

FICHE SOLUTION · GESTION UNIFIÉE DES TERMINAUX ET SÉCURITÉ (UEMS)

**ManageEngine**
Mobile Device Manager Plus

Smartphones, tablettes et ordinateurs portables : un seul poste de pilotage.

Inscrivez, configurez, sécurisez puis retirez du parc chaque appareil professionnel, qu'il appartienne à l'entreprise ou au collaborateur. Applications, messagerie, documents et données restent sous le contrôle du service informatique, sans dégrader l'expérience de l'utilisateur.

Android

iOS

iPadOS

macOS

tvOS

Windows

Chrome OS

TROIS ÉDITIONS · ABONNEMENT ANNUEL PAR APPAREIL

Gratuite · Standard · Professionnel

Tarif éditeur à partir de 10 € par appareil et par an en déploiement local — détail complet en page 5.

1 000 000+APPAREILS GÉRÉS
DANS LE MONDE**10 000**PROFESSIONNELS
DE L'INFORMATIQUE**190**PAYS
D'UTILISATION**18**LANGUES
D'INTERFACE

Un parc hétérogène. Une console unique.

Ce qu'est Mobile Device Manager Plus

Mobile Device Manager Plus est la solution de gestion des appareils mobiles de ManageEngine. Elle prend en charge le cycle de vie complet d'un terminal professionnel, de son inscription à sa sortie du parc, et couvre aussi bien les smartphones et les tablettes que les ordinateurs portables, les postes de travail, les téléviseurs et les appareils durcis.

L'administrateur travaille depuis une console unique : il y déclare ses appareils, y pousse les profils Wi-Fi, VPN et messagerie, y publie le catalogue d'applications autorisées, y applique ses règles de sécurité et y déclenche les actions à distance. Les données professionnelles sont isolées dans un conteneur chiffré : un appareil personnel peut donc être admis sans que l'administration ne touche aux contenus privés du collaborateur.

Ce que la solution rend possible

- ◆ Mettre en service des appareils neufs sans les déballer un par un, par inscription automatisée Apple, Android, Windows et Chrome OS.
- ◆ Réserver l'accès à la messagerie d'entreprise aux seuls appareils déclarés et conformes.
- ◆ Verrouiller un terminal sur une application métier unique, en magasin, en atelier ou sur le terrain.
- ◆ Effacer à distance les seules données professionnelles d'un appareil perdu, volé ou rendu par un collaborateur sortant.
- ◆ Documenter le chiffrement, les codes d'accès et les pistes d'audit attendus par le RGPD, la loi HIPAA ou les normes ISO/IEC 27001 et SOC 2.

SYSTÈMES GÉRÉS

Android 4.0+

iOS 4.0+

iPadOS 13.0+

macOS 10.7+

tvOS 7.0+

Windows 8+

Chrome OS 57.0+

MODES DE DÉPLOIEMENT

Local

SERVEUR

Cloud

SAAS

MSP

INFOGÉRANCE

DIMENSIONNEMENT SERVEUR

Jusqu'à 250 appareils Intel Core i3 2,0 GHz · 4 Go de RAM · 5 Go de disque

De 5 001 à 10 000 Intel Xeon E5 8 cœurs 2,6 GHz · 16 Go de RAM · 60 Go de disque

Au-delà de 1 000 appareils, l'éditeur recommande une installation sur Windows Server.

Le périmètre couvert par la plateforme – 8 domaines de gestion

MISE EN SERVICE

- ◆ Inscription et intégration des appareils
- ◆ Profils et configurations

USAGE QUOTIDIEN

- ◆ Applications et licences
- ◆ Messagerie d'entreprise

DONNÉES

- ◆ Diffusion et gestion du contenu
- ◆ Appareils personnels et conteneurisation

MAÎTRISE

- ◆ Sécurité et conformité
- ◆ Actifs, dépannage et rapports

Mise en service, configuration et applications

Inscription et intégration des appareils

APPLE · ANDROID · WINDOWS · CHROME OS

- ◆ **Automatisez l'inscription à la sortie du carton** — Apple Business Manager et Apple Configurator, Zero Touch, Samsung Knox Mobile Enrollment, jeton EMM et NFC pour Android, Windows ICD et Azure AutoPilot, inscription Chromebook.
- ◆ **Invitez les utilisateurs à s'inscrire** — lecture d'un QR code, import CSV en masse, SMS ou courrier électronique, selon la population visée.
- ◆ **Laissez l'utilisateur faire le premier pas** — portail d'auto-inscription pour les appareils personnels.
- ◆ **Contrôlez l'identité à l'inscription** — code à usage unique ou identifiants de l'annuaire d'entreprise.
- ◆ **Rattachez plusieurs appareils à un même utilisateur** — téléphone, tablette et portable sous un seul compte.

