ManageEngine
Mobile Device Manager Plus

# EN TOUTE TRANSPARENCE ET SÉCURITÉ

## CONFIGURER DES PERIPHERIQUES EN MODE KIOSQUE AVEC MOBILE DEVICE MANAGER PLUS

# Introduction

Les périphériques mobiles pour le travail sont répandus dans les entreprises de toutes tailles. Les entreprises des secteurs du commerce de détail, de la santé, de l'éducation et d'autres secteurs autorisent l'utilisation de périphériques mobiles, tels que les smartphones et les tablettes, parce qu'ils permettent la mobilité de la main-d'œuvre, contribuent à accroître la productivité et simplifient les tâches répétitives.

Cependant, les difficultés incluent le traitement de données sensibles, comme les informations d'identification personnelle, qui nécessitent le respect de règles de conformité strictes. Heureusement, les outils modernes de gestion des périphériques mobiles (MDM) et de gestion de la mobilité d'entreprise (EMM) aident les administrateurs informatiques à garantir une utilisation sécurisée des périphériques mobiles.

Le mode kiosque, ou verrouillage des périphériques, est une approche efficace que les solutions MDM ou EMM proposent pour sécuriser l'accès à ces périphériques de première ligne. La sécurité et les fonctions d'un kiosque dépendent entièrement de la façon dont il est configuré. Les scénarios courants en mode kiosque comprennent les applications de remontée d'informations destinées aux clients, les portails Web destinés aux employés et les périphériques partagés dans les écoles.

Ce guide étape par étape explique comment verrouiller en toute sécurité les périphériques mobiles dans votre entreprise, quel que soit l'endroit où ils doivent être placés.

# Un mode kiosque spécialisé comparé à une solution native au périphérique

Les options natives des périphériques, à savoir l'épinglage de l'écran (Android) et l'accès guidé (iOS/iPadOS) permettent de verrouiller les périphériques à une seule application, mais c'est tout ce qu'elles peuvent faire et cette méthode ne fournit que des fonctionnalités et une sécurité rudimentaires. Les administrateurs informatiques ne pourront pas verrouiller les périphériques à plus d'une application, déterminer l'apparence des écrans des périphériques ou personnaliser la barre de notification et les boutons physiques. Ils ne pourront même pas appliquer le verrouillage à distance, ce qui est pourtant essentiel pour gagner du temps et économiser des ressources.

Bien que l'utilisation des options natives des périphériques soit gratuite, l'étiquette de coût zéro qui leur est associée est superficielle, car elles ont souvent un impact négatif sur la productivité des employés, entraînent des dépenses supplémentaires dues au vol et aux violations de données, et augmentent les heures de travail des services informatiques consacrées à la gestion de ces périphériques.

La configuration des périphériques sans un outil de gestion approprié est une tâche fastidieuse, où les applications requises doivent être installées manuellement sur chaque périphérique, et la configuration de base des mots de passe, du Wi-Fi, du VPN, etc. doit également être effectuée séparément. Ce n'est peut-être pas la meilleure façon de verrouiller les périphériques dans les entreprises qui en possèdent un grand nombre.

# Un mode kiosque spécialisé pour une meilleure gestion et sécurité

Une fonctionnalité kiosque avancée doit pouvoir aider à la gestion du cycle de vie des périphériques. La gestion des kiosques ne consiste pas seulement à verrouiller un périphérique, mais aussi à s'assurer que les employés disposent d'une flexibilité suffisante pour accomplir leurs tâches sans problème. Pour gérer efficacement les périphériques en kiosque, il est essentiel que les aspects suivants soient couverts :

## 01

### Gestion a distance

La possibilité de verrouiller des terminaux de différents types et systèmes d'exploitation en mode kiosque à partir d'une console unifiée, et de s'assurer qu'ils restent verrouillés.

## 02

### Un déploiement flexible

Choisir quelles applications, portails web, ressources d'entreprise, paramètres et fonctions doivent être accessibles.

## 03

### Personnalisation de l'écran d'accueil

La possibilité de définir la disposition et l'ordre des icônes, de les organiser en dossiers, de définir l'orientation et d'appliquer le fond d'écran de votre choix.

