21 octobre 2025 - PARIS

IDENTITY DAYS

21 octobre 2025 - PARIS

Gérer et Sécuriser votre parc macOS

La gestion de macOS en entreprise a longtemps été compliquée et mise de coté mais ces dernières années la demande de mac est croissante et Microsoft a travaillé longuement avec Apple pour proposer une gestion fine qui vient se compléter avec des solutions Open Source de la communauté.

Nicolas CHEYMOL

Adrien DECOMBE

Nicolas CHEYMOL

Adrien DECOMBE

AGENDA DE LA CONFÉRENCE

- macOS en Entreprise ?
- Quelles sont les problématiques de macOS en entreprise
- Une experience Zero-touch OOBE
- Gestion de l'identité et des droits
- Chiffrement des postes
- Catalogue applicatif
- Gestion des mises à jours de l’OS
- ~~Comment Microsoft apporte un support 0-day avec Intune~~

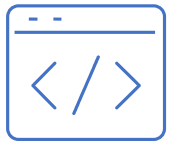
macOS en entreprise

Qui a des mac ?

Sont-ils gérés ?

Pourquoi avoir des mac?

Attractivité et rétention
Profiles : maketing, pub, digital, luxe



Nécessité technique
Profiles :
Développement de sites et applications pour iOS, iPadOS ou macOS

Outils répandus sur le marché
Profiles : montage vidéos

Pourquoi gérer vos macs ?

