

Simplifier l'accès : un guide complet sur l'authentification SSO dans l'enseignement primaire et secondaire

Introduction



Chaque minute de cours compte.

Pourtant, les problèmes de connexion freinent constamment l'apprentissage dans les établissements primaires et secondaires. Retards au début des cours, inégalités d'accès au sein des élèves, charge de travail accrue pour les services informatiques... les problèmes d'authentification ont des répercussions tangibles.

Ce guide explique comment l'authentification SSO simplifie l'accès aux ressources pédagogiques, allège la complexité et libère un temps précieux pour l'apprentissage. Pour les administrateurs informatiques, cette solution est un moyen sûr de simplifier la gestion des identités, de renforcer la sécurité et de mieux soutenir les enseignants et les objectifs de l'établissement.

Quand l'apprentissage doit attendre

9 h 00 : L'enseignante vient de terminer l'appel ; en levant les yeux de sa tablette, elle voit devant elle des sourires radieux. Les élèves sont d'autant plus impatients de découvrir le système solaire qu'ils ont assisté au lancement d'Artemis II la veille au soir. « Bonjour, chers collègues astronautes, c'est votre commandant de bord qui vous parle. Attrapez votre équipement spatial, car aujourd'hui... *nous* partons sur la Lune ! »

L'enseignante demande bien sûr à ses petits spécialistes de vol de sortir leurs iPad et de se connecter à leur portail pour ouvrir à la leçon du jour : « À la conquête de l'espace ! ».

Alors que l'enseignante s'apprête à commencer, Mateo l'interrompt : « Madame, ça dit que mon mot de passe n'est pas valide. » Samia ajoute : « Moi aussi. Je n'arrive pas à me connecter. » Après avoir poussé un léger soupir, Mme Pesquet pose son iPad avant de s'approcher pour inspecter l'équipement de mission.

Pendant qu'elle tente de résoudre les problèmes de connexion, certains membres de l'équipage sont « parés au décollage », tandis que d'autres restent n'ont pas accès à la rampe de lancement : ils ont oublié leur identifiant ou ont mal saisi leur mot de passe ; dans certains cas, les élèves ont accès au cours, mais c'est le site web consacré au système solaire qui refuse de s'ouvrir.

Au début du cours, le compteur était à T-30 secondes. Il est déjà à T+6 minutes, et ce n'est pas fini.

Le coût caché des difficultés de connexion



Chaque année scolaire, diverses perturbations liées à la technologie ont un impact sur le temps d'enseignement. L'éventail est large :



Budgets et financement



Risque de cybersécurité



Fracture numérique



Distractions en ligne



Problèmes d'intégrité des appareils

Si chacun de ces facteurs a un impact indéniable sur les établissements, un autre, souvent négligé, influe tout autant sur les résultats d'apprentissage : les difficultés de connexion.

Par exemple, il faut à un élève entre **30 secondes et trois minutes** pour se connecter à un appareil ou à un site web. Même si l'on dispose rarement de statistiques publiques, cette fourchette constitue une bonne indication. Elle tient compte de divers

facteurs : facilité de saisie, maîtrise du système, performances de l'appareil et vitesse de connexion Internet.

Même s'il ne faut que quelques secondes pour se connecter à un site ou s'authentifier sur un Mac, ces délais s'accumulent au fil de l'année scolaire et représentent en bout de ligne une perte de temps d'apprentissage considérable.

D'autres chiffres importants à connaître :

- Délais de réponse aux demandes d'assistance informatique pour les problèmes non urgents : **1 à 2 jours**
- Réinitialisation d'un mot de passe oublié ou déverrouillage d'un compte : **15 à 30 minutes**
- Réception d'une alerte de vérification d'authentification MFA : **8 secondes**

30 secondes par élève pour se connecter à un site web x 4 cours : **= 2 minutes par jour**

2 minutes x 5 jours par semaine : **= 10 minutes par semaine**

10 minutes x 36 semaines : **= 360 minutes**

360 minutes / 60 minutes : **= 6 heures par année scolaire**

Avant de nous pencher sur les calculs qui chiffrent les difficultés de connexion, définissons quelques variables propres à l'enseignement primaire et secondaire :

- Les élèves ont généralement **entre 4 et 8 cours par jour**.
- Une journée d'école type dure **7 heures**
- Les écoles sont ouvertes **5 jours par semaine**
- Une année scolaire compte en moyenne **180 jours** (soit 36 semaines)
- Le temps total d'apprentissage par année scolaire est de **1 260 heures**
- L'effectif moyen par école primaire (aux États-Unis) est de **470 élèves** Il y avait **780,85 millions d'élèves dans l'enseignement primaire à l'échelle mondiale en 2024**

Que signifient ces chiffres ?

À raison de seulement 30 secondes par connexion, chaque élève perd environ 6 heures de temps d'apprentissage par année scolaire, ne serait-ce que pour un seul site web. Prenez le temps d'y penser.

Ce chiffre ne tient pas compte des tentatives répétées après avoir mal saisi un mot de passe, ni du fait qu'il faut souvent consulter plusieurs sites éducatifs ayant chacun des identifiants spécifiques. Chaque erreur et chaque site de plus peuvent vous faire perdre 30 secondes supplémentaires.

