

Mobile Device Management 101



Get more out of iPad in Education

Table of Contents

INTRODUCTION TO MOBILITY



Education Technology

- Why iPad for Education
- Leverage iPad to Transform Learning



App Deployment

- Deploy Apps with MDM
- Managed Apple IDs



Security and Privacy

- Native Apple Security Features

MOBILE DEVICE MANAGEMENT OVERVIEW



Mobile Device Management (MDM) Overview

- What is MDM



Deployment

- Deployment Methods
- Best Practice: Zero-Touch Deployments with MDM and Apple School Manager



Inventory

- Collect Data with MDM



Configuration Profiles

- Available Profile Payloads for MDM



Management Commands

- Available Commands for MDM
- Manage Activation Lock with MDM

IPAD IN THE CLASSROOM



iPad in K-12

- iPad and Classroom Management
- Educational Apps and iBooks for iPad
- Secure Assessments with iPad



Jamf Pro

- Start a Trial



Appendix Checklists

- Profile Payload and Management Commands List

A young woman with dark hair tied back, wearing a light purple hoodie over a blue and white striped shirt, is looking down at a tablet computer she is holding. She is in a classroom setting, with other students blurred in the background. The text "Introduction to Mobility" is overlaid in a bold, yellow font on the left side of the image.

Introduction to Mobility



Why iPad for Education

Schools are not choosing just any mobile technology. They are adopting iPad because it is preferred by students and teachers, easier to manage, and secure. By putting iPad into the hands of students, schools pave the way for more creativity and productivity, better engagement, and spontaneous collaboration.

How Many Schools Choose iOS?

The 2015 Jamf Managing Apple Devices in K-12 Education Survey reveals nearly all education IT professionals say their internal teams support iPad (97%). Further, education participants cite an increase in the usage of iPad in 2015 (36%).





Leverage iPad to Transform Learning

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.

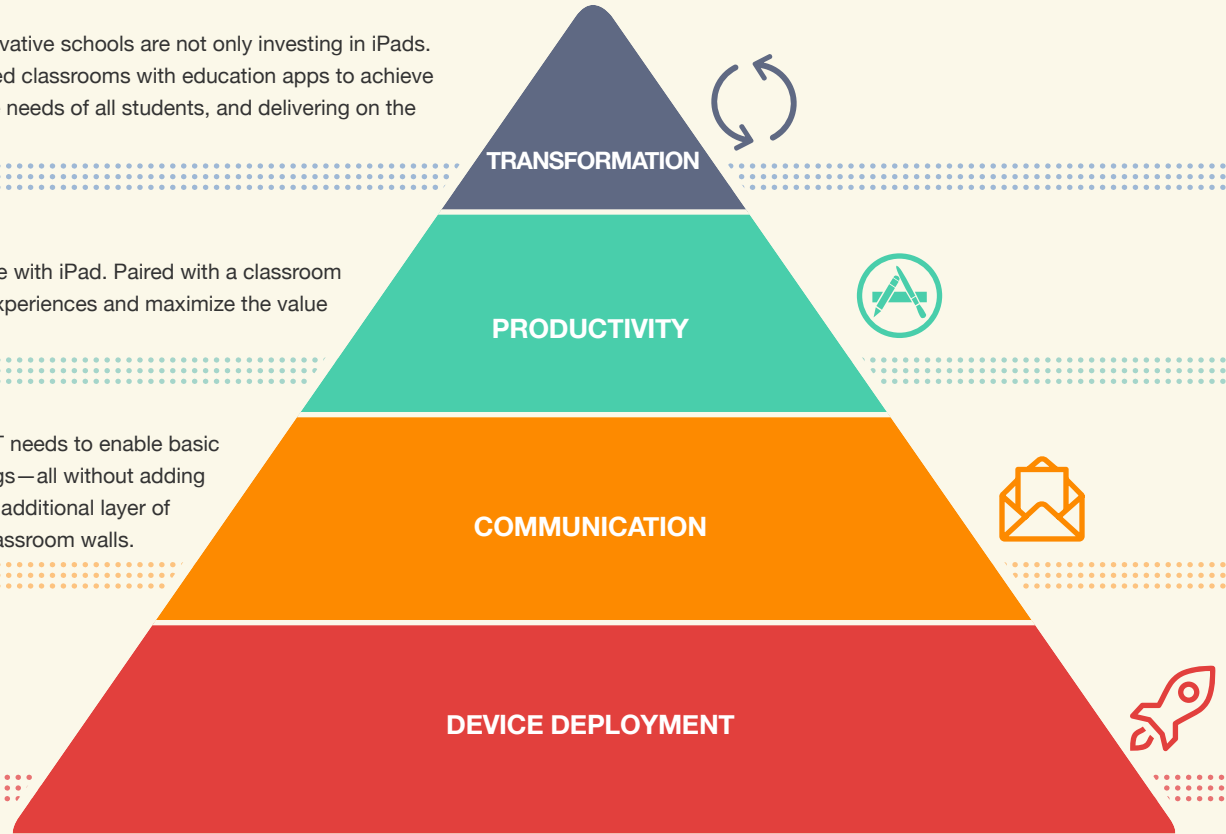
Maslow's hierarchy of needs serve as an analogy for what is possible in education with iOS. Device deployment and communication are the basic needs of any school. However, iOS is so much more. It is the gateway to educational transformation. As schools look to modernize teaching and personalize learning, iOS apps are a mechanism to turn classrooms into interactive environments and provide individualized learning paths.

