Introduction à la gestion des appareils mobiles (MDM)

POUR L'ENSEIGNEMENT SUPÉRIEUR

Mieux exploiter Apple dans l'enseignement supérieur

jamf

La position d'Apple dans les établissements d'enseignement supérieur

Pourquoi choisir l'iPad pour l'enseignement supérieur ?

Plus que jamais, les technologies éducatives modèlent et font progresser l'expérience universitaire moderne. Qu'il s'agisse des besoins administratifs, de l'utilisation par les professeurs ou d'un outil d'apprentissage crucial pour les étudiants, les appareils Apple jouent un rôle essentiel dans la productivité, la motivation et l'apprentissage au sein de l'enseignement supérieur.

Parmi les systèmes d'exploitation mobiles les plus répandus, iOS et iPadOS sont des plateformes spécialement conçues pour les consommateurs et très populaires auprès des universités. Elles se caractérisent par une interface utilisateur intuitive, un écosystème sécurisé d'applications commerciales et d'applications éducatives, ainsi que des outils intégrés qui permettent aux utilisateurs d'être plus productifs que jamais.

Apple autonomise les universités grâce aux outils suivants :

- le matériel mobile le plus rapide et le plus efficace ;
- le chiffrement basé sur le matériel natif pour garantir la sécurité des données ;
- Touch ID et Face ID pour la sécurité biométrique ;
- les applications de productivité pour créer des documents, des feuilles de calcul et des présentations incluant Microsoft Office pour iOS ;
- un écran partagé multitâche pour l'iPad ;
- prise en charge intégrée des réseaux sans fil modernes et sécurisés, tels que le VPN et le SSO;
- prise en charge de Microsoft Exchange pour la messagerie, les calendriers et les contacts.

Qui choisit l'iPad dans l'enseignement supérieur ?

Dans une récente **étude menée par Vanson Bourne** sur l'importance du choix des appareils pour les étudiants en vue de la préparation à la vie active moderne : **94 % des établissements d'enseignement supérieur disent utiliser l'iPad, pour améliorer l'apprentissage.**

Présentation de la gestion des appareils mobiles

Pourquoi une solution MDM est-elle nécessaire ?

La gestion des appareils mobiles (MDM) est le framework d'Apple pour la gestion iPadOS (système d'exploitation pour l'iPad) et d'iOS (système d'exploitation pour l'iPhone). Afin de gérer efficacement les appareils Apple et de libérer tout leur potentiel, les universités doivent disposer d'une solution MDM toute aussi puissante. Du déploiement et de l'inventaire des nouveaux appareils à la configuration des réglages, en passant par la gestion des applications ou l'effacement des données, MDM propose un ensemble d'outils complet pour répondre aux déploiements de grande envergure et garantir la sécurité des appareils.

- Déploiement
- Inventaire
- Profils de configuration
- Commandes de gestion
- Déploiement des applications
- Sécurité et Confidentialité

L’architecture MDM

Service de notification push d’Apple

Lorsque vous envoyez des commandes auprès des appareils Apple, votre serveur MDM communique avec le service de notification push d’Apple (APNs). L’APNs maintient une connexion constante avec les appareils pour que vous n’ayez pas à le faire. Les appareils communiquent avec le serveur MDM et reçoivent les commandes, les profils de configuration ou les applications que vous lui avez envoyés.

Déploiement

Avant de pouvoir utiliser une solution MDM pour gérer vos appareils Apple, vous devez d’abord les enrôler. Pour l’iPad, un outil MDM vous permet d’enrôler facilement les appareils, d’assurer une distribution cohérente des applications et du contenu, et de configurer des profils d’accès et de sécurité. Il existe plusieurs méthodes pour enrôler un iPad, y compris l’enrôlement via Apple Configurator, un enrôlement par utilisateur via une page web, ou un déploiement Zéro Touch automatisé avec la solution MDM et Apple School Manager.

Apple School Manager

Tout ce dont vous avez besoin au même endroit

D'abord lancé avec la version iOS 9.3, Apple School Manager est un outil qui permet aux administrateurs informatiques de gérer plus facilement les utilisateurs, les appareils et le contenu dans un portail central sur le Web. Apple School Manager simplifie les déploiements éducatifs en regroupant tous les anciens programmes de déploiement Apple au sein d'un seul système. En utilisant la version iOS 10.3 ou supérieure, il est encore plus facile de gérer les appareils éducatifs avec Apple School Manager.

Lorsque les établissements scolaires combinent l'iPad avec une solution de gestion des appareils mobile (MDM), ils sont en mesure :

- d'automatiser l'enrôlement de l'appareil, la configuration et la distribution des applications et du contenu ;
- de créer des identifiants Apple gérés ;
- d'utiliser l'iPad partagé.