Sécurité

Expérience utilisateur améliorée

Urbanisation / RSE

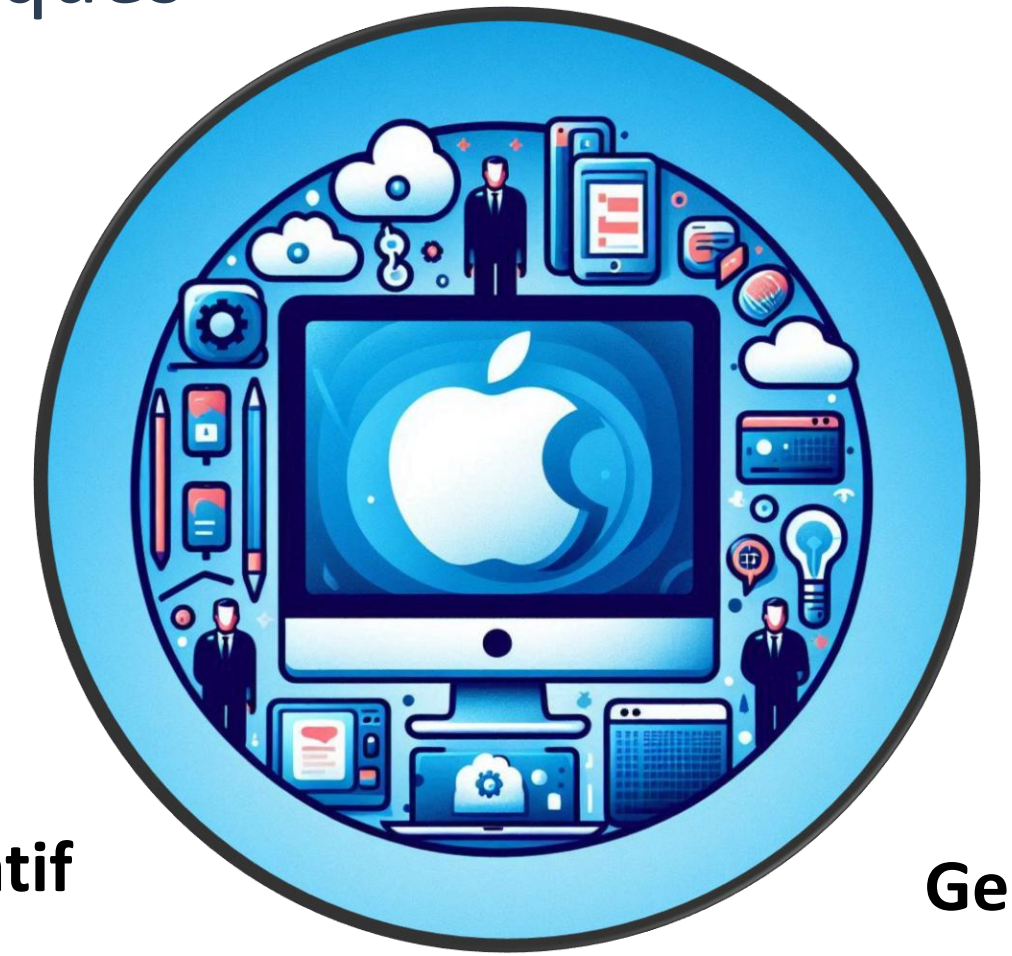
Pouvoir élargir l’offre mac

Les problématiques

Les Problématiques

SSO

Préparation



Protection des données

Support

Packaging Applicatif

Gestion des droits

Les Besoins par persona

- **Marketing**
  - FinalCut Pro (ou autre application métier)
  - Applications bureautiques
- **Développement Application Apple**
  - Applications bureautiques
  - Applications de développement
  - Être administrateur pour Installer des librairies, des nouveaux outils
- **Développement Web**
  - Applications bureautiques
  - Applications de développement
  - Vérifier le bon fonctionnement sur les navigateurs

Comment y repondre ?

Nico

Comment y repondre ?

- Via une gestion unifiée (coherence, experience administrateur)
- Rendre l’utilisateur automnome (ADE, PSSO, Catalogue d’applications)
- Acces aux outils et au SI comme tous les utilisateurs
- Une solution de gestion offrant un support 0-day pour les Nouvelles versions d’OS

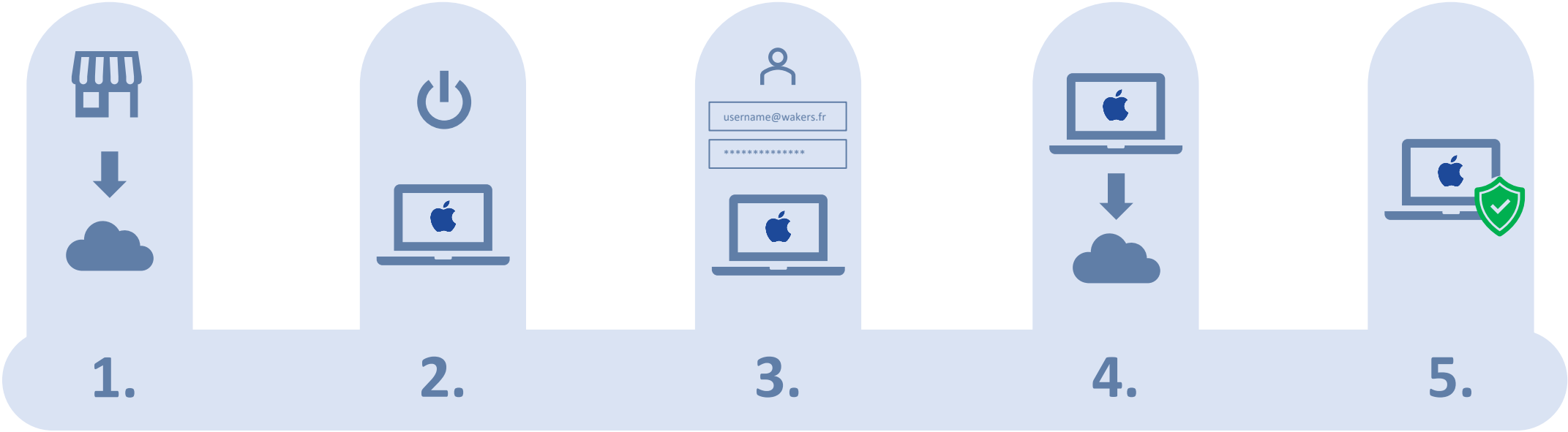









Inscription automatique de l'appareil



Le revendeur enregistre* l'appareil dans votre espace ABM

L'utilisateur démarre l'appareil pour la première fois

L'utilisateur doit s'authentifier avec un compte Microsoft 365

L'appareil est automatiquement inscrit à la solution MDM

L'utilisateur peut utiliser pleinement l'appareil après l'installation des configurations et des logiciels requis

*L'équipe informatique peut inscrire manuellement les appareils.

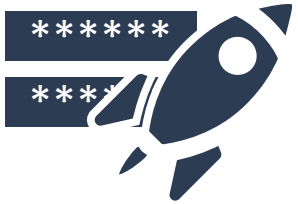
Gestion de l’identité et des droits

PlateformSSO

UXP Similaire à un Windows avec WHfB.

Permet de prendre en charge Touch ID.

Enfin du PasswordLess sur macOS managé ! 😁🙏



Minimise le nombre de fois ou l'utilisateur est invité à s'authentifier.

