Mobile Device Management

Features and Functionality

With our Mobile Device Management (MDM) solution, we can manage and secure your mobile devices remotely, safely and efficiently throughout their entire lifecycle. The following is a description of the features and services provided.

Enrollment	Apple*	Android**
Over-the-Air-Enrollment		
Enroll via SMS message As part of the enrollment process, an SMS text message with a URL pointing to the MDM server can be sent, enabling a new mobile device to be configured for managed services	✓	✓
Enroll via email As part of the enrollment process, an email with a URL pointing to the MDM server can be sent, enabling a new mobile device to be configured for managed services	✓	✓
Enroll via quick reference (QR) code As part of the enrollment process, a QR code with a URL pointing to the MDM server can be scanned by a device's camera, enabling a new mobile device to be configured for managed services	✓	✓
Enroll via uniform resource locator (URL) As part of the enrollment process, a URL can be published on a webpage or company portal pointing to the MDM server, enabling a new mobile device to be configured for managed services	✓	✓

	Apple*	Android**
Configuration		
Common Connection Settings		
Exchange ActiveSync email Instantly configures access to a corporate Exchange email account on a mobile device	✓	✗
IMAP/POP email Instantly configures access to a personal email account on a mobile device	✓	✗
Virtual private network (VPN) Simplifies mobile VPN setup by configuring VPN network settings	✓	✗
Wi-Fi Simplifies Wi-Fi setup by configuring Wi-Fi network settings	✓	✓
Lightweight directory access protocol (LDAP) Enables corporate directory search for a contact name or email address in the To/CC/BCC fields when composing emails	✓	✗
Inventory Management		
Device Inventory		
Unique device identifier (UDID) Collects and displays the UDID of a mobile device	✓	✓
Device name Collects and displays the device name used to connect to iTunes or Google Play	✓	✓
Build and version Collects and displays the OS version running on a mobile device	✓	✓
Model name and number Collects and displays the model details of a mobile device	✓	✓
Serial number Collects and displays the mobile device serial number	✓	✓
Capacity and space available Collects and displays the total drive space and free space remaining on the mobile device	✓	✓
International mobile equipment identity (IMEI) Collects and displays the IMEI used to identify devices on cellular networks	✓	✓

	Apple*	Android**
Modem firmware Collects and displays information related to the mobile device firmware version	✓	✓
Hardware inventory Collects and displays information related to common hardware components, including memory, drive space, CPU and battery life	✓	✓
Application inventory Collects and displays the name and version of all installed applications	✓	✓
Mobile device type Collects and displays information that identifies the device as either a smartphone or a tablet	✓	✓
Network Inventory		
Integrated circuit card identifier Collects and displays information related to a mobile device's ICCID number for SIM cards	✓	✓
Bluetooth and Wi-Fi media access control (MAC) addresses Collects and displays Bluetooth and Wi-Fi MAC addresses	✓	✓
Current carrier network Collects and displays the device's current network carrier, such as AT&T, Verizon, etc.	✓	✓
SIM carrier network Collects and displays the device's SIM card carrier settings	✓	✓
Phone number Collects and displays the device's phone number	✓	✓
Data roaming settings Collects and displays the configured data roaming settings of the device	✓	✓
Security/Risk Management		
Policy Profiles		
Require passcode Requires device users to setup a passcode to access the mobile device	✓	✓
Allow simple value Permits the use of repeating, ascending and descending character sequences in a user's passcode	✓	✓

	Apple*	Android**
Require alphanumeric passcode Requires the passcode set by the user to contain at least one letter	✓	✓
Set passcode length Requires a minimum number of characters for passcodes	✓	✓
Require number of complex characters Requires users to configure a minimum number of non-alphanumeric characters when setting up a passcode	✓	✓
Set maximum passcode age Specifies the number of days after which a passcode must be changed (i.e. passcode must be changed every 90 days)	✓	✓
Set time before auto-lock Specifies the number of minutes that elapse before a device automatically locks	✓	✓
Set passcode reuse requirement Specifies the number of times that a passcode can be reused	✓	✓
Set grace period before device lock Specifies how soon a device can be unlocked again after use, without re-entering the passcode	✓	✗
Set number of failed attempts before device wipe Specifies the number of times a passcode can be entered incorrectly before all data on the device is erased	✓	✓
Available Restrictions		
Access to app stores Restricts access to app stores	✓	✗
Access to explicit media and content ratings Restricts access to apps and media with an explicit content rating	✓	✗
Use of web browser Disables the device's web browser application and removes the icon from the home screen, as well as prevents users from opening web clips	✓	✗
Web browser security preferences Controls the device's browser security preferences, such as pop-ups, JavaScript, etc.	✓	✗

