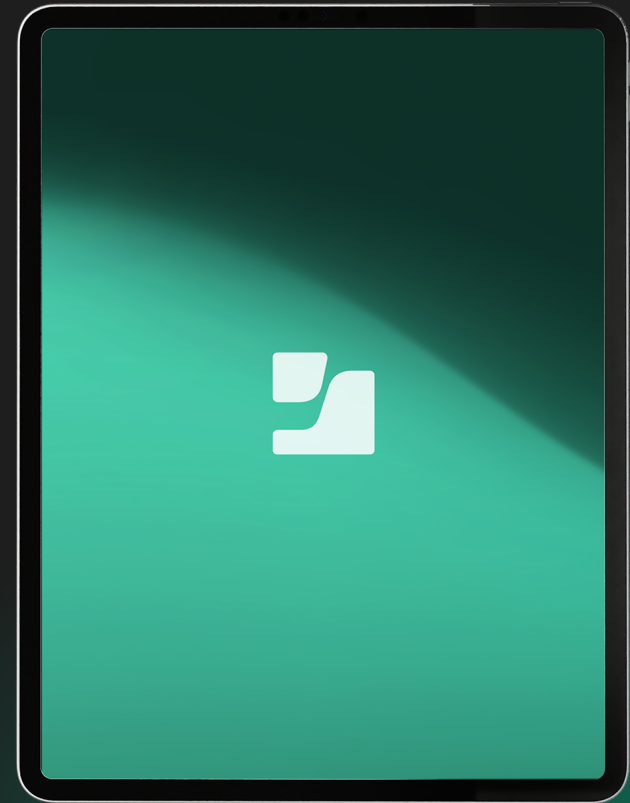




Identitäts- und Zugriffsverwaltung in Schulen für Einsteiger

Jeder Schüler ist anders. Der eine mag gerne Mathe, der andere liest vielleicht lieber. Der Nächste lernt besser mit einem interaktiven Spiel anstelle von verbalen Anweisungen. Und wieder ein Anderer hat aufgrund einer Behinderung Schwierigkeiten mit bestimmten Fächern.

Wenn Geräte das Lernen verbessern sollen, müssen sie sich an die Bedürfnisse der Lernenden anpassen. Wenn man ein gemeinsam genutztes iPad übernimmt, das eine Kopie des Geräts seines Freundes ist, holt man dann das Beste aus seinem Gerät heraus?

Aber wie können die Schulen sicherstellen, dass die Schüler:innen so lernen, wie es für sie am besten ist? Bevor man ein Gerät anpasst, muss man zunächst wissen, **wer** das Gerät benutzt – mit anderen Worten: die Identität des Schülers.

Die IT-Admins der Schulen leisten bereits eine Menge Arbeit hinter den Kulissen. Das Hinzufügen von Identitäts- und Zugriffsverwaltung (IAM) zu Ihren Aufgaben kann überwältigend klingen. Aber mit den richtigen Tools kann IAM Ihre Arbeitsabläufe vereinfachen und die Sicherheit verbessern – und gleichzeitig die Nutzung für die Schüler:innen im Klassenzimmer verbessern. Auf den folgenden Seiten werden wir uns ansehen, wie wir das erreichen.



In diesem E-Book gehen wir auf folgende Aspekte ein:



Was ist Identitäts- und Zugriffsverwaltung (IAM)?



Probleme mit der Identität an Schulen



Aufbau einer Identitätsgrundlage



Die Vorteile von IAM für Grund- und weiterführende Schulen



Eine Checkliste zur Vorbereitung auf IAM für Ihre Schule

IAM kann die Erfahrung im Klassenraum prägen.

Eine Unterrichtseinheit kann sehr unterschiedlich aussehen, je nach Ihren Identitäts-Workflows.



Durch Identitäts-Workflows verursachte Lernstörungen können sich auf verschiedene Weise äußern:



Lernende verwenden (oder vergessen) Passwörter für mehrere Accounts (z. B. für bestimmte Apps oder Tools)



