Mobile Device Management

101

Get more out of iPad and iPhone in business

Table of Contents

Introduction to Mobility

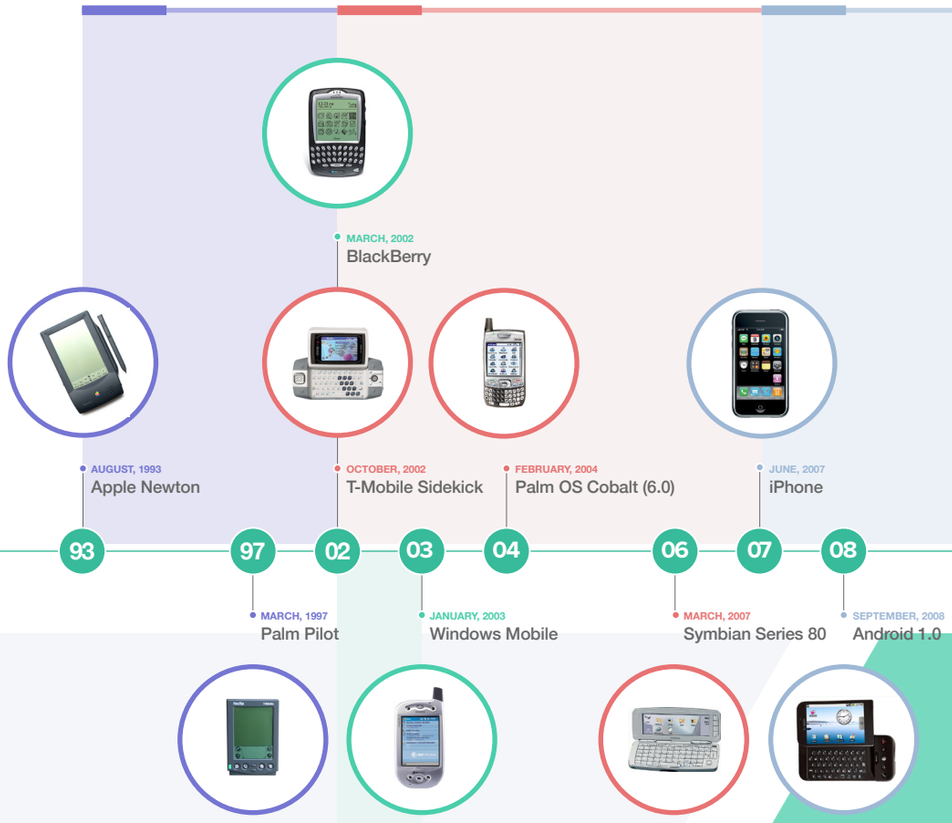
The Evolution of Mobility

Mobility began in the 1990s with handwriting recognition technology from Apple Newton and Palm Pilot, and the ability to connect to a dial-up modem.

The mid 2000s brought additional players to the smartphone market, with Symbian being the popular choice in Europe and Palm OS in the U.S. The market was crowded with five mobile operating systems and no clear winner.

The iPhone launched in 2007, followed by the first Android phone in 2008. Shortly after the iPhone launch, Apple's App Store gave developers the ability to build native apps for iOS, opening up a whole new world for mobile productivity and business process improvements.

Since 2007, BlackBerry and Windows Mobile users have declined drastically, while Palm, Symbian, and SideKick have been discontinued.



The early smartphones were dominated by BlackBerry and Windows Mobile, which opened the door for mobile communication.

iPhone

Android

Windows Phone

17

Today, the mobile landscape is comprised of three major OS players. Smartphones have evolved beyond simple communication tools, with apps serving as the vehicle for transformation of mobility and business.

Why Choose iOS

Out of the three prevailing mobile operating systems, iOS is the only platform that is designed for consumers and embraced by the enterprise. iOS boasts an intuitive user interface, a secure ecosystem of business-ready apps, and built-in tools that empower users to be more productive than ever before.

Fastest and most efficient mobile hardware

Runs on iPhone and iPad at different screen sizes

Native hardware-based encryption to keep data secure

Healthy developer ecosystem with 1.5 million apps in the App Store and $40B paid to developers

Touch ID for biometric security

Over 70% of users on latest OS with annual release cycles

Productivity apps to create documents, spreadsheets, and presentations including Microsoft Office for iOS

Split-screen multitasking for iPad

Built-in support for modern secure wireless networking, such as VPN and single sign-on

Built-in Microsoft Exchange support for email, calendars, and contacts

Why iOS for Business

According to a report from Harris Poll, enterprise mobility will top IT investments in 2016. The survey reveals that more than 90 percent of IT decision makers see enterprise mobility as the critical function for customer engagement, competitiveness and operational productivity in 2016.

Businesses are not choosing just any mobile technology to support their workforce. They are adopting iOS at increasing rates because it is preferred by users, easy to manage and secure. By putting iPad and iPhone into the hands of employees, organizations of all shapes and sizes pave the way for better engagement, enhanced business practices, and greater output of creative and innovative work.

How Many Businesses Choose iOS?

The 2017 Jamf Managing Apple Devices in the Enterprise Survey[1] reveals nearly all enterprise IT professionals say their internal teams saw a 76% year over year increase in iPad and iPhone usage within their environment. Additionally, 93% believe it's easier to deploy iPhone and iPad over any other platform.

76%

of organizations saw an increase in iPhone and iPad in their environment

93%

of respondants say it's easier to deploy iPhone or iPad over another platform

Source 1 - Jamf
https://resources.jamf.com/documents/books/managing-apple-devices-in-the-enterprise.pdf

Leverage iOS to Transform Business Processes

According to a theory proposed by American psychologist Abraham Maslow, all humans have the same fundamental needs. Basic needs (food, clothing and shelter) must be met before an individual is motivated to advance to a higher level of needs, such as love and self-esteem. In other words, constant betterment can only be achieved when certain needs are mastered.

Maslow's hierarchy of needs serve as an analogy for what is possible in business with iOS. Device deployment and communication are the basic needs of any business. However, iOS is so much more. It is a gateway to industry transformation. As businesses look to maximize productivity and customer satisfaction, iOS apps are a mechanism to streamline communications, improve transactions and transform business processes.

Process

To transcend what is possible in business, the most innovative companies are not only investing in hardware, but also in custom apps to transform their business processes. This can be done through IBM's MobileFirst program, Business-to-Business (B2B) apps or in-house enterprise apps.

