ManageEngine
Mobile Device Manager Plus

SEAMLESSLY AND SECURELY PROVISION DEVICES IN KIOSK MODE USING MOBILE DEVICE MANAGER PLUS

Introduction

Mobile devices for work are prevalent in organizations of all sizes. Firms in retail, healthcare, education, and other sectors enable the use of mobile devices, like smartphones and tablets, because they enable mobile workforces, help increase productivity, and simplify repetitive tasks.

However, challenges include dealing with sensitive data, like personally identifiable information, that requires adherence to strict compliance regulations. Fortunately, modern mobile device management (MDM) and enterprise mobility management (EMM) tools help IT admins ensure the secure use of mobile devices..

Kiosk mode, or device lockdown, is an effective approach MDM or EMM solutions offer to secure access to these frontline devices. The security and functions of a kiosk are completely dependent on the way it is set up. Common kiosk mode scenarios include customer-facing feedback apps, employee-facing web portals, and shared devices in schools.

This step-by-step guide discusses how you can securely lock down mobile devices in your organization, irrespective of where they have to be placed.

Dedicated kiosk mode versus the device-native alternative

Device native options namely, screen pinning (Android) and guided access (iOS/iPadOS) help lock the devices to a single app, but that is all that they can do and this method only provides rudimentary features and security. IT admins won't be able to lock down the devices to more than one app, determine how the device screens look, or customize notification bar, and hardware buttons. IT won't even be able to enforce the lockdown remotely, which is crucial to save time and resources.

While device-native options are free to use, the zero-cost tag associated with them is superficial as they often negatively impact employee productivity, incur additional expenses from theft and data breaches, and increase IT work-hours spent on managing these devices.

Setting up devices without a proper management tool is a painstaking effort, where the required apps have to be installed manually on every device, and basic setup of passcodes, Wi-Fi, VPN, etc. need to be accomplished separately as well. This might not be the most optimal way of locking down devices in organizations that have a large number of such devices.

Dedicated kiosk mode for a better management and security

An advanced kiosk feature should be able to help throughout the device life cycle management. Kiosk management is not about just locking a device down, but also about ensuring that sufficient flexibility is provided for employees to perform their tasks smoothly. For effectively managing kiosk devices, it is critical that the following aspects are covered:

01

Remote provisioning

The ability to lockdown endpoints of diverse types and OSs into kiosk mode from a unified console, and ensure that they stay locked down.

02

Flexible deployment

Choosing which apps, web portals, corporate resources, settings, and functions should be accessible.

03

Home screen customization

The option to set the icon layout and order, organize them in folders, set orientation, and apply a wallpaper of your choice.

04

Stolen and misplaced device management

Utilizing the lost mode to lock, locate, and erase devices when lost or stolen.

05

Data security

Setting proactive and reactive rules to ensure sensitive information is safeguarded.

06

Device profiles

This covers device management aspects other than kiosk and its auxiliary functions.

07

App management

Deploying, configuring, updating, and removing applications without user intervention.

08

Insights on device and battery

Receiving alerts on battery levels, location of device, app and OS updates, and the exhaustive inventory of device software and hardware.

09

Remote troubleshooting

The ability to remotely control or view screens of devices and possibly without needing user intervention.

3 things to ensure before provisioning devices into kiosks

There are three things to consider when devices are being locked down to ensure the best end user experience and security:

01

Compatible software

Ensure well in advance that all the devices in your organization are supported by lockdown software. When new devices and kiosk management software are required, consider the support available for a wide variety of OSs and device types for current and future device purchases.

02

Device baseline

It is crucial to have devices baselined as per the organization's IT and compliance policies. This enforces greater security when devices are being set up as kiosks.

03

Locking down devices

Making sure that the kiosk setup meets the expectations of the IT admins and respective departments enhances the user experience while boosting security.

Here are a few pointers towards **what could be configured for effectively locking down devices:**

01 Enroll a device with an MDM

While there are solutions dedicated to kiosks, an MDM can provide advanced features and customization unlike many kiosk-specific solutions available in the market. It is also important to ensure that the device is enrolled in “Device Owner” mode if it's running on Android, or is “Supervised” if it's running on iOS or iPadOS.

02 Baseline configurations as per organizational standards

Setup passcodes, distribute Wi-Fi, VPN, and proxy profiles and certificates to ensure seamless communication, block unwanted apps and websites, and setup app and OS updates. It is important to ensure that the update policies are set up to take place during non-work hour windows to prevent device downtime during work.

03 Distribute apps, web shortcuts and content

Distribute resources that your employees, students or customers need. This could include anti-virus applications, network monitoring tools, firewalls, employee and customer portals or important websites.

04 Setup kiosk-specific security policies

First, ensure that anything that is not required is turned off. Depending on your scenario of your deployment, you might need to turn off network protocols like Bluetooth, NFC, and Wi-Fi Direct, block USB sharing and cloud backup, and restrict clipboard and native share options present in apps.

Next, ensure everything that has to be mandated has been. Set Wi-Fi, location and, if required, mobile-data, to always on. Ensure that devices connect only to designated Wi-Fi SSIDs, and configure backup Wi-Fi profiles as a contingency when the primary network becomes unavailable.

