MOKI MOBILE DEVICE MANAGEMENT

Moki Total Control - Android Enterprise

Moki
moki.com
425 Soledad St. Suite 250
San Antonio, TX 78205
USA

V 1.0 (September 2019)

TABLE OF CONTENTS

INTRODUCTION

OBJECTIVE

In addition to instructing Moki customers about how to perform basic administrative tasks, the primary purpose of this document is to educate customers about how Moki's Android Enterprise solution works. This document is tailored toward deployment, system and device managers, and other administrators who will be managing their organization's Android device deployments.

ACCOUNT ADMINISTRATION

LOGGING IN TO MOKI

- **https://app.moki.com**
- Moki strongly recommends using **Google Chrome** to access your Moki account.
- Moki uses Google to authenticate users. Invitations must be sent to a Google-based email address in order to login and access Moki. Moki does support Active Directory. If you are interested in configuring Active Directory for your account, Please contact Moki Support.

Before logging in to Moki for the first time, make sure you accept your Moki administrator invitation by following the link provided in your email. Every subsequent log in can be done at **https://app.moki.com** in your web browser. Once logged in, you will need to configure your Moki account with Google so that you can begin using Android Enterprise. Instructions on how to do that are below.

CONFIGURE YOUR ANDROID ENTERPRISE ACCOUNT

Before you will have access to Android Enterprise, you will need to configure your account with Google. To do this, log in to your Moki account, and select your account name in the upper right-hand corner. Then, select the “Account Settings” option from the drop-down menu. Once the page loads, select the gray box that says “Setup Android Enterprise.” You will see a prompt telling you that you will be redirected to Google and then back to Moki once you are finished. Select “Yes” to agree. Once the Google Play page loads, select “Get Started”. On the next page, enter your business name, select Moki as your EMM provider, and click “Next.” Next, enter company contact information (optional), click the box to agree to the

Managed Google Play Agreement, and select "Confirm." Finally, select the blue box to "Complete Registration." If you have successfully completed the Android Enterprise configuration, you will now be redirected to Moki.
Note: you must be logged in to a Gmail email address to configure Android Enterprise. G Suite email accounts are not supported. If you reach a page that says that you need to sign in to another account, select the Google account logo in the top right-hand side of the page, and select "Add Account." Once you sign in to a Gmail account, you will be able to complete the configuration.

Now that you have configured your Android Enterprise settings, you will need to select the Android icon in the top right-hand corner of the screen and switch it to the Android Enterprise icon. This will allow you to manage Android Enterprise devices. You should now be able to see the following tabs (these tabs will be covered in detail below):

- **Devices:** Provides you a list of all of your devices, gives you the ability to manage them individually and provides useful information specific to each device.
- **Apps:** Allows users to assign Google Play applications, custom applications (.apks), and web apps to their accounts which can then be deployed to devices.
- **Policies:** Gives customers granular control over each device including, device settings, application settings, administrative settings, and more.

ADDING USERS

This is a very simple process consisting of the following steps:

1. Click on your account name in the upper right-hand corner of Moki Total Control and then select "Users."
2. On the next page, you can see the list of current users as well as users with pending invitations.
3. To create a new user, click on the plus icon, and fill out the form.
4. Choose a user role, such as Admin, Standard, View Only, or any of your custom created roles. **Note: Version 1.0 of Android Enterprise does not currently enforce user roles or permission levels. These features will be supported in later versions. These user roles and permission levels are still supported in the Device Admin version of Moki Total Control.**
5. Users will be activated once they have clicked the link provided in the invitation email and once they have accepted the terms and conditions.

MODIFY EXISTING USERS

If you need to modify or delete a user account, do one of the following:

- **Edit account:** Click on the pencil icon to bring up the user account editing interface, make needed changes, and save.
- **Delete account:** Click on trash can icon and confirm your choice.