Transactions

The rich App Store ecosystem with millions of apps offers opportunities to better conduct mobile transactions. Examples include Square and Salesforce1 to process credit card transactions or submit a purchase order to close a deal. App Store app deployment is crucial to unlocking the full potential of iOS devices.

Communication

Once devices are in the hands of users, IT needs to enable basic communications for them. This includes access to corporate email, Wi-Fi and VPN settings—all without adding unnecessary bloat.

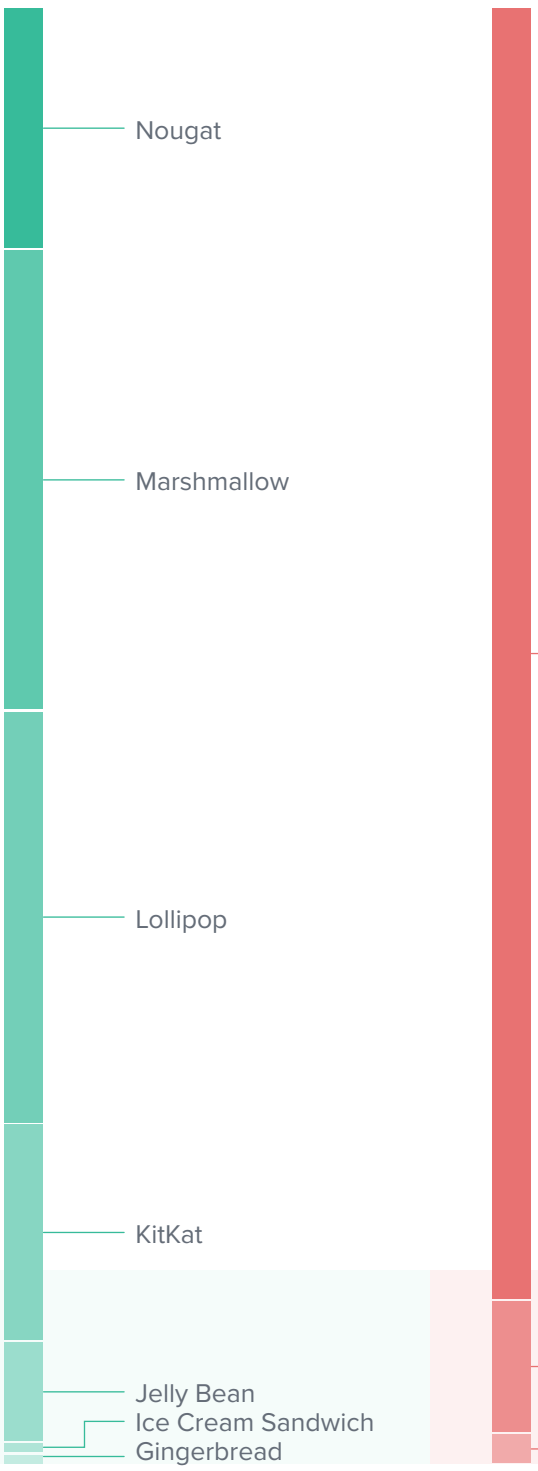
Deployment

Organizations need to tackle the business problem of deployment, device configurations and inventory. This is the lowest layer of the pyramid and the foundation for any organization looking at significant quantities of iOS devices.

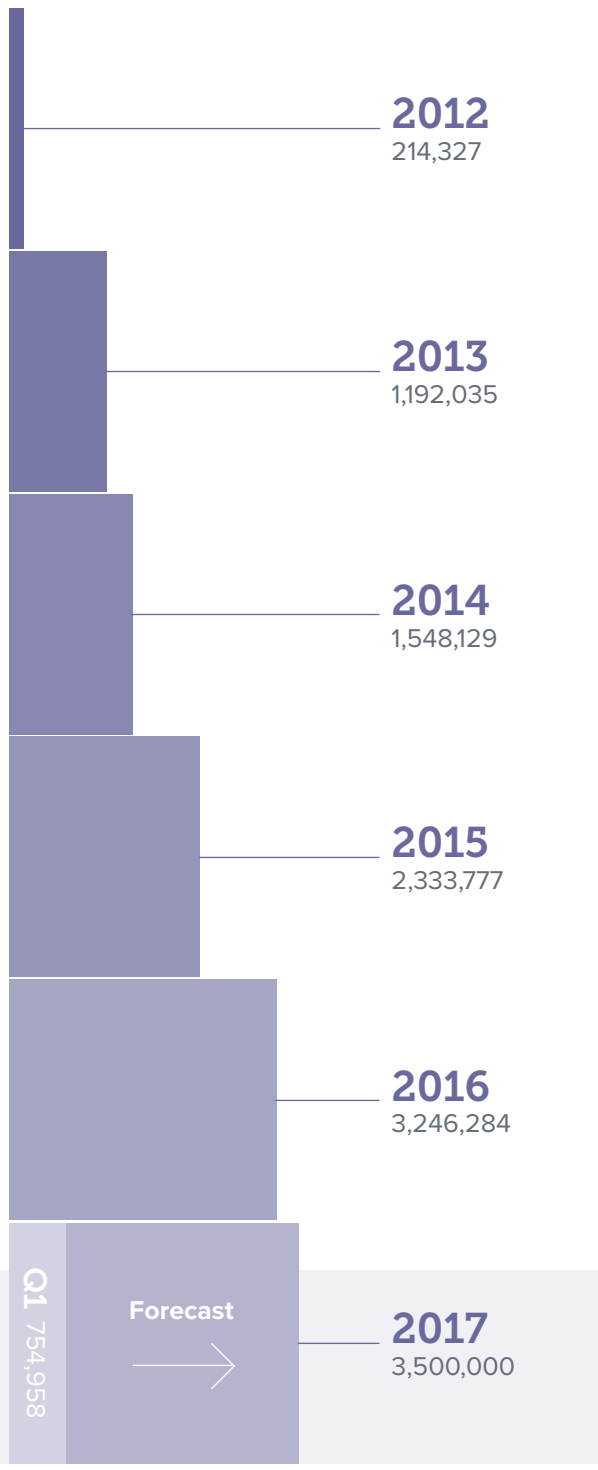
What About Android?

Google's Android operating system has risen in popularity due to its wide variety of form factors, a highly customizable operating system and often less expensive devices. Android can be a good choice for consumers or BYOD programs since users value features differently. For the enterprise, however, Android is difficult to standardize on and support due to fragmentation and security concerns.