TRANSFORMATION: To transform what is possible in education, the most innovative schools are not only investing in iPads. They are pairing innovative teaching methods such as blended learning or flipped classrooms with education apps to achieve individualized learning. The result is higher student engagement, addressing the needs of all students, and delivering on the goal of academic success.

PRODUCTIVITY: Communication is simply a stepping stone for what is possible with iPad. Paired with a classroom management app, teachers are better equipped to create productive learning experiences and maximize the value of precious classroom time.

COMMUNICATION: Once devices are in the hands of teachers and students, IT needs to enable basic communications for them. This includes access to email, Wi-Fi, and VPN settings—all without adding unnecessary bloat. On top of the basic communication functions, apps offer an additional layer of connectivity. For example, learning Edmodo enables communication beyond classroom walls.

DEPLOYMENT: Schools need to tackle the challenge of deployment, device configurations, and inventory. This is the lowest layer of the pyramid and the foundation for any school looking at significant quantities of iOS devices.



Mobile Device Management Overview

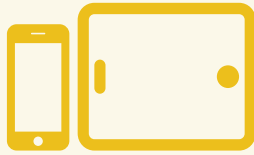


What is MDM?

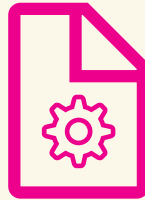
Mobile device management (MDM) is Apple's framework for managing iOS. To effectively manage iOS devices and unleash their full potential, organizations require an equally powerful MDM solution. From deploying new devices and gathering inventory, to configuring settings, managing apps, or wiping data,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



Deployment



Inventory



Configuration Profiles



Management Commands



App Deployment


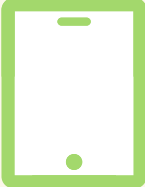




Security and Privacy

Deployment



Before you can use MDM to manage your iOS devices, you first have to enroll them. For iPad, 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 web page, or automated deployment with MDM.

		Description	User Experience	Supervision	Best For
 Automated deployment with MDM		Automatic enrollment over the air	User receives shrink-wrapped box, and the device is automatically configured when turned on	Yes—wirelessly	Everyone
Apple Configurator 2		Enrollment through a Mac app that connects to devices via USB	N/A—IT manages this process and hands devices to users	Yes—wired	iPad carts
User Initiated via URL		Manual enrollment over the air	User visits a specific URL to automatically configure their device	No	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 school-owned devices are put into supervision mode.

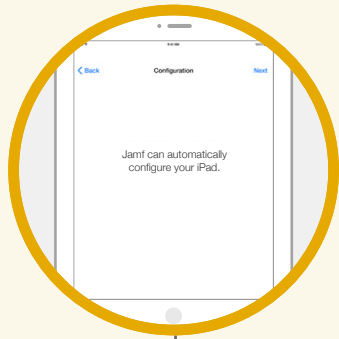
Examples of Supervision-only Commands:

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

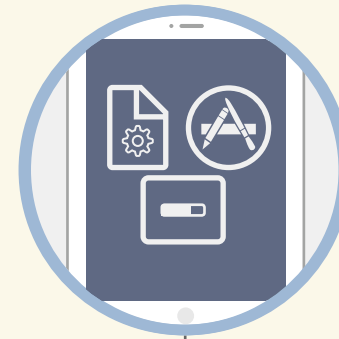
Best Practice: Automated Deployment with MDM and Apple School Manager



Sign up for Apple School Manager via <https://school.apple.com/> and add your MDM server to the Apple School Manager portal.