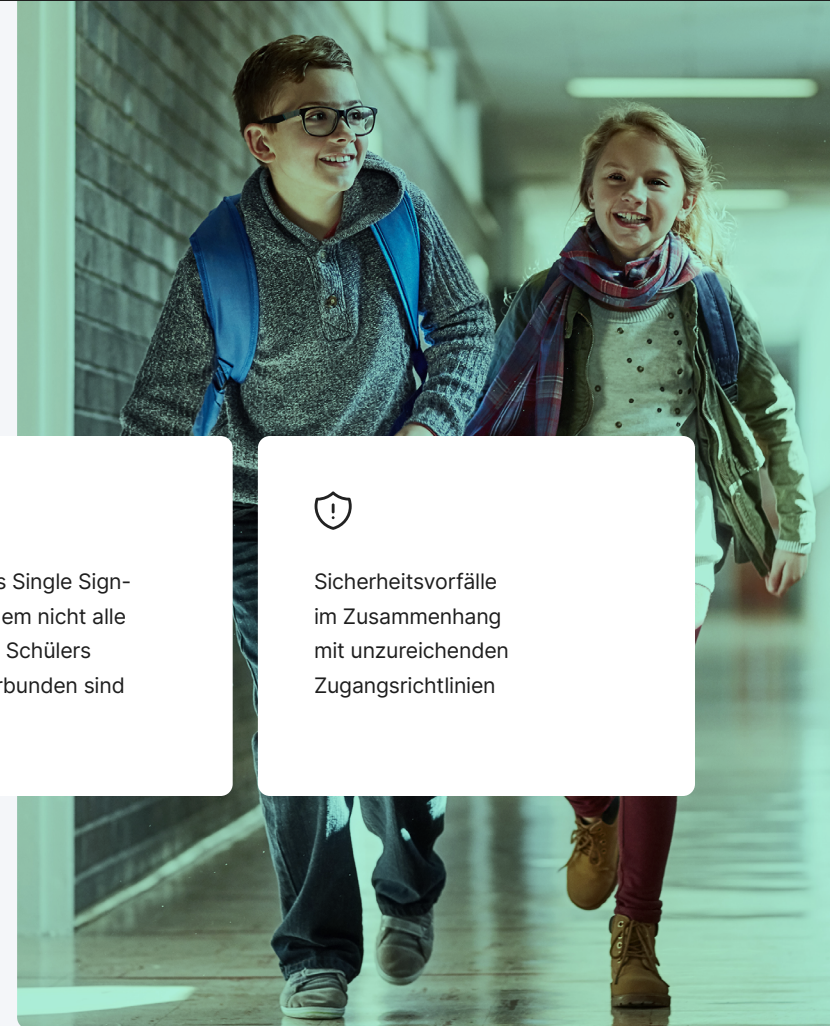
Schüler:innen haben aufgrund der Gerätekonfiguration Schwierigkeiten, dem Unterricht zu folgen



Unvollständiges Single Sign-On (SSO), bei dem nicht alle Accounts eines Schülers miteinander verbunden sind



Sicherheitsvorfälle im Zusammenhang mit unzureichenden Zugangsrichtlinien

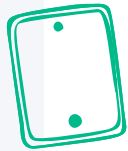


Das muss nicht so sein.





Stellen Sie sich folgende Situation vor:



1.

Ein Schüler holt sich ein gemeinsam genutztes iPad.

2.

Er tippt auf sein Bild und gibt einen Passcode ein.



3.



Das iPad ist auf die individuellen Apps und Einstellungen des jeweiligen Schülers konfiguriert, basierend auf seiner Klassenstufe, seinen Fächern und weiteren Faktoren.

4.

Mit einem verwalteten Apple Account und einem Identitätsanbieter kann sich der Schüler bei allen seinen Ressourcen anmelden, ohne sich eine Vielzahl von Passwörtern merken zu müssen.



5.

Wenn der Schüler fertig ist, wird seine Sitzung auf dem iPad gelöscht.



Dadurch lassen sich die Geräte problemlos in den Unterrichtsplan der Lehrkraft integrieren. Und mit der passwortlosen Authentifizierung muss man sich weniger Passwörter merken (oder stehlen).

Überblick über modernes IAM

Wir greifen hier etwas vor. Bevor wir zu diesen optimierten Arbeitsabläufen kommen, müssen wir verstehen, was IAM eigentlich bedeutet und wie es in Ihrer Schule funktioniert.

Es basiert auf zwei Schlüsselkonzepten:

1.

Authentifizierung



die Bestätigung,
wer ein Schüler oder Lehrer ist

2.

Autorisierung



Kontrolle darüber,
worauf sie zugreifen können

Zunächst müssen wir einen Überblick über alle unsere Benutzer bekommen und ihnen eine Möglichkeit bieten, ihre Identität nachzuweisen, z. B. einen Benutzernamen und ein Passwort. Dann müssen wir dieser Identität Berechtigungen zuordnen, z. B. auf welche Apps, Daten und Ressourcen sie zugreifen können.

Um dies zu erreichen, benötigen wir ein Verzeichnis, in dem jeder Benutzer erfasst wird. Dies könnte folgende Punkte enthalten:

- Vor- und Nachname
- Benutzername
- E-Mail-Adressen
- Attribute wie Klasse, Jahrgangsstufe oder Schulname
- Informationen zur Authentifizierung, wie Hashes

Mit diesen Informationen können wir beginnen, Berechtigungen festzulegen. Wenn Sie zum Beispiel wissen, dass ein Benutzer ein Fünftklässler in der Mathematikklasse eines bestimmten Lehrers ist, können Sie ihm Zugang zu einer App für mathematische Spiele geben, die dieser Lehrer gerne verwendet.