DEVICE ENROLLMENT

Before you can enroll a device, you will need to create and configure an Android Policy that will be applied to a device once it enrolls. The “Policies” tab will be covered in detail below. In addition, if you would like to install and manage third-party applications, either from the Google Play Store or Private Apps that you upload, you will need to configure those before you add them to a new policy. In the enrollment example below, we’ll assume that a policy has already been created, that apps have been assigned via the “Apps” tab, and that these apps have been added to your policy settings and configured appropriately.

ENROLL DEVICES

QR CODE ENROLLMENT

1. Once you are logged in to your account, select the “Devices” tab.
2. Once there, select the “+ Enroll Device” button towards the upper right-hand side of the “Devices” tab.
3. On the “Device Enrollment Token” page, select the duration of the token, the policy that you would like to apply, if the enrollment is a single-use enrollment or not, then select “Generate Token.”
4. You will now see a QR Code and an Enrollment Code.

Now, on your Android Device, you will need to do the following (all devices will need to be on the initial start-up page that says, “Welcome.” If a device has been previously configured, it will need to be factory reset):

1. Physically click the screen six times until you see the “QR Code Setup” option page.
2. Select “Next.”
3. The device will need to be connected to the internet; it will then check for updates, install a QR reader application (if needed), etc.
4. Once the device finishes updating, the camera will turn on, and you will be prompted to scan the QR code that you generated in Moki. Please do so now.

5. Once the QR code has been scanned, go through the registration prompts to finalize the enrollment process. Note: it may take a few minutes for the device to update, install an updated version of Google Play services, download, and update apps, apply policies, etc.
6. Once your device either shows your desktop or opens to your selected application (depending on policy settings), you are done, and your device has successfully been enrolled to Moki. You should now see your device listed on the "Devices" tab in your Moki account.

DPC IDENTIFIER ENROLLMENT

With Moki, customers do not need to install an Android Enterprise management application from the Google Play Store as the provisioning process is now handled 100% by Google.

1. Once you are logged in to your Moki account, select the "Devices" tab.
2. Once there, select the "+ Enroll Device" button towards the upper right-hand side of the "Devices" tab.
3. On the "Device Enrollment Token" page, select the duration of the token, the policy that you would like to apply, if the enrollment is a single-use enrollment or not, then select "Generate Token."
4. You will now see a QR Code and an Enrollment Code.

Now, on your Android Device, you will need to do the following (all devices will need to be on the initial start-up page that says, "Welcome." If a device has been previously configured, it will need to be factory reset):

1. Follow the setup wizard process.
2. Enter Wi-Fi login details to connect the device to the internet.
3. When prompted to sign in on the Google Account page, enter **afw#setup**, which downloads Android Device Policy.
4. Manually enter the enrollment code that you generated in Moki.
5. Once the enrollment code has been entered, go through the registration prompts to finalize the enrollment process. Note: it may take a few minutes for the device to update, install an updated version of Google Play services, download, and update apps, apply policies, etc.
6. Once your device either shows your desktop or opens to your selected application (depending on policy settings), you are done, and your device has successfully been enrolled to Moki. You should now see your device listed on the "Devices" tab in your Moki account.

ACCOUNT NAVIGATION

DEVICES TAB

The Devices tab gives you the ability to manage individual devices.

DEVICE INFORMATION

When you select a device on the Devices tab, a window will slide over from the right, and you will be able to see specific information unique to this device, such as device information (battery %, Network Status, etc.), currently applied policies, installed applications, etc. You will also have the ability to perform Commands to this device. Each one of these tabs will be covered in detail below.

