The Ultimate Guide to Kiosk Management

Everything your business needs to know

WHITE PAPER

hexnode

TABLE OF CONTENTS

1

The history and scope of kiosks

Kiosks have been around for well over a hundred years. Their first usage can be traced back to the 1880s where they served as vending machines, introducing the idea of a self-service kiosk for the very first time.

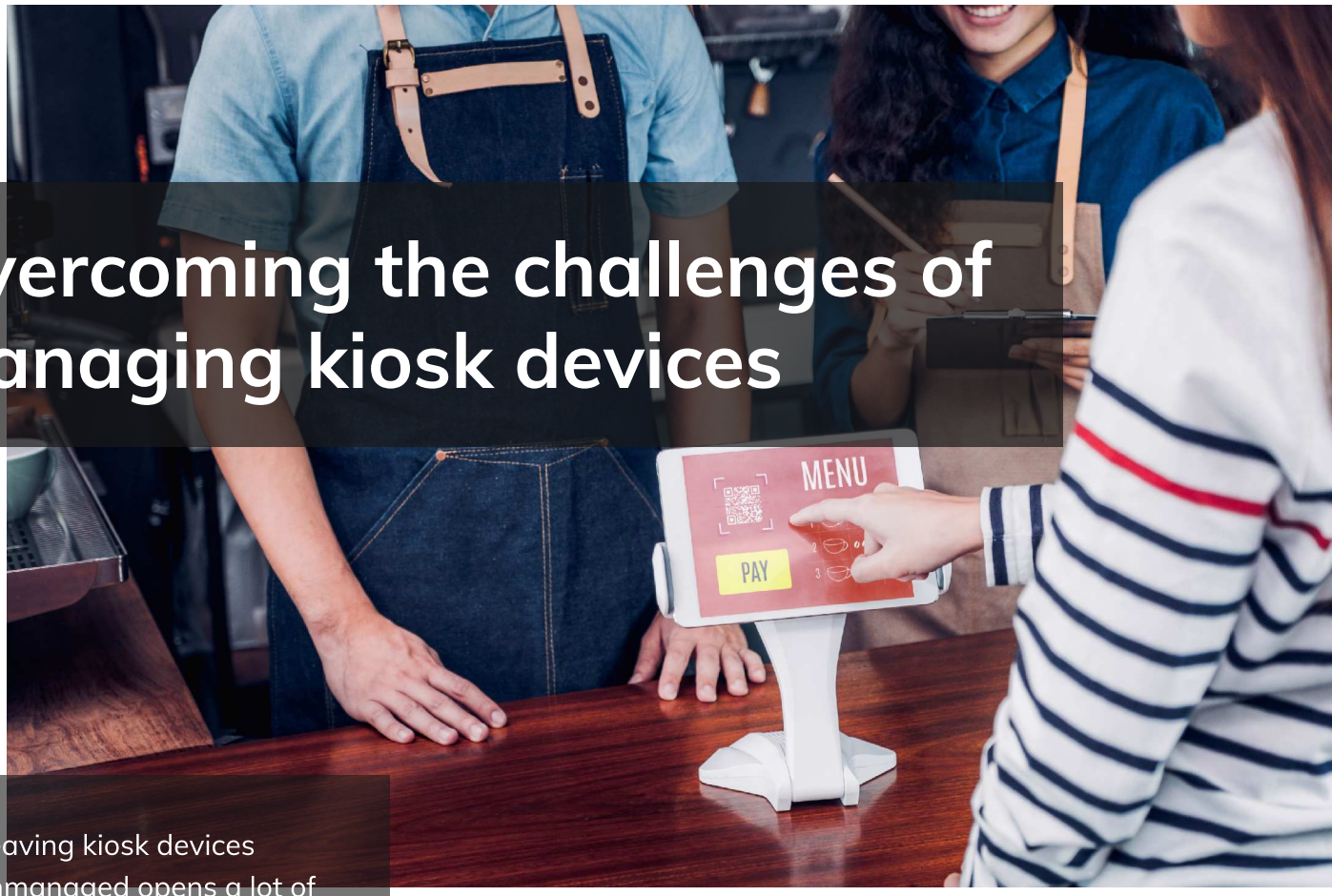
They evolved during the latter half of the 20th century to tackle more complex tasks such as handling financial transactions, enabling self-check-ins, acting as way finders, and more.

Many industries from retail, hospitality to enterprise, education and healthcare have adopted the use of kiosks due to the number of benefits they offer. They are used in classrooms to make learning more interactive and used in offices to automate multiple tasks and keep track of inventory within warehouses. Its hardware has evolved over the years to incorporate the use of new technologies and the industries they are deployed to function in. Some of the most commonly used kiosk devices include:

- Mobile point of sale
- Self-service kiosks
- Digital signages

2

Overcoming the challenges of managing kiosk devices



Leaving kiosk devices unmanaged opens a lot of threats leading to the compromise of sensitive data stored within those devices.

Users may also have access to explicit content and change the device settings previously configured by the admin.

Of course, choosing to manage your kiosk devices manually would look like the right choice initially, but you can't discount the various challenges this could pose.