Adoption Rates



New Android Malware Samples (per year)



Source 2 - Google: http://developer.android.com/about/dashboards/index.html
Source 1 - Apple: https://developer.apple.com/support/app-store/

Source 3 - G Data: https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/G_DATA_MobileMWR_Q3_2015_EN.pdf

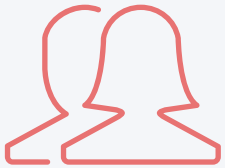
Mobile Device Management Overview

What is MDM?

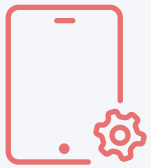
Mobile device management (MDM) is Apple's framework for managing iOS. To effectively manage iOS devices and unleash their full potential, organizations require an equally powerful MDM solution. From deploying new devices and gathering inventory, to configuring settings, managing apps, or wiping data, MDM provides a complete toolset to address large-scale deployments and ensure device security.

Deployment

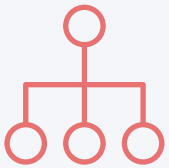
Inventory



Configuration Profiles



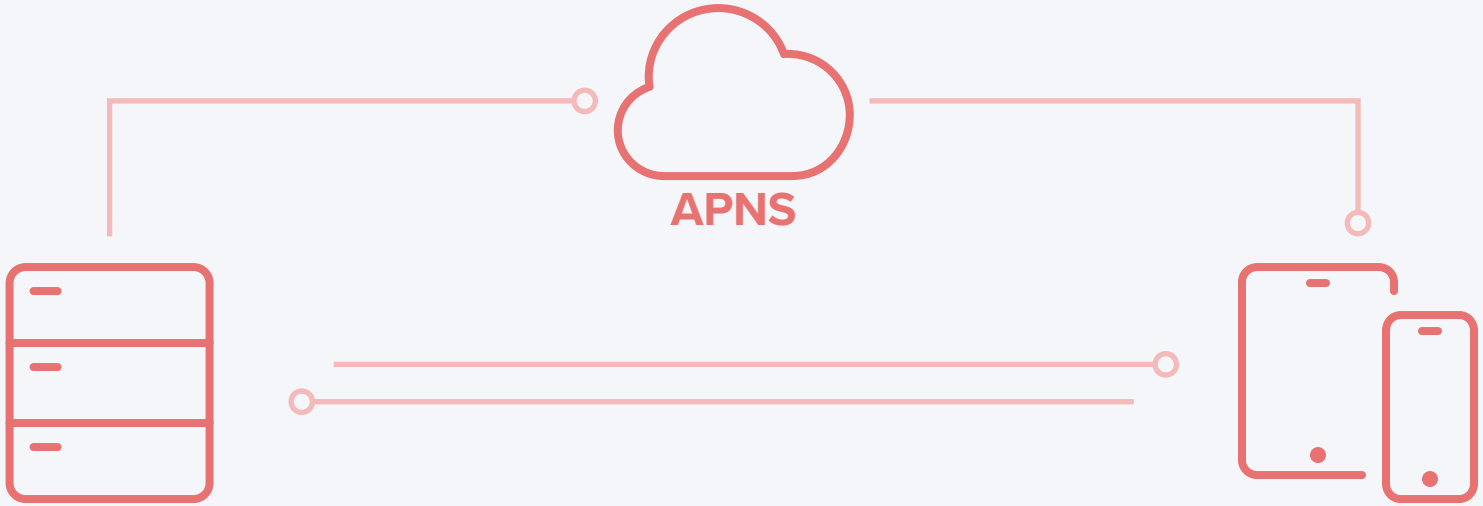
Management Commands



App Deployment

Security and Privacy

The Architecture for MDM



Apple Push Notification Server

When you send commands to Apple devices, your MDM server communicates with Apple's Push Notification Server (APNS). Apple's server maintains a constant connection to devices so you don't have to. Devices communicate back to the MDM server and receive the commands, configuration profiles or apps you send it.

Deployment Methods

Before you can use MDM to manage your iOS devices, you first have to enroll them. For iPad or iPhone, an MDM tool allows you to easily enroll devices into management, consistently distribute apps and content, and set up security and access profiles. There are several methods to enroll an Apple mobile device, including enrollment via Apple Configurator, a URL or Apple's Device Enrollment Program (DEP).

Deployment Methods

	Description	User Experience	Supervision	Best For
Device Enrollment Program (DEP)	Over-the-air automatic enrollment	User receives shrink-wrapped box, and the device is automatically configured when turned on	Yes–wirelessly	Sending devices directly to end users
Apple Configurator	Enrollment through a Mac app that connects to devices via USB	N/A—IT manages this process and hands devices to users	Yes—wired	Shared-models and carts
User Initiated via URL	Over-the-air manual enrollment	User visits a specific URL to automatically configure their device	No	Devices currently in the field that need to be enrolled or BYOD

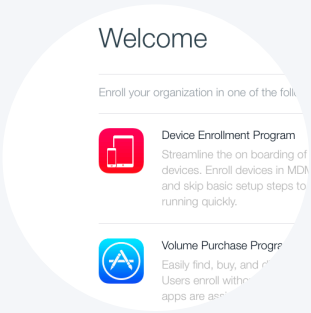
Supervision

Supervision is a special mode of iOS that enables deeper management by an MDM server. A growing number of configurations are only available if a device is supervised. It is recommended that corporate-owned devices are put into supervision mode.

Examples of Supervision-only Commands:

- Disable Camera
- Disable App Store
- Disable Safari
- Disable modifying wallpaper
- Disable adding email accounts
- Plus many more....

Best practice: Zero-Touch Deployments with MDM

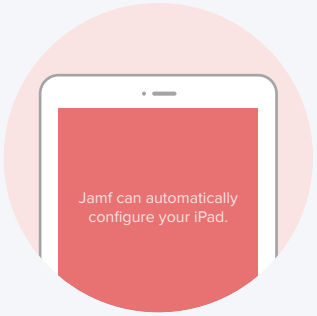


Sign up for DEP via Apple's website and add your MDM server to the DEP portal.

1

2

Purchase devices and link them to your DEP account. Ship them directly to users.



3

As a user turns their iOS device on for the first time, the device will automatically be enrolled—no additional interaction is needed.

4

Device enrolls with the MDM server. Prepare any configuration profiles and apps you'd like to apply to devices.

5

Device receives configurations and apps scoped to it, and the user is brought to the Home screen. The device is now managed and configured—all without IT having to touch it!

Inventory

MDM solutions are capable of querying an iOS device to collect a large amount of inventory data, ensuring you always have up to date device information to make informed management decisions. Inventory can be collected from a device at various intervals, and includes information, such as serial number, iOS version, apps installed and much more.