Ce chiffre n'inclut pas non plus compte les mots de passe oubliés ni des comptes bloqués

qui prolongent les retards de 15 minutes en moyenne pour le premier cas, voire d'une journée pour le second, s'il faut faire appel au service d'assistance.

30 secondes par site web et par élève représentent au total 2 820 heures cumulées de temps d'apprentissage perdu par établissement et par année scolaire aux États-Unis, et 4 680 510 000 heures pour l'enseignement primaire et secondaire du monde entier.

Et si les difficultés de connexion, qui englobent la réinitialisation des mots de passe et le déblocage des comptes, pouvaient être résolues en donnant aux élèves l'accès à tout ce dont ils ont besoin avec une seule authentification ?

Contenu de ce guide



Dans notre guide intitulé [Introduction à la gestion des identités et des accès dans l'enseignement primaire et secondaire](#), nous expliquons ce qu'est la gestion des identités et des accès (IAM) et son rôle crucial. Nous allons maintenant approfondir l'une des fonctionnalités les plus puissantes de l'IAM : **la simplification des accès grâce à l'authentification SSO.**

Vous découvrirez :

- Comment les difficultés de connexion font perdre du temps d'enseignement et créent des inégalités.
- Ce que signifie concrètement un accès simplifié.
- L'impact concret : gain de temps, diminution du nombre de tickets et continuité de l'apprentissage.
- Comment déterminer si votre établissement est prêt pour l'authentification SSO.

De petites perturbations, mais de grandes pertes

Nous avons appris que les difficultés de connexion nuisent à l'environnement pédagogique de chaque classe, dans le monde entier. Dans cette section, nous mettons en évidence l'éventail des impacts qu'elles exercent sur les performances des élèves, des enseignants et de l'équipe informatique.

Les petits problèmes coûtent cher lorsqu'ils s'accumulent.

Élèves

- Les inégalités d'accès (fracture numérique) les empêchent de s'impliquer dans un apprentissage moderne et mixte.
- Risque de perte d'élan dans les transitions pédagogiques cruciales, empêchant les élèves de suivre le rythme des programmes scolaires.
- Les lacunes dans l'apprentissage peuvent leur faire prendre du retard pendant la classe et à la maison.
- Ce frein à l'acquisition de capacités de réflexion critique suscite une frustration vis-à-vis de la technologie et une perte de concentration.
- La rupture des liens avec les camarades et les enseignants ralentit encore les progrès et accentue la démotivation.

Enseignants

- Les cours commencent plus tard que prévu, réduisant d'autant le temps d'enseignement.
- La personnalisation de l'apprentissage est affectée par le manque de fiabilité des outils numériques.
- La multiplication des perturbations rend difficile le bon déroulement des cours et empêche de maintenir l'attention des élèves.
- Les enseignants sont contraints de jouer les techniciens et d'adapter leurs plans de cours.
- Fatigue technologique due au stress lié à l'utilisation des technologies en classe.

Équipes informatiques

- Le nombre de tickets d'assistance augmente considérablement à la rentrée scolaire, ce qui alourdit la charge de travail et accroît le stress.
- Les retards liés aux processus manuels de provisionnement privent les élèves et les enseignants de l'accès aux outils pédagogiques.
- Le service d'assistance est inondé de problèmes liés aux mots de passe, ce qui affecte considérablement la productivité de toutes les parties prenantes.
- Les incidents de sécurité se multiplient en raison de la faiblesse des identifiants et du partage de mots de passe, ce qui s'accompagne de risques pour la confidentialité.
- L'équipe passe son temps à trier et corriger les problèmes dans l'urgence, au lieu de consacrer ses compétences à des initiatives stratégiques et à l'amélioration de l'expérience.



Une question d'équité

Posez-vous la question suivante : est-ce que certains élèves perdent plus de temps que d'autres à cause de problèmes de connexion ?

Avant de répondre, réfléchissez aux points suivants :

- Les plus jeunes élèves (CP et CE1) ont généralement plus de mal à mémoriser leurs mots de passe que les autres (à partir du CE2).
- La diversité des modes d'apprentissage accroît l'effort cognitif que doivent fournir les élèves pour traiter l'information.
- Lorsque la langue parlée en classe n'est pas la langue maternelle des élèves, ceux-ci doivent surmonter simultanément des obstacles linguistiques et technologiques pour réussir.
- Les élèves qui utilisent des appareils partagés rencontrent davantage de difficultés liées aux procédures d'authentification répétées.
- Les établissements où le nombre d'élèves par appareil est plus élevé observent d'importants retards cumulés, des ralentissements des performances et des interruptions techniques.

Revenons maintenant à notre question : **tous les élèves bénéficient-ils d'un accès égal à l'apprentissage grâce à la technologie ?**

Le fardeau informatique dont personne ne parle

Personne n'en doute, l'une des missions fondamentales du service informatique consiste à apporter un soutien aux élèves, aux enseignants et à l'établissement scolaire lui-même. Il trouve des solutions personnalisées aux problèmes, autonomise les parties prenantes, élabore des expériences numériques exceptionnelles et renforce l'infrastructure. Et toutes ces missions sont cruciales pour créer un environnement éducatif moderne.