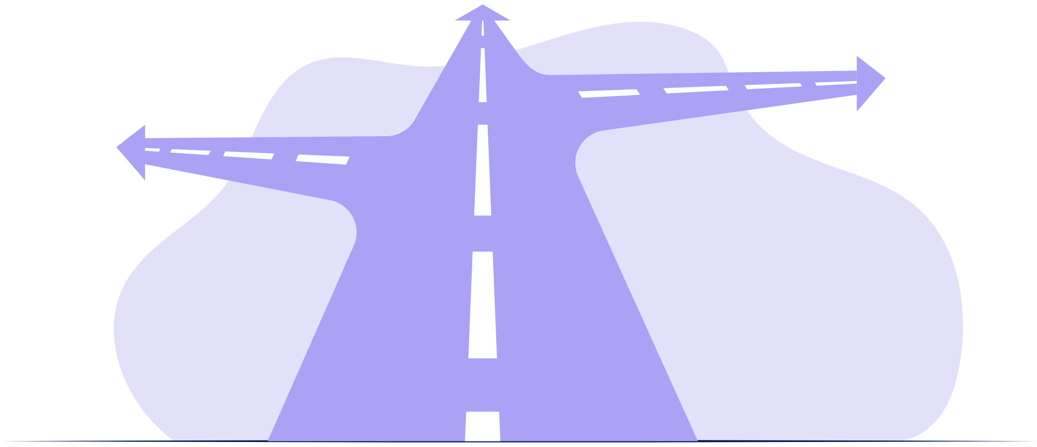
Finally, set up a geofence on the device. This ensures that the device gets locked and an alert is sent when the device leaves a preset location radius.

Ensure remote troubleshooting is set up 05

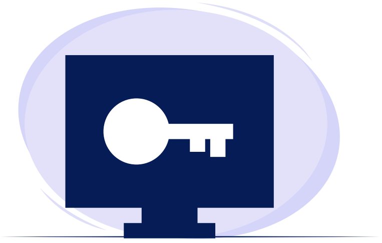
Depending on your MDM provider, you might need to go through integrations and complicated app setups to troubleshoot your devices. Ensure that these are all complete, and that unattended access or the ability to remotely control or view screens without user prompts is enabled. This saves a lot of time and coordination effort on devices that are not assigned to a specific user.

Locking devices down the right way

IT admins may need to configure kiosk mode on devices in different methods, depending on the use cases. Based on the scenarios, they might need to customize the lockdown based on these categories:



Mode of kiosk deployment

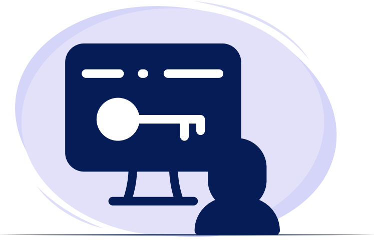


IT admins can lockdown most modern devices either into a single app like in the case of a public-facing feedback kiosk, or a set of apps like devices handed over to healthcare professionals in hospitals.

There could be scenarios where applications should not be exposed to the end-user but still have to be running in the background for smooth business operations. For example, it could be a VPN or anti-virus app that is running on devices. Such apps can be provisioned as hidden apps, provided your EMM vendor facilitates it.

Sometimes, it's vital to automate device lockdown and prevent iPads from accessing specific apps, such as when students are taking an exam. This can be achieved by leveraging the Autonomous Single App Mode from Apple. Conditions and custom actions can trigger the lockdown if it is configured beforehand on a supported application.

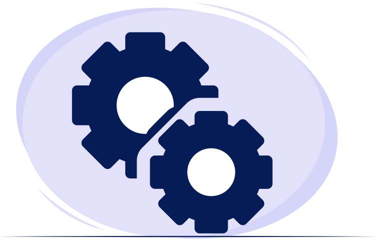
Providing leeway to the right personnel



The flexibility in device lockdown is achieved only when authorized personnel can access the entire device. This can be achieved by mandating passcodes to exit kiosk mode.

Similarly, it is important to provide access to device settings to quickly turn on and off functions in specific situations. But showcasing the entire settings available can threaten sensitive files because the user might obtain sufficient privilege to stop device lockdown. This is why it is important to establish custom settings app on your devices to only show settings that are vital for day-to-day operations.

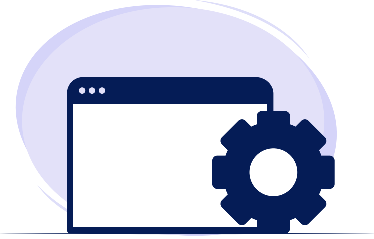
Customize device functions



Depending on the scenario of deployment, certain functions like notification menu, power and volume buttons, and call and SMS functions might need to be customized.

For example, truck drivers may need access to notifications, calls and SMS for last mile delivery, but with reduced device access to eliminate distractions. These also have to be determined by talking with the supervisors of the respective department and configured accordingly.

Customize the home screen



Finally, it is time to customize the wallpapers, and the overall aesthetics of the device to match the organization’s brand marketing needs.

It is also important to arrange the apps, dock them for easy access, organize them in folders, and set screen orientation based on the environment. IT admins can also add shortcuts to web portals like an employee self-service kiosk.

ManageEngine Mobile Device Manager Plus: Much more than a kiosk solution

ManageEngine Mobile Device Manager Plus simplifies the management and security of your mobile devices, apps and data. It is an end-to-end lifecycle management solution that provides automated device onboarding, baselining, app management, content management, and email management. There are several proactive and reactive policies, like conditional access and remote actions, that enhance data loss prevention.

The granular asset management capabilities provided by Mobile Device Manager Plus can be used to inventory apps, collect granular hardware and software, track device location in real time and maintain its location history.

Mobile Device Manager Plus also offers features like battery level tracking, remote shutdown and restart, geofencing, lost mode and unattended remote access that are particularly helpful in managing kiosk devices.

Mobile Device Manager Plus enables you to seamlessly and securely provision devices in your organization.

Download a free, fully functional 30-day trial of Mobile Device Manager Plus to explore, within minutes, how to enhance your kiosk management journey.

START A FREE TRIAL

BOOK A FREE DEMO