Profils et configurations

WI-FI · VPN · CERTIFICATS · RESTRICTIONS

- ◆ **Poussez les réseaux autorisés** — profils Wi-Fi et VPN, jusqu'au VPN par application, pour que l'accès aux ressources reste maîtrisé.
- ◆ **Imposez un code d'accès robuste** — longueur, complexité et renouvellement alignés sur la politique de sécurité de l'entreprise.
- ◆ **Désactivez les fonctions non souhaitées** — appareil photo, Bluetooth, appels, SMS, stockage externe, réinitialisation d'usine, sauvegarde iCloud.
- ◆ **Distribuez les certificats** — authentification par certificat via SCEP, avec intégration d'un serveur d'autorité de certification.
- ◆ **Filtrez la navigation** — blocage des sites malveillants ou non approuvés et acheminement du trafic par le proxy d'entreprise.
- ◆ **Synchronisez contacts et agendas** — annuaire et événements d'entreprise poussés sur les appareils, avec authentification unique.

Applications et licences

CATALOGUE D'ENTREPRISE · MODE KIOSQUE

- ◆ **Publiez un catalogue d'applications approuvées** — applications internes et applications des magasins, achetées en volume via Apple Business Manager, Google Play, Microsoft Store et Chrome Web Store.
- ◆ **Installez et désinstallez sans intervention** — déploiement silencieux, sans manipulation par l'utilisateur.
- ◆ **Testez avant de généraliser** — plusieurs versions d'une application interne peuvent être validées avant le passage en production.
- ◆ **Préconfigurez les applications** — paramètres et autorisations définis dès l'installation : l'application est utilisable immédiatement.
- ◆ **Verrouillez l'appareil en mode kiosque** — une application ou une série d'applications, avec disposition d'écran imposée et durée paramétrable.
- ◆ **Bloquez ce qui ne doit pas tourner** — liste rouge d'applications et interdiction de désinstaller celles de l'entreprise.

Messagerie d'entreprise

EXCHANGE · MICROSOFT 365

- ◆ **Préconfigurez le compte professionnel** — paramètres Exchange ActiveSync poussés à distance, sans saisie par l'utilisateur.
- ◆ **Réservez l'accès aux appareils déclarés** — accès conditionnel Exchange sur site et Microsoft 365 : les terminaux non gérés restent hors du flux.
- ◆ **Empêchez les transferts vers les comptes personnels** — le courrier d'entreprise ne sort pas du périmètre géré.
- ◆ **Cantonnez les pièces jointes** — consultation et enregistrement dans les seules applications autorisées, via l'application d'administration ManageEngine.
- ◆ **Verrouillez la configuration** — l'utilisateur ne peut modifier ni le compte ni les paramètres appliqués.

Plateformes prises en charge

APPLE

- ◆ iOS 4.0 et versions ultérieures · iPadOS 13.0 et versions ultérieures : iPhone, iPad, iPod Touch
- ◆ macOS 10.7 et versions ultérieures · tvOS 7.0 et versions ultérieures

GOOGLE

- ◆ Android 4.0 et versions ultérieures : smartphones et tablettes
- ◆ Chrome OS 57.0 et versions ultérieures : Chromebooks

MICROSOFT

- ◆ Windows 8 et versions ultérieures : smartphones et tablettes
- ◆ Ordinateurs portables Windows 10 · Surface Hub

Contenu, sécurité et appareils personnels

Diffusion et gestion du contenu

DOCUMENTS · MÉDIAS

- ◆ **Constituez un référentiel documentaire** — documents et médias critiques centralisés, puis diffusés sur les appareils.
- ◆ **Diffusez plus de dix formats de fichiers** — sans passer par un service de partage tiers.
- ◆ **Cloisonnez la consultation** — les documents s'ouvrent dans l'application d'administration ManageEngine, et nulle part ailleurs.
- ◆ **Mettez à jour automatiquement** — la nouvelle version remplace l'ancienne sur les appareils déjà servis.
- ◆ **Interdisez la sauvegarde dans un cloud tiers** — et le partage vers des appareils non gérés.
- ◆ **Retirez un document à distance** — suppression centralisée sur l'ensemble du parc.