Manual management of kiosk devices introduces numerous challenges for IT such as; ensuring the timely deployment of essential files to end users, enabling endpoint security, restricting users from making system-level changes, and more. Moreover, admins will find it harder to troubleshoot the devices when they encounter a problem and manage devices from multiple platforms. The use of kiosk management software gives businesses complete control over the devices they manage. It helps them:

- Set adequate restrictions
- Whitelist necessary applications
- Offer a more secure browsing experience
- Deploy content across multiple locations
- Personalize the user experience
- Manage both consumer and rugged kiosks
- Ensure device and data security

3

The 3-step guide to managing kiosk devices

Kiosks are deployed for a variety of applications. But whatever their function may be, they all call for a need to secure and manage these devices and optimize them into delivering a purpose-specific experience.

A Unified Endpoint Management (UEM) solution converts your devices into kiosk devices and blocks the users from accessing any apps or features of the device other than what is allowed by the admin.

GETTING THE DEVICE READY FOR USERS

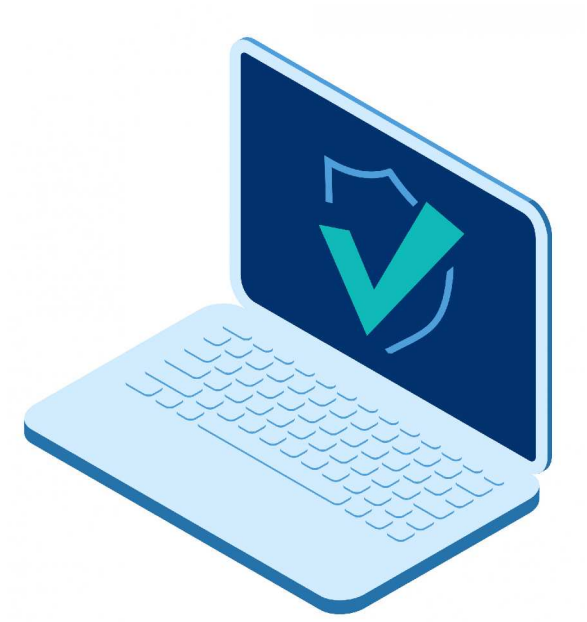
Android

A majority of kiosk devices run on Android. One of the main reasons behind their popularity is the flexibility in usage. Plenty of Android devices function as digital signages, point of sales systems, inventory scanners, etc.

These devices are best managed by a kiosk management solution as it provides IT admins, with everything, they need to make sure end users don't tamper with the device and leave it unmanaged.

System requirements:

- General Android – Android v4.1+
- Android Enterprise – Device owner mode



Sometimes getting the devices enrolled and connected to your organization's networks can be the hardest part. The coming of Android Enterprise in 2014 brought in a number of quick and remote enrollment methods where admins could enroll hundreds of devices within just a few minutes. Hexnode UEM provides multiple enrollment options, some of which are user centric while others are done remotely with no user intervention.

Small and Medium Businesses (SMBs) often found themselves balancing a limited budget while ensuring they have the proper tools to monitor and manage their servers and endpoints. However, protocols in connectivity establishment and reduced overhead of maintaining connections have made RMM affordable and scalable over the past decade. As a result, SMBs can now leverage RMM technology to provide remote support.

Zero touch enrollment

Enroll corporate owned devices in bulk over the air. It makes the enrollment process more secure by restricting unauthorized devices from joining the corporate network. Some of the perks of choosing this enrollment method include one-time setup, bulk enrollment of devices, enrollment as device owner and allow resellers to add devices to the portal. Your organization needs to first enroll within the Android Enterprise program.

Samsung Knox Mobile Enrollment

Another over the air enrollment method for bulk devices, where all the security configurations and required applications will be applied on the device as soon as it powers on. Some of the reasons why you want to choose this enrollment method include the automatic reenrollment of the device even after it is erased and support of multiple MDM configurations per account.

Android Enterprise

Enrolling the device in Android Enterprise helps you unlock a number of features to efficiently manage devices in an enterprise setup. It helps in the creation of a work container, which is an encrypted space within the managed device where all work-related data and applications are stored.

The devices could either be enrolled in a profile owner or device owner mode. Personally owned devices of employees are enrolled in profile owner mode whereas fully managed devices are enrolled in device owner mode. Android devices can only be locked down in a kiosk mode if they are enrolled in a device owner mode. In order to lock down your devices in a kiosk mode, your organization must first be enrolled within the Android Enterprise program and then enrolled in device owner mode. Once the device is enrolled, you can begin applying the required configurations and settings needed to secure the devices.

Enrolling as Device Owner via UEM app

You don't necessarily have to enroll in Android Enterprise in order to enroll the device in a device owner mode. The device can be enrolled into device owner mode with the help of the Hexnode UEM app via ADB. The devices should be running in an OS version 5 and above. All accounts previously associated to the device have to be removed before the device is enrolled.

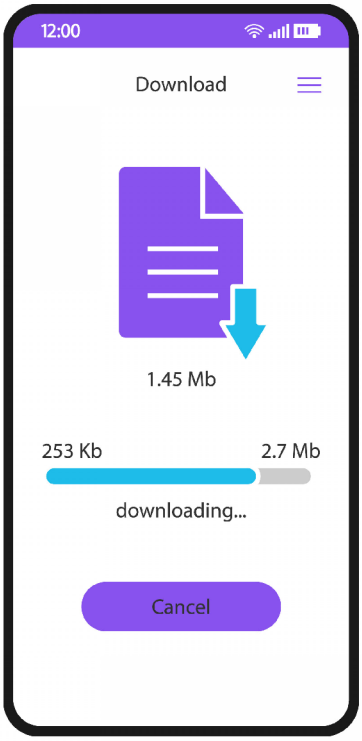
Enrolling devices without camera or playstore

This enrollment is ideal for organizations whose devices have playstore and camera disabled on the device. If the playstore alone is enabled, the user can download the app from the playstore. If the camera alone is enabled, then the user can download the apk file of the app and install it manually.