Réduit le nombre de mot de passe qu'un utilisateur doit retenir

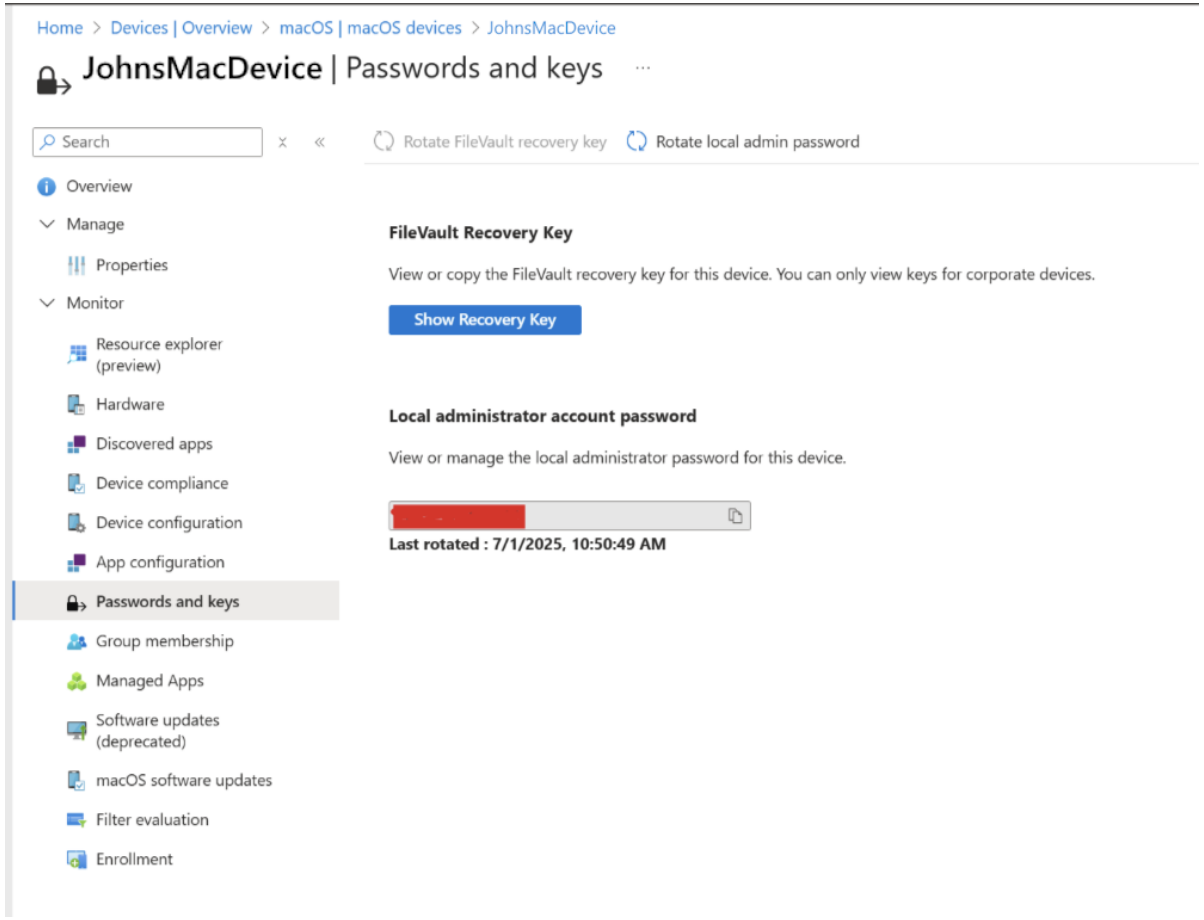
PlateformSSO - Secure Enclave

- Similaire à Windows Hello for Business
- Considéré comme Password Less
- Le compte local reste inchangé

DEMO

LAPS – Local Admin Password Solution

- **Création automatique de comptes locaux**
  - Configuré dans le profile d'enrôllement vu précédemment
  - Lors de l'inscription via ADE
  - Intune peut créer un compte administrateur local avec un mot de passe fort, aléatoire et chiffré



SAP Privilège

Élévation temporaire
Authentification biométrique
Réduction des droits après un délais ou au loggin
Envoie des logs à distance (syslog ou webhook)

