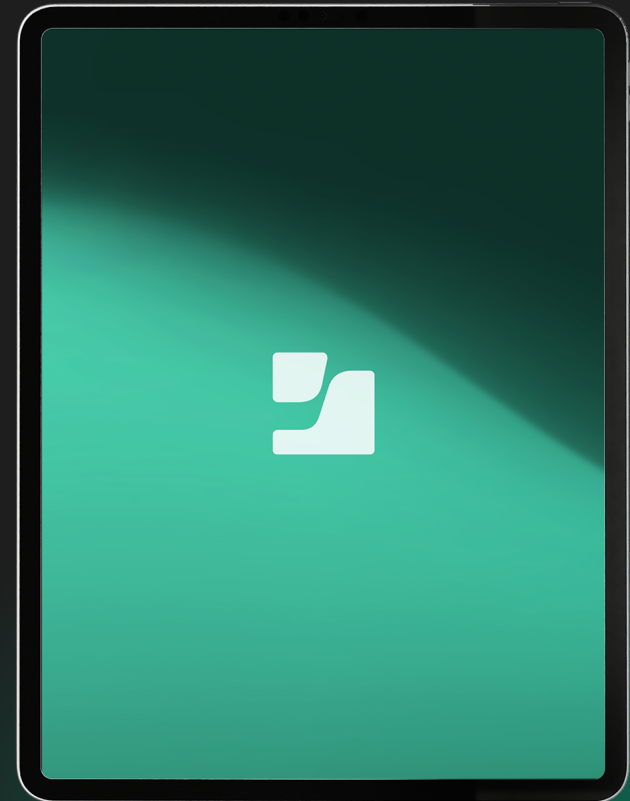




Introduction à la gestion des identités et des accès dans l'enseignement primaire et secondaire

Chaque élève est unique. L'un peut aimer les mathématiques, tandis que l'autre préfère lire. Certains apprennent mieux avec un jeu interactif qu'avec des instructions verbales. D'autres peuvent avoir des difficultés dans certaines matières en raison d'un handicap.

Pour enrichir l'apprentissage, les appareils doivent s'adapter aux besoins de l'élève. Si chaque élève, malgré ses caractéristiques uniques, prend un iPad partagé qui est une copie conforme de celui de son camarade, peut-il vraiment en profiter pleinement ?

Quant aux écoles, comment peuvent-elles faire en sorte que les élèves apprennent de la manière qui leur convient le mieux ? Pour personnaliser un appareil, il faut d'abord savoir **qui** utilise l'appareil ; autrement dit, il faut connaître l'identité de l'élève.

Les administrateurs informatiques des écoles font déjà beaucoup en coulisses. L'idée d'ajouter à leurs tâches la gestion des identités et des accès (IAM) peut sembler insurmontable. Pourtant, avec les bons outils, l'IAM peut simplifier vos workflows et renforcer la sécurité, tout en améliorant l'expérience des élèves en classe. Nous verrons quelle forme cela peut prendre dans les pages suivantes.



En lisant cet e-book, vous découvrirez :



Ce qu'est la gestion des identités et des accès (IAM)



Les défis liés à la gestion des identités dans l'enseignement primaire et secondaire



Comment bâtir un socle pour les identités



Les avantages de l'IAM dans l'enseignement primaire et secondaire



Une liste de contrôle de préparation à l'IAM pour votre établissement

L'IAM peut façonner l'expérience en classe.

Un cours peut se dérouler de manière très différente selon le fonctionnement de vos workflows d'identité.