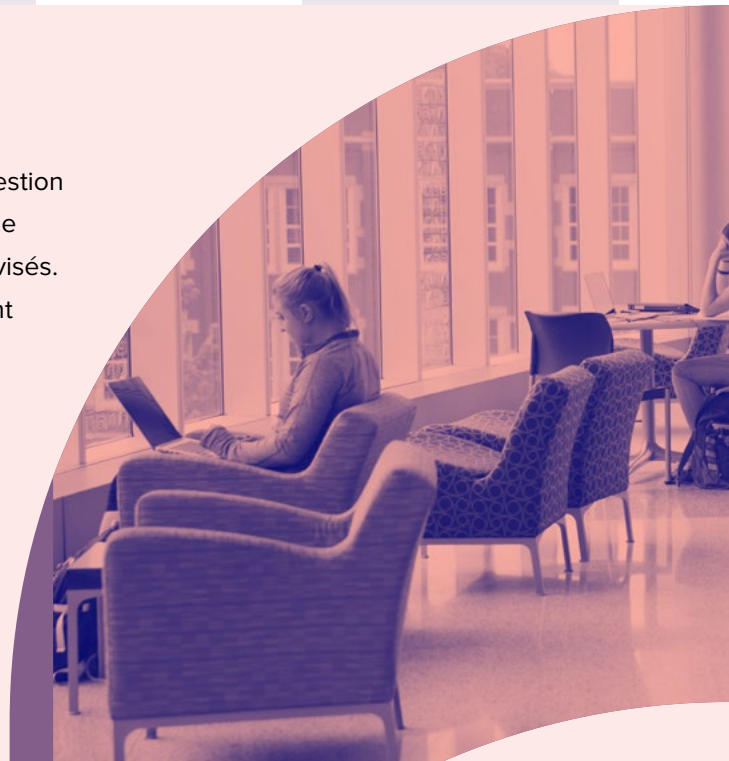
Méthodes de déploiement	Description	Expérience utilisateur	Supervision	Recommandé pour
Déploiement automatisé avec la solution MDM et Apple School Manager	Enrôlement automatique à distance (également appelé déploiement Zero-Touch)	L'utilisateur reçoit une boîte sous film plastique et l'appareil est automatiquement configuré dès qu'il l'allume	Oui, à distance.	Tous
Apple Configurator	Enrôlement via une application Mac connectée aux appareils via USB	S.O. : le service informatique gère ce processus et donne les appareils aux utilisateurs	Oui, filaire	Chariots pour iPad
Initié par l'utilisateur via une URL	Enrôlement manuel à distance	L'utilisateur accède à une URL donnée pour configurer automatiquement son appareil	Non	BYOD

Supervision

La supervision est un mode spécial d'iPadOS qui permet une gestion plus approfondie par une solution MDM. Un nombre croissant de configurations ne sont disponibles que sur des appareils supervisés. Il est recommandé que les appareils détenus par l'établissement soient en mode Supervision.

Exemples de commandes en mode Supervision uniquement :

- Désactiver la caméra ;
- Désactiver l'App Store ;
- Désactiver Safari ;
- Désactiver la modification du fond d'écran ;
- Désactiver l'ajout de comptes de messagerie ;
- Et bien plus encore…



Déploiements Zero-Touch avec une solution MDM et Apple School Manager pour l'enseignement supérieur.

1

Inscrivez-vous à Apple School Manager via **https://school.apple.com/** et ajoutez votre serveur MDM au portail Apple School Manager.

2

Achetez des appareils et associez-les à votre compte Apple School Manager. Pas besoin de déballer les appareils.