Was tut das IAM?

IAM ist mehr als ein Verzeichnis, das eine Liste von Schüleridentitäten enthält. Es enthält Account-Informationen – die Zugriffsrechte der Benutzer auf verschiedene Apps – und kann somit bestimmen, worauf die Benutzer zugreifen können und wie sie dies tun können.

IAM ist dynamisch und passt sich an den Kontext des Accounts eines Benutzers an. Wenn sie die Klasse wechseln und neue Apps benötigen, kann IAM die richtigen Apps bereitstellen und die nicht mehr benötigten Berechtigung entziehen. Ein Drittklässler und ein Zwölftklässler haben vielleicht beide Zugang zum Internet, aber der Zwölftklässler hat vielleicht weniger restriktive Inhaltsfilter. Wenn ein Elftklässler einen naturwissenschaftlichen Kurs abbricht, entzieht IAM ihm die Lizenz für teure Laborsoftware, die nur in diesem Kurs verwendet wird.

Mit anderen Worten: IAM ist wie Ihr Klassenbuch - nur intelligenter. Es ist wichtig, dass Sie die Sicherheit Ihrer Benutzerkonten und Daten gewährleisten. Und es macht den Unterricht sowohl für die Lernenden als auch für die Lehrenden besser; dazu später mehr.

Glossar der IAM-Begriffe für Schulen

Identitätsdienst (IdP)

Ihr „digitales Verzeichnis“, das Benutzer und deren Berechtigungen verifiziert, wie Google Workspace, Microsoft Entra ID oder Okta

Single Sign-On (SSO)

Eine Anmeldung für alle Ressourcen, einschließlich Apple, Google, Ihr Lernmanagementsystem und mehr

Multi-Faktor-Authentifizierung

Eine zusätzliche Ebene der Account-Sicherheit, die mehrere Faktoren für die Anmeldung erfordert, z. B. ein Passwort **und** Biometrie oder ein Einmalpasswort

Identitätsorchestrierung

Kontrollzentrum für Identitäten, das Verzeichnisse und Identitätsworkflows integriert und Funktionen wie SSO ermöglicht

Warum Grund- und weiterführende Schulen IAM brauchen

In den Schulen ist immer etwas los. Die Schüler:innen wechseln jedes Jahr die Klasse oder das Gebäude. Junge Schüler:innen vergessen ihre Passwörter. Geräte wechseln den Besitzer, gehen verloren oder werden von den Schüler:innen mit nach Hause genommen.

Chaos gehört in fast jeder Abteilung zum Alltag, doch die IT trifft es oft am härtesten. Oft müssen Lösungen mit Tools gefunden werden, die einem vorgesetzt wurden – während man gleichzeitig versucht, Apple, Google, Microsoft und das eigene SIS unter einen Hut zu bringen.