Les workflows liés à l'identité peuvent perturber l'apprentissage de plusieurs manières :



Les élèves doivent utiliser des mots de passe différents pour accéder aux outils et aux applications, et ils les oublient



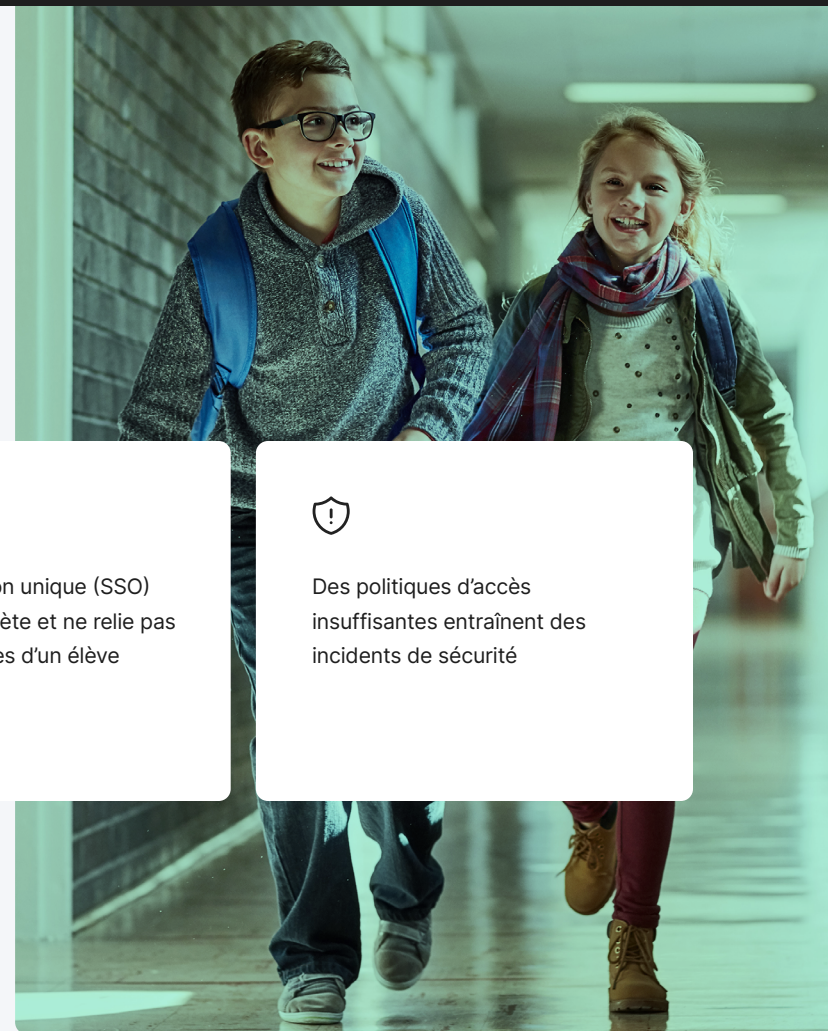
Les élèves ont du mal à suivre les cours en raison de la configuration de leur appareil



L'authentification unique (SSO) n'est pas complète et ne relie pas tous les comptes d'un élève



Des politiques d'accès insuffisantes entraînent des incidents de sécurité

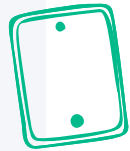


Il n'y a pas une fatalité.





Imaginez cette expérience :



1.

Un élève prend un iPad partagé sur le chariot de sa classe.

2.

Il appuie sur sa photo et saisit un code d'accès.



3.

L'iPad présente une configuration, des applications et des réglages propres à l'élève, en fonction de son niveau scolaire, de ses cours, etc.



4.

Avec un compte Apple géré et un fournisseur d'identité, l'élève peut se connecter à tous ses outils sans avoir à mémoriser une multitude de mots de passe.



5.

Lorsqu'il a terminé, sa session est effacée de l'iPad.



Les appareils se fondent parfaitement dans le plan de cours de l'enseignant. Et grâce à l'authentification sans mot de passe, il y a beaucoup moins de mots de passe à retenir (ou à voler).

Vue d'ensemble de l'IAM moderne

N'allons pas trop vite. Avant d'aborder ces workflows unifiés, nous devons comprendre ce que l'IAM signifie réellement et quelles sont ses implications pour votre établissement.

L'IAM repose sur deux concepts clés :

1.

Authentification



pour confirmer l'**identité**
d'un élève ou d'un enseignant

2.