3

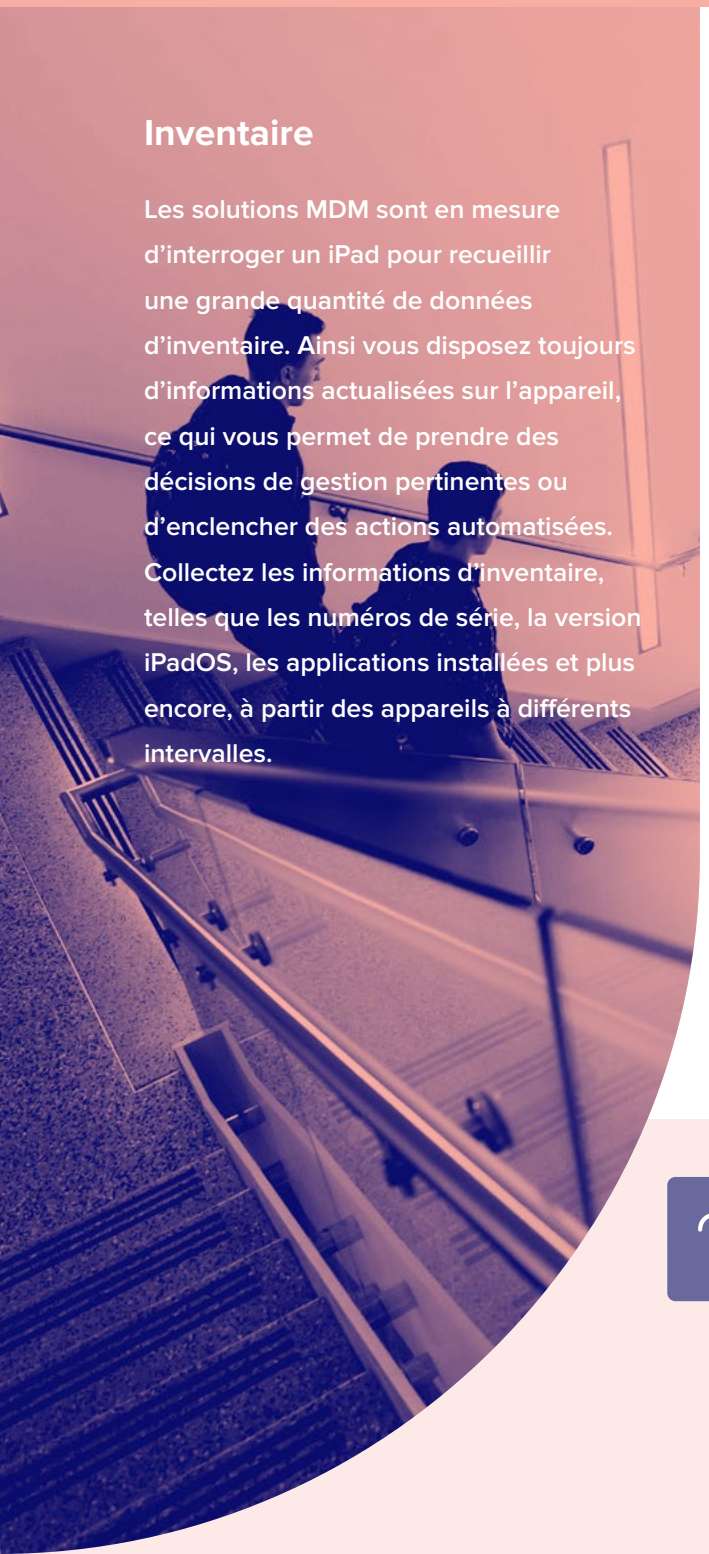
Lorsque l'utilisateur allumera son iPad pour la première fois, l'appareil sera automatiquement inscrit ; aucune interaction supplémentaire n'est requise.

4

L'appareil est enrôlé auprès du serveur MDM. Préparez tous les profils de configuration et les applications que vous souhaitez télécharger sur vos appareils via votre solution MDM.

5

L'appareil reçoit les configurations et les applications qui lui sont destinées, et l'utilisateur accède à l'écran d'accueil. L'appareil est maintenant géré et configuré, tout cela sans l'intervention du service informatique.



Inventaire

Les solutions MDM sont en mesure d'interroger un iPad pour recueillir une grande quantité de données d'inventaire. Ainsi vous disposez toujours d'informations actualisées sur l'appareil, ce qui vous permet de prendre des décisions de gestion pertinentes ou d'enclencher des actions automatisées. Collectez les informations d'inventaire, telles que les numéros de série, la version iPadOS, les applications installées et plus encore, à partir des appareils à différents intervalles.

Exemples de données collectées avec une solution MDM

Détails du matériel

- Type d'appareil
- Modèle d'appareil
- Nom de l'appareil
- Numéro de série
- UDID
- Niveau de la batterie

Détails du logiciel

- Version du système d'exploitation
- Liste des apps installées
- Capacité de stockage
- Espace disponible
- Statut iTunes Store

Détails de la gestion

- Statut géré
- Statut supervisé
- Adresse IP
- Mode d'enrôlement
- Statut de sécurité

Informations complémentaires

- Profils installés
- Certificats installés
- Statut du verrouillage d'activation
- Informations sur l'achat
- Dernière mise à jour de l'inventaire

Pourquoi l'inventaire est-il important ?

Utilisez les données d'inventaire de la solution MDM et vous avez tous les éléments en main pour répondre aux questions fréquentes telles que : Est-ce que tous mes appareils sont sécurisés ? Combien d'applications avons-nous déployées ? Quelle version d'iPadOS avons-nous déployée ?

Profils de configuration

Les profils de configuration vous permettent de dire à vos appareils comment se comporter. Au lieu d'avoir à configurer manuellement les appareils, la technologie de la MDM vous permet à présent d'automatiser le processus de configuration des réglages des codes secrets, des mots de passe Wi-Fi, des configurations VPN et plus bien encore. Les profils de configuration sont également en mesure de restreindre les éléments dans l'iPadOS, tels que l'appareil photo, le navigateur Safari ou même la possibilité de renommer l'appareil.