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



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!

1

2

3

4

5



Purchase devices and link them to your Apple School Manager account. No need to unbox devices before the school year begins.



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

Inventory

MDM is 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.



Collect Data 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 education 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

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 rename the device.











Available Profile Payloads for MDM





THE BASICS

-  **Passcode**
-  **Restrictions**
-  **Wi-Fi**
-  **VPN**
-  **Home Screen Layout**
-  **Single App Mode**








EMAIL ACCOUNTS

-  **Mail**
-  **Exchange ActiveSync**
-  **Google Account**
-  **LDAP**
-  **Calendar**
-  **Contacts**
-  **Subscribed Calendars**
-  **OS X Server Account**

INTERNET SETTINGS

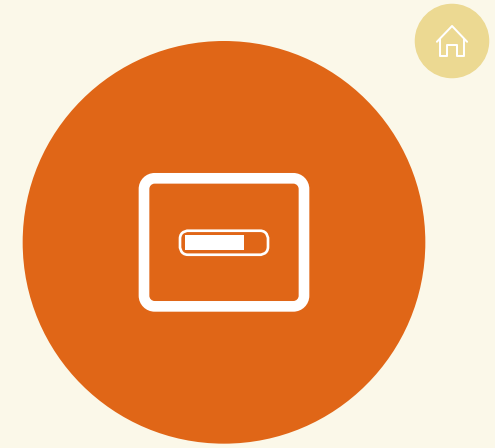
-  **Global HTTP Proxy**
-  **Content Filter**
-  **Domains**
-  **Cellular**

OTHER SETTINGS

-  **AirPlay**
-  **AirPrint**
-  **Fonts**
-  **Certificates**
-  **SCEP**
-  **Lock Screen Message**
-  **Notifications**

Management Commands

Management commands are specific actions that you can apply to individual devices to ensure security of student 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