Protection des données

FileVault

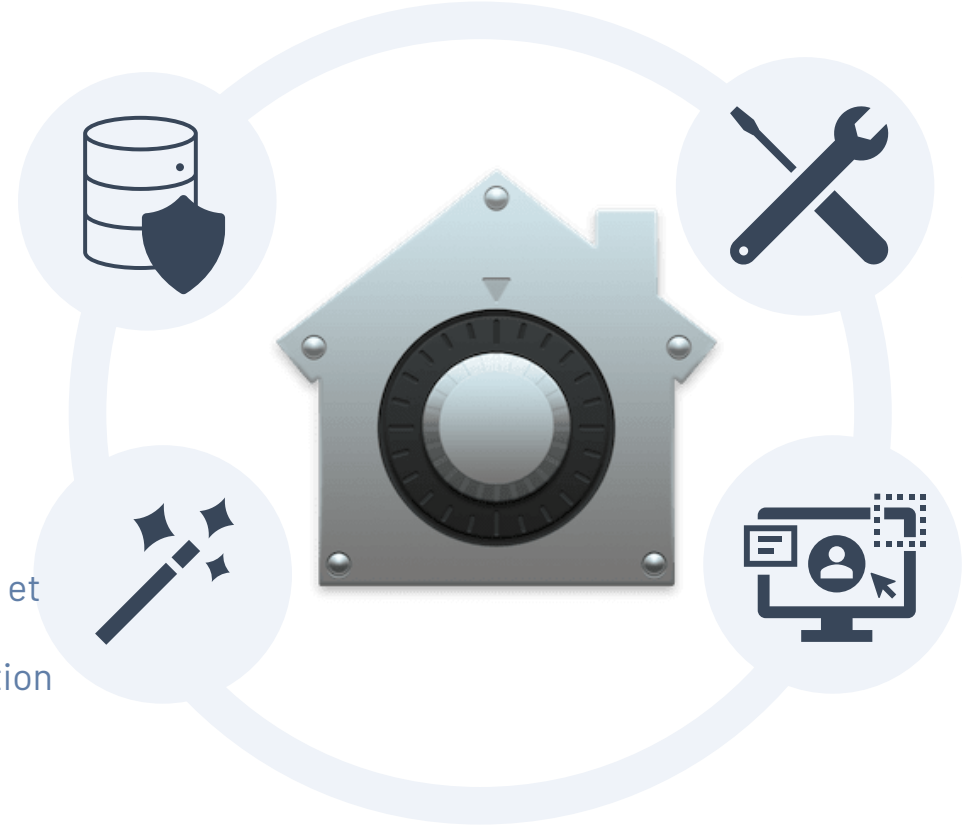
Chiffrement complet du disque pour macOS

Protection robuste des données

Chiffre l'intégralité du disque pour sécuriser les données au repos.
Empêche l'accès non autorisé en cas de vol ou de perte.

Intégration transparente avec Intune

Automatise les politiques de chiffrement et le déploiement.
Simplifie la gestion des clés de récupération et la surveillance de la conformité.



Gestion et récupération centralisées

Gestion à volet unique via Intune pour tous les appareils macOS.
Assure une récupération rapide des appareils cryptés en cas d'urgence

Convivial et transparent

Impact minimal sur les performances.
Totalement transparent pour les utilisateurs finaux, garantissant des taux d'adoption élevés.

Catalogue d’applications et gestion des mises à jour

PatchMyMac

Patch My PC prend désormais en charge la gestion des appareils macOS via Microsoft Intune !

Cela permet de déployer et de mettre à jour automatiquement des applications tierces sur Mac, sans avoir besoin d'une solution de gestion spécifique à macOS.

- **Intégration native à Intune**
  - Console simple pour créer les applications en quelques clics. (86 application au catalogue)
- **Déploiement et mises à jour automatisés**
  - Installation silencieuse et mise à jour automatique des applications macOS.
- **Compatibilité universelle**
  - Fonctionne avec les Mac Intel et Apple Silicon (formats DMG et PKG)
- **Types de déploiement flexibles**
  - Disponible, requis ou désinstallation.
- **Logique de détection cohérente** :
  - Évite les installations inutiles si l'application est déjà présente et à jour.
- **Gestion unifiée**
  - Administration des appareils Windows et macOS depuis une seule plateforme.

Intune Brew

IntuneBrew est un projet proposant un portail web, un script PowerShell et un runbook Azure pour automatiser la gestion des applications macOS dans Intune.