Profils disponibles

Réglages de base

- Code
- Restrictions
- Wi-Fi
- VPN
- Agencement de l'écran d'accueil
- Mode d'application unique
- LDAP
- Clips Web

Comptes de messagerie

- Mail
- Exchange ActiveSync
- Compte Google
- VPN
- Calendrier
- Contacts
- Calendriers souscrits
- Compte du serveur macOS

Réglages Internet

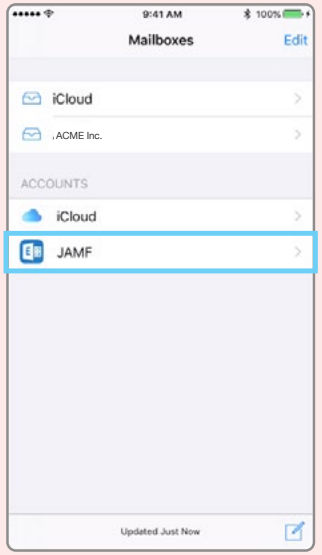
- Proxy HTTP global
- Filtre de contenu
- Domaines
- Cellulaire
- Règles d'utilisation du réseau
- Certificats

Autres réglages

- AirPlay
- Sécurité d'AirPlay
- Affichage des salles de conférence
- AirPrint
- Polices
- SCEP
- Message sur l'écran de verrouillage
- Notifications
- Authentification par signature unique
- Nom du point d'accès

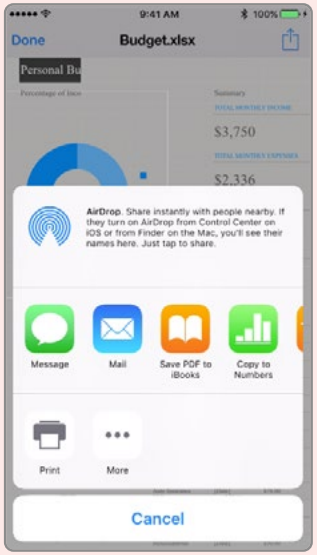
Élimination des conteneurs pour la gestion iPadOS

Dans le monde de la gestionn des appareils, un conteneur est une application supplémentaire conçue pour servir de point de contact sécurisé pour des informations telles que la messagerie, les calendriers, les contacts et même la navigation sur le Web. Ce concept attire les organisations, mais il entrave une bonne expérience utilisateur. Les conteneurs sont devenus populaires parmi certaines solutions MDM pour aider à remédier aux failles de sécurité. En réalité, les apps Apple (Mail, Calendrier, Contacts et Safari) sont déjà sécurisées. Nul besoin d'avoir un conteneur de messagerie « sécurisé ». Pour préserver la meilleure expérience utilisateur possible, il vous suffit d'utiliser les profils de configuration. Un profil est en mesure d'ajouter un compte Exchange, ce qui fournira un accès à la messagerie et aux calendriers d'entreprise.

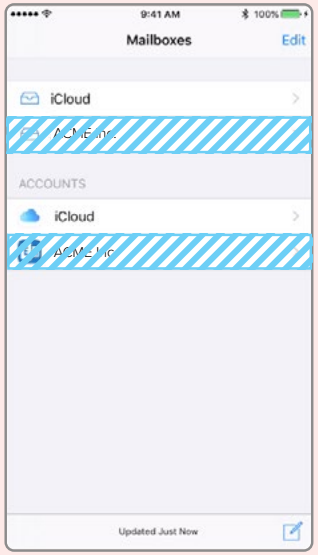


Un profil de configuration ajoute un compte Exchange en plus du compte de messagerie personnel d'un utilisateur dans l'app Mail native.

Les données d'entreprise sont maintenant juste à côté de données à caractère personnel dans les apps natives, ce qui permet la préservation de l'expérience et de la sécurité de l'utilisateur.



Le service informatique contrôle également le flux de données en empêchant les apps d'ouvrir des pièces jointes sur leur compte de messagerie d'entreprise.



Enfin, si un employé quitte une organisation, le service informatique n'a qu'à supprimer le profil de configuration et le compte de messagerie d'entreprise ainsi que les données seront supprimés. Les comptes personnels ne seront pas effacés.

Normalisation de l’iPad

Que les étudiants utilisent vos iPads pendant un cours magistral ou que le personnel enseignant les utilise dans le cadre de ses fonctions, ils améliorent la productivité en offrant une expérience cohérente sur les appareils appartenant à votre institution. La normalisation des appareils Apple pour vos utilisateurs crée un processus de configuration simplifié qui permet aux utilisateurs d’accéder rapidement aux applications dont ils ont besoin, quand et où ils en ont besoin. La réduction du temps de recherche des apps permet d’accroître la productivité des utilisateurs.

Voici trois manières de simplifier l’utilisation des iPads et des iPhones dans votre université :

1

Affichez/masquez les applications

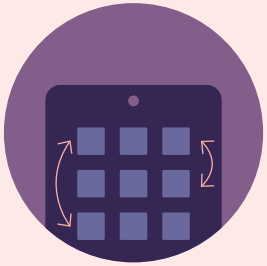
Affichez uniquement les apps dont votre personnel et vos étudiants ont besoin et cachez celles qui ne sont pas nécessaires à leur travail.

2

Définissez le fond d’écran d’accueil

Affichezt le logo de votre organisation sur le fond d’écran.

3



Préconfigurez la mise en page de l’écran d’accueil

Définissez le placement des apps et des dossiers ainsi que des vidéos sur l’écran d’accueil. Mettez les apps essentielles à l’enseignement sur la première page et les apps moins importantes sur les autres pages.