CUSTOMIZING YOUR VIEW

One convenient feature of the Moki user interface is that you can choose to arrange the columns in your device list view according to those elements that are most important to you. You can customize this view by selecting the three stacked lines (often referred to as the hamburger icon) in the top right-hand corner of the device list. You can choose to view the following items:

- **Device ID:** This is a unique, alphanumeric code generated for your Android devices. This code identifies your device similar to how IMEI number works.
- **Nickname:** This is a Moki feature that allows you to customize the name of your device on the dashboard to whatever name you'd like. Some examples of nicknames include; a unique company generated identifier, the device's serial number, the store ID where the device is located, an employee ID that the device is assigned to, etc.
- **Battery:** This is a battery indicator showing the current battery percentage.
- **State:** This will show the current status of the managed device (Active, Deleted, etc.).
- **Applied State:** This will show the status of the device which you last applied
- **Policy Compliant:** This will either show as True or False to let you know if your applied policy is currently being enforced on the device and if the device is in compliance.
- **Enrollment Time:** This will provide you with the exact day and time that your device was enrolled to Moki.
- **Last Status Report:** This will provide you with an exact date and time that your device last updated its status and device information.
- **Policy Name:** This is the name of the policy that is currently applied to your device.

- **Last Policy Sync:** This is the exact date and time that your policy was last applied to your device.
- **Applied Policy:** This will show you the name of the policy that you last applied to your device. Once the device picks up the change, it will show the name of the new policy under the “Policy Name.”
- **Applied Policy Version:** This will show you the currently applied version number of the policy currently on the device. Every change you make to a policy increases the number by a factor of 1.

When you make a change to your device list view, those changes are saved as part of your user profile and will remain the same every time you log in to your account.

DEVICE TABS

The following three sections will cover the three tabs found in the window when you select a device located on the “Devices” tab.

DETAILS TAB

In this tab, you can:

- **Edit the device’s nickname**: Rename your device by clicking on the title, typing or pasting the name, and then by clicking the “enter” key on your keyboard or by clicking on the check button in Moki.
- **Assigned Policy:** Here, you can see the currently applied policy installed on the device. To install a different policy, select the name of the policy from the drop-down menu.
- **Device Settings:** Here, you can see settings applied to the device that you configured when you created your policy.
- **Hardware:** Here, you will find the hardware information for the selected device (manufacturer, model number, serial number, etc.).
- **Software**: Here, you will find the software information for the selected device (Android build number, Android OS version, etc.).
- **Network Information**: Here you will find details about the device’s network connection.

INVENTORY

The inventory tab lists your device’s installed applications. You can filter the application list to find the exact application you need. You can also see details about your apps, including version and package name by expanding the application.

COMMANDS

Here you can view manually requested commands pushed to your device, including the time requested and whether or not the command completed.

ACTIONS BAR

COMMAND

Each device has a Commands drop-down menu that allows you to apply commands to your devices. Here are the currently supported commands:

- **Lock:** This command allows you to sleep/lock the screen on your device.
- **Reboot:** This command allows you to reboot your device.
- **Reset Password:** This command allows you clear out the current password set on the device. You will need to create a new password in a policy to reset it to something else.

Once you have completed the command, you can select the "Commands" tab to the right of the device to see whether or not the action was applied successfully. **Note: commands can be canceled from this tab as well as long as you terminate the command before the device picks it up.**

DELETE DEVICE

The trash can will allow you to remove unwanted or unused devices from your Moki account. **Please Note: by selecting the trash can icon to delete your device, your device will be factory reset.**

APPS TAB

The Apps tab allows you to add published (Google Play Store) and private applications to your account, which can then be added to your policies and ultimately, deployed to your devices.

ACTIONS BAR

REFRESH APPS

This button will refresh your apps list after you add or remove applications.