Autorisation



pour contrôler **ce à quoi**
ils ont accès

Tout d'abord, nous devons assurer le suivi de tous nos utilisateurs et leur offrir un moyen de prouver leur identité, avec un nom d'utilisateur et un mot de passe par exemple. Ensuite, nous devons associer des permissions à cette identité, par exemple en désignant les applications, les données et les ressources auxquelles ils peuvent accéder.

Pour ce faire, nous avons besoin d'un répertoire afin de nommer chaque utilisateur. Cet annuaire peut contenir différentes informations :

- Nom et prénom
- Nom d'utilisateur
- Adresse e-mail
- Divers attributs : classe, niveau scolaire, nom de l'établissement, etc.
- Informations d'authentification (hashes)

Ces informations nous permettent ensuite de définir des autorisations. Par exemple, si vous savez qu'un utilisateur est un élève de CM1 et qu'il est dans la classe d'un certain professeur de mathématiques, vous pouvez lui donner accès à l'application de jeux mathématiques prise en compte de cet enseignant.

Que fait l'IAM ?

L'IAM est bien plus qu'un répertoire contenant la liste des identités des élèves. Il abrite des informations sur leur compte, et en particulier des autorisations d'accès à diverses applications, grâce auxquelles il dicte ce à quoi les utilisateurs peuvent accéder et selon quelles modalités.

L'IAM est dynamique et s'adapte au contexte du compte de l'utilisateur. S'il change de classe et qu'il a besoin d'un nouvel ensemble d'applications, l'IAM peut les lui fournir et révoquer les autorisations de celles qui sont devenues inutiles. Un élève de CE2 et un élève de terminale peuvent tous deux avoir accès à Internet, mais les filtres de contenu seront moins restrictifs pour le second que pour le premier. Si un élève de première abandonne un cours de sciences, l'IAM lui retire sa licence pour un logiciel de laboratoire coûteux utilisé uniquement dans ce cours.

En d'autres termes, l'IAM est une version intelligente de la liste des élèves de votre classe. Elle est la clé qui garantit la sécurité des comptes et des données de vos utilisateurs. Elle améliore également l'expérience en classe, tant pour les élèves que pour les enseignants – nous y reviendrons plus tard.

Glossaire des termes IAM pour les établissements scolaires



Fournisseur d'identité (IdP)

C'est l'« annuaire numérique » qui vérifie les utilisateurs et leurs autorisations, comme Google Workspace, Microsoft Entra ID ou Okta.



Authentification unique (SSO)

Un seul identifiant pour accéder à toutes les ressources : Apple, Google, votre système de gestion de l'apprentissage, etc.



Authentification multifacteur

Couche de sécurité supplémentaire qui exige plusieurs facteurs d'authentification pour se connecter à un compte, comme un mot de passe **et** une caractéristique biométrique ou un code à usage unique.



Orchestration de l'identité

Centre de contrôle de l'identité intégrant les annuaires et les workflows liés à l'identité, pour prendre en charge des fonctionnalités telles que la SSO.

Pourquoi les établissements primaires et secondaires ont besoin de l'IAM

Il se passe toujours quelque chose dans une école. Chaque année, les élèves changent d'année scolaire, de classe ou de bâtiment. Les jeunes élèves oublient leurs mots de passe. Les appareils changent de mains, se perdent ou suivent les élèves chez eux.

Le chaos guette tous les services, et en particulier le service informatique. Il faut souvent exploiter des outils que l'on n'a pas choisis, ou essayer de mettre de l'ordre dans un environnement qui mélange Apple, Google, Microsoft et un système d'information sur les étudiants (SIS).