Malheureusement, certains aspects de ce soutien tendent à monopoliser les ressources informatiques, ce qui limite l'étendue et la profondeur du soutien que l'équipe peut apporter à toutes les parties prenantes.

Parmi eux, les problèmes liés aux mots de passe occupent une place prépondérante, bien qu'ils passent souvent inaperçus. Levons le voile sur ces coûts cachés :

- Selon des études, jusqu'à **50 % des demandes adressées à l'assistance informatique** concernent la réinitialisation de mots de passe.
- Une enquête de **Forrester Research** nous dit que la réinitialisation d'un mot de passe coûte environ 70 dollars. Autrement dit, des investissements considérables en temps et en argent sont consacrés à la gestion des mots de passe tout au long de l'année scolaire.
- Ces ressources pourraient être mises au service d'initiatives stratégiques visant à mieux aligner la technologie sur les objectifs d'apprentissage.

Le risque de sécurité (involontaire) : lorsque la technologie devient un poids, les parties prenantes trouvent des solutions de contournement. Cela vaut également pour les mots de passe, avec les conséquences que l'on imagine sur la sécurité :

- Mots de passe faciles à deviner : près de **6 mots de passe sur 10 utilisés dans la vie quotidienne peuvent être piratés** en moins d'une heure, et près de la moitié en quelques secondes seulement.
- Réutilisation du même mot de passe sur plusieurs comptes : les cybercriminels **automatisent les tentatives de connexions à l'aide des identifiants volés sur des centaines de sites web** ; un mot de passe réutilisé donne davantage d'accès.
- Mots de passe notés sur des post-it : tout le monde sait que **le mot de passe de votre ordinateur est noté sur un post-it** collé sous le clavier.
- Partage de comptes : une étude révèle que **16 % des gens partagent leurs mots de passe avec des amis, et 22 % avec des collègues**.
- Pas de rotation des mots de passe : une fuite de données survenue en 2025 **a exposé 16 milliards d'identifiants et de mots de passe** récoltés lors de multiples violations de sécurité, et prêts à être utilisés pour mener des cyberattaques.

Pourquoi ces comportements à risque ont-ils un tel impact sur la cybersécurité dans l'enseignement primaire et secondaire ?

La réponse est simple : **compromission des identifiants**.

Selon IBM, elle représente un peu plus de 10 % des vecteurs d'attaque initiaux à l'échelle mondiale, ce qui lui donne la troisième place du classement. On peut trouver que 10 % reste un pourcentage négligeable par rapport aux menaces qui ciblent spécifiquement le secteur de l'éducation, comme l'hameçonnage et les ransomwares. Mais sachez ceci :

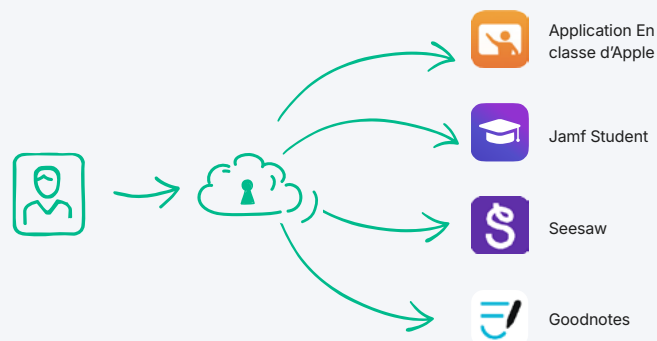
- La plupart des campagnes d'hameçonnage servent de prélude ; elles visent souvent à obtenir les identifiants de leurs victimes pour lancer des cyberattaques de plus grande envergure, comme la propagation de logiciels malveillants ou des vols de données.
- Les secteurs réglementés, comme l'enseignement primaire et secondaire, sont soumis à des lois locales, régionales et fédérales visant à protéger les informations sensibles et confidentielles. Les données à caractère personnel (PII) et les informations médicales protégées (PHI) présentent un intérêt particulier pour les cybercriminels. Le secteur de l'éducation, qui en possède une grande quantité, est donc une cible de choix pour les cyberattaques.
- Selon une étude du **rapport sur le Coût des violations de données 2025**, le coût moyen d'un incident de sécurité résultant de la compromission d'identifiants est estimé à 4,67 millions de dollars.



Qu'est-ce que l'accès simplifié ?

Un seul identifiant Un apprentissage sans limites.

L'accès simplifié vise à ce que tous les acteurs du monde de l'éducation n'aient à s'authentifier qu'une seule fois, au début de la journée. Ils peuvent ensuite passer sans difficulté d'un outil numérique à l'autre – applications, sites web éducatifs ou services pédagogiques – sans avoir à saisir à nouveau un mot de passe.



ÉLÈVE UNE SEULE CONNEXION PLUSIEURS APPLICATIONS

Une journée dans la vie d'un élève



À son arrivée le matin (8 h 15) :

Maya prend un iPad partagé dans le chariot de la classe. Elle appuie sur sa photo et saisit un code d'accès simple à 4 chiffres. Elle a accès aux applications adaptées à son niveau scolaire, aux paramètres d'accessibilité et à ses fichiers personnels.