Sécurité et conformité

CHIFFREMENT · VERROUILLAGE · EFFACEMENT

- ◆ **Chiffrez les données** — chiffrement imposé sur l'appareil et sur le stockage externe, FileVault et mot de passe de microprogramme sur Mac.
- ◆ **Réagissez à la perte d'un appareil** — verrouillage, alarme sonore, mode perte, réinitialisation du code d'accès, effacement total ou effacement des seules données d'entreprise.
- ◆ **Écartez les appareils compromis** — détection des terminaux débridés ou rootés et retrait du réseau de l'entreprise.
- ◆ **Délimitez une zone autorisée** — le géorépérage déclenche des restrictions dès que l'appareil sort du périmètre défini.
- ◆ **Maîtrisez les mises à jour du système** — déploiement silencieux, immédiat, différé ou par fenêtre, avec blocage des montées de version non souhaitées.
- ◆ **Reprenez la main sur un appareil rendu** — la protection étendue contre la réinitialisation d'usine évite qu'un terminal restitué ne devienne inexploitable.

Appareils personnels et conteneurisation

BYOD · APPAREILS D'ENTREPRISE

- ◆ **Isolez le professionnel du personnel** — les données d'entreprise sont stockées dans un conteneur chiffré, distinct du profil privé.
- ◆ **Ne touchez pas aux contenus privés** — photos, messages et applications personnelles du collaborateur restent hors de portée de l'administration.
- ◆ **Ouvrez l'accès au cas par cas** — messagerie, Wi-Fi et comptes d'entreprise attribués selon le profil du collaborateur.
- ◆ **Bloquez les échanges entre les deux mondes** — pas de transfert entre applications professionnelles et personnelles, ni vers un appareil non géré ou un cloud tiers.
- ◆ **Appliquez vos règles aux applications Microsoft 365** — les stratégies MAM s'appliquent même sur un appareil non enrôlé.

Actifs, dépannage et rapports

INVENTAIRE · CONTRÔLE À DISTANCE

- ◆ **Tenez l'inventaire à jour** — matériel, applications installées, certificats et mémoire, avec analyses planifiées.
- ◆ **Localisez le parc** — position à la demande, historique des trajets et vue d'ensemble sur une carte unique.
- ◆ **Dépannez sans déplacement** — prise de contrôle à distance depuis la console, sans application complémentaire à installer.
- ◆ **Surveillez le niveau de batterie** — alerte dès qu'un appareil passe sous le seuil défini.
- ◆ **Prévenez les utilisateurs** — annonces poussées sur les appareils pour une urgence ou une maintenance planifiée.
- ◆ **Exploitez plus de dix rapports prêts à l'emploi** — applications par appareil, modèles, types de code d'accès, date d'inscription, appareils inactifs ; rapports planifiés et requêtes personnalisées.

Intégrations natives

GESTION DES SERVICES INFORMATIQUES

- ◆ ServiceDesk Plus · ServiceNow
- ◆ Jira Service Desk · Zendesk

ANALYSE ET AUTOMATISATION MÉTIER

- ◆ Analytics Plus, pour la restitution décisionnelle
- ◆ Zoho CRM et Zoho Creator, pour l'automatisation des processus

DÉVELOPPEMENTS SPÉCIFIQUES

- ◆ API publiques ouvertes aux intégrations tierces

Trois éditions. Deux modes d'hébergement.

ÉDITION GRATUITE

25 appareils

- ◆ Gestion complète de 25 appareils mobiles au maximum
- ◆ Destinée aux petits parcs et à la validation d'un projet avant généralisation

ÉDITION STANDARD

10 € / appareil / an

- ◆ Gestion des appareils mobiles
- ◆ Distribution d'applications
- ◆ Gestion des configurations
- ◆ Gestion des restrictions
- ◆ Mode kiosque
- ◆ Géolocalisation
- ◆ Commandes à distance

ÉDITION PROFESSIONNEL

18 € / appareil / an

- ◆ Toute l'édition Standard
- ◆ Gestion de contenu
- ◆ Configurations personnalisées
- ◆ Stratégies de mise à jour des applications et du système d'exploitation
- ◆ Stratégies d'accès conditionnel
- ◆ Contrôle à distance
- ◆ Géorépérage

ABONNEMENT ANNUEL PAR APPAREIL	DÉPLOIEMENT LOCAL	DÉPLOIEMENT CLOUD
Édition Standard gestion des appareils de base	10 €	13 €
Édition Professionnel gestion complète des appareils mobiles	18 €	24 €

Serveur de basculement
déploiement local uniquement

Sur devis

Pack multilingue

Sur devis

Serveur de passerelle sécurisée
module facultatif, local uniquement

Sur devis

Tarifs publics éditeur, abonnement annuel par appareil. Prix indicatifs et non contractuels : le montant applicable dépend de l'édition, du mode d'hébergement, du volume d'appareils et des extensions retenues. Devis personnalisé LAZAR SOFT sur demande.

Contactez-nous.

Une question ou un chiffrage précis : un #RocketExpert vous répond sous 24 h ouvrées.

TÉLÉPHONE

+33 (0)1 76 21 60 43

E-MAIL

sales@lazarsoft.com