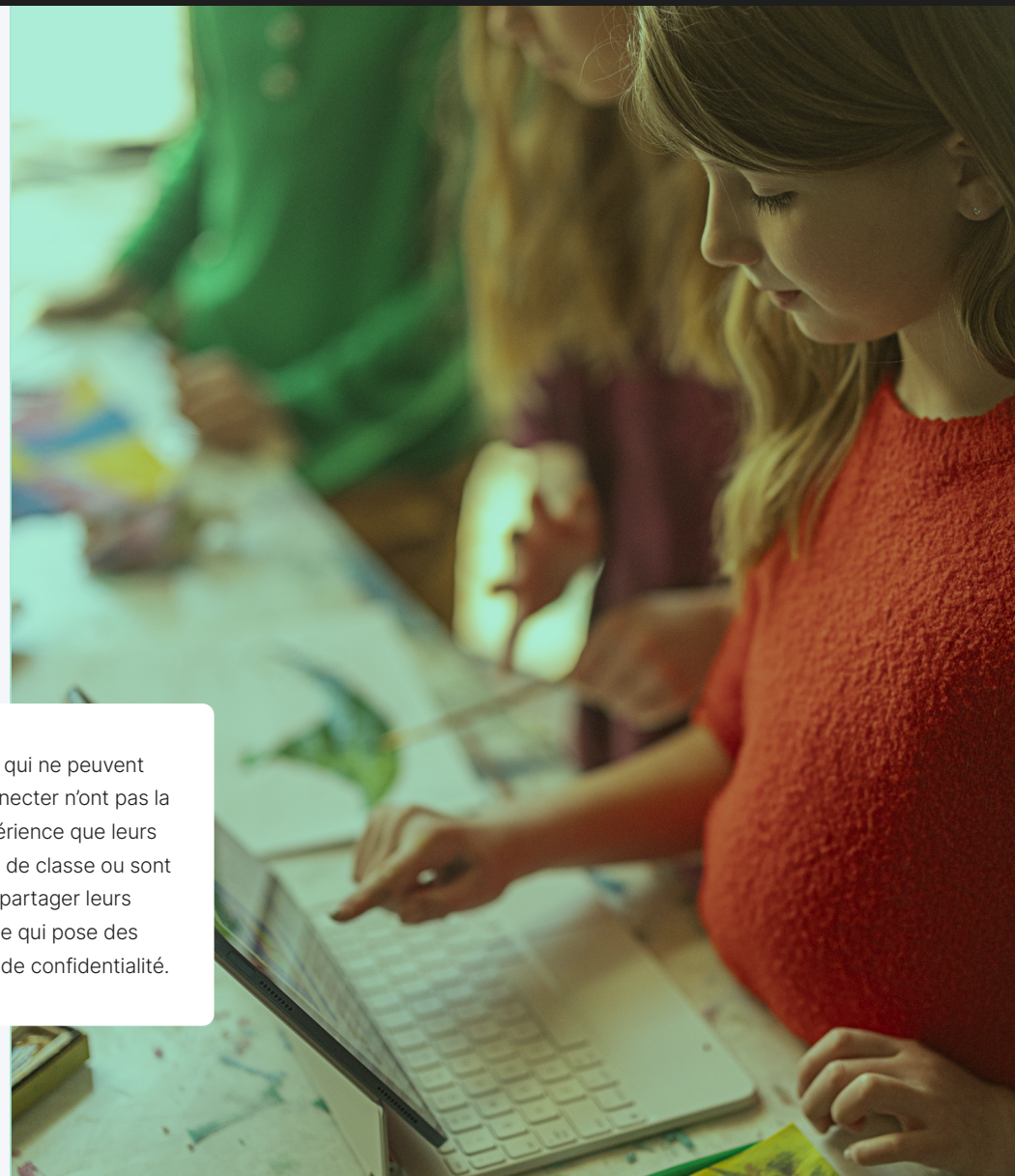
Sans IAM, l'authentification devient un véritable défi.

Tout le monde en pâtit :

Les équipes informatiques doivent faire face à des connexions instables, à d'innombrables tickets d'assistance et à des retards de provisionnement.

Les enseignants perdent du temps de cours, ce qui entraîne des frustrations et peut les contraindre à modifier les programmes.

Les élèves qui ne peuvent pas se connecter n'ont pas la même expérience que leurs camarades de classe ou sont obligés de partager leurs comptes, ce qui pose des problèmes de confidentialité.



