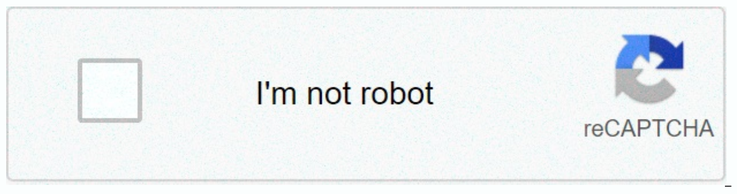

Continue

Guided access on samsung tablet

Android Guided Access is a security feature that allows users to pin their device screens to a single screen and control the features they're accessible to, similar to Apple's interactive approach. Although interactive access is created as an accessibility feature, it is also used to provide dedicated devices with the desired application. This is a common way to lock devices to be used as self-service kiosks, pos in self-service restaurants, digital signage, dedicated displays used for advertising, etc. When you turn on interactive access on your device, you can control specific device settings, such as volume buttons, sleep/wake button, touch, etc. After the interactive access session is over, you must enter the wizard passcode that was configured earlier at the beginning. This Android Guide contains the following: Interactive Access for Android Implementation of Interactive Access to Android using MDM Benefits Android Interactive Access Prerequisites for Enabling Interactive Access to Samsung and Android Devices How to Enable Interactive Access to Android and Samsung Devices? Interactive access for Android You can use a feature called Pin screen to restrict devices' access to specific apps for interactive access on Samsung and Android devices. Here you can set up a PIN, which you must enter whenever an app is disconnected or removed from the screen. Configuring screen pinning, the equivalent of interactive access on Android, on all devices in your organization means only manually turning on the feature on each device, followed by setting a password for each user. Also, as dedicated devices are widely used in industrials such as construction, healthcare, education and retail, deploying multiple devices with the required app and device limitations would be a lengthy task using interactive access in Samsung and Android devices. Implementing interactive access to Android using MDM interactive access for Android devices can be better implemented using Mobile Device Manager Plus, a comprehensive mobile device management solution. In Android Kiosk mode, devices (Samsung and non-Samsung) can be remotely controlled by the desired app (single app Kiosk) or a set of applications (multi-app Kiosk) and with advanced limitations to ensure better control over devices. One Kiosk app works much like Android Guided Access and ensures that your device is locked to only one specific app when you block access to the rest of your features and settings. For example, a device can be provided to a driver who is to be used only for navigation and is therefore provided with the Maps app. The rest of the device's functionality is limited. Benefits Interactive interactive access access on Android using Mobile Device Manager Plus provides organizations with various advantages, including: Deployment with ease Unlike Android Interactive Access, where devices must be manually locked to the desired application, MDM allows multiple Android device devices in the kiosk at once without problems. Since MDM provides bulk device registration using a variety of enrollment techniques to support BYOD, COPE, and COSU environments, the on-boarding process is fast and hassle free. This is particularly beneficial in large organizations with multiple departments and specific equipment requirements. Customize settings and limitations When devices are provided manually using Android Interactive Access, the user will also not be able to access basic settings such as Wi-Fi, Bluetooth, Brightness, etc., while MDM provides the means to configure these settings even when the devices are locked in kiosk mode. For example, the device is available in Kiosk with one app used for exams at school, and the student who uses the device wants to adjust the brightness. This can be achieved by turning on the Custom Settings app. Users may be allowed to view or modify certain settings configured for MDM. Restrictions can also be applied to Task Manager, status bar, physical buttons on the Kiosk to prevent the user from navigating outside the desired screen or resetting the device. These restrictions may be lifted as necessary from the MDM. Store and Enterprise support To manually allow Android access, apps must be manually installed on devices and supported only for Play Store apps, while use of MDM, Play Store apps, and organization-specific in-house apps can be quietly installed as Kiosk apps on your devices. System applications that are preinstalled with your device may also be available as Kiosk applications. Because MDM supports complete application lifecycle management directly from application installation, application update management, as well as application removal, the exhaustive process of manual application management is eliminated. In addition to applications, MdM supports the provision of specific web applications or websites in the kiosk that lock the device's access to specific URL content. Testing and deploying applications Because Kiosk's functionality is largely dependent on the application provided, MDM provides the ability to test the app on specific devices before deploying to device groups, eliminating security and productivity issues caused by errors. This includes testing app updates using beta. Remote troubleshooting Kiosk devices used for self-service purposes are mostly unattended. Device problems can usually be