ROM enrollment

A custom ROM is an Android OS customized by the ROM builder to make the device function faster. It also helps in the addition of new features to make the device run more efficiently and specific to your organization's requirements. Flashing a custom ROM with Hexnode UEM as a system app is yet another way in which you can get the devices enrolled. In this enrollment method, the device usually consists of a configured ROM with all the necessary permissions granted to the Hexnode UEM app. As soon as the user turns on the device for the first time, the device will be enrolled with Hexnode UEM. Some of the benefits of using a custom ROM Android device include:

- better performance and instant access to new features
- removal of bloatware that hampers the performance of your device
- customize the appearance of the device
- update the device to its latest OS version
- silent installation and uninstallation of applications
- upgrade and downgrade applications without any user intervention
- turn off and reboot device without the help of users
- lock down lost or stolen devices in a lost mode
- make the Hexnode UEM app non-removable
- disable systems bars on the device when locked in a kiosk mode.



Bulk enrollment

Allow admins to enroll devices in bulk. Send the invitation request to users and upload the CSV file containing the required information such as their name, email and ownership.

Pre-approved enrollment

Gives admins the flexibility to setup policies on the device even before it is enrolled within the UEM portal. All the configurations will be automatically applied on the device once it is enrolled. You can setup this enrollment method by adding the CSV file with the required device details.

Open enrollment

This is the quickest and easiest way to get the devices enrolled. Devices enrolled via this method will be assigned a default user. This is a good choice if you are managing a small number of devices and want to get the devices enrolled quickly without much of a technical hassle. It does not require authentication. You can set the request mode as either email or text. You could either enroll it as a new device or re-enroll it by retaining the existing configurations on the device and changing the owner.

Enrollment with authentication

You would have to enter the server name and the authentication password. This is a more secure way for enrollment as it helps businesses to ensure that only authorized users are enrolling the devices.

Self enrollment

Permits users to directly enroll the devices using their Active Directory credentials. You need to first configure the Active Directory settings to enable self enrollment and import AD users to the UEM console. This method also works for Azure AD users, local users, GSuite users and Okta users.

iOS

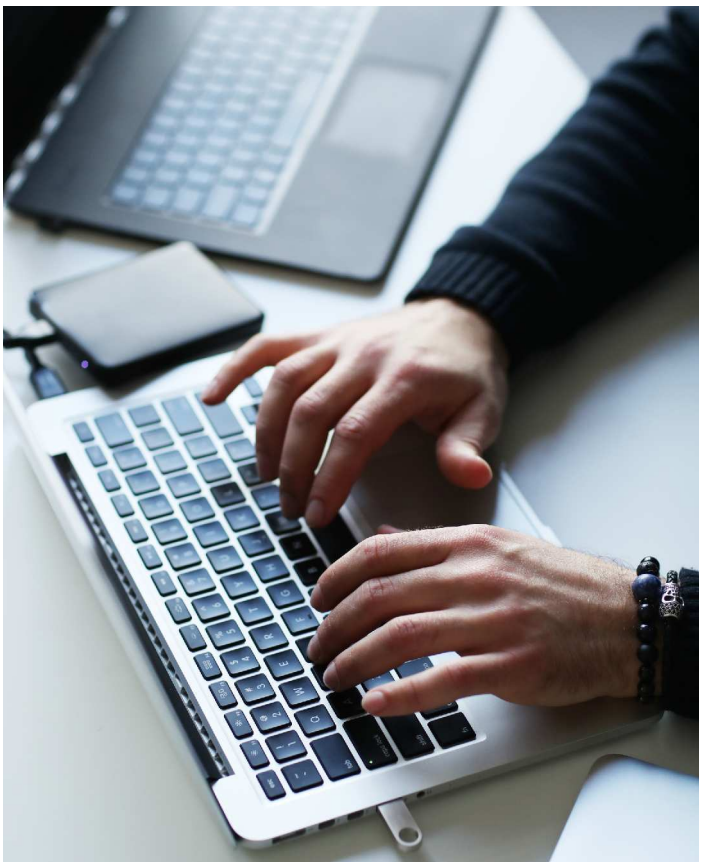
Various Apple devices such as iPhones and iPads are increasingly being used as kiosks as they are visually appealing and are a preferred choice for customers, most of whom grew up using these devices at home. A number of restrictions and configurations can be remotely configured on the device to make them secure and more intune with your organization's requirements.

There are various ways in which iOS devices can be enrolled and managed. You could either go for general enrollment methods such as open, authenticated or bulk enrollment to enroll the devices quickly to the UEM portal or go for platform specific enrollment methods such as DEP, Apple Configurator and GSuite to bulk enroll a number of devices over the air and pre-configure all the necessary settings.