## 04

### Gestion des périphériques volés et perdus

Utiliser le mode perdu pour verrouiller, localiser et effacer les périphériques en cas de perte ou de vol.

## 05

### Sécurité des données

Définir des règles proactives et réactives pour garantir la protection des informations sensibles.

06

## Profils des périphériques

Ce point concerne les aspects de la gestion des périphériques autres que les kiosques et leurs fonctions annexes.

07

## Gestion des applications

Déploiement, configuration, mise à jour et suppression d'applications sans intervention de l'utilisateur.

08

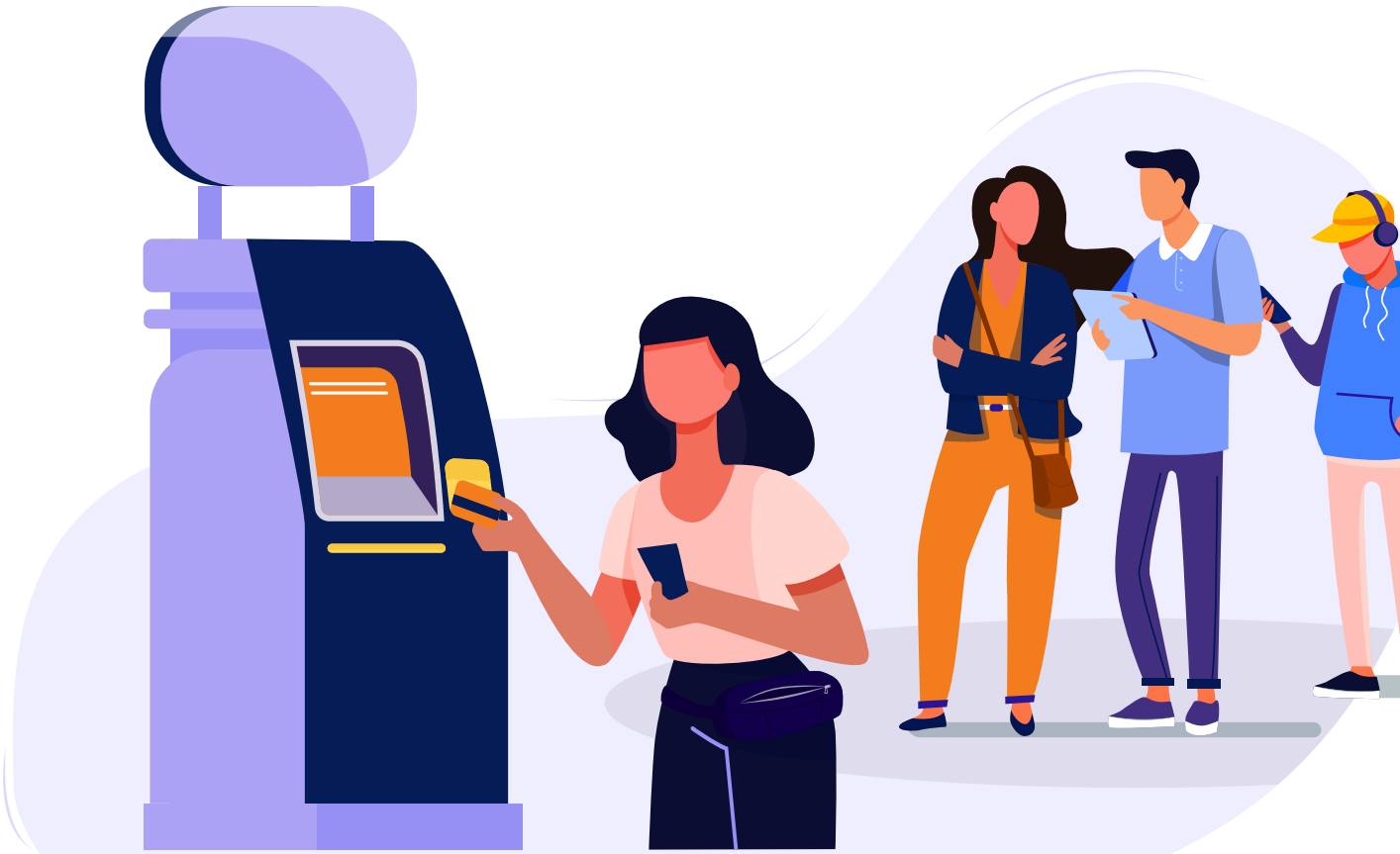
## Informations sur le périphérique et sa batterie

Réception d'alertes sur le niveau de la batterie, la localisation du périphérique, les mises à jour des applications et du système d'exploitation, ainsi que l'inventaire exhaustif des logiciels et du matériel du périphérique..

