Ensemble
powered by Conversa Solutions

FEATURES

FEATURE	ANDROID VERSION	DESCRIPTION
DEVICE PROVISIONING		
DPC-First Profile Provisioning	5.1+	End users can provision a work profile after downloading their EMM's DPC from Google Play.
QR Code Device Provisioning	7.0+	IT admins can use new or factory-reset device to scan a QR code generated by the EMM's console to provision the device, according implementation guidelines defined in the Android Management API developer documentation.
Zero-touch Enrollment	8.0+	IT admins can preconfigure devices purchased from authorized resellers and manage them using your EMM console.
KME Enrollment	7.0+	IT admins can preconfigure Samsung devices purchased from authorized resellers and manage them using our EMM console.
KIOSK MODE		
Single App Kiosk	6.0+	IT admins can lock the device down to one application.
Multi-App Kiosk	6.0+	IT admins can lock the device down to one or more customizable landing pages with shortcuts to applications, content, or web bookmarks.
Whitelist Kiosk Apps	6.0+	IT admins can whitelist additional applications that need to be opened while in kiosk mode. This is useful when a custom app launcher is being used.
Exit Pin	6.0+	It admins can set a PIN that must be entered before being able to exit the kiosked screen.
Enable Global Actions Dialog	9.0+	IT admins can control whether or not global action dialogs (i.e. power menu) can be displayed while in kiosk mode.
Enable System Info	9.0+	IT admins can choose to display the status bar while in kiosk mode (i.e. battery life, Wi-Fi connection etc)
Enable Keyguard	9.0+	IT admins can choose whether or not a device security challenge (e.g. PIN/pattern/password) can be used during kiosk mode.
Enable Home Button	9.0+	IT admins can choose to enable the home button. Pressing it will return the user to the Ensemble landing page.
Enable Overview Button	9.0+	IT admins can choose to enable the overview button which allows the user to view recent applications or applications that are still running.
Enable Notifications	9.0+	IT admins can choose to enable the notification shade. This is a modified version of the full notification shade that does not include the quick actions or a way to enter the settings menu.
Show Date	6.0+	IT admins can choose to display the current time and date on the Ensemble landing page.
Show Action Bar	6.0+	IT admins can choose to display the action bar. If this is not enabled, the IT admin must add a settings shortcut to the home page to have access to the Ensemble menu.
Font Color	6.0+	IT admins can control the color of the font on the Ensemble multi-kiosk pages.
Wallpaper	6.0+	IT admins can control the wallpaper image on the Ensemble multi-kiosk page.
Screen Orientation	6.0+	IT admins can control the orientation of the device while in kiosk mode. This will not affect any applications that are launched while in kiosk mode.
Wallpaper Scale Type	6.0+	IT admins can control how the wallpaper images scales to fit the screen.
Custom Shortcuts	6.0+	IT admins can add shortcuts to the Ensemble mulit-kiosk pages. These can be icons to open applications, content, bookmarks, folders or Ensemble settings menu. The label, font color, icon and icon color can all be customized.
Screen on while plugged in	6.0+	IT admins can force the device screen to remain on while the device is plugged in.
DEVICE SECURITY		
Device Security Challenge	5.0+	IT admins can set and enforce a device security challenge (e.g. PIN/pattern/password) of a certain type and complexity on managed devices.
Work Security Challenge	7.0+	IT admins can use the EMM's console to remotely lock and wipe work data from a managed device.
Advanced Passcode Management	5.0+	The EMM restricts access to work data and apps on devices that are not in compliance with security policies.
Smart Lock Management	6.0+	EMMs must enforce the specified security policies on devices by default, without requiring IT admins to configure or customize any settings in the EMM's console.
Wipe & Lock	5.0+	The EMM uses the SafetyNet Attestation API to ensure devices are valid Android devices.
Compliance Enforcement	5.0+	IT admins can set and enforce a device security challenge (e.g. PIN/pattern/password) of a certain type and complexity on managed devices.
Default Security Policies	5.0+	IT admins can use the EMM's console to remotely lock and wipe work data from a managed device.
Safe Boot	6.0+	The EMM restricts access to work data and apps on devices that are not in compliance with security policies.
SafetyNet Support	NA	EMMs must enforce the specified security policies on devices by default, without requiring IT admins to configure or customize any settings in the EMM's console.
Verify Apps Enforcement	5.0+	The EMM uses the SafetyNet Attestation API to ensure devices are valid Android devices.
Direct Boot Support	7.0+	The EMM restricts access to work data and apps on devices that are not in compliance with security policies.
Hardware Security Management	5.1+	EMMs must enforce the specified security policies on devices by default, without requiring IT admins to configure or customize any settings in the EMM's console.
Enterprise Security Logging	7.0+	The EMM uses the SafetyNet Attestation API to ensure devices are valid Android devices.
Suspend applications if device is not compliant	6.0+	IT admins can setup a list of applications to suspend if the device has a pending security patch to install. The app cannot be used until the device OS has been patched.
Device suspension	6.0+	IT admins can setup suspension criteria or send a suspension command to lock down the device to a single screen with custom branding, a custom message and a custom service number.
ACCOUNT & APP MANAGEMENT		
Managed google play accounts enterprise enrollment	NA	IT admins can create a managed Google Play Accounts enterprise—an entity that allows managed Google Play to distribute apps to devices.
Managed google play account provisioning	5.0+	The EMM can silently provision enterprise user accounts, called managed Google Play accounts.
Silent app distribution	NA	IT admins can silently distribute work apps on users' devices without any user interaction.