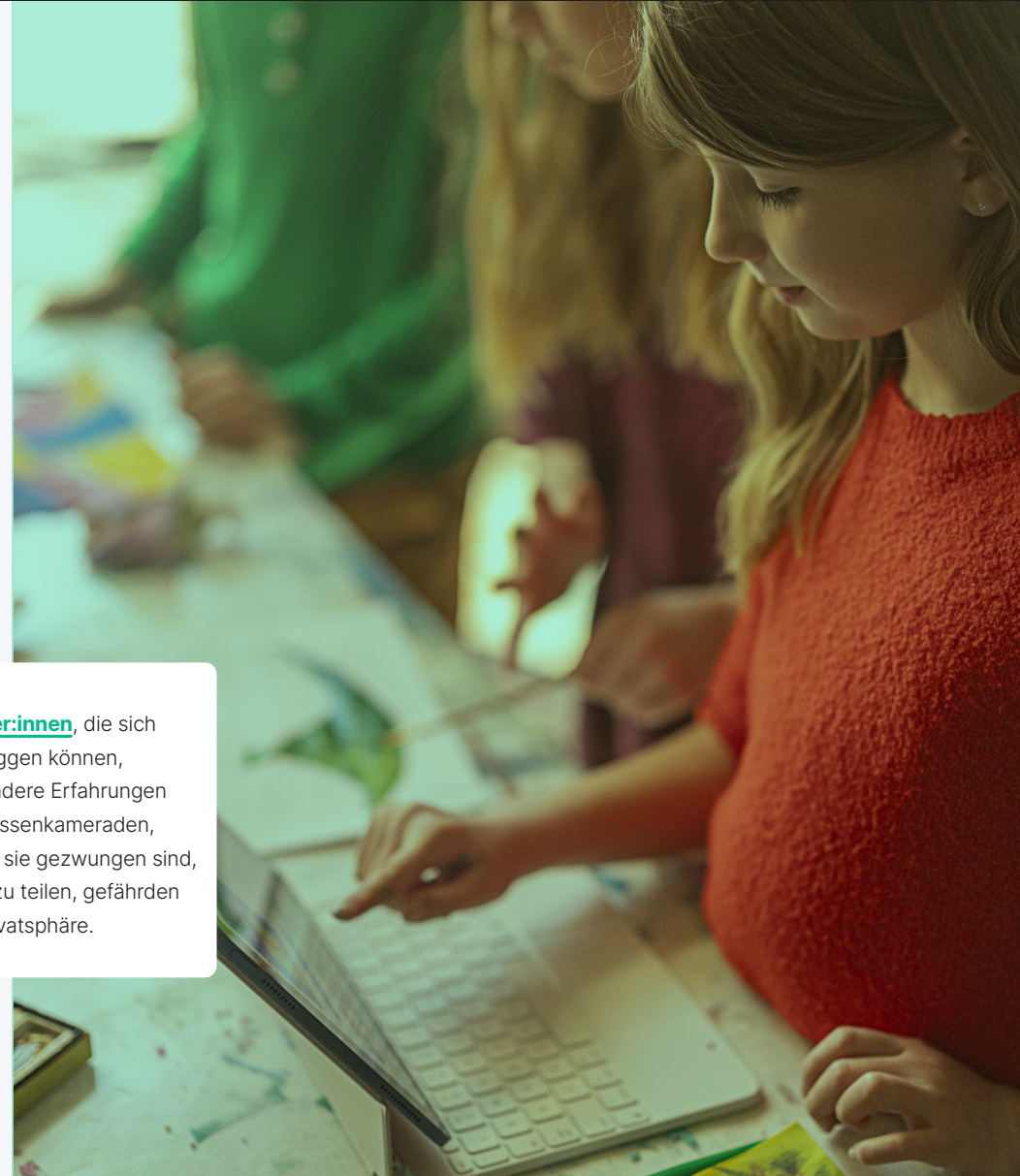


**Ohne IAM ist die Authentifizierung schwieriger.
Das betrifft jeden:**

IT-Teams müssen sich mit chaotischen Anmeldungen, mehr Support-Tickets und Verzögerungen bei der Bereitstellung auseinandersetzen.

Die Lehrkräfte verlieren Zeit im Unterricht, was zu Frustration und möglichen Änderungen der Lehrpläne führt.

Die Schüler:innen, die sich nicht einloggen können, machen andere Erfahrungen als ihre Klassenkameraden, oder wenn sie gezwungen sind, Accounts zu teilen, gefährden sie ihre Privatsphäre.



Mit und ohne IAM in Apple Umgebungen

Mit IAM werden die Identitäten der Lernenden und der Mitarbeiter:innen zur Grundlage Ihrer Apple Umgebung. Durch die Kombination von IdP, Apple School Manager und Mobile Device Management (MDM) können Sie einfache, sichere und personalisierte Lernerfahrungen bieten.



Mit IAM

- 🔑 **Eine** Anmeldung für alle Ressourcen
- ⚙️ **Automatisierte** Bereitstellung und Zugriff
- 👤 **Personalisierte** Erfahrung auf gemeinsam genutzten iPads
- 🛡️ **Erhöhte Sicherheit** mit SSO und MFA



Ohne IAM

- 🗑️ **Mehrere** Anmeldungen pro Schüler
- 💬 **Manuelle** Account-Einrichtung und -Bearbeitung
- 🕒 Verlorene Unterrichtszeit und eine steigende Anzahl an Helpdesk-Tickets
- 🔒 **Uneinheitliche Sicherheit** und Zugriff



Aufbau einer Identitätsgrundlage

Okay, Sie wollen also IAM an Ihrer Schule implementieren. Wie fängt man an?

1.