09

## Dépannage à distance

La possibilité de contrôler ou de visualiser à distance les écrans des périphériques et éventuellement sans intervention de l'utilisateur.



# 3 points à vérifier avant de déployer des périphériques en kiosque

Il y a trois éléments à prendre en compte lorsque les périphériques sont verrouillés afin de garantir une expérience optimale pour l'utilisateur final et la sécurité :

01

## Logiciels compatibles

Assurez-vous bien à l'avance que tous les périphériques de votre entreprise sont pris en charge par le logiciel de verrouillage. Lorsque de nouveaux périphériques et un logiciel de gestion de kiosque sont nécessaires, tenez compte du support disponible pour un large éventail de systèmes d'exploitation et de types de périphériques pour les achats actuels et futurs de périphériques.

02

## Device baseline

Il est essentiel que les périphériques soient alignés sur les stratégies informatiques et de conformité de l'entreprise. Cela permet de renforcer la sécurité lorsque les périphériques sont configurés comme des kiosques.

03

## Verrouillage des périphériques

S'assurer que la configuration du kiosque répond aux attentes des administrateurs informatiques et des départements concernés en améliorant l'expérience de l'utilisateur tout en renforçant la sécurité.

Voici quelques conseils concernant
**ce qui pourrait être configuré pour verrouiller efficacement les périphériques :**

## 01 Inscrire un périphérique dans un MDM

Bien qu'il existe des solutions dédiées aux kiosques, un MDM peut fournir des fonctionnalités avancées et une personnalisation contrairement à de nombreuses solutions spécifiques aux kiosques disponibles sur le marché. Il est également important de s'assurer que le périphérique est inscrit en mode "Propriétaire du périphérique" s'il fonctionne sous Android, ou est "Supervisé" s'il fonctionne sous iOS ou iPadOS.

## 02 Configurations de base selon les normes de l'entreprise

Configurer les mots de passe, distribuer les profils et certificats Wi-Fi, VPN et proxy pour assurer une communication fluide, bloquer les applications et sites Web indésirables, et configurer les mises à jour des applications et du système d'exploitation. Il est important de s'assurer que les stratégies de mise à jour sont configurées pour avoir lieu en dehors des heures de travail afin d'éviter que le périphérique ne soit indisponible pendant le travail.

## 03 Distribuer des applications, des raccourcis web et du contenu

Distribuez les ressources dont vos employés, étudiants ou clients ont besoin. Il peut s'agir d'applications antivirus, d'outils de surveillance du réseau, de pare-feu, de portails pour les employés et les clients ou de sites Web importants.