Examples of Data Collected with MDM

Hardware Details

- Device Type
- Device Model
- Device Name
- Serial Number
- UDID
- Battery Level

Software Details

- iOS Version
- List of Apps Installed
- Storage Capacity
- Available Space
- iTunes Store Status

Management Details

- Managed Status
- Supervised Status
- IP Address
- Enrollment Method
- Security Status

Additional Details

- Profiles Installed
- Certificates Installed
- Activation Lock Status
- Purchasing Information
- Last Inventory Update

Why Does Inventory Matter?

You can't manage what you can't measure. The inventory data that MDM collects can be used for a wide range of business needs and empower you to answer common questions like: Are all my devices secure? How many apps do we have deployed? What version of iOS do we have deployed?

Configuration Profiles

Configuration Profiles give you the ability to tell your devices how they are supposed to behave. While you once had to manually configure devices, MDM technology allows you to automate the process of configuring passcode settings, Wi-Fi passwords, VPN configurations and more. Profiles also have the ability to restrict items in iOS such as the Camera, Safari web browser or even renaming the device.

Available Profiles for MDM

The Basics

- Passcode
- Restrictions
- Wi-Fi
- VPN
- Home Screen Layout
- Single App Mode
- LDAP
- Web Clips

Email Accounts

- Mail
- Exchange ActiveSync
- Google Account
- VPN
- Calendar
- Contacts
- Subscribed Calendars
- macOS Server Account

Internet Settings

- Global HTTP Proxy
- Content Filter
- Domains
- Cellular
- Network Usage Rules
- Certificates

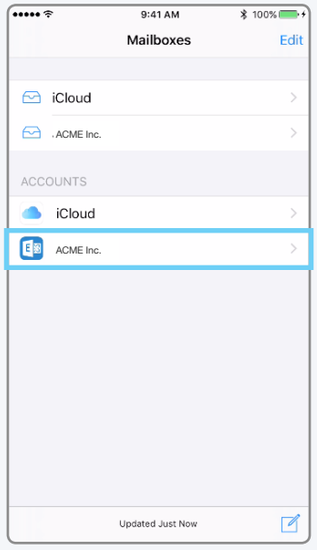
Other Settings

- AirPlay
- AirPlay Security
- Conference Room Display
- AirPrint
- Fonts
- SCEP
- Lock Screen Message
- Notifications
- Single Sign-on
- Access Point Name

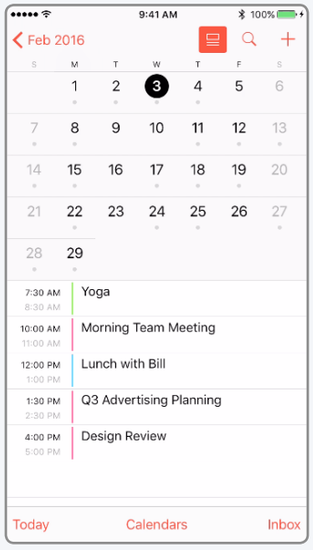
Best Practice: Eliminate Containers for iOS Management

In the world of MDM, a container is an additional app designed to serve as a secure location for corporate info such as email, calendars, contacts and even web browsing. Organizations are drawn to this concept, but it gets in the way of a good user experience. Containers became popular among some MDM solutions to help overcome Android security flaws.

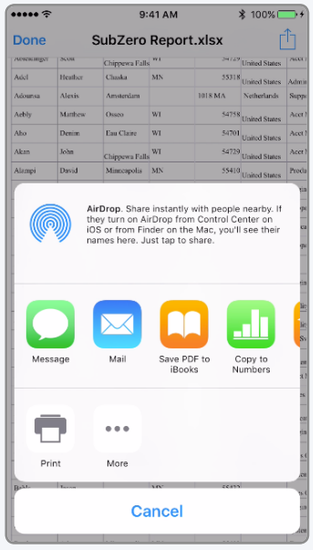
The reality is that iOS native apps (Mail, Calendar, Contacts and Safari) are already secure. There is simply no need for a “secure” email container. To preserve the best experience for users, simply use configuration profiles. A profile has the ability to add an Exchange account to iOS, which will in turn provide access to corporate email and calendars.



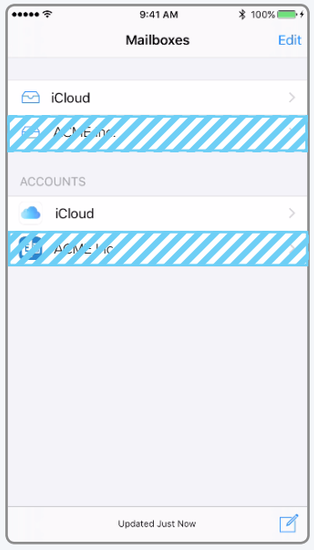
A configuration profile adds an Exchange account next to a user’s personal email account in the native Mail app.



Corporate data now lives right next to personal data in the native apps, preserving user experience and security.



IT can also control the flow of data by preventing apps from opening attachments in their corporate email account.



Finally, if an employee leaves an organization, IT can simply remove the configuration profile and the corporate email account is removed along with the data. Personal accounts are not deleted.

Best Practice: Standardize iPad

Help improve employee productivity by offering a consistent experience on your organizationally owned devices. Standardizing Apple devices for your workforce creates a streamlined setup process that allows users to quickly access the apps they need, when and where they need them. Less time searching for apps leads to increased productivity from users.

Here are three ways you can standardize iPad and iPhone devices in your organization:

Set the Home screen wallpaper

Create brand consistency by displaying your organization's logo on the wallpaper.

Pre-design the Home screen layout

Define the placement of apps and folders, along with web clips, on the Home screen. Put mission critical apps on the first page and less important apps on other pages.

Show/hide apps

Display only the apps your employees need. Hide the ones that are not necessary for their work.

Management Commands

Management commands are specific actions that you can apply to individual devices to ensure security of corporate data. Leverage this capability within MDM to take action on lost or stolen devices by locking a device or wiping it completely. Additional commands allow you to send push notifications, update iOS to the latest version and change the device name to make it easier for IT to manage their fleet of devices.