Avec et sans IAM dans les environnements Apple

Avec l'IAM, les identités des élèves et du personnel deviennent la base de votre environnement Apple. En connectant votre IdP, Apple School Manager et la gestion des appareils mobiles (MDM), vous pouvez offrir des expériences d'apprentissage simples, sécurisées et personnalisées.



Avec IAM

- 🔑 **Un seul** identifiant pour toutes les ressources
- ⚙️ Approvisionnement et accès **automatisés**
- 👤 Expérience **personnalisée** sur les iPads partagés
- 🛡️ **Sécurité renforcée** par l'authentification SSO et l'AMF



Sans IAM

- 👤 **Plusieurs** identifiants par élève
- 💬 Processus **manuels** de création et de maintenance des comptes
- 🕒 Heures de cours perdues et augmentation du nombre de tickets d'assistance
- 🔒 **Manque de cohérence** des mesures de sécurité et des accès



Bâtir un socle pour les identités

Très bien, vous voulez introduire l'IAM dans votre école. Par où devez-vous commencer ?

1.

Établissez une source unique de vérité

Intégrez vos systèmes : connectez votre SIS à votre IdP pour assurer la continuité des données en temps réel.

Automatisez le provisionnement des comptes : créez, gérez et supprimez des comptes utilisateurs sur la base des données de votre SIS. Vous éviterez l'apparition de goulets d'étranglement au début et à la fin de l'année scolaire, et garantirez aux élèves un accès fiable dès le premier jour d'école.

Maintenez la synchronisation : synchronisez constamment les listes de classes, les affectations d'appareils et les accès aux applications pour un maximum de cohérence. Les élèves pourront être affectés à leurs cours et accéder aux applications qui leur ont été attribuées en fonction de ces informations.

Avez-vous des données cohérentes ?

L'IAM fonctionne mieux lorsque les données des différents systèmes sont cohérentes. Mais cet objectif n'est pas toujours facile à atteindre. Les outils de gestion des données d'identité ajoutent une couche d'orchestration à l'IAM pour convertir vos données en enregistrements propres et normalisés. Pensez-y si vos données vous posent trop de problèmes.