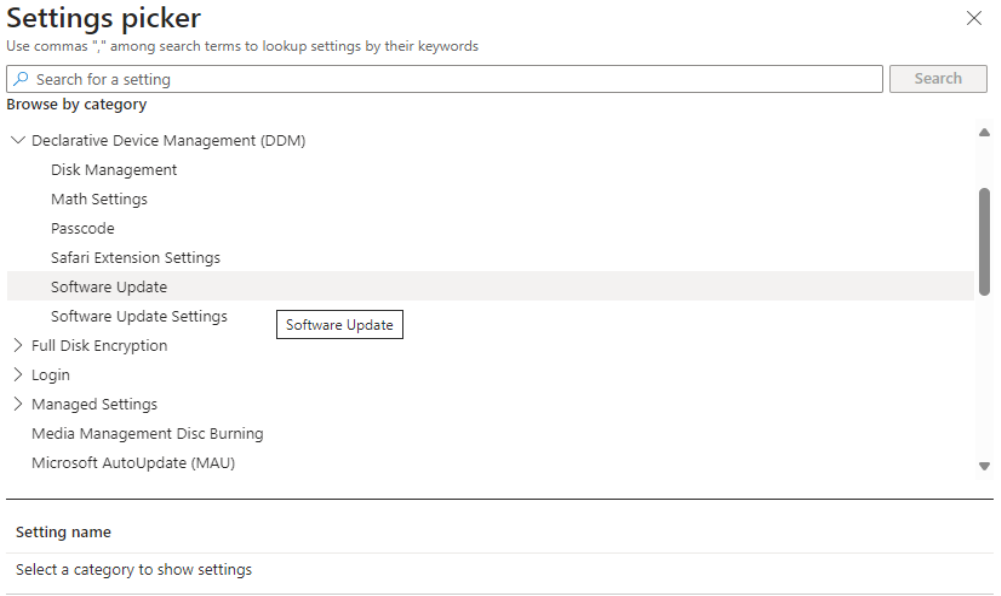
- **Projet Open Source actif et très récent**
  - Initial Commit 22/10/2024
  - Déjà plus de 500 applications au catalogue
- **Téléchargement et mise à jour d'applications macOS dans Intune.**
  - Installation silencieuse et mise à jour automatique des applications macOS.
- **Automatisation avec Azure Runbook**
  - Vérifie automatiquement les mises à jour et évite les doublons
- **Compatibilité universelle**
  - Fonctionne avec les Mac Intel et Apple Silicon (formats DMG et PKG)

Intune Brew vs PatchMyPC

Feature / Aspect	IntuneBrew	Patch My PC
Purpose	Outil open source pour automatiser le packaging d'applications macOS sur Intune	Plateforme SaaS commerciale pour l'application automatisée de correctifs et le déploiement d'applications tierces dans Intune.
Platform Focus	macOS uniquement	Windows et macOS
Integration	Script PowerShell, runbook Azure et Portail web	Intégration complète avec Microsoft Intune Cloud Portal
App Sources	Utilise des fichiers Homebrew et JSON pour les métadonnées de l'application	Gère son propre catalogue d'applications tierces
File Support	.pkg et .dmg	.pkg et .dmg
Price	Free + Runbook price	**3.5$**/Appareil/ans

Demo

DDM



Avec la gestion déclarative des appareils (**DDM**) dans Intune pour macOS, les organisations bénéficient d'une approche plus efficace et sécurisée par rapport aux méthodes de **gestion des appareils héritées**, offrant une application de la conformité en temps réel, des mises à jour automatisées et une sécurité renforcée pour se protéger contre les menaces en constante évolution.

📣 Vous devriez implémenter ces nouvelles configurations avec DDM et migrer le profil existant vers la méthode DDM.

4 avantages clés de la gestion déclarative des appareils

Automatisation en temps réel
Les configurations et la conformité sont appliquées instantanément sans dépendre de synchronisations manuelles ou programmées

Sécurité renforcée
Les politiques sont appliquées de manière proactive, ce qui minimise les risques de retards ou de vulnérabilités non corrigées

Réduction de la charge du serveur
Les appareils prennent en charge les tâches de gestion, ce qui réduit les demandes de serveur et améliore l'efficacité globale

Prêt pour l'avenir avec les normes Apple
Conçu pour prendre en charge nativement les dernières fonctionnalités de macOS, garantissant une compatibilité et une évolutivité à long terme

Q&A

@IdentityDays
#identitydays2025

Liens utiles

- https://github.com/microsoft/shell-intune-samples
- https://aka.ms/MacAdmins
- https://ncheymol.github.io
- https://PatchMyMac.com
- https://www.intunebrew.com/