Available Commands for MDM


INTERNET SETTINGS


LOCK DEVICE


CLEAR PASSCODE


CLEAR RESTRICTIONS


UNMANAGE DEVICE


WIPE DEVICE


SEND BLANK PUSH


SET WALLPAPER


SEND NOTIFICATION


UPDATE IOS


CHANGE NAME


SHUTDOWN DEVICE

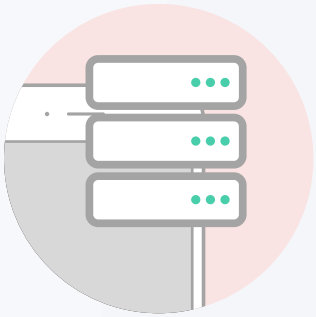

RESTART DEVICE


LOST MODE & SOUND

Best Practice: Manage Activation Lock with MDM

Activation lock is designed to prevent theft of iPhones and iPads. By requiring an Apple ID and password, not just anyone can activate a device. This feature is great for theft prevention, but can cause problems when IT admins need to reassign devices to students if they are not managing their students' Apple IDs. However, when pairing Activation Lock with an MDM solution, IT admins are able to manage Activation Lock much easier. As long as a device is enrolled in an MDM server and is supervised, you can generate an Activation Lock Bypass Code in case you receive a device that is locked to a previous Apple ID. Once you have the code, you can enter it into the password field during the Setup Assistant and the device is unlocked.

1



Device is already enrolled in an MDM server and is supervised. An Activation Lock Bypass Code is generated and stored in the MDM server.

2

A locked device is returned to IT, so they retrieve the Bypass Code stored in the MDM server.

3

IT reboots the device into the Setup Assistant and the first screen asks for the previous student's Apple ID and password. To bypass the Activation Lock, IT enters the code in the password field and leaves the Apple ID field blank. The device is now unlocked.

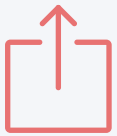
App Deployment

An iOS device serves as a great communication tool out of the box, but the rich library of personal and business apps in the iOS App Store can enhance user productivity and help your employees achieve even more. Further, you can use iOS App Store apps to turn an iPad into a cash register, create and submit expense reports on the go, and even transform business processes such as managing a sales cycle or signing contracts. With an app strategy and MDM to manage your app deployments, you will ensure users have the apps they need—configured and secure for your environment.

App Management Strategies

What is a Managed App?

Introduced in iOS 5, managed apps differ from a standard app because they are flagged as owned by an organization. Specifically, managed apps are distributed via MDM technology and can be configured to prevent backup of the app's data and deleted when the MDM profile is removed.



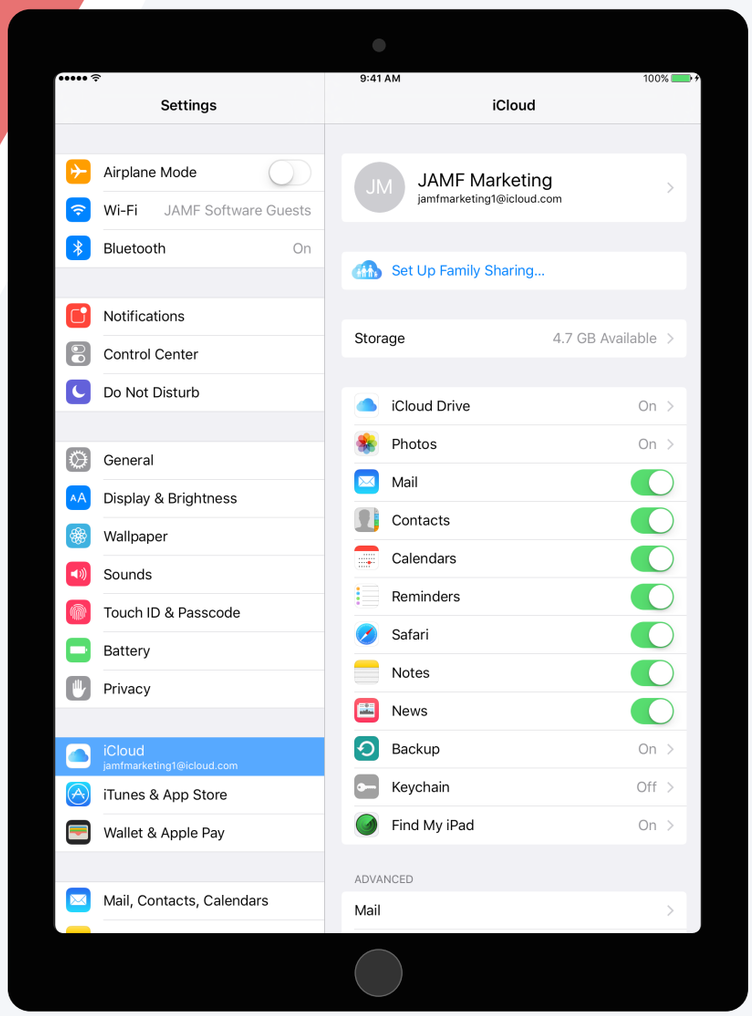
Managed Open In

Managed Open In takes the concept of managed apps a step further by controlling the flow of data from one app to another. Organizations can restrict what apps are presented in the iOS share sheet for opening documents. For example, you could define rules that state mail attachments from corporate email accounts can only be opened in the Box app and not in a personal Dropbox account. This allows for truly native data management without the need for a container.

App Configurations

Sometimes deploying an app isn't enough and you'd like to pre-customize some of the settings. This is the premise for App Configurations. App developers can define what settings can be pre-configured by an MDM server for their app. For example, you could deploy the Box app with the server URL pre-populated so users only need to enter their username and password to get the app up and running.

Best Practice: Individual Apple IDs for Users



Individual personal Apple IDs help increase adoption of iOS and encourage your users to find unique solutions to business problems.

What is an Apple ID?

An Apple ID is a personal account for users to access Apple services such as the App Store, iTunes, iCloud, iMessage, FaceTime, and more. An Apple ID consists of an email address and password, as well as contact, payment and security details.

Why Are Apple IDs Important for Users?

An Apple ID allows users to take full advantage of iOS and the App Store. For example, allowing users to have an Apple ID enables them to access free communication services from Apple such as FaceTime and iMessage, as well as other services like Find My iPhone and iCloud.

What About Corporate-owned Apps?

Since the VPP store now allows you to license apps via the “Managed Distribution” method, you can simply assign apps to a user’s device or Apple ID without permanently transferring ownership to the user. This way, IT doesn’t have to spend hours creating Apple IDs specific to a device.