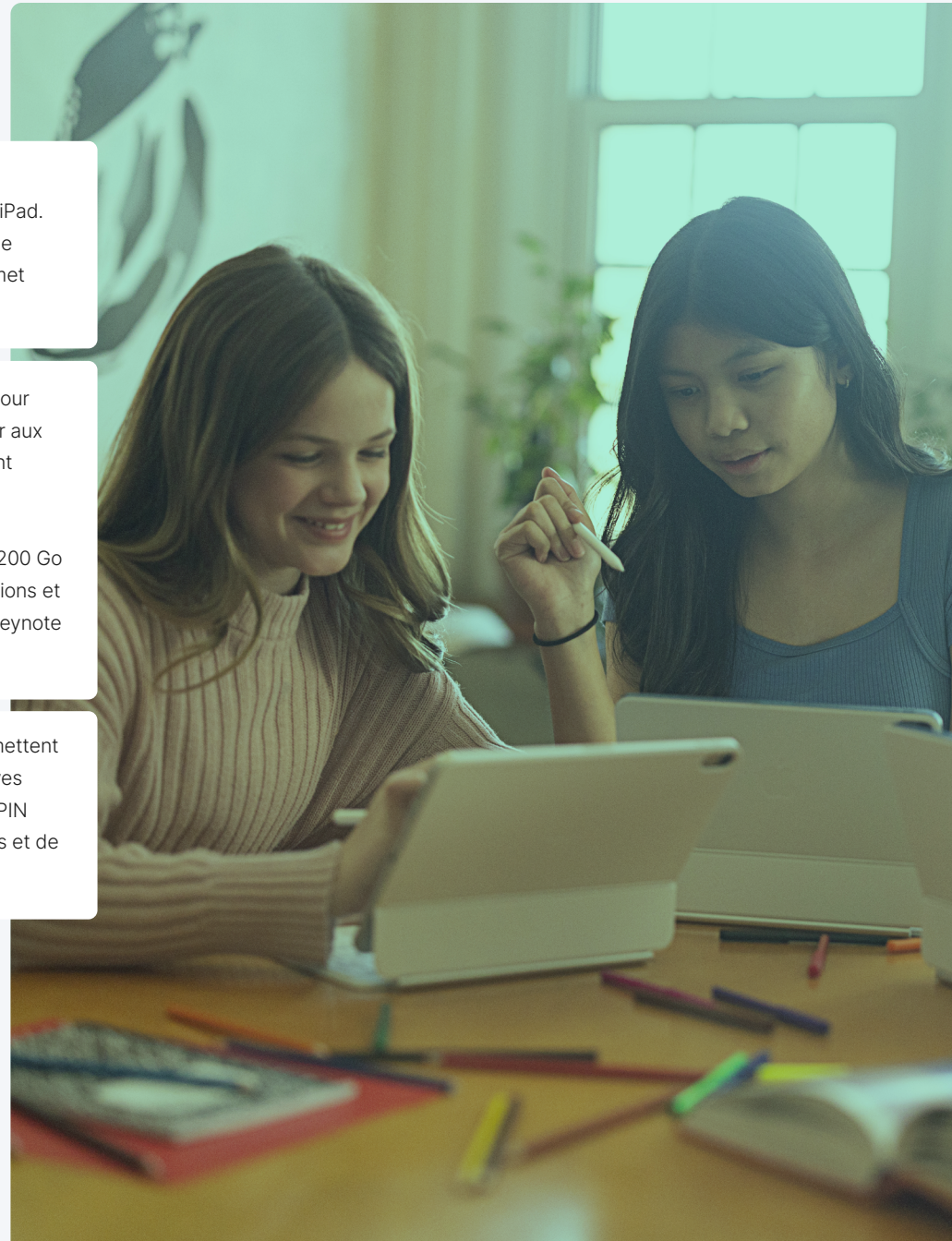
2.

Intégration avec Apple School Manager

Optimisez votre déploiement : Apple School Manager (ASM) vous aide à exploiter tout le potentiel de votre déploiement d'iPad. Pour commencer, cet outil active des fonctionnalités telles que l'inscription automatisée des nouveaux appareils et vous permet d'acheter des applications et des livres.

Automatisez les identités : ASM peut s'intégrer à votre SIS pour créer automatiquement des comptes Apple gérés et s'adapter aux changements tout au long de l'année scolaire. Particulièrement pratiques, ces comptes permettent aux administrateurs informatiques de réinitialiser les mots de passe et d'exécuter d'autres fonctions administratives. Les élèves bénéficient de 200 Go d'espace de stockage iCloud et d'un accès à d'autres applications et services Apple. Ils peuvent, par exemple, collaborer sur une Keynote avec leurs camarades de classe.

Apprentissage personnalisé : les comptes Apple gérés permettent de mettre sur pied des programmes d'iPad partagés. Les élèves n'ont qu'à cliquer sur leur image de profil et à saisir leur code PIN pour que l'iPad soit configuré en fonction de leurs préférences et de leurs besoins.



3.

Connexion à la solution MDM



Tirez parti de votre IdP :

en intégrant votre solution MDM à votre IdP, vous pouvez piloter l'inscription, les profils et les politiques d'accès à vos appareils.

Automatisez le provisionnement :

fournissez automatiquement les applications et les paramètres correspondant au rôle de l'utilisateur.

Rationalisez l'installation :

attribuez des appareils en fonction des identités et remettez à tous des appareils prêts à l'emploi dès le premier jour d'école.





Mise en œuvre des bonnes pratiques en matière d'identité

Implémentez la SSO : l'authentification unique simplifie la connexion des élèves et des enseignants et leur permet d'accéder plus rapidement à leurs applications. Comme ils ont moins de mots de passe à retenir, ils demandent moins souvent de les réinitialiser. Quant aux pirates, ils ont moins d'occasions de compromettre des comptes.