System requirements:

- Supervised iOS v9.3+ (Multi app Mode)
- Supervised iOS v6.0+ (Single app Mode)
- Supervised iOS v7.0+ (Autonomous Single App Mode)
- Supervised iOS v9.3+ (Web clips)

DEP (Automated Device Enrollment)



Now known as Automated Device Enrollment with its integration into the ABM platform, this is an over-the-air enrollment method that helps in simplifying the initial device setup and getting the devices ready for users without any user intervention. The benefits of enrolling your devices via Automated Device Enrollment include:

- Make the MDM profile non-removable
- Prevent users from removing the MDM configuration
- Wirelessly turn on supervision on the device
- Simplify the initial device setup
- Silent app installation
- Add in more restrictions and configurations to make the devices secure

Apple Configurator

This is an application found within Macs and iPhones that allow admins to create configuration profiles for a wide range of Apple devices. You could set all the required settings, configurations and apps on the Blueprint via Apple Configurator and apply it on the device. The device can then be applied to a user.

DEP enrollment using Apple Configurator

The initial setup process is the same as Apple Configurator. The only thing you need to note is that you need to choose the ‘Add to Device Enrollment Program’ option in order to set up the devices via DEP enrollment. Only supervised iOS devices can function as kiosk devices and supervision can only be enabled if the devices are enrolled via DEP.

G Suite Enrollment

Helps users to enroll the device using their GSuite credentials. Configure GSuite with the UEM portal. The enrolled device will be assigned to each GSuite user. Policies and remote actions can be associated to devices, users and the entire domain.

Pre-approved enrollment

this gives admins the convenience to configure policies on the device even before they are enrolled within the UEM portal. These would be enabled on the device as soon as they are enrolled. There are two ways in which you can go about this enrollment method, you could either do so by adding the CSV file with all the details or add DEP devices as pre-approved devices within the portal.

Bulk enrollment

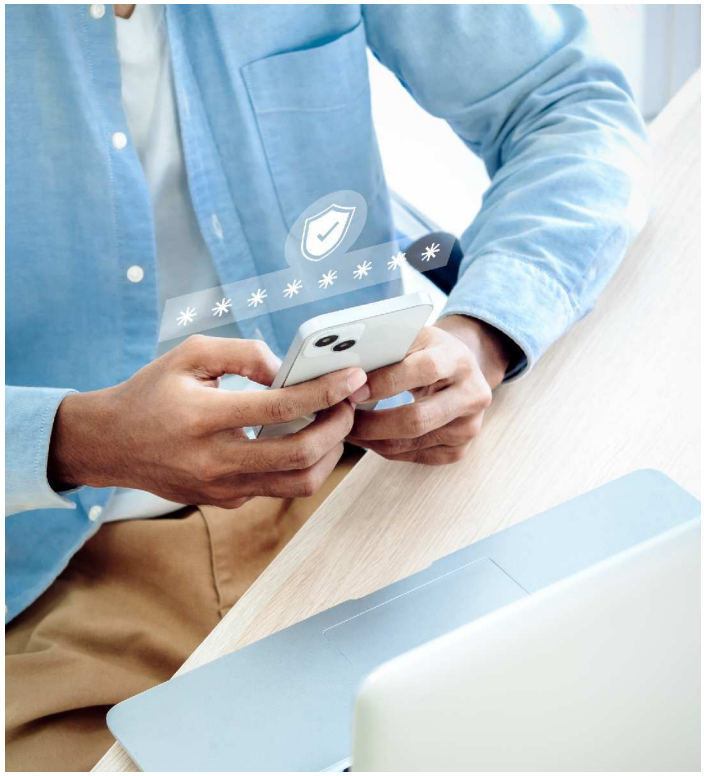
This involves enrolling the devices in bulk. Users would be sent the enrollment request via email. The CSV file consisting of the necessary fields required for the enrollment would be uploaded in the UEM portal. You can verify the details given within the CSV file and send the enrollment request to large number of users remotely from the portal.

Open enrollment

This entails enrolling the device with the server name. Once the user enters the enrollment URL, the configuration profile will be downloaded on the device. Devices enrolled with this method will be assigned to a default user defined within the enroll tab within the portal. You may not want to choose to use this enrollment method if you want to securely enroll the devices to the UEM portal as anyone with the enrollment URL would be able to get the devices managed. This is just one of the quick ways in which you can get the devices enrolled.

Authenticated enrollment

This is similar to open enrollment, the only difference being that it requires the authentication credentials of the user such as the username and password. This is a more secure way in which you can get the devices enrolled as it makes sure only authorized users are able to get the devices enrolled.



Self enrollment

This helps users to enroll their devices using their Active Directory credentials, Okta credentials, GSuite credentials or the credentials generated by the UEM portal at the time of the enrollment process.

Windows

Windows can be locked down to function as kiosk using the assigned access feature within the UEM portal. You could go for the open enrollment option to enroll the devices quickly or authenticate users while enrolling the device using authenticated enrollment or enrollment via Google Workspace credentials. PPKG enrollment helps in the bulk enrollment of devices where configuration settings can be applied beforehand, making it ready for users as soon as they power it on.

System requirements:

- Windows 10 device v1709+ (Pro, Enterprise and Education edition)

Google Workspace Enrollment

Makes it easy for GSuite users to enroll their device by using their GSuite credentials. It involves configuring the GSuite account within the UEM portal, syncing GSuite users to the portal so that the enrollment requests can be sent to the users. The users would authenticate themselves by entering the GSuite username and passwords.