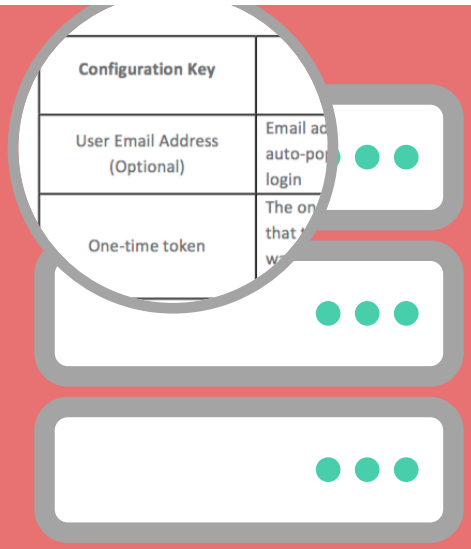
What About Security Risks?

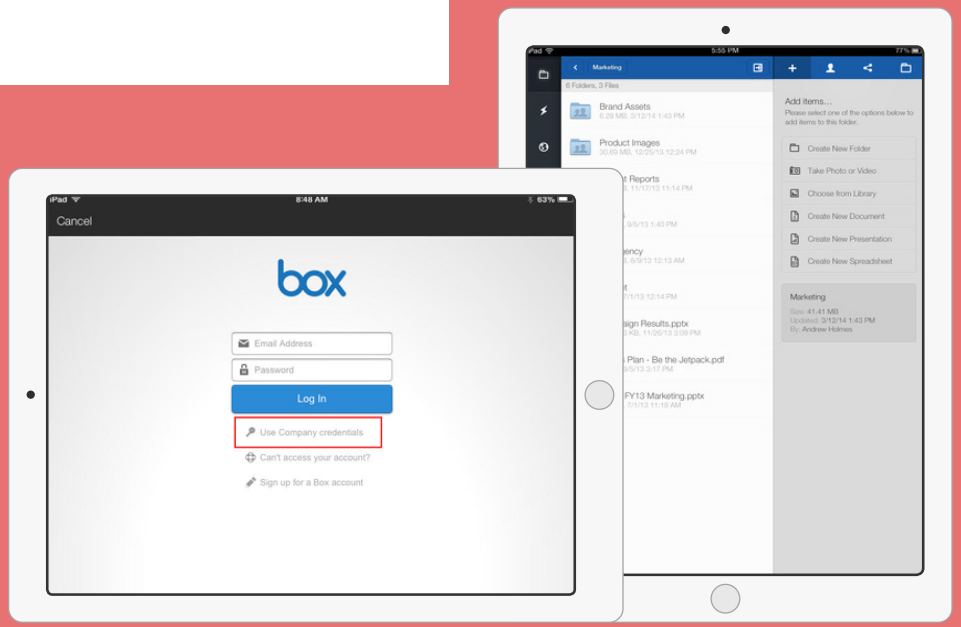
Utilizing MDM features such as Managed Open In and restrictions within a Configuration Profile, IT can better mitigate security risks as opposed to prohibiting Apple IDs altogether. Apple’s services are known for their security, and adding a personal Apple ID to a corporate device does not reduce the overall security. In some cases, you can even increase security since Apple IDs support two-step authentication.

Best Practice: Managed App Configuration Deployment Example

Box for iPhone and iPad helps you get work done on the go. It's fast, secure, and simple to use, so you can be productive from anywhere, which is the reason more than 25 million users and 225,000 companies use Box.

Deploy Box using VPP with options pre-configured to ensure adoption among your users.

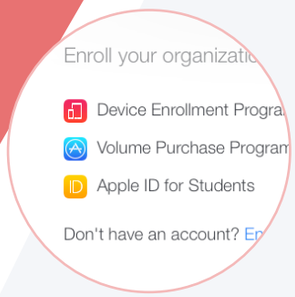




Box provides a set of configuration keys that pre-populate items such as the URL, user email address, a one-time token, and more. These configuration keys can be added to your MDM server to help automate the initial set up of Box.

When the app has been deployed via your MDM server, the configuration keys carry through. If you pre-configured the URL, for example, the first time Box is launched users will automatically be brought to the company login screen and not presented with the default personal account login screen.

Best Practice: Deploy Apps with the Volume Purchase Program (VPP)



1

Sign up for VPP via Apple's website and link your VPP account to your MDM server.

3

Add your app licenses to your MDM server, including free apps.

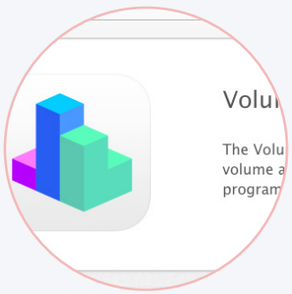
4

Apps are deployed directly to the device. No interaction or Apple ID required.

?

Choose to assign apps to either devices directly or to a user's Apple ID.

2



Find and purchase app licenses from the VPP web store. You will also need to "purchase" free apps.

4

Invite users to participate in your VPP deployment via email or push notification.

5

Apps are linked to a user's Apple ID and are found in the Purchased tab of the App Store.

Security and Privacy

Security and privacy concerns are a serious issue for organizations. iOS has a number of security features built right into the mobile operating system. Coupled with a mobile device management solution, you can ensure that your devices are not only secure, but your apps and network are as well.

Native Apple Security Features

Pre-App VPN

Virtual Private Networks (VPN) have long been implemented in the enterprise as a means to encrypt traffic over the internet. Traditional desktops can operate by routing all traffic over VPN; however, that model can break down when it comes to mobile. Apple solves this by allowing organizations and app developers to define, at the app level, what data gets routed through VPN. This helps save bandwidth and improve network speed.

Touch ID

A fingerprint sensor is now included in most of Apple's new iOS devices, adding biometric security to the operating system. Touch ID can be used to unlock a device and sign into certain apps. Fingerprint and facial recognition data is stored locally on the device and is never shared with Apple.

Encryption

iOS has 256-bit encryption built in and is automatically enabled if a passcode is enabled. This means the data on your devices remain secure without having to add any additional software bloat to the operating system. Since Apple makes both the hardware and software, the encryption is so fast that it is unnoticeable to the user.

Best practice: Using an MDM Solution for Loss Prevention

The ability to use MDM to place a supervised device into Managed Lost Mode is a key security enhancement available on iOS 9.3 or later. This setting can provide the device location, which is instrumental in finding lost or stolen devices. Additionally, only when Lost Mode is disabled will the user be able to unlock their device. At that time, any location information that was accessed will be shared with the user.