Appliquez l'AMF : l'authentification multifacteur ajoute une couche de sécurité supplémentaire aux comptes du personnel et des administrateurs.

Automatiser le provisionnement et le déprovisionnement : en intégrant votre solution MDM, votre IdP et vos autres systèmes, vous pouvez automatiser le provisionnement et le déprovisionnement des utilisateurs. C'est un excellent moyen de combler des lacunes de sécurité sans les retards causés par une intervention manuelle.

Effectuez des audits réguliers : dans l'idéal, le principe de l'accès basé sur le rôle ou d'autres attributs d'un utilisateur ne lui permet de voir que ce dont il a besoin. Mais la situation peut évoluer : vérifiez donc régulièrement que les politiques d'accès n'accordent que le minimum de privilèges nécessaires.



5.



Créez un projet pilote avant de passer à l'échelle supérieure

Optez pour des débuts modestes : commencez par un seul niveau scolaire ou un seul bâtiment. Vous aurez la possibilité de corriger les faiblesses de votre processus et de vos outils avant de les mettre en œuvre à grande échelle.

Adaptez et optimisez : recueillez les réactions des enseignants. Observent-ils une baisse des interruptions ? Est-ce que les élèves se connectent facilement à leur compte ? Ces commentaires vous aideront à répondre à toutes les préoccupations, pour que la technologie soit un appui à l'apprentissage, et non un frein.

Mettez l'accent sur la collaboration : pour maximiser l'impact de la technologie, elle ne doit pas rester cloisonnée dans le service informatique. C'est en collaborant avec les administrateurs des écoles et les responsables des programmes scolaires que l'équipe informatique créera la meilleure expérience pour tous. Et les élèves en profiteront pleinement.



L'IAM améliore les workflows informatiques, la sécurité et l'expérience en classe.

Une fois ce socle en place, il ne reste qu'à récolter les fruits.



Rationalisez les opérations informatiques :

lorsque vous associez vos systèmes à une IAM centrale, vous ouvrez la porte à de puissants automatismes qui simplifient les processus.



Automatisez le cycle de vie des identités :

avec la bonne configuration, vous pouvez gérer automatiquement les identités tout au long de l'année scolaire (et au-delà). L'IAM s'adapte en toute autonomie aux modifications des listes, des rôles, des bâtiments, des classes et d'autres caractéristiques, si bien que les autorisations d'accès sont attribuées avec le minimum d'intervention pour l'équipe informatique.



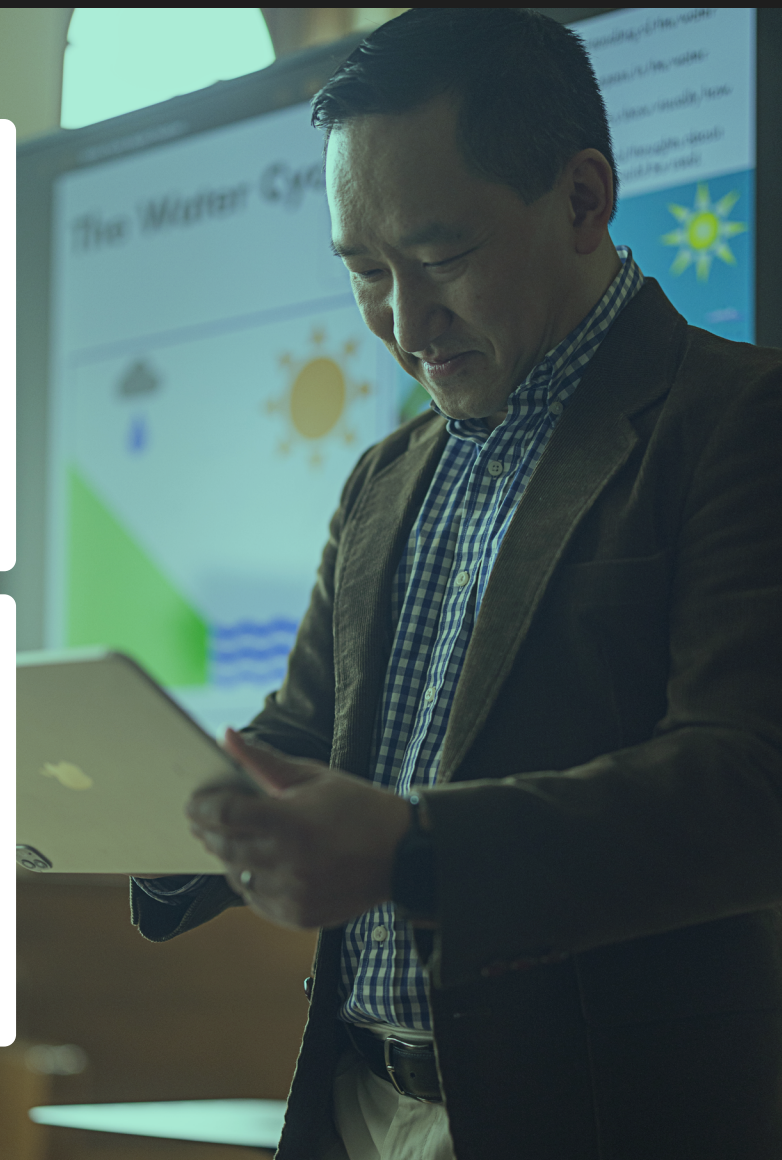
Renforcez la cybersécurité et la conformité :