LOST
MODE

Shared iPad Only



LOGOUT
USER



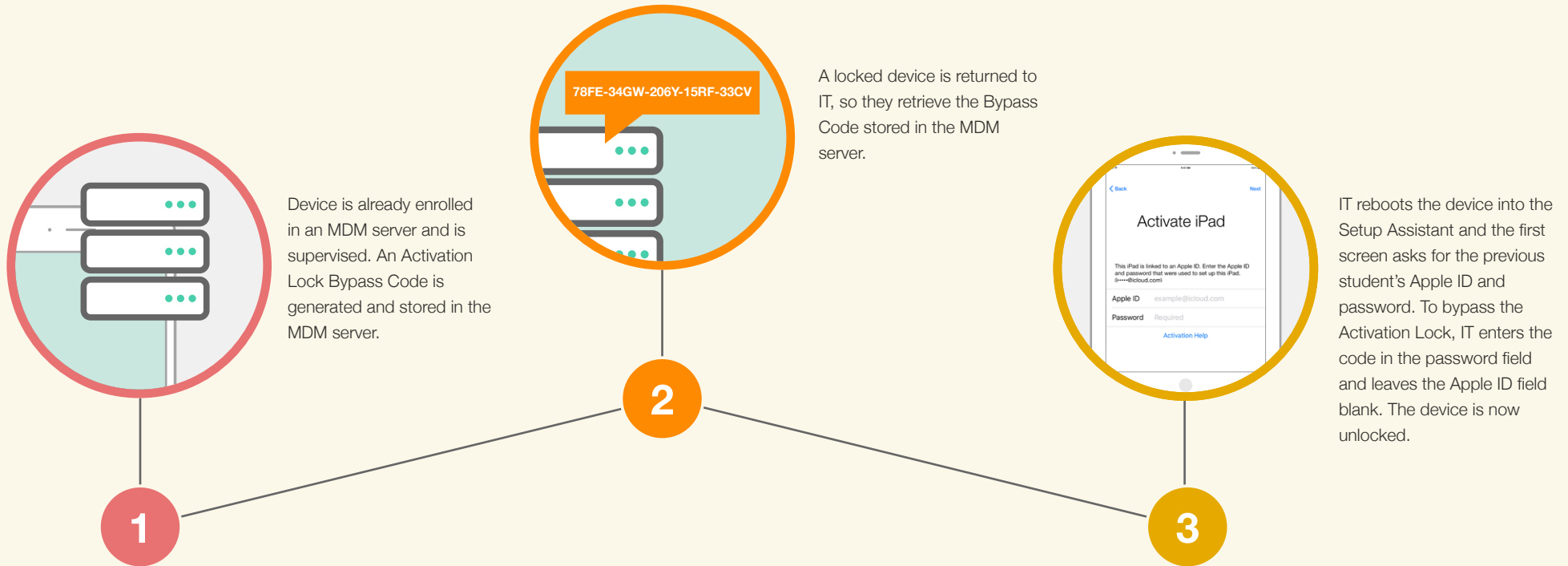
DELETE
USER



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.



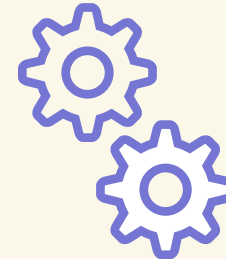


App Deployment

An iOS device serves as a great communication tool out of the box, but the rich library of personal and education apps in the iOS App Store can enhance user productivity and help your students achieve even more. Further, you can use iOS App Store apps to turn an iPad into a video production studio, science laboratory, planetarium, and much more. With an app strategy and MDM to manage your app deployments, you will ensure students and teachers have the apps they need—configured and secure for your school.



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 and reassigned by MDM.

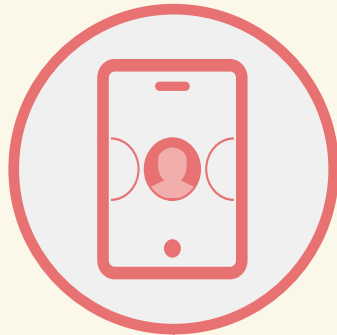
Managed Open In

Managed Open In takes the concept of managed apps a step further by controlling the flow of data from one app to another. With MDM, organizations can restrict what apps are presented in the iOS share sheet for opening documents. 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: Deploy Apps with MDM



Sign up for Apple School Manager via <https://school.apple.com> and link to your MDM server.

1



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

3



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

2



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

4

Best Practice: Managed Apple IDs



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 is identified by an email address and password, and may be linked to contact, payment, and security details.

Why Are Apple IDs Important for Schools?

An Apple ID allows students to take full advantage of iOS and the App ecosystem. For example, students can download educational apps, ebooks, and iTunes U content using their Apple ID.

Best Practice: Managed Apple IDs

Schools can create Managed Apple IDs in bulk for all teachers, students, and staff across an entire district. Unlike a personal Apple ID, a Managed Apple ID is controlled by the school, and can be customized with specific user roles and service restrictions. For example, Managed Apple IDs cannot be used with Apple Pay or to purchase apps through the App store. When a student graduates or leaves the district, their school administrator can transfer their Apple ID account, giving them the ability to take all their school-related work with them.

Shared iPad: Managed Apple ID Required

With Shared iPad, a student can leverage their Managed Apple ID to log into a specific iPad to access their assigned apps and content as well as their individual school work.



Security and Privacy

Security and privacy concerns are major issues for schools. iOS has a number of security features built right into the mobile operating system to keep both student and teacher data safe. Additionally, with Apple's commitment to student privacy, parents and students can feel safe knowing that Apple does not allow geo-tracking for devices. Coupling these features with MDM, you can ensure that your devices, apps, and network are secure while users feel safe using their devices.



Native Apple Security Features



Lost Mode

With Lost Mode, schools now have the ability to locate and recover lost or stolen Apple devices without compromising student privacy through ongoing location tracking. When Lost Mode is activated, the iOS device receives a customized lock screen message, is disabled from use, and sends its location to IT.



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.

iPad in the Classroom



iPad and Classroom Management



iPad changes the way teachers teach and the way students learn. With the right classroom management strategy and a robust tool to support it, teachers feel more confident enhancing the classroom experience with technology.