	Apple*	Android**
Use of YouTube Disables the device's YouTube application and removes the icon from the home screen	✓	✗
Use of app store and in-app purchase Restricts the ability for users to make purchases through an application running on the device	✓	✗
Ability to screen capture Prevents users from saving a screenshot of the device display	✓	✗
Automatic sync while roaming Disables automatic syncing when a user is roaming so the device only syncs when an account is accessed by the user	✓	✗
Use of voice dialing or voice assistant Prevents the user from dialing the phone using voice commands or using voice command assistants such as Siri	✓	✗
Enforce encrypted iTunes backups Requires device backups performed in iTunes to be stored in encrypted format on the user's computer	✓	✗
Use of the camera Disables the use of the device camera and removes the icon from the home screen so that users cannot take photographs or videos, nor can they use FaceTime	✓	✗
Service		
On Demand Support Functions		
Instant device lock Allows a technician to instantly lock the device in the event a device is lost or stolen	✓	✓
Full device wipe Allows a technician to instantly erase all data on a device and reset it to factory settings	✓	✓
Selective device wipe Allows a technician to erase only those policies that were deployed to the device when it was under management	✓	✗
Passcode reset Allows a technician to reset the device passcode to a default passcode	✓	✓

	Apple*	Android**
Geographical location lookup Allows a technician to pinpoint the physical location of a mobile device on a geographical map	✓	✓
End-User Self Service Functions		
Send screenshot Enables the device user to take a screenshot of a problem area when in the mobile device and attach it to a ticket, which is sent directly to the helpdesk to aid in a faster troubleshooting and support process	✓	✓
Log ticket Enables the device user to easily log a support ticket with the helpdesk directly from the mobile device	✓	✓
Centralized Control Center Integration		
Technician access control Sets a service technician's access permissions to different mobile device groups	✓	✓
Auto wipe through intelligent groups Enables automatic device wipe in the event a device is added to a configured group, whether manually added or added through dynamic search criteria	✓	✓
Auto-lock through intelligent groups Enables automatic device lock in the event a device is added to a configured group, whether manually added or added through dynamic search criteria	✓	✓
Under contract vs. not under contract Enables clear distinction of devices under contract and those not under contract	✓	✓
Lost or retired device groups Enables clear distinction of devices lost or retired	✓	✓

	Apple*	Android**
Data Plan Management		
Detailed data usage tracking Enables quick access and viewing of data plan usage across all managed mobile devices to proactively assist in avoiding data plan overages	✓	✓
Data usage threshold alerting Creates an alert when activity spikes occur based on pre-configured thresholds to avoid costly overage charges	✓	✓
Geo Management and Tracking		
Historical device location Identifies the physical locations a device has been in a given period of time	✓	✓
Visual global map interface Enables a technician to view all geo-location tracking information on an interactive onscreen geographical map	✓	✓
Reporting		
Mobile device asset summary report Provides a variety of summary information, such as data plan summary, devices by operating system/type and a list of mobile devices by location	✓	✓
Mobile device detailed inventory report Provides a detailed list of devices and device attributes	✓	✓
Mobile device software inventory report Provides a detailed list of applications running on the mobile device	✓	✓
Mobile device data usage report Provides detailed statistics on data plan usage	✓	✓

** Requires iPhone or iPad iOS 3.1 or greater. ** Requires Android OS 2.0 or greater. iPhone® and iPad® are registered trademarks of Apple, Inc., registered in the U.S. and other countries. Android is a trademark of Google, Inc.*

Computer Emergency Room

229 Vestal Parkway East
Vestal, NY 13850
607-785-4357
www.computeremergencyroom.com