downloaded or viewed on the device screen, allowing the user to access it. But in this case, troubleshooting can be difficult due to the absence of the user. Also the user, although present could be a contract employee who is not technically adept to rely on. To resolve the issue of device problems in these situations, MDM provides Remote access for Android devices, where problems on devices can be fixed without any user intervention. In addition, MDM supports remote chat, where security commands can be used to exit and re-enter the kiosk on your device, saving your organization time and costs. Secure devices and data As one application Kiosk devices are generally used by remote or contract employees, there is a high possibility that devices are lost or stolen. MDM provides a remote alarm feature that helps you load your device, as well as Geotracking to track it. Also, devices can be locked completely using Lost Mode. Security commands such as full wipe or corporate deletion can be initiated on the device if necessary. In addition, mobile devices can be easily carried out from organizational premises, which in most cases is not ideal, since the devices are intended for use only in the premises. To resolve these cases, virtual fences can be set up using Geofencing so that access to the device is blocked after it leaves the organization's premises or a specific area. Devices may also be preconfigured to erase all fencing leaving data if necessary. To implement interactive access for Android devices, register devices using MDM, add the app you want to the app repository, and add a Kiosk profile to your devices. Prerequisites for interactive access on Samsung and Android devices To enable interactive access on Samsung tablets, mobile devices, and other non-Samsung devices, make sure that the following prerequisites are met: Samsung devices and non-Samsung devices should be secured as the device owner. How do I enable interactive access on Android and Samsung devices? To allow interactive access on Android and Samsung devices using kiosk mode, follow the steps below: On your MDM console, click the Device Mgmt tab. Select profiles from the left pane and go to Create profile->Android. Enter the name and description of the profile, and then click Continue. In the left pane, select Kiosk. Now select one app (or Multi App Kiosk type if needed). On the Allowed Applications tab, type the name(s) of the application or volume IDs. Additionally, you can configure the wallpaper. Configure other device restrictions, custom settings, and advanced settings for your Kiosk profile. Then save and publish the profile. Go to Mgmt->Groups & Devices->Devices. Select the specific device on which to test profile functionality, and in the Action drop-down list, select Assign profile. Select the profile that was just created from the available options, and then click Select. The Kiosk profile is associated with the device, successfully implementing the equivalent of interactive access for Android. IOS Controlled Access Mode was introduced in iOS 6.0 and is used to help focus on one app when using your iOS device. This feature restricts iOS devices from running only one app. Interactive access can be used to achieve the following -. Restrict your iOS device to one App Disable hardware buttons Disable touch input on your device Disable device movement makes it easy to lock and use iOS devices as kios, dedicated displays, or digital signage. Controlled access mode for Android devices, surelock single-app mode is equivalent to iOS controlled access mode. However, with SureLock's single application mode, you can do much more. SureLock allows you to lock your device more securely and gives you more control over what the user can access. Introducing SureLock mode one app Locks your android device on just one app Hides the bottom navigation bar Prevents access to device settings and notifications password protected lockdown Single app mode settings in SureLock 1. Download and install SureLock on your Android 2 device. Access SureLock Admin Settings by tapping the SureLock screen 5 times in 3 seconds 3. When prompted for your administrator's surelock password, tap Go to Admin Settings 4. Tap Enabled apps and select the app you want in single app mode 5. Go to the surelock settings and enable single application mode. 6. Once done, the user will be prompted with a description of the mode of one application. In the row, tap OK. This starts single-app mode on your Android device. For details on setting up device in single-app mode, see Info. How to run other apps in single app mode To allow access to apps other than the main app, go to SureLock admin Settings > Enabled apps > select and allow another app to be accessible in single app mode > Tap the same app and check hide icon on start > Done. These steps will allow and hide the application from the SureLock home screen. However, the main application in single-app mode can run it. For example, you can enable the camera to run as a single application on the SureLock home screen and enable and hide Gallery, This will allow users to run the gallery on the device through the Camera app. Learn more about SureLock for Android. Try SureLock Android for free