la SSO et l'automatisation comblent les failles de sécurité avant qu'elles ne deviennent une source de problème. L'IAM réduit la lassitude liée aux mots de passe, gère les autorisations de manière autonome, empêche les accès non autorisés et fait gagner du temps au service informatique – autant d'atouts pour la sécurité et la conformité des systèmes.



Améliorez l'expérience utilisateur :

comme nous l'avons déjà mentionné, moins il y a de mots de passe à retenir, mieux c'est. Et comme les accès dépendent du rôle de l'utilisateur, celui-ci peut immédiatement utiliser toutes les applications dont il a besoin. Cette approche réduit les interruptions pendant les cours, les réinitialisations de mots de passe, les tickets d'assistance et la frustration des enseignants.



L'IAM est un parcours : commencez simplement.

Il y a beaucoup à apprendre. Si vous partez de zéro, la mise en œuvre de l'IAM peut sembler insurmontable. Heureusement, le changement n'a pas besoin d'être radical. Commencez par ce qui est à votre portée. Vous devrez peut-être d'abord vérifier la cohérence de vos données sur l'ensemble de votre pile technologique. Ou intégrer Apple School Manager à votre solution MDM. Vous constaterez certainement que chaque petite étape apporte un bienfait à votre établissement, en évitant les frustrations, en fluidifiant les connexions et en sécurisant les élèves.





Liste de contrôle : est-ce que mon établissement est prêt pour l'IAM ?

Utilisez cette petite liste de contrôle pour déterminer si votre école est prête à ajouter l'IAM à sa pile technologique.



Ayez une vision claire de votre environnement actuel

☐

Je sais comment les comptes des étudiants et du personnel sont créés et supprimés.

☐

Nos données sont cohérentes d'un système à l'autre (SIS, Google, Microsoft, etc.)



Mettez en place les fondations

☐

Nous avons, ou prévoyons d'avoir, un IdP cloud comme Google Workspace, Microsoft Entra ID ou Okta.

☐

ASM et notre solution MDM (Jamf School ou Jamf Pro, par exemple) sont configurés et connectés.



Appliquez les bonnes pratiques

☐

Nous utilisons la SSO pour les principaux outils d'apprentissage.

☐

Nous protégeons les comptes du personnel et des administrateurs avec l'AMF.

☐

Nous automatisons le provisionnement des utilisateurs et révisons régulièrement les accès accordés.

Si vous avez coché la plupart de ces cases, vous avez toutes les cartes en main pour simplifier les connexions, renforcer la sécurité et améliorer l'expérience d'apprentissage grâce à l'IAM.



[Essayez Jamf](#)