With Apple's Classroom app, configured by MDM, teachers have a tool to manage four common classroom challenges:



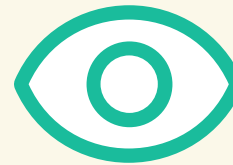
Transitions

Streamline transitions to maximize class time. Easily switch students from one app to the next as the lesson continues. Regain attention on the teacher by momentarily locking the screen. And, reset forgotten passwords immediately without calling IT.



Collaboration

Encourage interactivity and collaboration through the Classroom app. When it's time to share work with the class, a teacher can easily project a student's iPad to the big screen using Apple TV—making the transition seamless for the student when it's time to present.



Focused Engagement

To help students stay on task, teachers can easily focus a student's iPad on a specific app or webpage. This can be helpful during both work time or when it's time for an assessment or quiz.



Classroom Awareness

Check in with each student and see where they are at in the lesson or how they are tackling an assignment. Teachers can view what each student is working on and see what they see on their iPad. Nothing replaces 1:1 interaction, but with the Classroom app, teachers are able to turn their attention to who needs it the most.



Educational Apps and iBooks for iPad

With over 170,000 education apps in the App Store designed specifically for iPad, Apple has the strongest education app ecosystem for students of any grade level, age, or learning style. In addition to a wide variety of education apps, students enjoy a whole new learning experience through interactive iBooks.



Schoology: A learning management system (LMS) that helps teachers prepare and engage with students through engaging content, interactive lessons, and dynamic assessments.



eSpark: Delivers a personalized learning experience for each student based on curated educational app content provided by eSpark.



eBackpack: Creates a paperless classroom by assigning, collecting, review, annotating, and returning student work through eBackpack.



Edmodo: Provide teachers a safe and easy way to communicate, engage, and collaborate with students for free any time, anywhere.



Nearpod: Easily manage student iPad content and seamlessly combine interactive presentations, collaboration, and real-time assessments tools into one integrated solution.



Socrative: Students can now easily share their lesson understanding by answering formative assessment questions in a variety of formats.

Education apps for parents too!

Many of the education apps found in the App Store provide a parent's version available for download. That way parents can stay more involved with what their students are learning, and how they're progressing.