Ein Informationszentrum schaffen

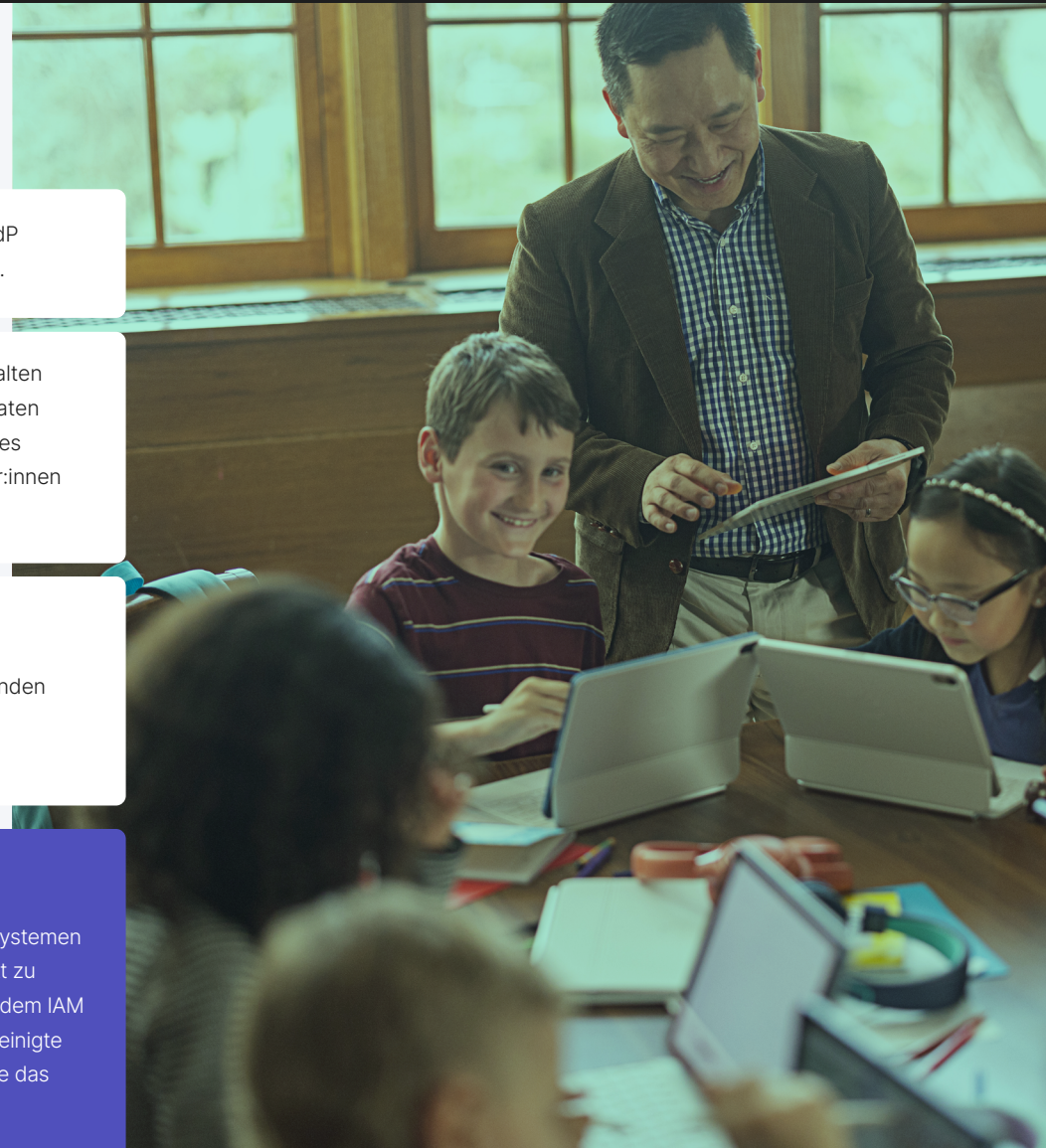
Integrieren Sie Ihre Systeme: Wenn Sie Ihr SIS mit Ihrem IdP verbinden, erhalten Sie kontinuierlich Ihre Daten in Echtzeit.

Automatisieren Sie die Kontoeinrichtung: Erstellen, verwalten und entfernen Sie Benutzer-Accounts basierend auf den Daten in Ihrem SIS. Dies hilft, Engpässe zu Beginn und am Ende des Schuljahres zu vermeiden und sorgt dafür, dass die Schüler:innen vom ersten Schultag an Zugang erhalten.

Seien Sie immer up-to-Date: Halten Sie Ihre Lehrpläne, Gerätezuweisungen und den App-Zugriff konsistent und synchronisiert. Die Schüler:innen können in die entsprechenden Klassen eingeteilt werden und auf der Grundlage dieser Informationen auf die ihnen zugewiesenen Apps zugreifen.

Wie konsistent sind Ihre Daten?

IAM funktioniert am besten, wenn die Daten zwischen den Systemen konsistent sind. Aber es ist nicht immer einfach, diesen Punkt zu erreichen. Tools für das Identitätsdaten-Management fügen dem IAM eine Datenorchestrierungsebene hinzu, um Ihre Daten in bereinigte und standardisierte Datensätze umzuwandeln. Vergessen Sie das nicht, wenn Ihre Daten Ihnen Probleme bereiten.