1er cours – Français (8 h 30) :

Elle accède à la plateforme de gestion de l'apprentissage ; aucune connexion ne lui est demandée, car elle est déjà authentifiée. Elle consulte les devoirs du jour, passe sans difficulté au manuel numérique, surligne un passage et ajoute une note dans Pages. Sans jamais avoir à saisir un autre mot de passe.

Deuxième cours – Mathématiques (9 h 30) : Maya

clique sur l'application de maths pour s'entraîner aux fractions. Encore une fois, pas d'écran de connexion. Elle se met tout de suite à étudier en reprenant exactement là où elle s'était arrêtée la veille, car l'application sait qui elle est.

Projet collaboratif (10 h 30) :

pour travailler sur une présentation de groupe avec trois camarades de classe, elle ouvre Keynote. Comme les authentifications sont associées à des comptes Apple gérés, tous les utilisateurs peuvent travailler simultanément sur le même fichier. Nul besoin de partager un mot de passe ni de problèmes d'accès : la collaboration est fluide.

Fin de la journée (15 h 00) :

avant de remettre l'iPad dans le chariot, Maya se déconnecte de sa session. Ses données sont synchronisées dans iCloud, sa session est effacée et l'iPad est prêt à être remis à l'élève suivant. Demain, elle pourra s'authentifier sur n'importe quel iPad de l'établissement et retrouver exactement la même session personnalisée.

Du point de vue de l'enseignant

Avant le cours :

vous passez en revue le plan de cours sans perdre de temps à résoudre des problèmes de connexion ni à préparer les iPad, car l'authentification SSO est déjà en place.

Pendant le cours :

les élèves se connectent et sont prêts à suivre le cours en moins de 30 secondes. Le cours commence à l'heure, ce qui contribue à maintenir le rythme et la motivation des élèves.

Après le cours :

vous pouvez vous consacrer à évaluer et commenter le travail des élèves, au lieu de résoudre des problèmes informatiques ou d'envoyer des demandes à l'assistance.

Comment tout cela fonctionne-t-il ? Les trois piliers :

- 1. Des comptes Apple gérés :**
intégrés à votre fournisseur d'identité cloud (Google Workspace, Microsoft Entra ID ou RapidID) pour un provisionnement automatique et un accès unifié aux services Apple.
- 2. Processus sans mot de passe :**
Une authentification rapide et efficace par simple pression, pour réduire la charge cognitive tout en garantissant la sécurité. Idéal pour les jeunes élèves ou les utilisateurs ayant des besoins spécifiques en matière d'accessibilité.
- 3. Authentification unique :**
un même compte permet d'accéder à toutes les applications fédérées, qu'il s'agisse d'applications web ou d'applications natives.

L'impact concret d'un accès continu

Temps d'enseignement libéré

Le temps consacré à l'enseignement est limité, et les petites perturbations s'accumulent rapidement. Les difficultés de connexion représentent un obstacle récurrent qui retarde les cours et brise la dynamique de la classe. Lorsqu'on réduit ces interruptions, les enseignants restent concentrés sur leur mission pédagogique, et le service informatique a le temps de créer des expériences d'apprentissage plus efficaces et plus fluides.

Les recherches sur le temps perdu

Comme nous l'avons vu dans la première partie, une année scolaire compte en moyenne 1 260 heures. Ce chiffre peut varier selon votre région, mais nous l'utiliserons dans cette section pour illustrer l'importance cruciale de rattraper le temps d'enseignement perdu.

En 2024, des chercheurs de l'université Brown ont constaté que près de **25 % du temps d'enseignement par année scolaire était perdu en raison d'interruptions** et d'absences. Même si certains exemples cités dans cette étude peuvent sembler mineurs, comme une interruption de 30 secondes du système d'interphone, ils s'accompagnent souvent de perturbations de plusieurs minutes, car il faut du temps aux élèves pour retrouver leur concentration.

Pertes de temps liées à la technologie

Lors d'une étude similaire menée en 2021, des chercheurs ont relevé que la technologie figurait parmi les causes d'interruptions les plus courantes. À partir de données issues d'observations et d'enquêtes, ils ont mis en évidence qu'une interruption initiale, même minime, entraîne une chaîne de perturbations qui affectent durablement les opportunités des élèves.

Plus de 50 % des interruptions ont entraîné une perte de temps d'apprentissage prolongée ; les chercheurs indiquent que cela « détournait l'attention des élèves » et « obligeait l'enseignant à interrompre son cours ».



Les difficultés de connexion se produisent dans tous les contextes d'apprentissage, que ce soit dans l'enceinte de l'établissement ou en dehors. Chaque jour en apporte de nouveaux exemples :

- Retards dus à des interfaces utilisateur mal conçues
- Temps de chargement longs dus à des systèmes d'authentification inefficaces
- Fatigue liée à la gestion simultanée de plusieurs comptes
- Refus d'accès liés à un mot de passe incorrect
- Mots de passe non valides en raison d'exigences de complexité variables
- Comptes verrouillés suite au déclenchement d'une règle de mot de passe

Que fait l'authentification SSO

Pour dire les choses simplement, l'authentification SSO réduit considérablement les difficultés liées aux mots de passe et les perturbations d'ordre technique qui en découlent. Grâce à cette méthode, les élèves s'authentifient une fois pour toutes en début de journée, puis naviguent en toute fluidité entre les applications, les sites web et les services qu'ils utilisent pour apprendre.