## 04 Mise en place de stratégies de sécurité spécifiques aux kiosques

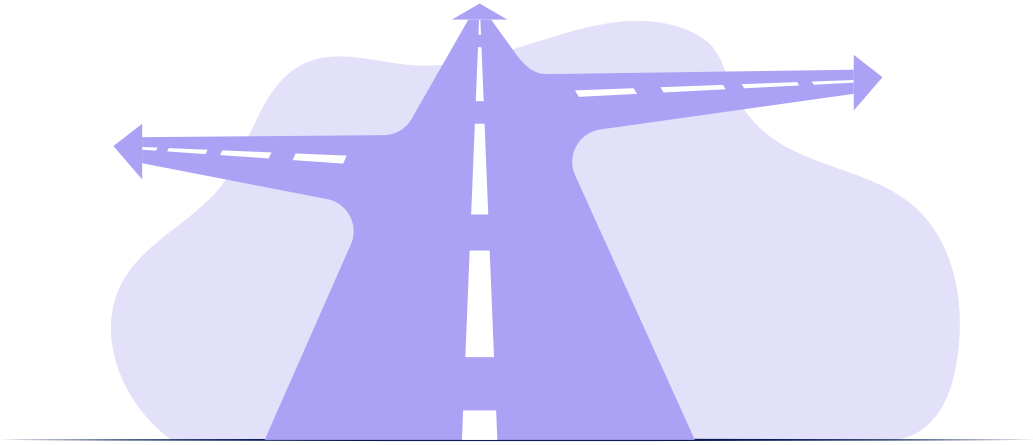
Tout d'abord, assurez-vous que tout ce qui n'est pas nécessaire est désactivé. En fonction du scénario de votre déploiement, vous devrez peut-être désactiver les protocoles réseau tels que Bluetooth, NFC et Wi-Fi Direct, bloquer le partage USB et la sauvegarde sur le cloud, et restreindre les options de presse-papiers et de partage natif présentes dans les applications. Ensuite, assurez-vous que tout ce qui doit être obligatoire a été mis en place. Paramétrez le Wi-Fi, la localisation et, si nécessaire, les données mobiles, pour qu'ils soient toujours actifs. Assurez-vous que les périphériques se connectent uniquement aux SSID Wi-Fi spécifiés et configurez des profils Wi-Fi de secours en cas d'indisponibilité du réseau principal. Enfin, mettez en place une délimitation géographique sur le périphérique. Ainsi, le périphérique est verrouillé et une alerte est envoyée lorsqu'il quitte un rayon de localisation prédéfini.

## S'assurer que le dépannage à distance est configuré 05

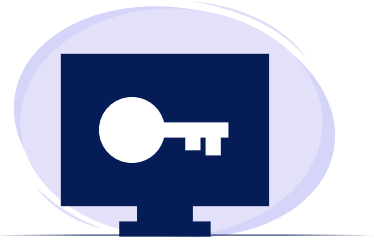
En fonction de votre fournisseur MDM, vous devrez peut-être passer par des intégrations et des configurations d'applications compliquées pour dépanner vos périphériques. Assurez-vous qu'elles sont toutes complètes et que l'accès sans surveillance ou la possibilité de contrôler ou de visualiser les écrans à distance sans que l'utilisateur ne soit invité à le faire est activé. Cela permet d'économiser beaucoup de temps et d'efforts de coordination sur les périphériques qui ne sont pas affectés à un utilisateur spécifique.

# Verrouillage des périphériques la bonne méthode

Les administrateurs informatiques peuvent avoir besoin de configurer le mode kiosque sur les périphériques selon différentes méthodes, en fonction des cas d'utilisation. En fonction des scénarios, ils peuvent avoir besoin de personnaliser le verrouillage en se basant sur ces catégories :



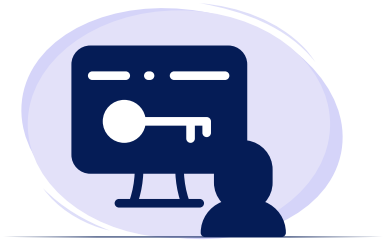
## Mode de déploiement des kiosques



Les administrateurs informatiques peuvent verrouiller la plupart des périphériques modernes, soit dans une seule application, comme dans le cas d'un kiosque de consultation publique, soit dans un ensemble d'applications, comme les périphériques remis aux professionnels de la santé dans les hôpitaux.
Il peut y avoir des scénarios dans lesquels les applications ne doivent pas être exposées à l'utilisateur final, mais doivent tout de même fonctionner en arrière-plan pour assurer le bon fonctionnement de l'entreprise. Par exemple, il peut s'agir d'un VPN ou d'une application anti-virus qui fonctionne sur les périphériques. Ces applications peuvent être provisionnées en tant qu'applications cachées, à condition que votre fournisseur EMM le permette.