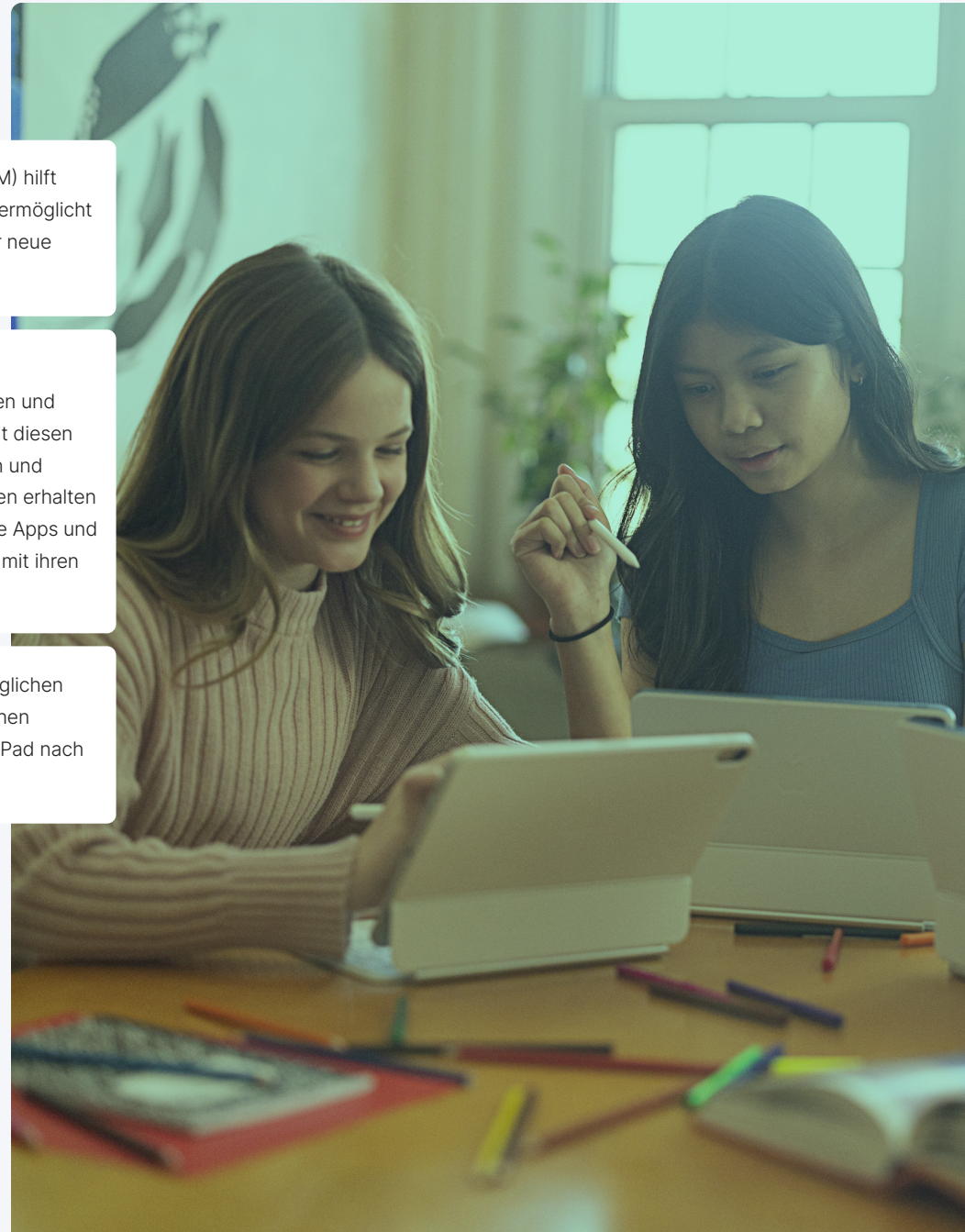
2.

Integration mit Apple School Manager

Optimierte Bereitstellung: Der Apple School Manager (ASM) hilft Ihnen, das Beste aus Ihren iPads herauszuholen. Zunächst ermöglicht es Funktionen wie die automatische Geräteregistrierung für neue Geräte und den Kauf von Apps und Büchern.

Automatisierung der Identitäten: ASM kann sich in Ihr SIS integrieren, automatisch verwaltete Apple Accounts erstellen und sich an Änderungen im Laufe des Schuljahres anpassen. Mit diesen Accounts können IT-Admins auch Passwörter zurücksetzen und andere administrative Aufgaben ausführen. Die Schüler:innen erhalten 200 GB iCloud-Speicherplatz und Zugang zu anderen Apple Apps und Diensten, z. B. für die gemeinsame Arbeit an einer Keynote mit ihren Klassenkameraden.

Personalisiertes Lernen: Verwaltete Apple Accounts ermöglichen Funktionen auf gemeinsam genutzten iPads. Die Schüler:innen können auf ihr Profil tippen und ihre PIN eingeben, um das iPad nach ihren Wünschen und Bedürfnissen zu konfigurieren.



3.