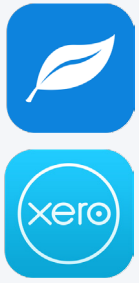
Managed Lost Mode is controlled by the administrator and must be disabled by the administrator before the device can regain operability. Similar to Find My iPhone, an administrator can send messages to the device while it is in Managed Lost Mode.

Scenarios

Retailers are working harder than ever before to connect with their customers via technology and reduce purchasing friction. Retailers need to consider their point of sale (POS) systems, loyalty programs, employee schedules, accounting and more. iPad and iPhone, combined with powerful apps, have made it easy for any retail startup to tackle these issues quickly and affordably. However, with thousands of retail apps in the App Store, it can be difficult to find the right solution. Below is a curated collection of retail apps for you to consider.

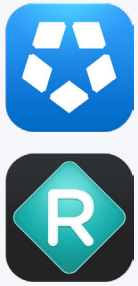
Point of Sale

POS systems used to be large, bulky, not user friendly, and not mobile. Now that iPad and iPhone are as powerful as traditional POS computers, you can be mobile while reinventing your business. Apps like Square, Vend and Revel are all customizable POS apps that can connect to hardware like a cash drawer, credit card reader, or scanner. Square even supports Apple Pay—the easiest way for iPhone users to pay at the register.



Accounting

Accounting can be time consuming, but at least you can now do it on-the-go thanks to some great apps from FreshBooks and Xero. Both of these solutions offer cloud-based accounting systems that can be accessed via mobile apps. These systems are designed to help you streamline your expense tracking and revenue.



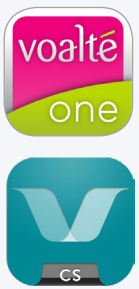
Time Tracking

Managing schedules, time punches, and employee communication is a large set of tasks and is often done via pen and paper. With Deputy and Replicon, you can move your manual systems to the cloud and interface with them through your mobile devices. Both of these solutions offer scheduling, time tracking, and a platform for employee communications.

Rewards Program

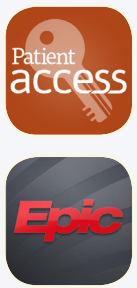
Loyalty programs are a great way to keep your customers coming back. However, implementing your own system can be very difficult. This is where Belly can help. Belly is a loyalty rewards program that works with over 12,000 businesses and six million customers. Simply sign up for their program and start building loyalty with your customers.

Healthcare providers are looking for new ways to provide faster, more personalized care to their patients, while also improving communication among doctors and nurses. To do this, medical records are stored in a secure central location where doctors and nurses can access information from a mobile device. With the addition of third-party apps and hardware for home health monitoring, Apple and the organizations below are truly transforming healthcare.



Communication

Communication is an essential component for timely patient healthcare, and iOS provides a platform for rich and engaging communication apps. Voalte and Vocera are two leading companies that give healthcare organizations powerful tools to communicate while leveraging Apple technology.

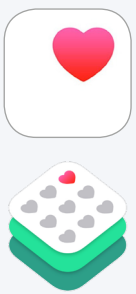


Clinical Care

A modern Electronic Medical Record (EMR) system should be designed to meet healthcare workers where they are at—regardless of whether they are at home, at the hospital, or on the go. Both Emis and Epic are EMR solutions designed for iOS. Their mobile apps help doctors and nurses stay up to date with their patients right from their iPhone, iPad, and even Apple Watch.

Patient Care

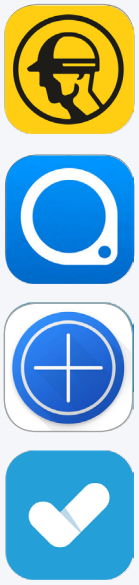
Clinical care can only go so far. For chronic health conditions, home monitoring is often recommended. Thanks to iPad and iPhone, combined with third-party hardware, you can accomplish health monitoring with consumer-level products. Focus Cura, Physitrack, and Withings are companies leading the way by empowering users to track their health conditions on their personal mobile devices.



Apple and Health

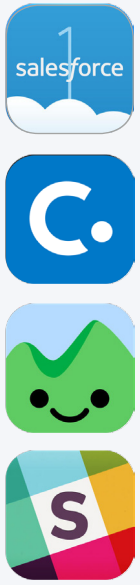
Apple has empowered users with powerful health monitoring and tracking tools built into iPhone and Apple Watch. The Health app allows users to track their health in a single app—all with the confidence that their health data is secure.

Organizations with employees in the field need to ensure access to the right tools and information when and where employees need it. To help on-the-go employees, crafting an app strategy to empower field teams is crucial for success and productivity. Highlighted below are a few examples of what's possible in the construction vertical, as well as general field sales, when resources are paired with iOS.



Construction

iOS has become an important tool in the construction industry toolbox thanks to products that put blueprints and CAD plans on iPads. Apps from Fieldwire, PlanGrid and FinalCAD all help construction teams access blueprint files, so they no longer need to carry large printed papers with them. You can even make auditing easier with SafetyCulture and their iAuditor app.



Field Sales

Customer relationship management, project management, team management and expense tracking are all essential business functions that most sales organizations interact with on a daily basis. To support those road warriors, you can provide them with solutions from organizations like Salesforce1, Concur, Basecamp and Slack to make mobile access and the mobile experience top priorities.

Transform Business Processes with Custom Apps

Any organization deploying iOS can utilize the built-in apps like Mail, Notes, and Calendar for basic communications. But, iOS offers so much more. With access to a powerful platform for custom apps, you have the potential to transform business processes or even an entire industry.

For example, Apple is working with IBM to create industry-specific apps that help enhance and enable a greater, more efficient level of productivity. To date, Apple and IBM have created more than 100 apps for industry-specific functions—including finance, high-tech, government, healthcare, insurance, retail and transportation.

With over 1.5 million apps in the App Store, chances are you might find an app that does 90 percent of what you want it to do for your business. This is where the B2B App Store can help. Apple helps connect organizations with developers to provide a customized version of an app. Companies can do simple branding or can tailor existing apps to meet their business process needs.

The most innovative companies are not just inventing hardware, but also software. Investing in developer resources to build in-house apps will help your organization rethink what is possible on a mobile platform. Apple offers one of the best mobile development platforms available—Swift. Swift is a powerful and intuitive programing language for all of the Apple operating systems. Since Swift is also open source, you can find free resources from the Apple community and start building right away!

Transform Business

Moving the enterprise forward with Apple TV

As mobile demands increase within the workplace, your technology needs to keep up. With the latest tvOS, Managed Apple TV now allows IT to transform consumer Apple TV devices into managed work tools.