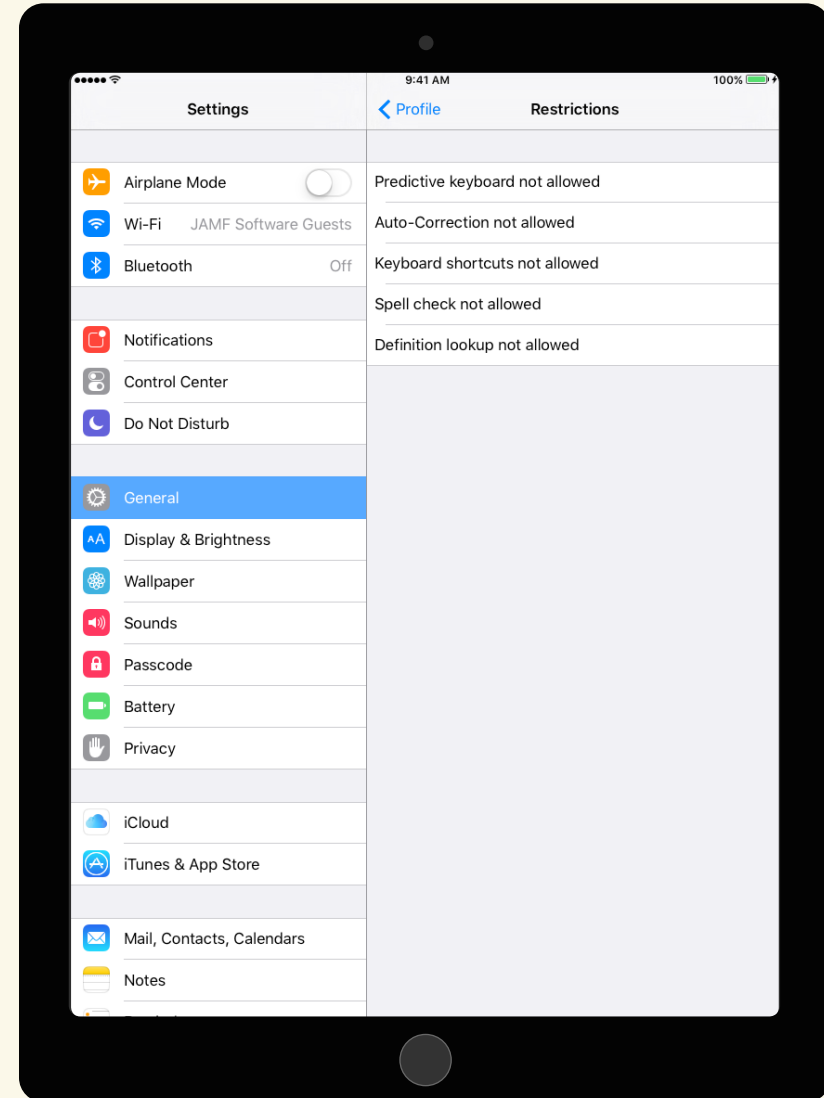
Secure Assessments with iPad

Whether administering formative or summative assessments, have peace of mind that iPad provides a secure platform. By combining MDM restrictions and a classroom management app, you can focus each student on a specific webpage or app until the assessment is complete.

With MDM, IT can configure restrictions on an iPad during the assessment.

Common restrictions include the ability to disable:

- ✓ Predictive keyboard
- ✓ Keyboard shortcuts
- ✓ Auto correct
- ✓ Check spelling
- ✓ Definition look up





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, the Jamf Pro makes mobile device management easy, so you can better ensure a transformative learning experience.



Deploy



Inventory



Configuration Profiles



Management Commands



App Deployment



Security



Self Service



Apple School Manager



Classroom Management

[Start Managing iOS with a Free Trial](#)

Appendix: 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 - Functionality

- Allow use of camera
- Allow screenshots
- Allow voice dialing
- Allow Siri
- Allow Siri while device locked
- Allow installing apps using Apple Configurator and iTunes
- Allow In-App Purchase
- Require iTunes password for all purchases
- Allow iCloud backup
- Allow iCloud keychain
- 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 internet results in Spotlight
- 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

Restrictions payload - Apps

- Allow iTunes Store
- Allow Safari
- Enable AutoFill
- Force fraud warning
- Enable JavaScript
- Block pop-ups
- Accept cookies

Restrictions payload - Media Content

- Select ratings region
- Set content rating for Movies, TV Shows, and Apps
- Allow playback of explicit media
- Allow explicit sexual content in iBooks Store

Other Payloads

- Wi-Fi payload
- Domains payload
- VPN payload
- AirPlay payload
- AirPrint payload
- Mail payload
- Google Account payload
- LDAP payload
- Calendar payload
- Contacts payload
- Subscribed Calendars payload
- Web Clips payload

Management Commands

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

Managed + Supervised

Make MDM Profile Mandatory (DEP only)

Restrictions payload - Functionality

- Allow FaceTime
- Allow AirDrop
- Allow iMessage
- Allow screen observation by Classroom
- Allow Apple Music
- Allow Apple Radio
- Enable Siri profanity filter
- Allow user-generated content in Siri
- Allow iBookstore
- Allow apps from App Store
- Allow automatic app downloads
- Allow removing apps
- Allow iCloud documents & data
- Allow managed apps to store data in iCloud
- Allow Erase All Content and Settings
- Allow installing configuration profiles
- Allow modifying account settings
- Allow modifying cellular data app settings
- Allow modifying device name
- Allow modifying Find My Friends settings
- Allow modifying passcode
- Allow modifying Touch ID fingerprint
- Allow modifying restrictions
- Allow modifying Wallpaper
- Allow pairing with non-Configurator hosts
- Allow pairing with Apple Watch
- Allow predictive keyboard
- Allow keyboard shortcuts
- Allow Auto-Correction
- Allow Check Spelling
- Allow definition lookup

Restrictions payload - Apps

- Allow News
- Allow Podcasts
- Allow Game Center
- Allow multiplayer gaming
- Allow adding Game Center friends
- Restrict App Usage



Other Payloads

- Global HTTP Proxy payload
- Content Filter payload
- Single App Mode
- OS X Server Account payload
- Notifications payload
- Lock Screen Message payload
- Home Screen Layout payload

Management Commands

- Set Wallpaper
- Bypass Activation Lock
- Update iOS (DEP Enrollment Required)
- Lost Mode
- Delete User (Shared iPad only)
- Logout User (Shared iPad only)