Les gains de temps s'accumulent au fil des cours, tout au long de l'année scolaire, et les avantages sont nombreux :

- Gains d'efficacité et de productivité, en classe comme dans les opérations scolaires
- Réductions des risques et des expositions, et atténuation des failles.
- Harmonisation homogène de la conformité et de la gouvernance entre les institutions.
- Amélioration du retour sur investissement grâce à la réduction du coût total de possession.

Les avantages du gain de temps pour les enseignants

Tout au long de ce guide, nous avons vu à quel point un gain de temps pourrait être utile aux enseignants :

- Commencer les cours sans attendre, en préservant le dynamisme et l'implication des élèves.
- Consacrer plus de temps à l'enseignement et moins au dépannage.
- Couvrir davantage de contenu sans précipitation.
- Prévoir davantage de temps pour répondre aux questions des élèves et différencier l'enseignement.

Mais, plutôt que de donner des réponses, nous invitons les acteurs du monde de l'éducation à réfléchir à une question. Dans la première partie de cet article, nous avons calculé que chaque élève perdait environ 6 heures de temps d'enseignement par année scolaire, en partant du principe que la connexion à un site web entraînait une interruption de 30 secondes à chaque cours.

Pendant ce délai, les enseignants doivent interrompre leur cours et attendre que tous les élèves soient prêts pour reprendre leur cours. D'où la question suivante :

Que pourraient faire vos enseignants s'ils récupéraient le temps perdu à cause des interruptions quotidiennes, des perturbations et des retards prolongés ?

L'impact du service informatique : de la gestion des urgences à l'élaboration de stratégies

Outre les gains de productivité et la réduction des failles de sécurité liées aux mots de passe, la mise en place de l'authentification SSO permet également **de réduire les coûts d'assistance de 40 % en moyenne.**

Les promesses de l'authentification SSO

Il faut en effet savoir que la moitié des demandes d'assistance concerne la résolution de difficultés liées aux comptes et aux mots de passe. En atténuant ce problème, on donne au service informatique les moyens de traiter plus rapidement les problèmes les plus critiques. Par exemple, sur 10 tickets d'assistance, la répartition des problèmes critiques et non critiques passe de 1 pour 2 (sans SSO) à 7 pour 3 (avec SSO).

Dans quels domaines le service informatique peut-il investir le temps ainsi gagné ?

Ce progrès n'affecte pas seulement la charge de travail, elle libère aussi du temps. Avec l'automatisation, la centralisation et la rationalisation des processus de connexion via l'authentification SSO, le service informatique peut désormais consacrer plus de temps à des objectifs :

- Améliorer l'expérience des parties prenantes grâce à la technologie.
- Développer de meilleurs processus de production et d'exploitation.
- Moderniser et améliorer les infrastructures informatiques de l'établissement scolaire.
- Renforcer les compétences des parties prenantes grâce à des initiatives de formation aux technologies.
- Aligner les outils informatiques sur les objectifs d'apprentissage.

L'impact sur l'égalité des chances

Disparités d'accessibilité

Les élèves ne retrouvent pas tous leur concentration en même temps après une interruption ordinaire. Des chercheurs l'ont d'ailleurs confirmé en 2025 : **leurs conclusions indiquent** que « *l'élève moyen perd 25 % de son temps d'enseignement à cause de ces nombreuses interruptions* ». L'éventail des interruptions est large :

- Élèves en retard
- Enseignants absents
- Annonces par interphone
- Visites en classe

Elles sont même fréquentes dans les établissements primaires et secondaires du monde entier. Sur une journée d'école moyenne de 7 heures, une perte de 25 % (soit 1,75 heure) réduit le temps d'enseignement à 5,25 heures.

Ajoutez à cela qu'il faut un certain temps pour que les élèves retrouvent leur concentration après une interruption causée par des difficultés de connexion.

Les élèves ne vivent pas tous de la même façon les obstacles liés à la technologie. Différents facteurs d'accessibilité viennent encore aggraver cette perte de temps d'enseignement :

- Mémorisation
- Charge cognitive
- Barrières linguistiques
- Handicap physique

✂ L'intérêt de l'authentification SSO

Tous les élèves bénéficient d'un accès équitable et peuvent apprendre partout, indépendamment de leurs compétences technologiques. L'authentification SSO a été conçue pour répondre à plusieurs critères :

- Les élèves n'ont qu'un seul compte à retenir.
- La sécurité est intégrée ; il est possible d'utiliser des mots de passe complexes ou de configurer des codes d'accès simples en garantissant la sécurité.
- Les processus d'authentification sont simplifiés pour présenter une interface et un comportement identiques à tous les utilisateurs, à chaque fois.
- Les identifiants sont centralisés et peuvent être facilement gérés en libre-service, ou avec l'aide d'un enseignant ou d'un technicien informatique.

👤 Le « facteur dignité »

Lorsqu'un élève est le seul de sa classe à éprouver des difficultés de connexion, le problème n'est pas seulement technique, il est aussi émotionnel. L'authentification SSO élimine cette source de frustration et d'embarras pour contribuer à un environnement scolaire plus inclusif.