PPKG Enrollment

This is an efficient method to bulk enroll and apply necessary configurations to a large number of devices. PPKG are provision packaging files which consist of a number of configuration settings. They can be created within a Windows 10 device and used to set up the devices for users without their intervention. Some of the benefits of enrolling the device via the ppkg file include getting the devices quickly setup for users, as soon as they install the ppkg file the configurations would get applied on the device making it readily available for the user to begin using the devices at once.

Open Enrollment

This could be done in two ways, you could either enroll the device via the Hexnode Installer App or go to settings to enroll the device with device management. Just type in the server URL, enter the work email ID and follow the setup instructions to get the devices enrolled.

Authenticated Enrollment

It provides a more secure way of getting the devices enrolled. This ensures only the right user enrolls the device by means of a username and password. If you are planning to install via the Hexnode Installer App, the Hexnode Installer would check for the enrollment authentication settings within the portal. If your users are using their local or AD credentials for enrollment, they would have to enter their email ID or SAM Account name to authenticate themselves. Users can also use their Microsoft, Google or Okta credentials for authentication.

tvOS

System requirements:

- · tvOS 10.2+ (Supervised)

Apple TVs are a great medium to instruct students and can be a great addition in conference rooms. These devices can be easily managed with the help of a UEM solution.

You could get the devices all set up for users either using Apple Configurator and Apple Business Manager.

Apple Business Manager

This is a web console provided by Apple that allows admins to seamlessly enroll bulk number of devices over the air, purchase and manage apps and books for their organization.

Apple Configurator

Admins can use the Apple Configurator app to enroll the devices and apply the necessary configurations to the device via Blueprint.

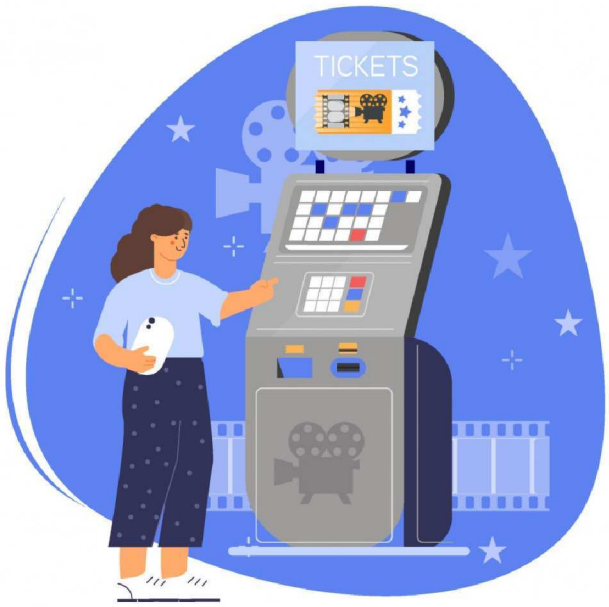
MANAGE ESSENTIAL APPLICATIONS AND FILES

Android

Single app kiosk mode

When you deploy a device in a single app kiosk app mode, the device will be locked down to function in just a single application. The application would run in the foreground with the barest device functionalities enabled. The app would relaunch even after the device is rebooted and shutdown.

One of the main purposes of locking devices down in a kiosk mode is to make sure the devices continue to function with the deployed application without any user distractions. The device can be locked down to function in just a single application or file. You can customize the kiosk launcher settings and define the time period in which the app should be launched on the device.



Multi app kiosk mode

This locks down the devices to a set of applications. Users would only have access to those specified applications. Multi app kiosk can be deployed on both Android and Android TV devices.

When deploying the multi-app kiosk policy for Android devices, you can choose how the applications can be displayed in two methods, these include basic view and advanced view. It provides a simplified view of the apps and file shortcuts that need to be deployed. You can customize the app and file icon size. Advanced view gives you a real representation of how the apps would actually look on the device.

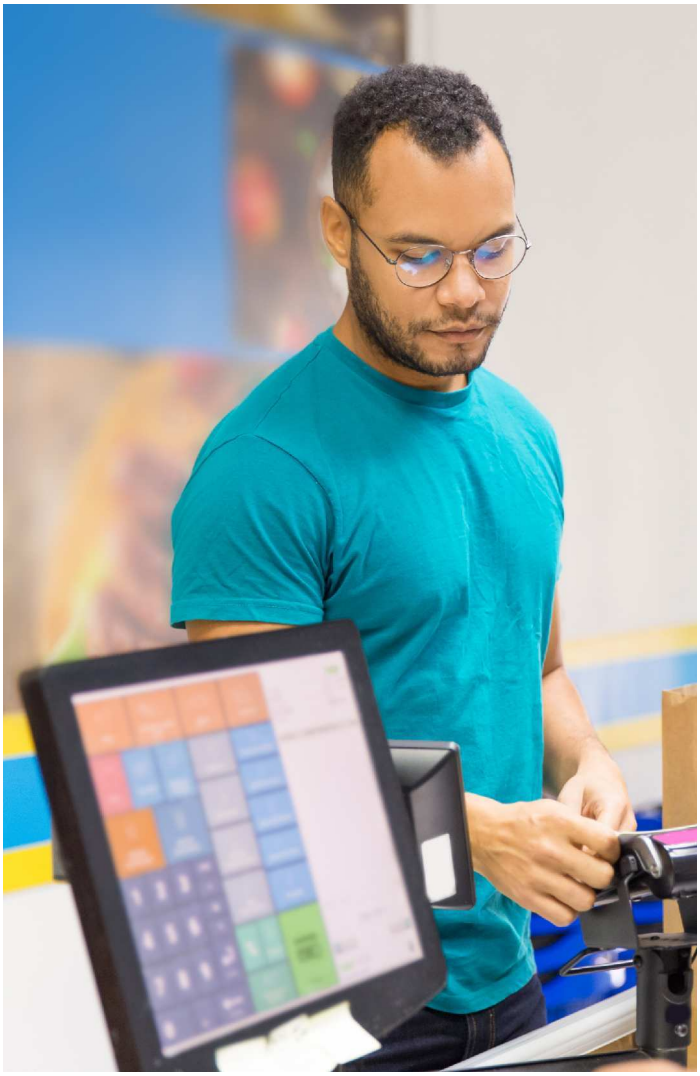
Admins can customize the way they look on the screen and define the icon size of the applications. A wide variety of applications can be added such as Enterprise apps, web apps, managed google apps, system apps and store apps. You can also customize the screen orientation and add more pages to the device screen. You can drag and drop applications to the virtual screen and define the position of each of these applications.