ADD APPS

This button will allow you to add Android applications to your account. There are three app options available in Android Enterprise. These options are found by hovering over the icons to the right of the "Managed Google Play Applications" window. Here are the details for each option:

- **Search Play Store:** This will allow you to search for applications published to the Google Play Store. Select the "Search Play Store" option on the left-hand side of the Google Play window. Then, type the name of the desired application in the search bar, press enter on your keyboard or click the blue search button. Once you locate the application you'd wish to use, click the

app to open it, then click the green “Select” button. You should see a blue confirmation window in the top right-hand corner of the screen that says “Success. Selected app request sent.” You can continue to search and add additional applications. Once you are finished adding applications, you can close the window by selecting the X in the top right-hand corner or by clicking outside of the window. You should now see your selected applications listed in on the apps list. You may need to click the refresh button to update your app list. **Note: if you are not signed in to a Gmail account, the above process will not work, and you will be directed away from Moki when performing a search. To fix this, simply sign in to your Gmail account and try your search again.**

- **Private Apps:** This option will allow you to upload your own applications in .apk format. To do this, select the “Private Apps” option from the left-hand side of the Google Play window. Then select the + icon on the bottom right-hand side of the window. Note: you might need to scroll down to see it. On the next page, name your application and upload it. Lastly, click the blue “Create” button. Note: you might need to scroll to the right to see it. You will be prompted to enter your email address so that Google can contact you if needed. If you were successful, you will now see the application listed on the Apps list. **Note: in order to use this function, Google requires that your application be zip aligned. Your Android developers should be able to take care of that for you and provide you with an application that is compatible.**
- **Web Apps: NOT YET SUPPORTED IN V1 OF MOKI’S ANDROID ENTERPRISE SOLUTION.** This option will allow you to display an application that opens directly to a website or a web application. To do this, select the “Web Apps” option from the left-hand side of the Google Play window. Then select the + icon on the bottom right-hand side of the window. Note: you might need to scroll down to see it. Configure your web app settings, including a custom icon and title. Lastly, click the blue “Create” button. Note: you might need to scroll to the right to see it. After a few minutes, your newly created web app will appear in the Web App window.
- **Organize Apps:** This option will allow you to create a collection of apps that you can use on your devices. You can organize the applications by folders and arrange the order of the applications.

DELETE APP

This button will allow you to remove unwanted applications from your apps list. Simply select the application that you want to remove and click the trash can icon.

ADD CONFIGURATION

Some applications, like email, web browser, phone, messaging, etc. allow you to customize in-app settings. These settings can be configured by selecting the application in the apps list and then by clicking the “Add Configuration” button. Once you have configured your applications, select “Save” at the bottom of the page.

POLICIES TAB

Policies provide a way to control individual settings and configurations on your Android devices.

CREATING A POLICY

1. Once you are logged in to your Moki account, select the “Policies” tab.
2. When the page loads, select the green “+ New Policy” button.
3. Configure your policy to meet your requirements or needs (a detailed explanation of each policy setting is available below).
4. Select “Save” in the top right-hand side of the page once you are finished.

CHANGE A POLICY

1. Once you are logged in to your Moki account, select the “Policies” tab.
2. When the page loads, select the policy that you would like to change from the policy list on the right side of the screen.
3. Make the necessary changes to your policy to meet your requirements or needs (a detailed explanation of each policy setting is available below).
4. Select “Save” in the top right-hand side of the page once you are finished.
   Note: when you make a change to a policy, those changes will automatically apply to all devices that currently have that policy assigned.

DELETE A POLICY

1. Once you are logged in to your Moki account, select the “Policies” tab.
2. When the page loads, select the policy that you would like to delete from the policy list on the right side of the screen.
3. Once the policy is selected, click the “Delete” button in the upper right-hand corner of the screen and confirm your selection.
   Note: before you can delete a policy, the policy must be removed from all of your devices by assigning a different policy to each device. That

can be done by selecting the device on the "Devices" tab, and by selecting a different policy from the "Assigned Policy" drop-down menu.