Verbindung mit Ihrem MDM



Nutzung Ihres IdP: Durch die Integration Ihres MDMs in Ihren IdP können Sie die Registrierung, Profile und Zugriffsrichtlinien für Ihre Geräte steuern.

Automatische Bereitstellung: Stellen Sie Apps und Einstellungen automatisch basierend auf der Rolle eines Benutzers bereit.

Optimierte Einrichtung: Weisen Sie Geräte auf der Grundlage von Identitäten zu, damit die Geräte am ersten Schultag einsatzbereit sind.





Best Practices bei der Implementierung von Identitäten

Verwendung von SSO: SSO erleichtert den Schüler:innen und den Lehrkräften die Anmeldung bei ihren Apps. Da man sich weniger Passwörter merken muss, werden Passwörter seltener vergessen und zurückgesetzt, und Cyberkriminelle haben weniger Möglichkeiten, Accounts zu kompromittieren.

Erzwingung von MFA: Multi-Faktor-Authentifizierung bietet eine weitere Sicherheitsebene für Mitarbeiter- und Administrator-Accounts.

Automatisierte Bereitstellung und Entziehung von Zugriffsrechten: Durch die Integration Ihres MDM, IdP und anderer Systeme können Sie die Bereitstellung und Entziehung von Benutzerrechten automatisieren. So werden Sicherheitslücken ohne zeitaufwändige und verzögerte manuelle Eingriffe geschlossen.

Regelmäßige Durchführung von Audits: Idealerweise sollte der Zugriff auf der Grundlage der Rolle oder anderer Attribute eines Benutzers nur auf die Ressourcen gewährt werden, die er benötigt. Aber die Dinge ändern sich. Deswegen sollten Sie regelmäßig überprüfen, ob die Zugriffsrichtlinien die geringsten Privilegien gewähren.



5.



Erst testen, dann skalieren

Fangen Sie klein an: Beginnen Sie mit einer Klassenstufe oder einem Gebäude. So können Sie vor einer groß angelegten Implementierung die Fehler in Ihren Prozessen und Tools beseitigen.

Anpassen und optimieren: Bitten Sie um Feedback von den Lehrkräften: Gibt es weniger Störungen? Wie einfach können sich die Schüler:innen bei ihren Accounts einloggen? Anhand dieses Feedbacks können Sie auf alle Bedenken eingehen und sicherstellen, dass die Technologie das Lernen fördert und nicht behindert.

Betonen Sie die Zusammenarbeit: Technologie ist am wirkungsvollsten, wenn sie nicht in der IT isoliert ist. Durch die Zusammenarbeit mit den Admins und den Lehrplanverantwortlichen in den Schulen wird sichergestellt, dass alle Beteiligten die Technik bestmöglich nutzen. Und das gilt auch für die Schüler:innen.



IAM verbessert die IT-Arbeitsabläufe, die Sicherheit und die Erfahrung im Klassenraum.

Sobald Sie diese Grundlage geschaffen haben, können Sie die Früchte ernten.



Optimierte IT-Abläufe:

Wenn Sie Ihre Systeme mit einem zentralen IAM kombinieren, können Sie leistungsstarke Automatisierungen nutzen, die die Prozesse vereinfachen.



Automatisierung des Lebenszyklus von Identitäten:

Mit der richtigen Einrichtung können Sie Identitäten während des gesamten Schuljahres (und darüber hinaus) automatisch verwalten. Mit IAM, das sich selbstständig an Änderungen von Lehrplänen, Rollen, Gebäuden, Klassen und anderen Attributen anpasst, werden Zugriffsberechtigungen mit minimalem IT-Eingriff zugewiesen.