Commandes de gestion

Les commandes de gestion (également appelées les commandes MDM), sont les spécifications que vous pouvez appliquer aux appareils individuels pour garantir la sécurité des données de l'élève. Profitez de cette fonctionnalité pour agir sur l'appareil en cas de perte ou de vol en le verrouillant ou en l'effaçant complètement. Des commandes supplémentaires vous permettent d'envoyer des notifications push, d'installer la dernière version d'iPadOS et de changer le nom de l'appareil pour aider le service informatique à gérer ses appareils.

Commandes disponibles pour la MDM

Mettre à jour l'inventaire

Verrouiller l'appareil

Effacer Code

Effacer Restrictions

Révoquer la gestion de l'appareil

Effacer l'appareil

Envoyer une notification push vide

Définir le Fond d'écran

Envoyer Notification

Mettre à jour iOS

Modifier Nom

Mode Perdu et son

Désactiver l'appareil

Redémarrer l'appareil

iPad partagé uniquement

Déconnecter l'utilisateur

Supprimer l'utilisateur

Gérer le verrouillage d’activation avec une solution MDM

Le verrouillage d’activation est conçu pour prévenir le vol des appareils iPhone et iPad. Ces derniers exigent un identifiant Apple et un mot de passe, ce qui signifie que seuls ceux qui disposent de ces informations peuvent activer les appareils. Cette fonctionnalité est excellente pour la prévention du vol, mais peut également causer des problèmes aux administrateurs informatiques s’ils ne gèrent pas les identifiants Apple de leurs élèves. Cela est cependant plus facile à gérer lors du jumelage du verrouillage d’activation avec une MDM. Si un appareil est enrôlé dans une MDM et qu’il est supervisé, un code de contournement du verrouillage d’activation permettra à l’administrateur informatique de déverrouiller l’appareil.

1

L’appareil est déjà enrôlé auprès d’un serveur MDM et supervisé. Un Code de contournement du verrouillage d’activation est généré et stocké dans le serveur MDM.

2

Un appareil verrouillé est rendu au service informatique. Ils récupèrent le code de contournement stocké sur le serveur MDM.

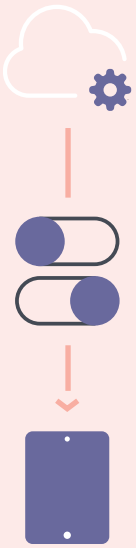
3

Le service informatique redémarre l’appareil dans l’assistant Réglages et le premier écran demande l’identifiant Apple et le mot de passe de l’élève précédent. Pour contourner le verrouillage d’activation, l’équipe informatique saisit le code dans le champ de mot de passe et laisse le champ Identifiant Apple vide. L’appareil est maintenant déverrouillé.

Déploiement des applications

L'iPad est un excellent outil de communication prêt à l'emploi en tant que tel, mais la riche bibliothèque des applications personnelles et éducatives dans l'App Store peut améliorer la productivité de l'élève et l'expérience didactique dans son ensemble. Les applications peuvent transformer un iPad en un véritable studio de production vidéo, un laboratoire scientifique, un planétarium et bien plus encore. Avec une stratégie de gestion des applications et une solution MDM pour gérer vos déploiements, vous pourrez mettre à la disposition des élèves et des enseignants toutes les applications dont ils ont besoin et les configurer de manière sécurisée pour votre établissement scolaire.

Stratégies de gestion des applications



Qu'est-ce qu'une application gérée ?

Introduites sous iOS 5, les applications gérées se distinguent des applications standard par le fait qu'elles sont désignées comme appartenant à une organisation. Plus précisément, les applications gérées sont réparties via une solution MDM et peuvent être configurées et réaffectées par cette dernière.