Renforcement de la sécurité

Saviez-vous que « *les mots de passe sont à l'origine de plus de 80 % des fuites de données* » ? Selon l'Alliance FIDO (Fast Identity Online), les identifiants représentent un vecteur de choix pour les acteurs malveillants, car ils sont **faciles à obtenir par hameçonnage, interception ou autre méthode**.

🔒 Avantages de sécurité de l'authentification SSO

L'un des principaux avantages réside dans la centralisation des règles relatives aux mots de passe au niveau de l'IdP. Cette approche n'est pas seulement un atout pour la conformité (sur laquelle nous reviendrons dans la section suivante) ; elle renforce également la sécurité des mots de passe en harmonisant les mesures de sécurité à l'échelle des infrastructures éducatives. Chaque application, chaque site web et chaque service bénéficient du même niveau de protection. À cela s'ajoutent bien d'autres avantages pour la sécurité des écoles primaires et secondaires :

- Plus besoin de créer ni de mémoriser plusieurs mots de passe différents.
- Une règle commune imposant l'utilisation d'un mot de passe fort.
- Des droits d'accès simplifiés et définis par rôle, plutôt que de manière individuelle ou manuelle.
- Recul du partage de comptes (une pratique courante lorsque les utilisateurs ne parviennent pas à se connecter).
- Automatisation de la suppression des comptes inactifs au départ d'un utilisateur.
- Possibilité d'ajouter la MFA pour renforcer encore la sécurité des comptes et empêcher les accès non autorisés.

🔍 Une conformité digne de confiance

Les mesures de protection ne représentent qu'un aspect de la sécurité. Il est tout aussi crucial de veiller à ce que les différentes couches de contrôle fonctionnent conformément à leur configuration. Et chacune de ces fonctions a pour but de soutenir la stratégie opérationnelle de votre établissement. Il s'agit donc de préserver la conformité et de donner au service informatique un moyen standardisé de :

- Mettre en place une surveillance centralisée de toutes les tentatives d'accès.
- Documenter les contrôles d'accès pour réviser les règles en place.
- Fournir des preuves claires de l'existence des garde-fous appropriés.
- Tenir à jour des pistes d'audit détaillées à des fins de conformité réglementaire.



Coût total de possession (TCO)

Une image complète

Les coûts liés aux technologies éducatives ne se limitent pas au prix du matériel informatique à proprement parler. Si l'on ajoute à cela les coûts d'infrastructure (licences logicielles, garanties et assistance, formation, maintenance et mise hors service), le coût total de possession (TCO) d'un appareil atteint plusieurs milliers de dollars sur l'ensemble de sa durée de vie utile. Si votre établissement compte plusieurs milliers d'appareils, ce coût peut largement dépasser **les dépenses d'acquisition initiales**.

Prenons la formule de base suivante pour calculer le coût total de possession (TCO) à partir des moyennes du secteur :

Prix d'un iPad Apple (128 Go) :	329 \$
AppleCare+ pour les établissements scolaires (3 ans) :	79 \$
Étui pour iPad (renforcé) :	20 \$
329 \$ + 79 \$ + 20 \$	= 428 \$ (par appareil)

Nombre d'élèves (programme individuel) :	1 000
428 \$ x 1 000	= 428 000 \$

Estimation du TCO par appareil (sur 3 ans) :	194 \$
194 \$ x 1 000	= 194 000 \$

Coût total de propriété (matériel et garantie uniquement) :	
428 000 \$ + 194 000 \$	= 622 000 \$
194 000 \$ / 428 000 \$	= 0,45
0,45 x 100	= 45 %

Les coûts liés aux licences logicielles, à la formation, à la maintenance et à la mise hors service varient considérablement en fonction des besoins de chaque établissement, ce qui les rend difficiles à chiffrer. De plus, les variations selon les établissements et les modes de gouvernance peuvent avoir une incidence supplémentaire sur les coûts.

Domaines de réduction des coûts

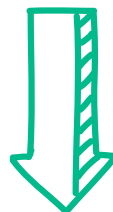
Compte tenu des coûts liés à l'acquisition, à la gestion et à la sécurisation des technologies, les établissements cherchent naturellement les domaines dans lesquels ils peuvent réduire le coût total de possession (TCO), voire augmenter le rendement de l'investissement (ROI).

En 2023, Forrester Consulting a mené une étude sur l'**Impact économique de Microsoft Entra** afin d'évaluer le ROI de la solution IdP de Microsoft par rapport aux solutions multipoints. L'analyse finale a permis de mettre en évidence deux conclusions intéressantes :

- Moderniser la gestion des appareils, l'identité et la sécurité, c'est aussi réduire la complexité et centraliser les outils.
- L'abandon d'une « approche fragmentée » (nous y reviendrons dans la section suivante) basée sur des solutions multipoints a permis d'atteindre un rendement de 240 %, tout en renforçant la sécurité et en réduisant les coûts.

L'authentification SSO contribue également à réduire d'autres coûts :

- Main-d'œuvre informatique : la standardisation de la gestion et du provisionnement des comptes permet de réduire considérablement les coûts liés aux tickets d'assistance et aux réinitialisations de mots de passe.
- Temps d'enseignement : le fait de récupérer ne serait-ce qu'une partie des 25 % de temps perdus par élève représente un gain considérable pour toutes les parties prenantes.
- Optimisation des licences : l'automatisation de la désactivation des licences permet de réattribuer celles qui ne sont plus utilisées.