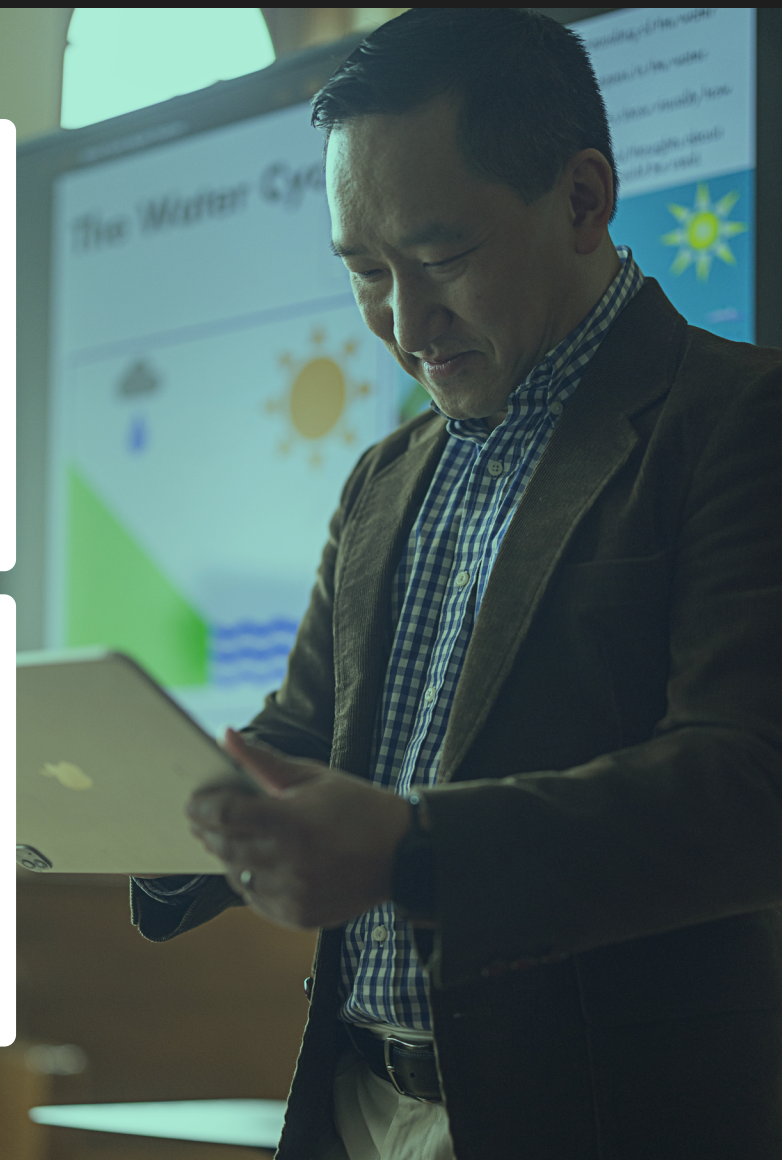
Verbesserte Cybersicherheit und Konformität:

SSO und Automatisierung schließen Sicherheitslücken, bevor sie zu einem Problem werden. IAM reduziert die Passwort-Müdigkeit, verwaltet Berechtigungen autonom, verhindert unbefugten Zugriff und spart der IT wertvolle Zeit – alles Funktionen, die auf die eine oder andere Weise die Sicherheit und Konformität stärken.



Verbesserte Benutzerfreundlichkeit:

Es gilt weiterhin: Je weniger Passwörter sich die Schüler:innen merken müssen, desto besser. Und da der Zugang auf der Rolle des Benutzers basiert, erhält er von Anfang an Zugriff auf alle Apps, die er benötigt. Das bedeutet weniger Unterbrechungen während der Unterrichtszeit, weniger Passwortrücksetzungen, weniger Helpdesk-Tickets und weniger Kopfzerbrechen für die Lehrkräfte.



IAM ist ein Prozess: **Fangen Sie einfach an.**

Es gibt eine Menge zu lernen. Wenn Sie bei Null anfangen, kann die Implementierung von IAM wie eine unüberwindbare Hürde erscheinen. Zum Glück geht es nicht um alles oder nichts. Beginnen Sie mit den Komponenten, die Ihnen zur Verfügung stehen. Das kann beispielsweise bedeuten, dass Sie sicherstellen, dass Ihre Daten über Ihre gesamte Technologieplattform hinweg konsistent sind. Oder die Integration von Apple School Manager in Ihr MDM. Wahrscheinlich werden Sie feststellen, dass auch kleine Schritte für Ihre Schule von Vorteil sind: weniger Probleme, schnellere Anmeldungen und mehr Sicherheit für die Schüler:innen.



Checkliste: Ist meine Schule bereit für IAM?

Anhand dieser kurzen Checkliste können Sie herausfinden, ob Ihre Schule bereit für ein IAM ist.



Wie ist der Istzustand?

☐

Ich weiß, wie Accounts für Lernende und Mitarbeiter:innen erstellt und gelöscht werden.

☐

Unsere Daten sind systemübergreifend konsistent (SIS, Google, Microsoft, usw.)



Eine Grundlage schaffen

☐

Wir haben oder planen einen Cloud-IdP wie Google Workspace, Microsoft Entra ID oder Okta.

☐

ASM und unser MDM (wie Jamf School oder Jamf Pro) sind eingerichtet und miteinander verbunden.



Bewährte Praktiken befolgen

☐

Wir verwenden SSO für die wichtigsten Lernwerkzeuge.

☐

Wir schützen die Accounts der Mitarbeiter:innen und Admins mit MFA.

☐

Wir automatisieren die Bereitstellung von Benutzern und überprüfen den Zugang regelmäßig.

Wenn Sie die meisten dieser Kästchen angekreuzt haben, sind Sie bereit, die Anmeldung zu vereinfachen, die Sicherheit zu erhöhen und die Lernerfahrung mit IAM zu verbessern.



Probieren Sie Jamf aus