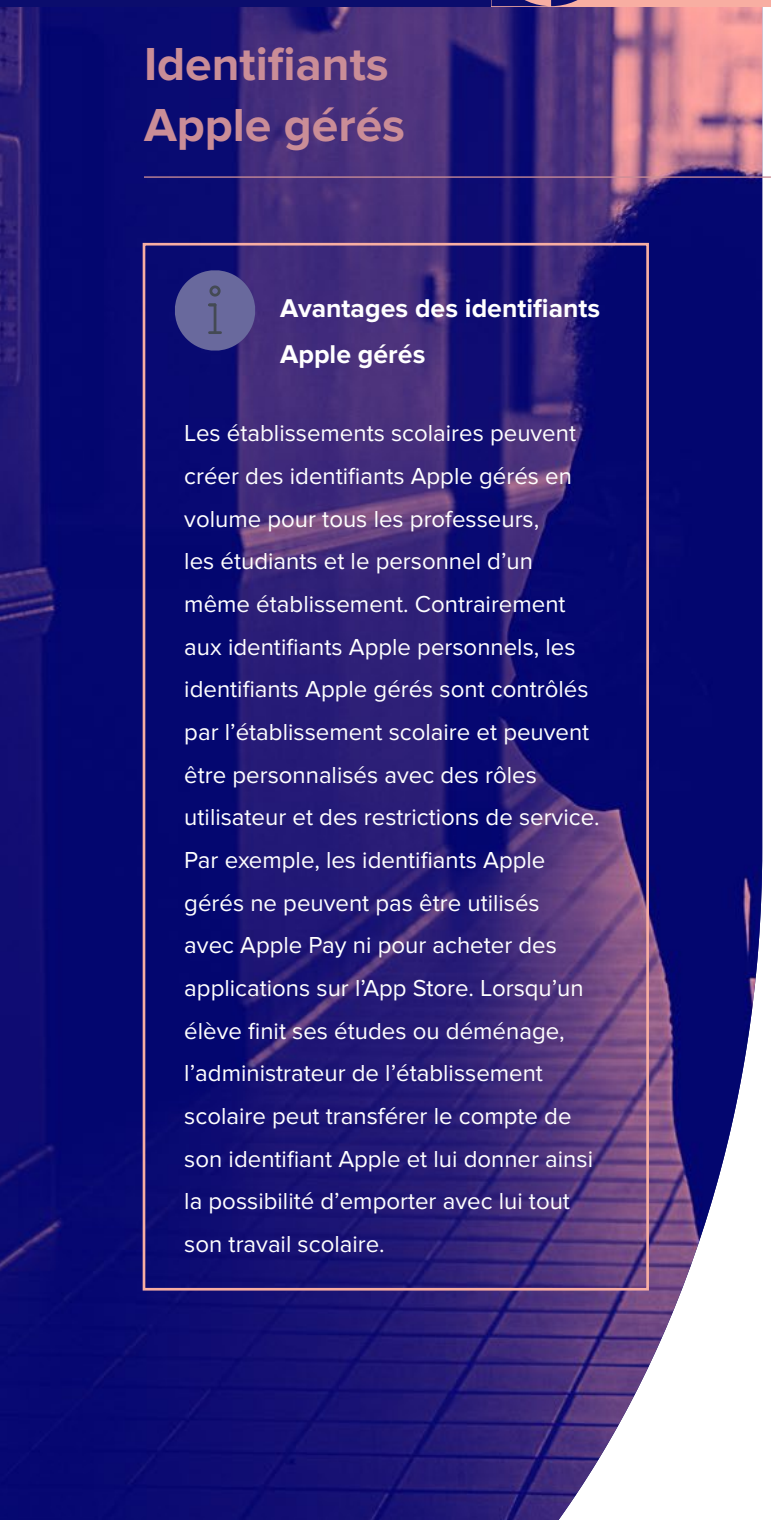
Configuration des applications gérées

Parfois, déployer une application ne suffit pas et vous souhaitez personnaliser à l'avance certains paramètres. C'est exactement le principe de la configuration des applications. Les développeurs d'applications peuvent personnaliser les réglages qui peuvent être préconfigurés par un serveur MDM pour leur application. Par exemple, vous pouvez déployer l'app Box avec une URL du serveur prérenseignée. Après avoir saisi le nom d'utilisateur et le mot de passe, l'application est opérationnelle.

Gestion des autorisations d'ouverture

La Gestion des autorisations d'ouverture pousse le concept d'applications gérées encore plus loin en contrôlant le flux de données qui transitent d'une application à l'autre. Grâce à une solution MDM, les organisations peuvent restreindre les applications présentées sur la feuille de partage iPadOS pour ouvrir les documents. Cela permet une gestion native des données sans avoir recours à un conteneur.

Identifiants Apple gérés



Avantages des identifiants Apple gérés

Les établissements scolaires peuvent créer des identifiants Apple gérés en volume pour tous les professeurs, les étudiants et le personnel d'un même établissement. Contrairement aux identifiants Apple personnels, les identifiants Apple gérés sont contrôlés par l'établissement scolaire et peuvent être personnalisés avec des rôles utilisateur et des restrictions de service. Par exemple, les identifiants Apple gérés ne peuvent pas être utilisés avec Apple Pay ni pour acheter des applications sur l'App Store. Lorsqu'un élève finit ses études ou déménage, l'administrateur de l'établissement scolaire peut transférer le compte de son identifiant Apple et lui donner ainsi la possibilité d'emporter avec lui tout son travail scolaire.

Qu'est-ce qu'un identifiant Apple (Apple ID) ?

Un identifiant Apple est un compte personnel qui permet aux utilisateurs d'accéder aux services Apple, tels que l'App Store, iTunes, iCloud, iMessage et FaceTime et bien d'autres encore. Un identifiant Apple est défini par une adresse électronique et un mot de passe et peut être associé à des coordonnées, des modes de paiement et des données de sécurité.

Qu'en est-il des applications appartenant à l'université ?

Comme l'App Store vous permet désormais de breveter les Apps via la méthode de la distribution gérée, vous n'avez qu'à attribuer des Apps à l'appareil d'un utilisateur ou à l'identifiant Apple sans transférer la propriété à l'utilisateur de manière permanente. Ainsi le service informatique n'a pas besoin de passer des heures à créer des identifiants Apple spécifiques à un appareil.

Pourquoi les identifiants Apple sont-ils importants pour les établissements ?