POLICY CONFIGURATIONS

There are a lot of different settings and configurations that you can apply, and the following six sections will explain all of the policy options available:

GENERAL SETTINGS

The general settings section of Android Enterprise policies allows you to configure things like the device's settings. The following items can be configured (if an explanation is needed, it will be included):

- **Version:** This is show the version number of the policy. Every change you make to a policy, increases the number by a factor of 1.
- **Default Permission Policy:** This setting defines the default permission policy for requests for runtime permissions. The possible values include:
    - **Default:** If the policy is left blank, it will use the default device setting.
    - **Prompt:** Users are prompted to approve the permission.
    - **Grant:** Permissions are automatically granted.
    - **Deny:** Permissions are automatically denied.
- **Location Mode:** This setting allows you to select the permission policy for location services. The possible values include:
    - **Default:** If the policy is left blank, it will use the default device setting.
    - **High Accuracy:** GPS is turned on and set to the most accurate setting.
    - **Sensors Only:** This will activate the GPS only and will not utilize network-provided location.
    - **Battery Saving:** This will limit the update frequency of the GPS to save battery.
    - **Off:** GPS and location tracking will be turned off.
- **App Auto Update Policy:** This setting controls when automatic app updates can be applied. The possible values include:
    - **Default:** If the policy is left blank, it will use the default device setting.
    - **User Choice:** The end user can control auto-updates.
    - **Never:** Apps are never updated.
    - **WiFi Only:** Apps are auto-updated over Wi-Fi only.
    - **Always:** Apps are auto-updated at any time. Data charges may apply.
- **Encryption Policy:** This setting allows you to create and enforce an encryption policy on the device for internal and external storage. The possible values include:

    - **Default:** If the policy is left blank, it will use the default device setting.
    - **Enable Without Password**
    - **Enable With Password**
- **Play Store Mode:** This setting will allow you to whitelist and blacklist applications installed on the device. The possible values include:
    - **Default:** If the policy is left blank, it will default to **Whitelist.**
    - **Whitelist:** Only apps that are in the policy are available and any app not in the policy will be automatically uninstalled from the device.
    - **Blacklist:** All apps are available and any app that should not be on the device should be explicitly marked as 'Blocked' in the applications policy.
- **Screen Capture Disabled**
- **Camera Disabled**
- **Add User Disabled**
- **Adjust Volume Disabled**
- **Factory Reset Disabled**
- **Install App Disabled**
- **Mount Physical Media Disabled:** Users will not be able to use external media devices such as SD card or USB storage.
- **Modify Accounts Disabled**
- **Safe Boot Disabled**
- **Uninstall Apps Disabled**
- **Keyguard Disabled:** This setting will disable the device's lock screen password requirements, allowing the device to auto-launch into an application.
- **Bluetooth Contact Sharing Disabled**
- **Bluetooth Config Disabled**
- **Cell Broadcasts Config Disabled**
- **Credentials Config Disabled**
- **Mobile Networks Config Disabled**
- **Tethering Config Disabled**
- **VPN Config Disabled**
- **Create Windows Disabled:** This setting will prevent a window from being created and launched when users use multi-window.
- **Network Reset Disabled**
- **Outgoing Beam Disabled:** This setting will disable users from using NFC to beam out data from applications.
- **Outgoing Calls Disabled**
- **Remove User Disabled**

- **Share Location Disabled**
- **SMS Disabled**
- **Unmute Microphone Disabled**
- **USB File Transfer Disabled**
- **Ensure Verify Apps Enabled:** This setting scans apps installed on devices for malware before and after they are installed, helping to ensure that corporate data can't be compromised by malicious apps.
- **Set User Icon Disabled:** This setting will prevent end users from changing or setting their user icon of the device.
- **Set Wallpaper Disabled**
- **Data Roaming Disabled**
- **Network Escape Hatch Enabled**: This setting will enable the escape hatch feature on your device. If a network connection is not established when a device boots, then the escape hatch asks to temporarily connect to a network and refresh the device policy. After applying the policy, the temporary network is forgotten and the device continues booting. This feature connects devices to a network if one of the following criteria are met:
    - There is not a suitable network in the last policy.
    - The device boots into an app in lock task mode.
    - The user is unable to reach the device settings.
- **Bluetooth Disabled**
- **Install From Unknown Sources Allowed**
- **Debugging Features Allowed**
- **Fun Disabled:** Controls whether the Easter egg game in Settings is disabled.
- **Auto Time Required:** This setting will prevent end users from manually setting the date and time.
- **Kiosk Custom Launcher Enabled:** This setting replaces the home screen with a launcher that locks down the device to the apps installed via the applications setting. Apps appear on a single page in alphabetical order. The status bar is disabled when this is set. **Note: applications configured via the "Application Control" section of this profile cannot be set to "Kiosk" under "Install Type" or the policy will fail to install.**
- **Skip First Use Hints Enabled:** This setting can enable the system recommendation for apps to skip their user tutorial and other introductory hints on first start-up.
- **Private Key Selection Enabled:** This setting allows showing UI on a device for an end user to choose a private key alias if there are no matching rules configured.