Background app

Background apps are useful when you need to hide the application from the user but need to run it in the background. Say you've deployed an essential application for users but it requires the use of a camera, you don't want users to have access to the camera as they may use it to take photos of sensitive documents.

You can deploy the camera as a background app. In this way the application will run in the background and stay hidden from users.

Web app kiosk



This is a url that is added as an application. You can launch your website as a web app and deploy it to the managed devices to function either as a single app or a multi app kiosk. You can choose the app icon you want to display on the screen. In case of some specific websites, you can pass the device information along with the url with the use of a wildcard. You can use Hexnode's native native browser – Hexnode Lite and Hexnode Kiosk Browser to customize the way in which the apps would appear to your users.

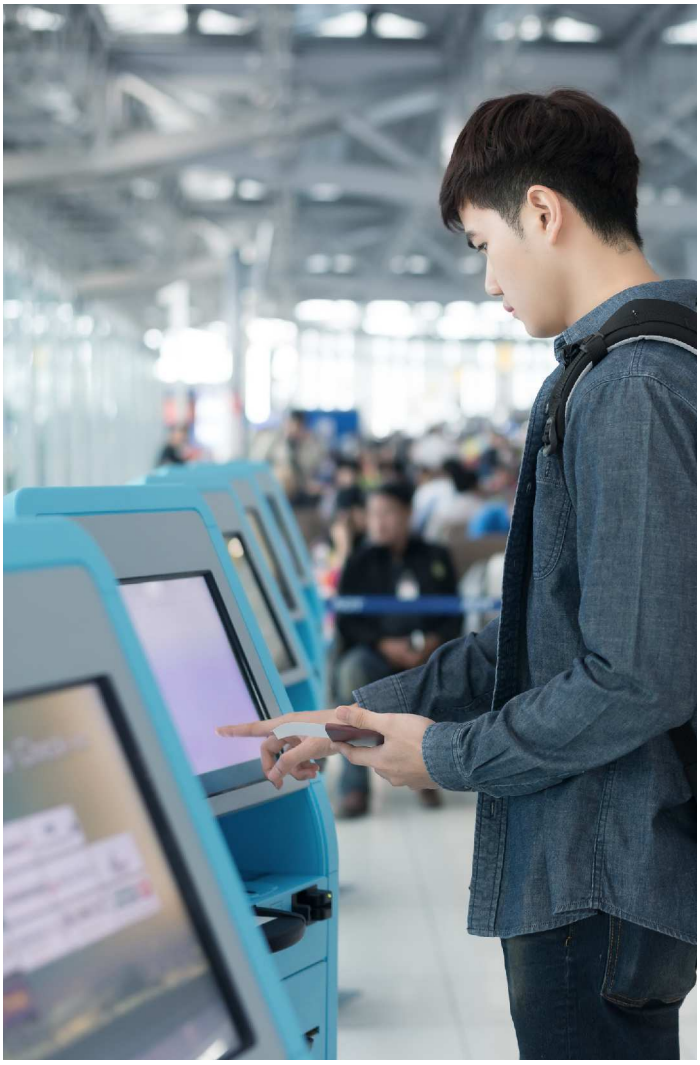
In addition to using Hexnode's native kiosk browser, you can choose to use other third-party browsers if they are added as background or multi app kiosk. Hexnode's native kiosk browser also gives you the option to open the apps in a single tab and multi tab browser. Hexnode Browser Lite supports multi tab browsing whereas Hexnode Lite supports single tab browsing.

Updating enterprise applications in kiosk mode

Enterprise applications are private applications used by organizations to carry out their daily tasks. These are specific to the organization that deploy them and are not usually found in public app stores. These applications can be installed and updated remotely in kiosk mode without any user intervention.

You could go about this in two ways, you could either replace the old APK file with a new one in the app inventory or add the new APK file as a new application within the app inventory and push it as a policy to the managed devices. Updating the required application doesn't mean you have to exit from kiosk mode. Doing so not only inconveniences the user but also gives admins the additional task of enabling kiosk mode on the devices again. The whole process involves uploading the latest app version to the app inventory and pushing it silently to the devices without leaving any dependency on the user.

iOS



Single app kiosk

This works on supervised iOS devices running on iOS version 6 and above. Before you apply the single app kiosk policy, you need to make sure that the application is already installed on the device. Even though the kiosk policy already locks the device to function with just the required settings, you can set additional restrictions to restrict the functionalities of the device even further. These include:

- Disabling touch
- Disabling volume buttons
- Disabling device screen rotation
- Disabling sleep wake button
- Disabling autolock
- Disabling sensitive touch

A number of user enabled options can be configured as well such as disabling VoiceOver, zoom, invert colors and AssistiveTouch.