L'authentification SSO pour les profanes

Comprendre la technologie sans se perdre dans sa complexité

Nul besoin d'être un expert en cybersécurité pour comprendre que l'authentification SSO ne se contente pas de protéger l'accès aux appareils et aux ressources de l'établissement ; elle préserve également le temps d'enseignement :

« La complexité est l'ennemie de la sécurité. »
– Bruce Schneier

- ✓ En minimisant la complexité technologique
- ✓ En améliorant la visibilité sur l'authentification
- ✓ En atténuant les failles cachées
- ✓ En renforçant la posture de sécurité



- ✓ En réduisant l'erreur humaine
- ✓ En automatisant la gestion des comptes
- ✓ En simplifiant les procédures de connexion
- ✓ En consolidant les outils informatiques

Après la théorie, voyons un cas d'utilisation réel impliquant l'utilisation d'iPad Apple dans l'enseignement primaire et secondaire.



La cloche sonne, le cours va commencer. Dans un même geste, les élèves sortent leurs iPad et se connectent via l'authentification SSO pendant que l'enseignant prépare son cours. Au bout de quelques minutes, toute la classe est connectée.



Pause.

Les élèves ont besoin de quelques minutes pour se connecter à leur portail, qui utilise une deuxième solution d'authentification SSO. Les élèves peuvent alors suivre leur professeur jusqu'à la fin du cours. Ils ouvrent ensuite leur logiciel de traitement de texte.



Nouvelle pause.

Un troisième produit SSO est utilisé exclusivement pour cette application. Nouvelle pause jusqu'à ce que tout le monde se soit authentifié pour la troisième fois.

Parfait, nous sommes désormais dans l'application de traitement de texte, nous pouvons commencer à travailler sur notre projet de groupe.



Oh non, pas encore ! Et si. Pour travailler ensemble simultanément, les élèves doivent accéder à l'application de collaboration qui, comme vous l'avez deviné, utilise une autre instance de SSO. Les élèves s'interrompent encore quelques minutes pour se connecter pour la quatrième fois.

Mais le temps que les élèves soient tous prêts à travailler, l'heure de cours touche à sa fin ; ils ont passé environ 15 minutes, soit 25 % du temps d'enseignement, à s'authentifier sur différentes versions de SSO qui ne fait qu'imiter un processus d'authentification unique.

Si certains produits vont jusqu'à promettre une fonctionnalité d'authentification SSO pour iPadOS, une SSO véritable doit offrir un accès continu à l'apprentissage, après une seule identification lors de la connexion à l'iPad. Cette étape doit donner accès à toutes les destinations :

- Portails institutionnels
- Ressources scolaires
- Sites web éducatifs
- Services cloud
- Applications intégrées à l'appareil

L'authentification initiale se maintient en arrière-plan et connecte automatiquement les utilisateurs aux ressources demandées sans manipulation ni délai.

Concept fondamental

Une seule connexion, plusieurs applications :

l'authentification SSO est une sorte de pass « backstage » à un concert. Il vous suffit de présenter vos identifiants à l'entrée pour accéder à toutes les zones sans vous justifier à nouveau. Votre fournisseur d'identité (Google Workspace, Microsoft Entra ID ou Okta) joue le rôle de point de contrôle de sécurité ; c'est lui qui approuve votre accès à toutes les applications.



Une sécurité sans obstacle

Loin de compromettre la sécurité, l'authentification SSO la renforce. La synthèse ci-dessous vous explique comment l'authentification SSO garantit la sécurité des identités dès la conception :

1.

Les utilisateurs s'authentifient une fois auprès de l'IdP à l'aide de leurs identifiants (généralement lorsqu'ils se connectent à leur appareil en début de journée).

2.

Une fois les identifiants validés, le fournisseur d'identité (IdP) émet un jeton numérique qui garantit de manière cryptographique l'identité de l'utilisateur.

3.

Lorsque l'utilisateur accède à un fournisseur de services (pour consulter une ressource protégée, par exemple), l'IdP lui transmet le jeton numérique.

4.

Le fournisseur valide le jeton et autorise la demande d'accès en toute sécurité, sans mot de passe !

Ça fonctionne partout



Applications en ligne :

plateformes de gestion de l'apprentissage, Canvas, Khan Academy, BrainPOP... Les élèves accèdent à tout en un clic.

Applications natives de l'iPad :

Pages, Keynote, GarageBand et les applications éducatives telles que Seesaw et Goodnotes reconnaissent le compte Apple géré de l'élève et le connectent automatiquement.

iPad partagés :

chaque élève bénéficie d'une expérience personnalisée sur n'importe quel appareil de l'établissement. Lorsqu'il se déconnecte, la session est effacée, mais les travaux restent stockés en toute sécurité dans iCloud.