REPORTING SETTINGS

The following settings control the behavior of application reports. Note: battery percentage and some other reports will not be displayed in Moki unless they are enabled here.

- **Application Reports Enabled:** This setting will allow reports to be generated, which show details of apps installed on the device.
- **Device Settings Enabled:** This setting enables reporting information about security-related device settings on devices.
- **Software Info Enabled:** This setting enables reporting of device software.
- **Network Info Enabled:** This setting enables reporting of device network information.
- **Power Management Events Enabled:** This setting enables reporting of power management events.
- **Hardware Status Enabled:** This setting enables hardware reporting to capture device hardware information.

APPLICATION CONTROL

Application control allows you to limit application access on your devices. Before you can figure the policy, all applications that you would like to manage will need to be added to the "Apps" tab first. Once you have added all of your applications to the Apps tab, select the + on the "Add policy for an individual app" bar. Now, under the "General" section, you will configure what applications will do on your devices. The following options are configurable:

- **App:** Select your application from the available list of apps.
- **Install Type:**
    - **Default:** Unspecified. Defaults to Available.
    - **Pre-Installed:** The app is automatically installed and can be removed by the user.
    - **Force Installed:** The app is automatically installed and cannot be removed by the user.
    - **Blocked:** The app is blocked and cannot be installed. If the app was installed under a previous policy, it will be uninstalled.
    - **Available:** The app is available to install.
    - **Required For Setup:** The app is automatically installed and cannot be removed by the user and will prevent setup from completion until installation is complete.
    - **Kiosk:** The app is automatically installed in kiosk mode: it is set as the

preferred home intent and whitelisted for lock task mode. Device setup won't complete until the app is installed. After installation, users will not be able to remove the app. You can only set this Install Type for one app per policy. When this is present in the policy, status bar will be automatically disabled.

- **Managed Config:** If you have an app configuration created, you can select it from this drop-down menu.
- **Permissions:** Default Permission Policy
    - **Default:** If no policy is specified for a permission at any level, then the prompt behavior is used by default.
    - **Prompt:** Will prompt the end user to grant permissions.
    - **Grant:** Will automatically grant permissions.
    - **Deny:** Will automatically deny permissions.

Note: you can also grant permission for specific requests by selecting the + icon under "Grants." You can then select the permission and the policy for each individual permission.

PASSWORD REQUIREMENTS

This section will cover the optional requirements that you can use to unlock a device. The following password requirement options are available:

- **Quality:** The required password quality.
    - **Default:** There are no password requirements.
    - **Biometric Weak:** The device must be secured with a low-security biometric recognition technology, at minimum. This includes technologies that can recognize the identity of an individual that are roughly equivalent to a 3-digit PIN (false detection is less than 1 in 1,000).
    - **Something:** A password is required, but there are no restrictions on what the password must contain.
    - **Numeric:** The password must contain numeric characters.
    - **Numeric Complex:** The password must contain numeric characters with no repeating (4444) or ordered (1234, 4321, 2468) sequences.
    - **Alphabetic:** The password must contain alphabetic (or symbol) characters.
    - **Alphanumeric:** The password must contain both numeric and alphabetic (or symbol) characters.
    - **Complex:** The password must meet the minimum requirements specified in password Minimum Length, password Minimum Letters, password Minimum Symbols, etc