Un identifiant Apple permet aux élèves de profiter pleinement d'iPadOS et de l'écosystème d'applications. Avec leur identifiant Apple, les élèves peuvent, par exemple, télécharger des applications éducatives, des livres numériques et du contenu iTunes U.

Qu'en est-il des risques de sécurité ?

Grâce aux fonctionnalités de la gestion des appareils mobiles, telles que la gestion d'autorisations d'ouverture et les restrictions dans un profil de configuration, le service informatique peut mieux atténuer les risques de sécurité plutôt qu'interdire totalement les identifiants Apple. Les services d'Apple sont connus pour leur sécurité et l'ajout d'un identifiant Apple personnel à un appareil d'entreprise ne réduit pas la sécurité dans son ensemble. Dans certains cas, vous pouvez même augmenter la sécurité car les identifiants Apple prennent en charge la double authentification.

Sécurité et confidentialité

Les questions de sécurité et de confidentialité sont les préoccupations majeures des établissements scolaires. iPadOS est doté d'un certain nombre de fonctionnalités de sécurité directement intégrées au système d'exploitation afin de protéger les données des élèves et des enseignants. De plus, grâce à l'engagement d'Apple envers la protection de la vie privée des élèves, les parents et les élèves peuvent se rassurer en sachant qu'Apple n'autorise pas la géolocalisation des appareils. En combinant ces fonctionnalités avec une solution MDM, vous pouvez garantir que vos appareils, vos applications et votre réseau sont sécurisés et que les utilisateurs se sentent en sécurité.

Mode Perdu

Avec le mode Perdu, les établissements sont en mesure de localiser et de retrouver des appareils Apple perdus ou volés sans compromettre la vie privée des élèves avec un suivi continu de la localisation. Lorsque le mode Perdu est activé, l'appareil iOS reçoit un message personnalisé sur l'écran de verrouillage, son utilisation est désactivée et sa position géographique est envoyée au service informatique.

Chiffrement

iPadOS dispose d'un chiffrement intégré 256 bits et est automatiquement activé si un code secret est utilisé. Cela signifie que les données stockées sur vos appareils sont sécurisées sans que vous ayez à ajouter de logiciel supplémentaire qui risquerait de surcharger le système. Comme Apple fabrique le matériel et logiciel, le chiffrement est pratiquement imperceptible pour l'utilisateur.

VPN pré-application

Les réseaux privés virtuels (VPN) sont depuis longtemps mis en œuvre dans les établissements d'enseignement supérieur afin de chiffrer le trafic sur Internet. Les ordinateurs de bureau traditionnels sont en mesure de fonctionner en acheminant tout le trafic sur le VPN ; ce modèle peut cependant s'effondrer lorsqu'il s'agit d'un appareil mobile. Apple résout ce problème en permettant aux universités et aux développeurs d'applications de définir, au niveau de l'application, les données transmises via le VPN. Cela permet d'économiser la bande passante et d'améliorer la vitesse du réseau.

Touch ID et Face ID

Un capteur d'empreintes digitales et la reconnaissance faciale ont été rajoutés aux nouveaux appareils iPadOS, ajoutant la sécurité biométrique au système d'exploitation. Touch ID et Face ID peuvent être utilisés pour déverrouiller un appareil et s'identifier dans certaines Apps. Les données de l'empreinte digitale et du visage sont stockées localement sur l'appareil et ne sont jamais partagées avec Apple.

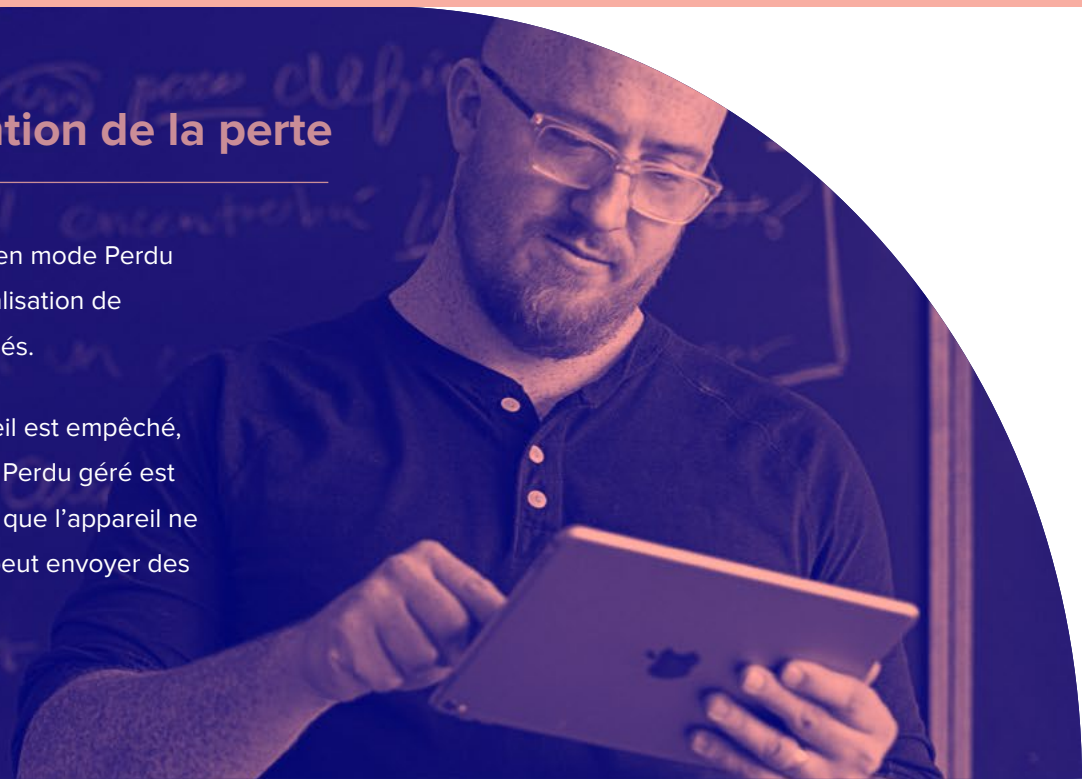
Mise en place du chiffrement sur les appareils gérés