Multi app kiosk

This locks down the device to function in a set of whitelisted applications. The apps can also be grouped together in app groups making it easier to categorize the applications when handing it out to users. A wide range of applications can be added from the app repository such as VPP apps, enterprise apps, store apps and system apps. The settings and the phone app will be added to the policy by default, therefore users cannot be restricted from accessing them.

The homescreen layout policy makes it easy for admins to customize the layout of the applications, app groups and web clips within the kiosk homescreen. New pages can be added within the layout to expand the number of applications and web clips you want to have deployed on the device.

Autonomous single app kiosk

This locks the device down in a single app mode continually running in the foreground with the ability to come out of the kiosk mode once the purpose of the specified application is over.

Web app kiosk

Web apps direct users to a website or a file. Users could either choose to open the web apps using Safari or Hexnode Browser Lite. If users are using Safari to access the web apps, the apps can be accessed from the bookmarks section from the browser. Normally external links are not accessible within the web apps, admins can whitelist the external links to provide access to users.

Silently install and update applications

You could either associate the app to the device via a kiosk policy or install it manually remotely from the UEM portal. It will be installed within the device but will stay hidden from the user. These apps would appear to user when they exit from kiosk mode. Enterprise applications can be updated on the device without any user intervention in two ways. You could either replace the old IPA file with a new one in the app inventory or remotely push the updated app to the device from the UEM console.

Windows

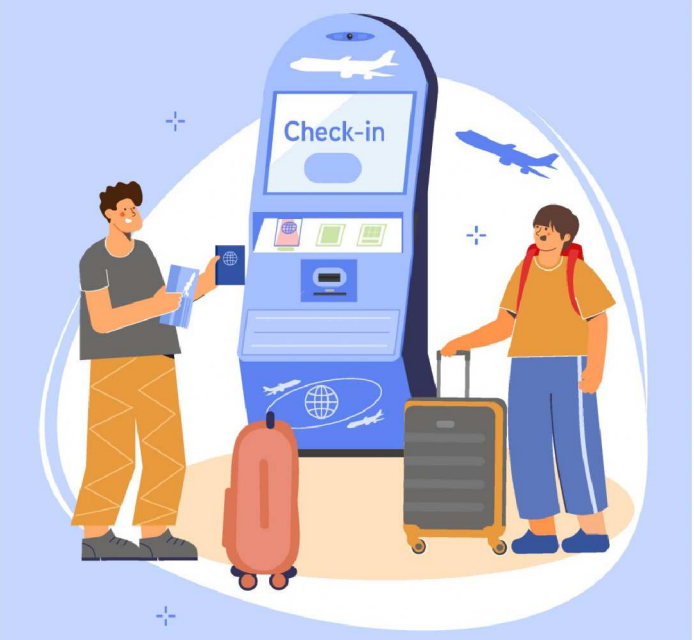
Single app kiosk

Admins can run a Universal Windows Platform (UWP) app (these are apps pre-installed on the device, Microsoft Store apps and desktop apps) on Windows 10 PCs. A local user account should be required in order to run the UWP app in a full screen. The single app kiosk policy can also be associated with an AD account, but the user must log in to the device at least once before the policy is applied. The whole process includes:

- Creation of local user account on the device
- Installation of the kiosk app within the account
- Creation of the kiosk policy from the UEM console and associating it to the device

Silently install and manage applications

The applications can be silently installed on the device either by associating a policy pushing the app to the device or remotely deploying it via the UEM portal. Enterprise applications are private applications specific to the organizations that use them. They can be silently installed on user end devices by adding the app within the app inventory either as a MSI file or manifesting the URL. You can specify the command line parameters to define how the configuration settings and actions should be applied on the device.



tvOS

Single app mode

Deploy the application you need remotely from the UEM portal and make it run on the foreground, restricting users from using any other applications. Configure the application to make it launch automatically. Only enterprise apps can be added as kiosk applications within the device. You can configure the kiosk settings to define how the device needs to appear to end users and lock the devices in an immersive kiosk experience.

SECURE THE DEVICE WITH ADDITIONAL MANAGEMENT CAPABILITIES

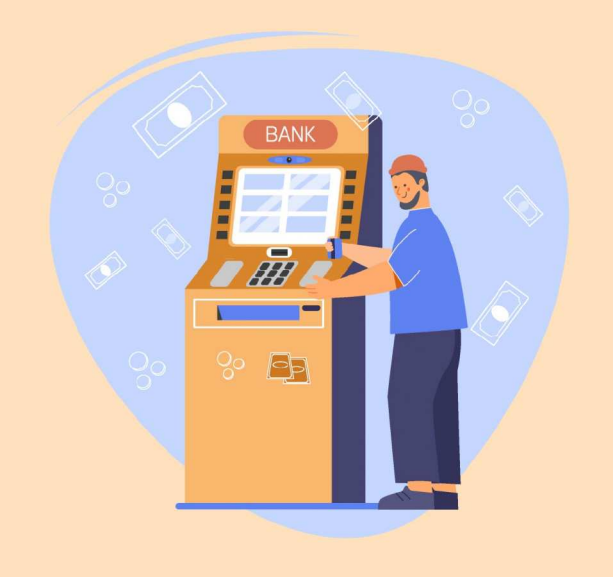
Android

Digital signage kiosks

Digital signages are a great way to enhance your digital marketing efforts. They have a widespread usage across various industries ranging from retail and hospitality to healthcare and education. Plenty of Android devices are used to function as digital signages. You can find them pretty much everywhere from transit hubs to schools, corporate offices and your local museum.