Managed configuration management	5.0+	IT admins can view and silently set managed configurations for any app that supports managed configurations.
App catalog management	NA	IT admins can import a list of all the apps approved for their enterprise from managed Google Play (play.google.com/work).
Programmatic app approval	NA	The EMM's console uses the managed Google Play iframe to support Google Play's app discovery and approval capabilities.
Basic store layout management	NA	End users can use the managed Google Play store app on their device to install and update work apps.
Google-hosted private app management	NA	IT admins can update Google-hosted private apps through the EMM console instead of through the Google Play console.
Self-hosted private app management	NA	IT admins can configure and publish self-hosted private apps.
Clear App Data	9.0+	The EMM can clear app data either on reboot or by remote command.
Managed Google Play Accounts G-Suite Enrollment	NA	IT admins can use their existing G-Suite account to link their managed applications to Ensemble.
Block Applications	6.0+	IT admins can create a list of packages to disable. The user will not be able to open those applications.
Device Application Information	NA	Devices report all currently installed applications to the Ensemble management console. This allows IT admins to update or uninstall applications.
DEVICE MANAGEMENT		
Runtime permission policy management	6.0+	IT admins can silently set a default response to all runtime permission requests made by work apps.
Runtime permission grant state management	6.0+	After setting a default runtime permission policy, IT admins can silently set responses for specific permissions from any work app built on API 23 or above.
Device tracking	NA	IT admins have the capability of tracking a specific device with multiple variations of accuracy.
Wi-Fi configuration management	6.0+	IT admins can silently provision enterprise Wi-Fi configurations on managed devices.
Account Management	5.0+	IT admins can ensure that only authorized corporate accounts can be added to the device.
G Suite Account Management	5.0+	IT admins can ensure that only authorized G Suite accounts can interact with corporate data.
Certificate Management	5.0+	Allows IT admins to deploy identity certificates and certificate authorities to devices to enable access to corporate resources.
Advanced VPN Management	7.0+	Allows IT admins to specify an Always On VPN to ensure that data from specified managed apps will always go through a configured VPN.
Location Sharing Management	5.0+	IT admins can prevent users from sharing location data with apps in the work profile.
Advanced Location Sharing Management	5.0+	IT admins can enforce a given location sharing setting on a managed device. (i.e. High accuracy. Sensors only, for instance GPS, but not including network-provided location. Battery saving, which limits the update frequency or Off)
Factory Reset Protection Management	5.1+	Enables IT admins to protect company-owned devices from theft by ensuring only authorized users can factory reset devices.
Advanced App Control	5.0+	IT admins can prevent the user from uninstalling or otherwise modifying managed apps through Settings, for instance force closing the app or clearing an app's data cache.
Screen Capture Management	5.0+	IT admins can block users from taking screenshots when using managed apps.
Disable Cameras	5.0+	IT admins can disable use of device cameras by managed apps.
Network Statistics Collection	6.0+	IT admins can query network usage statistics from a device's work profile.
Reboot Device	7.0+	IT admins can remotely reboot managed devices.
System Radio Management	7.0+	IT admins can control system network radios. (Disable cell broadcasts, prevent user from modifying mobile network settings, prevent user from resetting all network settings, allow data roaming, prevent calls, prevent SMS, disable tethering, prevent
System Audio Management	5.0+	IT admins can silently control device audio features, including muting the device, preventing users from adjusting volume settings, and preventing users from unmuting the device microphone.
System Clock Management	5.0+	IT admins can control device clock and time zone settings and prevent users from modifying automatic device settings.
Advanced VPN Management	7.0+	Allows IT admins to specify an Always On VPN to ensure that the data from specified managed apps will always go through a set up Virtual Private Network (VPN). Note: this feature requires deploying a VPN client that supports both Always On and
Contact Management	6.0+	IT admins can load a list of phone book contacts to the device including phone or email addresses.
Network Usage	6.0+	IT admins can ping devices to retrieve their network usage over a selected timeframe.
DEVICE USABILITY		
Managed provisioning customization	7.0+	IT admins can modify the default managed provisioning flow UX to include enterprise-specific features.
Enterprise customization	7.0+	IT admins can customize aspects of the work profile with corporate branding, for instance by setting the work profile user icon to the corporate logo or configuring the background color of the work challenge.
Lock screen messages	7.0+	IT admins can set a custom message that is always displayed on the device lock screen and does not require device unlock to be viewed.
Policy transparency management	7.0+	IT admins can customize the help text provided to users when they attempt to modify managed settings on their device or deploy an EMM-supplied generic support message.
Cross-profile contact management	7.0+	IT admins can control what contact data can leave the work profile.
Cross-profile data management	6.0+	Grants IT admins control over what data can leave the work profile, beyond the default security features of the work profile.
System update policy	6.0+	IT admins can configure and apply over-the-air (OTA) system updates for devices.
Keyguard feature management	7.0+	IT admins can control the features available to users before unlocking the device keyguard (lock screen) and the work challenge keyguard (lock screen).
MAC address retrieval	7.0+	Fetch device's MAC address
Schedule Ensemble Check-In	NA	IT admins can set a timeframe during which the devices on the project will check-in to the Ensemble servers during a 24hr period.
Device Notes	NA	IT admins can make notes per device to keep track of important information about that device.
ORGANIZATIONS		
Logo	NA	Admins can setup a custom organization logo to brand the Ensemble management portalper-app VPN features.
Primary / Secondary Colors	NA	Admins can setup a custom color scheme to brand the Ensemble management portal
White Label / Custom Name	NA	Ask us how to white label the Ensemble management portal login / sign-up pages to match your branding.