Pour préserver la confidentialité des données, il est fortement recommandé de mettre en place un chiffrement sur tous les appareils gérés. L'application d'un profil de configuration aux appareils Apple gérés nécessitant un code d'accès active le chiffrement des données.

Dans les réglages de votre configuration, vous pouvez spécifier les éléments suivants :

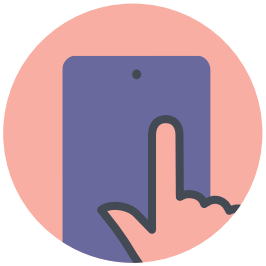
- Longueur du code d'accès
- Codes d'accès simples ou complexes
- Fréquence de changement du code d'accès
- Autoriser ou refuser les codes d'accès déjà utilisés
- Durée avant le verrouillage automatique
- Nombre maximal de tentatives infructueuses de saisie du code d'accès avant effacement de l'appareil

Utiliser une solution MDM pour la prévention de la perte



La possibilité d'utiliser une solution MDM pour placer un appareil supervisé en mode Perdu géré est une fonctionnalité de sécurité clé. Ce paramètre peut fournir la localisation de l'appareil, ce qui est essentiel pour la recherche des appareils perdus ou volés.

De plus, en exigeant un code d'accès sur l'appareil, l'accès à l'écran d'accueil est empêché, la confidentialité des données reste intacte et l'appareil est chiffré. Le mode Perdu géré est contrôlé par l'administrateur et doit être désactivé par l'administrateur avant que l'appareil ne redevienne opérationnel. Comme Localiser mon iPhone, un administrateur peut envoyer des messages sur l'appareil pendant qu'il est en mode Perdu géré.



Assurez-vous que les appareils sont supervisés et désactivez la suppression du profil MDM avec votre solution MDM.

Définissez un message d'écran et appliquez des étiquettes physiques qui montrent clairement que l'appareil appartient à l'établissement. Cela aidera à dissuader le vol.

Utilisez le mode Perdu si un appareil disparaît. Cela désactive l'appareil, affiche un message personnalisé et signale les coordonnées GPS.

Faire progresser l'enseignement supérieur grâce à l'Apple TV

Au fur et à mesure que les demandes mobiles augmentent dans les établissements d'enseignement supérieur, il est primordial que toutes vos technologies puissent répondre à la demande. Avec la dernière version de tvOS, le mode Apple TV géré permet désormais aux services informatiques de transformer les appareils Apple TV grand public en outils de travail gérés.

Salle de conférence sans fil

Pour créer une salle de conférence moderne, configurez un adaptateur et un affichage sans fil. Ensuite, activez le mode affichage des conférences et créez un message de bienvenue personnalisé qui comprend des instructions supplémentaires ou des informations spécifiques à chaque salle.

Affichage numérique

Avec l'Apple TV, l'affichage numérique devient plus abordable, accessible, évolutif et gérable. Grâce aux logiciels MDM, les établissements scolaires sont en mesure de contrôler facilement ce qui est montré à un seul endroit ou sur plusieurs sites.

Collaboration spontanée

La gestion des appareils Apple TV et AirPlay simplifie le déploiement immédiat des écrans d'un appareil sur un écran partagé. Cela crée le cadre idéal pour la collaboration dans les salles de classe et les bureaux.

MDM pour l'enseignement supérieur

Jamf Pro est le principal outil de gestion des appareils mobiles pour Apple dans l'enseignement supérieur. Conçu pour automatiser les tâches courantes autour du déploiement Apple, de l'inventaire et de la sécurité, Jamf facilite la gestion des appareils pour vous permettre de mieux transformer l'expérience d'apprentissage tout en maintenant un environnement sécurisé.

Prêt à vous lancer ?
Mettez les capacités de gestion d'iPad de Jamf à l'épreuve avec un essai gratuit dès aujourd'hui.

Demander un essai