- **Minimum Length:** The minimum allowed password length. A value of 0 means there is no restriction. Only enforced when password Quality is Numeric, Numeric Complex, Alphabetic, Alphanumeric, or Complex.
- **History Length:** The length of the password history. After setting this field, the user will not be able to enter a new password that is the same as any password in the history. A value of 0 means there is no restriction.
- **Maximum Failed Passwords For Wipe:** Number of incorrect device-unlock passwords that can be entered before a device is wiped. A value of 0 means there is no restriction.
- **Expiration Timeout:** Password expiration timeout. Duration in days.

SYSTEM UPDATES

The type of system update configuration.

- **Default:** Follow the default update behavior for the device, which typically requires the user to accept system updates.
- **Automatic:** Install automatically as soon as an update is available.
- **Windowed:** Install automatically within a daily maintenance window. This also configures Play apps to be updated within the window. **This is strongly recommended for kiosk devices because this is the only way apps persistently pinned to the foreground can be updated by the Google Play Store.**
- **Postpone:** Postpone automatic install up to a maximum of 30 days.

ENFORCEMENT RULES

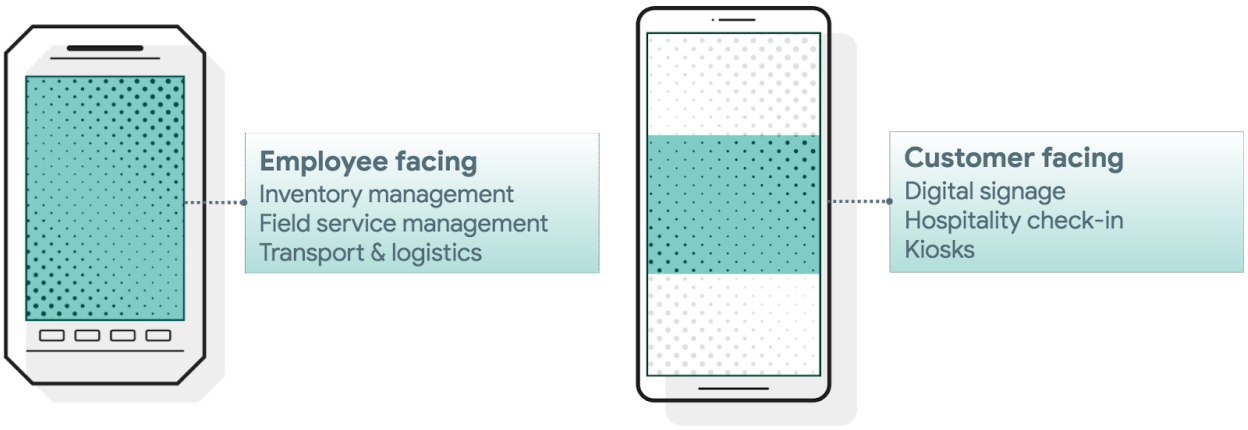
A rule that defines the actions to take if a device or work profile is not compliant with the policy specified in setting name.

- **Setting Name:** The top-level policy to enforce. Define the actions to take if a device is not compliant with the specified setting. The following options are available:
  - **Application Policies**
  - **Password Policies**
  - **Encryption Policies**
- **Block After Days:** Number of days the policy is non-compliant before the device is blocked. To block access immediately, set to 0. Block After Days must be less than Wipe After Days.
- Wipe After Days: Number of days the policy is non-compliant before the device is wiped. Wipe After Days must be greater than Block After Days.
- **Preserve Data:** Whether the factory-reset protection data is preserved on the device.