Wireless Conference Room

To create a modern conference room, set up an adapter and wire-free display. Then enable Conference Display Mode and create a customized welcome message that includes additional instructions or information specific to each room.

Digital Signage

Apple TV makes digital signage more affordable, accessible, scalable and manageable. And, with MDM software, companies can easily control what is shown at a single location or across multiple sites.

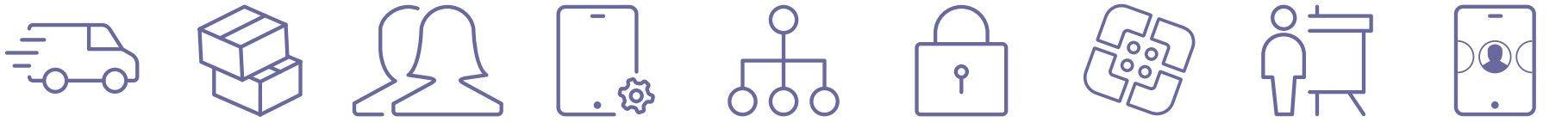
Spontaneous Collaboration

Managed Apple TV and Airplay makes it easier than ever to instantly display screens from a device onto a shared screen. This creates a setting perfect for collaboration within the workplace.

jamf | PRO

MDM for iOS

The Jamf Pro is the leading mobile device management tool for iOS. Designed to automate common tasks around Apple deployment, inventory and security, Jamf Pro makes mobile device management easy, so you can better ensure a transformative learning experience.



Deployment | Inventory | Configuration Profiles | Management Commands | App Deployment | Security and Privacy | Self Service | Apple School Manager | Classroom Management

Start Managing iOS with a Free Trial

Configuration Profile Payloads and Management Commands List

Managed Only

Passcode payload

- Allow simple value
- Require alphanumeric value
- Minimum passcode length (0-16)
- Minimum number of complex characters (0-4)
- Maximum passcode age (0-730 days)
- Maximum Auto-Lock time
- Passcode history (0-50 passcodes)
- Maximum grace period for device lock
- Maximum number of failed attempts

Restrictions payload

- Allow use of camera
- Allow screenshots and screen recording
- Allow voice dialing while device is locked
- Allow Siri
- Allow Siri while device locked
- Allow installing apps using Apple Configurator and iTunes
- Allow In-App Purchase
- Require iTunes Store password for all purchases
- Allow iCloud backup
- Allow iCloud keychain
- Allow managed apps to store data in iCloud
- Allow backup of enterprise books
- Allow notes and highlights sync for enterprise books
- Allow iCloud Photo Sharing
- Allow iCloud Photo Library
- Allow My Photo Stream
- Allow automatic sync while roaming
- Force encrypted backups
- Force limited ad tracking
- Allow users to accept untrusted TLS certificates
- Allow automatic updates to certificate trust settings
- Allow trusting new enterprise app authors
- Allow documents from managed sources in unmanaged destinations
- Allow documents from unmanaged sources in managed destinations
- Treat AirDrop as unmanaged destination
- Allow Handoff
- Allow sending diagnostic and usage data to Apple
- Allow Touch ID to unlock device
- Force Apple Watch wrist detection
- Require passcode on first AirPlay pairing
  Allow Wallet notifications in Lock screen
- Show Control Center in Lock screen
- Show Notification Center in Lock screen
- Show Today view in Lock screen
- Set ratings region
- Set allowable content ratings for Movies, TV and Apps
- Allow explicit sexual content in iBooks Store

Other Payloads

- Wi-Fi payload
- VPN payload
- Mail payload
- Exchange ActiveSync payload
- Google Account payload
- LDAP payload
- Calendar payload
- Contacts payload
- Subscribed Calendars payload
- Web Clips payload
- macOS Server Accounts payload
- Domains payload
- Certificates payload
- SCEP payload
- APN payload
- Cellular payload
- Single Sign-On payload
- Fonts payload
- AirPrint payload
- Network Usage Rules payload

Management Commands

- Remote Lock
- Remote Wipe
- Clear Passcode
- Un-Manage Device
- Update Inventory
- Send Blank Push

Managed + Supervised

Enrollment (DEP Only)

- Supervise Device
- Make MDM Profile Mandatory
- Disallow pairing to Mac computers
- Disallow the user from removing the MDM profile
- Enable Shared iPad
- Require credentials for enrollment
- Skip Setup Assistant options
- Define a naming method for devices

Restrictions Payload (Supervised Only)

- Allow FaceTime
- Allow screen observation by Classroom app
- Allow modifying the AirPlay and View Screen permission for managed classes
- Allow AirDrop
- Allow iMessage
- Enable Siri profanity filter
- Allow user-generated content in Siri
- Allow iBooks Store
- Allow installing apps using App Store
- Allow automatic app downloads
- Allow removing apps
- Allow Apple Music
- Allow Radio
- Allow iCloud documents & data
- Allow Erase All Content and Settings
- Allow installing configuration profiles
- Allow modifying account settings
- Allow modifying Bluetooth settings
- Allow modifying cellular data app settings
- Allow modifying device name
- Allow modifying Find My Friends settings
- Allow modifying notifications settings
- Allow modifying passcode
- Allow modifying Touch ID fingerprints
- Allow modifying restrictions
- Allow modifying Wallpaper
- Allow pairing with non-Configurator hosts
- Allow modifying diagnostics settings
- Allow pairing with Apple Watch
- Allow connection to unmanaged Wi-Fi networks
- Allow predictive keyboard
- Allow keyboard shortcuts
- Allow auto correction
- Allow spell check
- Allow Define
- Allow dictation
- Allow use of iTunes Store
- Allow use of News
- Allow use of Podcasts
- Allow use of Game Center
- Allow use of Safari
- Enable AutoFill
- Force fraud warning
- Enable JavaScript
- Block pop-ups
- Block Cookies
- Allow playback of explicit music, podcasts and iTunes U
- Autonomous Single App Mod
- Hide/Show Apps
- Restrict AirPlay destinations

Other Payloads (Supervised Only)

- Home Screen Layout payload
- Single App Mode
- Global HTTP proxy payload
- Content Filter payload
- Lock Screen Message payload
- Notifications payload

Management Commands (Supervised Only)

- Set Wallpaper
- Bypass Activation Lock
- Lost Mode with Sound
- Update iOS (DEP enrollment only)
- Clear Restrictions
- Rename Device
- Restart Device
- Shut Down Device
- Delete User (Shared iPad only)
- Logout User (Shared iPad only)