff
Examples: **DUO Provided Methods** (U2F/SMS/Voice)			
PRO: Leverage investments in DUO		**CON:** Requires DUO licensing	
TOTP via Mobile App			
	II	MEDIUM	HS Faculty, Staff
Examples: **Google Authenticator, Windows, etc.**			
PRO: Common for remote access, leverages existing device, time-based expiration		**CON:** Requires an app download onto a smart phone	
Kerberos			
	I	MEDIUM	Domain Joined Users
Examples: **Windows Machine on Local Networks**			
PRO: No additional action to authenticate, uses Kerberos ticket with user credentials		**CON:** Requires domain connection	

	FACTOR	ASSURANCE	USER GROUP
Social Login			
	I	MEDIUM	Guardians
Examples:	**Login via Facebook, Twitter, Google, Linkedin**		
	PRO: Ease of use, Familiarity and user control	**CON:** Some networks block social, Longer login workflows, Relies on third party integration	
Email			
	II	MEDIUM	HS Faculty, Staff
Examples:	**OTP Sent to Alternate/Personal Email**		
	PRO: No hardware/enrollment needed	**CON:** Emails intercepted , Verification spoofed, Requires alternate email	
Pictograph			
	II	LOW	Pre-K, Elementary
Examples:	**Predefined Custom or Sample Pictures Provided During Authentication**		
	PRO: Easy to access and administrate	**CON:** Requires enrollment	
SMS			
	II	LOW	HS Faculty, Staff
Examples:	**OTP Sent via Mobile Number**		
	PRO: Do not need a smartphone	**CON:** SMS codes intercepted, Verification spoofed	
QR Code			
	II	LOW	Pre-K, Elementary
Examples:	**Printed QR Codes Presented Embedded or External Webcam**		
	PRO: Easy to access and administrate Student-friendly form factor	**CON:** Need device/hardware to authenticate QR code	
Security Question			
	I	LOW	Secondary/Alt Factor
Examples:	**User Verifies Identity By Answering Predefined Secret Questions**		
	PRO: Traditional user, Secondary factor	**CON:** Can be guessed, Can be forgotton by user	
Password/Passphrase			
	I	LOWEST	Default
Examples:	**LDAP Based Password/Passphrase**		
	PRO: Traditional user experience	**CON:** Single factor, Must remember password/phrase, Most likely to be compromised	

Recommended Authentication Methods Per User Type

Pre-K, Elementary and Special Needs	***QR Code, Pictograph*** 
Middle School Students	***QR Code, Password*** 
High School Students	***SMS, OTP, Passphrase. or Kerberos*** 
General Faculity and Staff	***WebAuthn/, Push Auth, SMS, OTP*** 
IT Staff and Privileged Users	***FIDO2, Push Auth*** 
Parents and Gardians	***Social Login*** 
Third Parties	***email, OTP WebAuthn/*** 

Procurement Considerations and Recommendations

In 2020, COVID-19 created a shift in many public learning institutions from a majority on-campus environment to a majority remote population. The shift caused many major public learning institutions to seriously pursue university, district, and even statewide MFA programs to proactively increase security posture and ensure consistent pricing for cyber-security insurance. Since the global pandemic ended, MFA and remote access has continued to be a part of a strategy for both on-campus and remote users. Identity Automation has had the privilege to engage with these institutions, share our field experience, and gain feedback on how their programs are progressing.

Many institutions are following the strategy of forming or leveraging an existing committee of diverse department stakeholders. In addition, they also provide multiple workflows and opt-in options for end-users. This has become a major focus, as MFA requirements are extending to teachers and users that may not have institution-issued resources (think BYOD).

While 95% of your users prefer the ease of access associated with using a mobile device for secure authentication, how do you address the remaining 5%? Instead of leaving these individuals unsecured, or forcing them (good luck) to enroll, institutions are providing contextual-based workflows where users can leverage a mobile device, personal email account, or even hardware tokens to perform a multi-factor login. This offers users who are unwilling to use a personal cell phone to download an app administered by their employer alternatives that better fit their preferences.

Why Options are the Key to MFA Adoption

K-12 education has been **THE** prime target for ransomware, phishing, and other cyberattacks. To add to this, the unique user groups and workflows that need to be managed are more complex than those that traditional, enterprise MFA solutions cater to, where only the corporate employee and standard business processes are handled.

In order to successfully deploy MFA across your organization, careful planning must first occur. That begins with forming a committee, taking a complete inventory of current resources, and recording cybersecurity risks with respective mitigation and recourse.

But ultimately, **the secret to achieving districtwide MFA adoption** is that options equal adoption. It's critical to identify each of your user group's needs and abilities, as well as their risk level and the sensitivity of resources they access.

As K-12 IT teams manage diverse groups of individuals at all ages and stages in life and learning, providing a broad range of methods ensures your users will have a method available that they are comfortable using. As ease of access increases, so does MFA adoption, which in turn, heightens your district's security posture.

Want to download the resources from this eBook to take back to your team?

- **Chart**: Authentication Methods by Highest Level of Assurance
- **Infographic**: Recommended Authentication Methods By User Type

Author Bio

Kevin Satterfield is a Senior Product Manager & Solution Architect at Identity Automation. Since 2015, he has worked with hundreds of institutions from K-12 districts, higher education, public safety, healthcare, and enterprise to address cybersecurity posture and implement MFA. His best piece of advice for implementing MFA districtwide is: options equal adoption.

SOURCES

1. *https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf*
2. *https://www.nist.gov/back-basics-multi-factor-authentication*
3. *https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/*
4. *https://www.cognyte.com/blog/ransomware_2021/*
5. *Verizon Business 2020 Data Breach Investigations Report, https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report*
6. *https://www.help.senate.gov/imo/media/doc/McLaughlin%20Testimony%20Final2.pdf*
7. *https://www.techtarget.com/searchsecurity/feature/Top-10-ransomware-targets-in-2021-and-beyond*

Identity Automation
a Jamf company

FOR MORE INFORMATION CONTACT

sales@identityautomation.com
877.221.8401
www.identityautomation.com