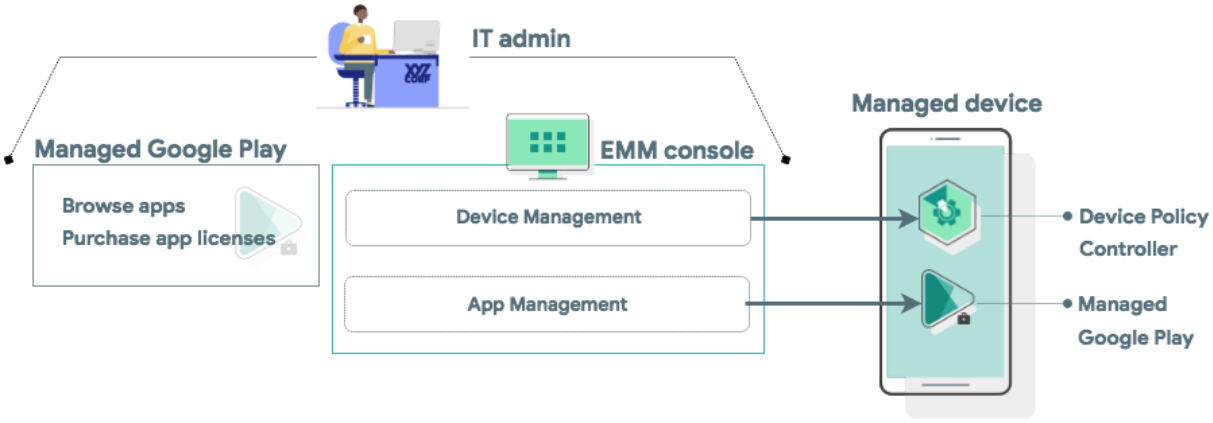
HOW MOKI'S ANDROID ENTERPRISE SOLUTION WORKS

Android Enterprise is a Google-led initiative to enable the use of Android devices and apps in the workplace. The program offers APIs and other tools for developers to integrate support for Android into their enterprise mobility management (EMM) or mobile device management (MDM) solutions.

There are three use cases supported on Android Enterprise. Moki's Android Enterprise solution was built to manage company-owned devices for dedicated use. Dedicated devices are a subset of company-owned devices that serve a specific purpose. Android comes with a broad set of management features that allow organizations to configure devices for everything from employee-facing factory and industrial environments, to customer-facing signage and kiosk purposes. Dedicated devices are typically locked to a single app or set of apps. Android 6.0+ offers granular control over a device's lock screen, status bar, keyboard, and other key features, to prevent users from enabling other apps or performing other actions on dedicated devices.



An Android Enterprise solution is a combination of three components: your Moki Total Control console, a device policy controller (DPC), and managed Google Play.



Moki's MDM Console

Moki's MDM console is a cloud-based web application that allows admins to manage their organization, devices, and apps. Moki's console has been integrated with the APIs and UI components provided by Android Enterprise.

DPC

All Android devices that Moki manages use Android's DPC. A DPC is an agent that applies the management policies set in your Moki console to devices.

Managed Google Play

Managed Google Play is an enterprise app platform based on Google Play that is free to Android Enterprise customers and fully integrated into Moki's MDM console. It combines the familiar user experience and app store features of Google Play with a set of management capabilities designed specifically for enterprises.

IT admins can use managed Google Play to discover apps, view app details, and purchase app licenses. IT admins can curate, manage, and distribute apps through Moki's MDM console.

Using Android Enterprise APIs, Moki can distribute apps to managed devices. Apps can be remotely installed on a device or added to the device's managed Google Play store.

On managed devices, managed Google Play is the user's enterprise app store. The interface is similar to Google Play—users can browse apps, view app details, and install them. Unlike the public version of Google Play, users can only install apps from managed Google Play that are whitelisted for them.

CHANGE HISTORY

Version	Date	Change Description
1.0 AE ALPHA	September 1, 2019	Alpha version of Moki's Android Enterprise solution. V1.0 covers account basics, the Devices tab, Apps tab, and Polices tab.