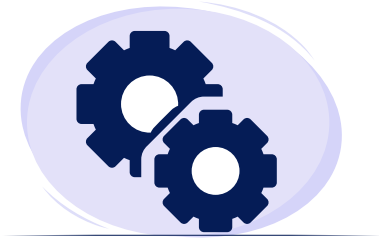
Parfois, il est vital d'automatiser le verrouillage des périphériques et d'empêcher les iPads d'accéder à des applications spécifiques, par exemple lorsque les étudiants passent un examen. Pour ce faire, il est possible de tirer parti du mode autonome à application unique d'Apple. Des conditions et des actions personnalisées peuvent déclencher le verrouillage s'il est configuré au préalable sur une application prise en charge.

## Donner de la marge de manœuvre au personnel compétent



La flexibilité dans le verrouillage des périphériques est obtenue que lorsque le personnel autorisé peut accéder à l'ensemble du périphérique. Cet objectif peut être atteint en imposant des codes d'accès pour sortir du mode kiosque.

De même, il est important de donner accès aux paramètres du périphérique pour activer et désactiver rapidement des fonctions dans des situations spécifiques. Mais l'affichage de l'ensemble des paramètres disponibles peut menacer les fichiers sensibles car l'utilisateur pourrait obtenir un privilège suffisant pour mettre fin au verrouillage du périphérique. C'est pourquoi il est important de disposer d'une application de paramètres personnalisés sur vos périphériques afin de n'afficher que les paramètres qui sont vitaux pour les opérations quotidiennes.

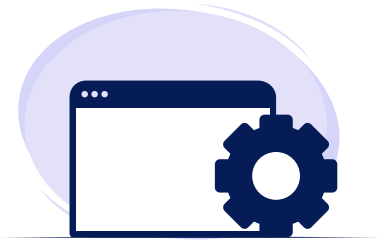


## Personnaliser les fonctions du périphérique

En fonction du scénario de déploiement, certaines fonctions comme le menu de notification, les boutons d'alimentation et de volume, et les fonctions d'appel et de SMS peuvent devoir être personnalisées.

Par exemple, les chauffeurs routiers peuvent avoir besoin d'accéder aux notifications, aux appels et aux SMS lors des derniers kilomètres d'une livraison, mais avec un accès réduit aux périphériques pour éliminer les distractions. Ces besoins doivent également être déterminés en discutant avec les superviseurs du service concerné et configurés en conséquence.

## Personnaliser l'écran d'accueil



Enfin, il est temps de personnaliser les fonds d'écran et l'esthétique générale du périphérique pour répondre aux besoins marketing de l'entreprise.

Il est également important d'organiser les applications, de les ancrer pour un accès facile, de les classer dans des dossiers et de définir l'orientation de l'écran en fonction de l'environnement. Les administrateurs informatiques peuvent également ajouter des raccourcis vers des portails Web, comme un kiosque en libre-service pour les employés.

# ManageEngine Mobile Device Manager Plus: Bien plus qu'une solution de kiosque

ManageEngine Mobile Device Manager Plus simplifie la gestion et la sécurité de vos périphériques, applications et données mobiles. Il s'agit d'une solution de gestion du cycle de vie de bout en bout qui permet d'automatiser l'intégration des périphériques, la définition des bases, la gestion des applications, la gestion du contenu et la gestion des e-mails. Plusieurs stratégies proactives et réactives, comme l'accès conditionnel et les actions à distance, renforcent la prévention des pertes de données.

Les fonctionnalités de gestion granulaire des équipements fournies par Mobile Device Manager Plus peuvent être utilisées pour inventorier les applications, collecter des données précises sur le matériel et les logiciels, suivre l'emplacement des périphériques en temps réel et conserver l'historique de leur localisation.

Mobile Device Manager Plus offre également des fonctionnalités telles que le suivi du niveau de la batterie, l'arrêt et le redémarrage à distance, le geofencing, le mode perdu et l'accès à distance sans surveillance, qui sont particulièrement utiles pour la gestion des périphériques kiosques.

Mobile Device Manager Plus vous permet de configurer les périphériques de votre entreprise de manière transparente et sécurisée.

Téléchargez une version d'essai gratuite et entièrement fonctionnelle pendant 30 jours de Mobile Device Manager Plus pour découvrir, en quelques minutes, comment améliorer la gestion de vos périphériques.

**COMMENCER UN ESSAI GRATUIT**

**RÉSERVER UNE DÉMO GRATUITE**