Managing your kiosk devices with a UEM solution makes it easy to customize the signages and manage it the way you want to. Files of varied formats can be remotely deployed to the devices such as jpg and png (images), mp4 and mkv (videos), mp3 and ogg (audio). While adding the files, you can also include sub folders and categorize it by name and type. Other customizations include playing a custom background music, trim clips, define the display duration to display the images, define the screen orientation and brightness level.

Lock task mode



This strictly locks down the device to function as an immersive kiosk. It disables most of the UI features restricting users from making changes to any of the device's settings. Only applications previously whitelisted by the admin would be allowed to function on the device. Any Android devices running on v5.0 and above can be locked down in a lock task mode. The devices would have to enrolled in Android Enterprise as a Device Owner.

Configure website kiosk settings

You can customize the way the web apps appear to your user by customizing the website kiosk settings. Customization can only be done on Hexode's native kiosk browsers – Hexnode Lite and Hexnode Kiosk Browser. Some of the options you could customize include customizing the toolbar setting: these include displaying the clear session option, the browser title on the toolbar. Customizing the theme color settings, the appearance, refresh settings, privacy and security settings, content, browsing history, forms, location, hardware and software keys.

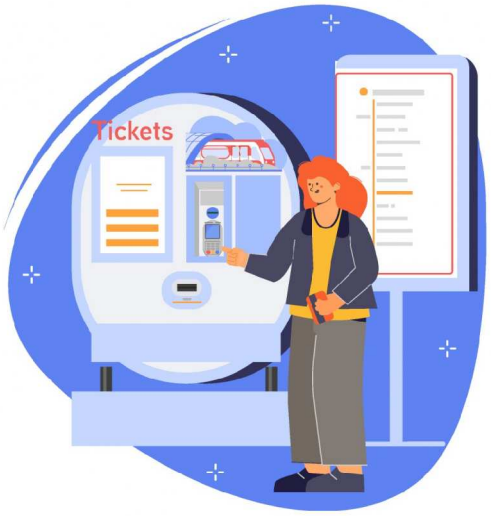
Android launcher

When a device is locked down in a single app mode, the app would launch automatically on the device when it enters the kiosk mode. If the device is locked down in a multi app mode, you can choose the Android launcher to deploy a specified application and define the time period in which the application needs to be launched. If you associate the kiosk policy with a single app kiosk, the kiosk homescreen with the single app will be displayed on the device. The launcher can be configured in a number of ways, these include customizing the app icon size, the title bar dimensions, title bar logo and more. If users wish to leave the kiosk mode, they could tap on the corner of the homescreen and enter the kiosk exit password to release the device from kiosk mode.

Configure the peripheral settings

Configuring the peripheral settings would restrict user access to device settings and allow them to access only what is essential. This would only work if the device is either locked down in a single app or multi app kiosk. Some of the configurations include:

- Configuring Wi-Fi, flight mode and display
- Enabling lock task mode
- Permitting the UEM agent to grant permissions manually
- Access app catalogs in kiosk mode
- Configure application settings
- Allow users to add location notes
- Allow user to view messages sent by admin



Hexnode messenger

Hexnode's in-built kiosk messenger makes it easy for admins to communicate with end users even when the devices are locked down in a kiosk mode. As soon as the admin sends the message from the portal, the user would receive the message on their device as a pop up. It would be easy to distinguish between read and unread messages as the unread messages would be highlighted prompting the readers to check them out.

iOS

Configure website kiosk settings

Customize the website kiosk settings to make it more specific to your organization's needs. You can define the screen orientation to make it easier for users to navigate, enable web apps to use location services, configure browsing history settings, enforce private browsing, save and share webpages as pdfs and enable the navigation gesture to make it easier for users to return to the kiosk homescreen when the devices are locked in a multi app kiosk mode.

Windows

Kiosk exit

There are multiple ways in which you can exit the device from kiosk policy. You could either disassociate the policy from the device, archive it, or sign out the kiosk user.

4

The future of kiosks

According to a report by fortunebusinessinsights, retail and BFSI (Banking, Financial Services and Insurance) continue to contribute a major chunk of the global kiosk market share.

Moreover, the global interactive kiosk market share is predicted to be valued at USD 39.1 billion by 2027.

The kiosk landscape keeps growing at a rapid pace. Some of the technological advancement within the industry includes the enablement of autonomous AI to speedily execute various tasks, incorporation of Augmented and Virtual Reality, chatbots and speech recognition. Some of the factors contributing to this rise include emphasis on better customer experience, increased demand for self-service kiosk in banking and financial industry and advancement in touch screen displays.

Kiosks are predicted to have a bright future due to their adaptability across various industries and the ease with which users are able to use them.

Mitsogo Inc., Unites States (HQ), 111 Pine St #1225,
San Fransisco, CA 94111
Tel: Intl +1-415-636-7555, Fax: Intl +1-415-646-4151