Couche de contrôle informatique

Une authentification SSO performante permet aux élèves et aux enseignants de bénéficier d'un accès fluide, tandis que le service informatique conserve, en coulisses, le contrôle de la sécurité et de la conformité. Dans le cadre d'une stratégie plus large de défense en profondeur, intégrant la gestion des appareils, la gestion des identités et des accès, et la sécurité des points de terminaison, l'authentification SSO fait office de couche de contrôle : elle protège l'ensemble des acteurs, des appareils et des données sensibles des établissements primaires et secondaires. Pour le service informatique, les atouts sont nombreux :



Visibilité en temps réel sur les accès des utilisateurs aux ressources.



Contrôles d'accès basés sur des règles tenant compte du niveau scolaire, du rôle ou du modèle de déploiement.



Provisionnement systématique lors de l'inscription des élèves et du changement de classe.



Désactivation automatique lorsque les élèves terminent leur scolarité ou changent d'établissement.



Des protocoles de sécurité robustes pour des communications multiplateformes sécurisées.

Votre établissement est-il prêt pour l'authentification SSO ?

Évaluation de la préparation à l'authentification SSO

Avec notre check-list, faites le point sur votre situation actuelle et identifiez les mesures à prendre pour mettre en œuvre l'accès continu à l'apprentissage.



Infrastructure d'identité

- ☐ Fournisseurs d'identité (IdP) basés sur le cloud (Google Workspace, Microsoft Entra ID, RapidID)
- ☐ SIS intégré à l'IdP
- ☐ Les données d'identité sont cohérentes d'un système à l'autre
- ☐ Apple School Manager en place
- ☐ Des comptes Apple gérés sont (ou peuvent être) créés pour les élèves et le personnel

Gestion des appareils

- ☐ Solution MDM en place (Jamf School ou Jamf Pro)
- ☐ MDM intégrée à l'IdP
- ☐ iPad partagés, appareils individuels ou modèle hybride
- ☐ Appareils inscrits dans Apple School Manager

Préparation des applications

- ☐ Les 10 applications éducatives les plus utilisées ont été identifiées
- ☐ Les applications prenant en charge SAML, OAuth ou d'autres protocoles d'authentification unique ont été identifiées
- ☐ Un plan a été créé pour les applications incompatibles avec l'authentification SSO
- ☐ Les modalités actuelles de licence et d'utilisation des applications sont comprises

Préparation organisationnelle

- ☐ Les dirigeants comprennent l'importance de préserver le temps d'apprentissage et les arguments d'équité d'accès en faveur de l'authentification SSO
- ☐ Adhésion des parties prenantes (informaticiens, administrateurs, enseignants) obtenue
- ☐ L'établissement est prêt à lancer un projet pilote avec un groupe test avant de passer à l'échelle supérieure
- ☐ Ressources indispensables (temps et budget) allouées à la mise en œuvre
- ☐ Mise en place d'un programme de formation destiné aux enseignants et aux élèves

Indicateurs de référence

- ☐ Le temps d'enseignement perdu en raison de problèmes de connexion a été chiffré
- ☐ Suivi des tickets de réinitialisation de mot de passe et des indicateurs relatifs au temps d'assistance informatique
- ☐ Les retours des enseignants sur les difficultés d'accès actuelles ont été recueillis
- ☐ Les populations d'élèves qui rencontrent le plus de difficultés ont été identifiées

Résultats :

Si vous **avez coché 12 à 15 cases** : vous êtes désormais prêt à mettre en place l'authentification SSO. Les données démontrent clairement la rentabilité de la démarche, et vous disposez déjà des bases technologiques nécessaires.

Vous avez coché 8 à 11 cases : vous y êtes presque. Veillez à combler les lacunes de votre infrastructure d'identité avant de lancer un programme pilote.

Vous avez coché 4 à 7 cases : vous devez consolider vos bases. Consultez notre guide « Introduction à la gestion des identités et des accès dans l'enseignement primaire et secondaire » pour mettre en place les composants essentiels avant de revenir à la planification de l'authentification SSO.

Vous avez coché 0 à 3 cases cochées : commencez par les fondamentaux. Mettez en place votre infrastructure d'identité et Apple School Manager avant de passer à l'authentification SSO.



Conclusion

Les difficultés de connexion érodent insidieusement le temps d'enseignement, créent des inégalités d'accès entre les élèves et alourdissent la charge du service informatique. Chaque retard freine la dynamique de classe, dégrade la motivation des élèves et aggrave les écarts d'apprentissage dans les classes hétérogènes.

Et tous ces désagréments s'accumulent. Trente secondes par connexion, multipliées par le nombre de cours, d'élèves et de jours d'école, représentent des milliers d'heures d'apprentissage perdues à jamais.

L'**authentification unique (SSO)** est à la base de l'accès continu à l'apprentissage, un principe qui change réellement la donne pour les élèves. En simplifiant l'authentification, en renforçant la sécurité et en permettant de consacrer davantage de temps à l'enseignement, l'authentification SSO fait disparaître un obstacle quotidien pour les élèves et les enseignants.

Les enseignants peuvent alors se consacrer pleinement à l'enseignement, libérés de la résolution des problèmes. Les cours commencent à l'heure. Le service informatique peut abandonner ses pratiques réactives pour une approche proactive : offrir de meilleures expériences, rationaliser les opérations et aligner la technologie sur les besoins pédagogiques réels.



Avec Jamf, le service informatique garantit à chaque élève un accès sécurisé et évolutif et préserve les conditions d'apprentissage.