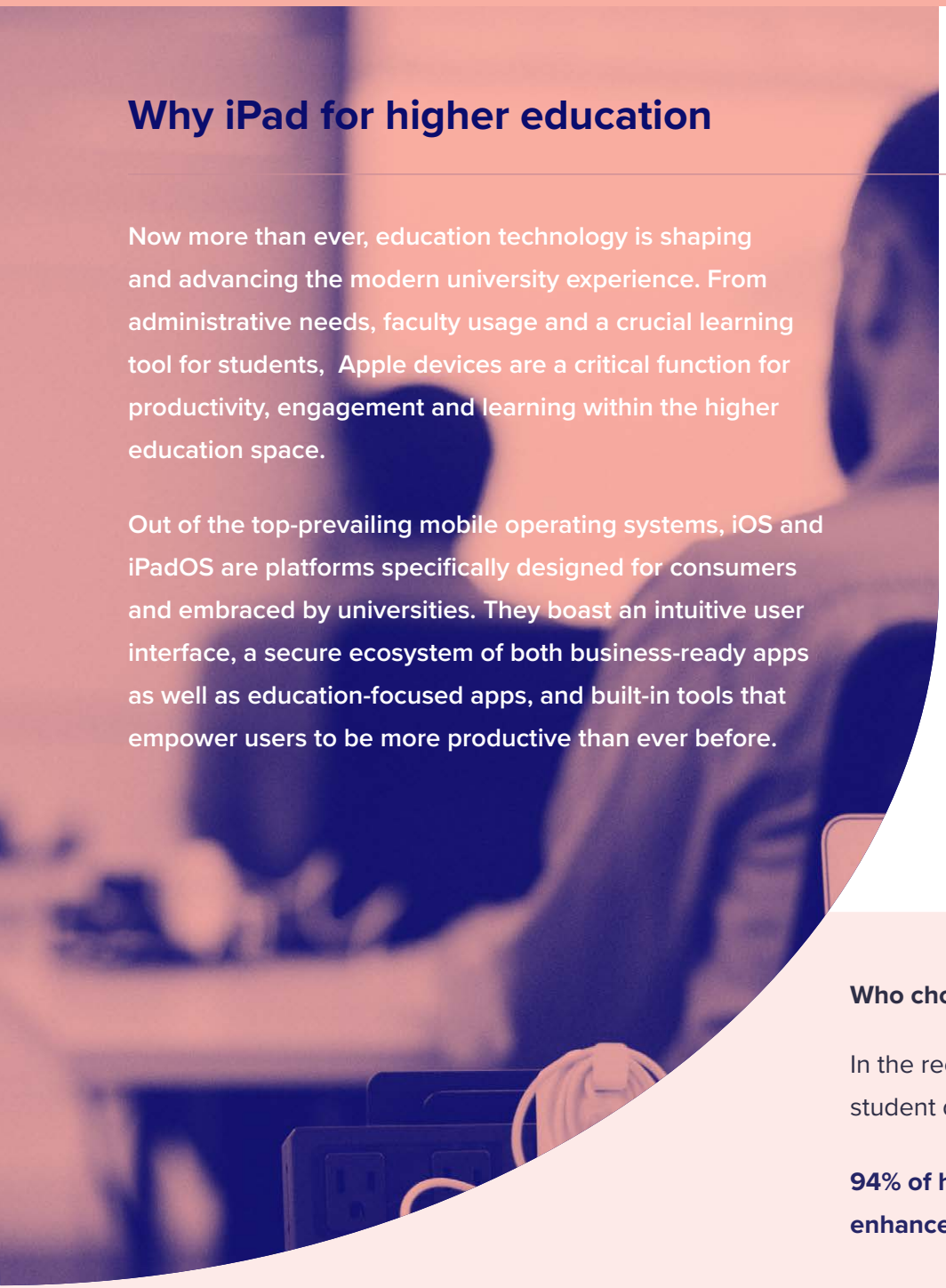
Mobile Device Management 101

FOR HIGHER EDUCATION

Get more out of Apple in higher education

jamf

The state of Apple in higher education



Why iPad for higher education

Now more than ever, education technology is shaping and advancing the modern university experience. From administrative needs, faculty usage and a crucial learning tool for students, Apple devices are a critical function for productivity, engagement and learning within the higher education space.

Out of the top-prevailing mobile operating systems, iOS and iPadOS are platforms specifically designed for consumers and embraced by universities. They boast an intuitive user interface, a secure ecosystem of both business-ready apps as well as education-focused apps, and built-in tools that empower users to be more productive than ever before.

Apple empowers universities with:

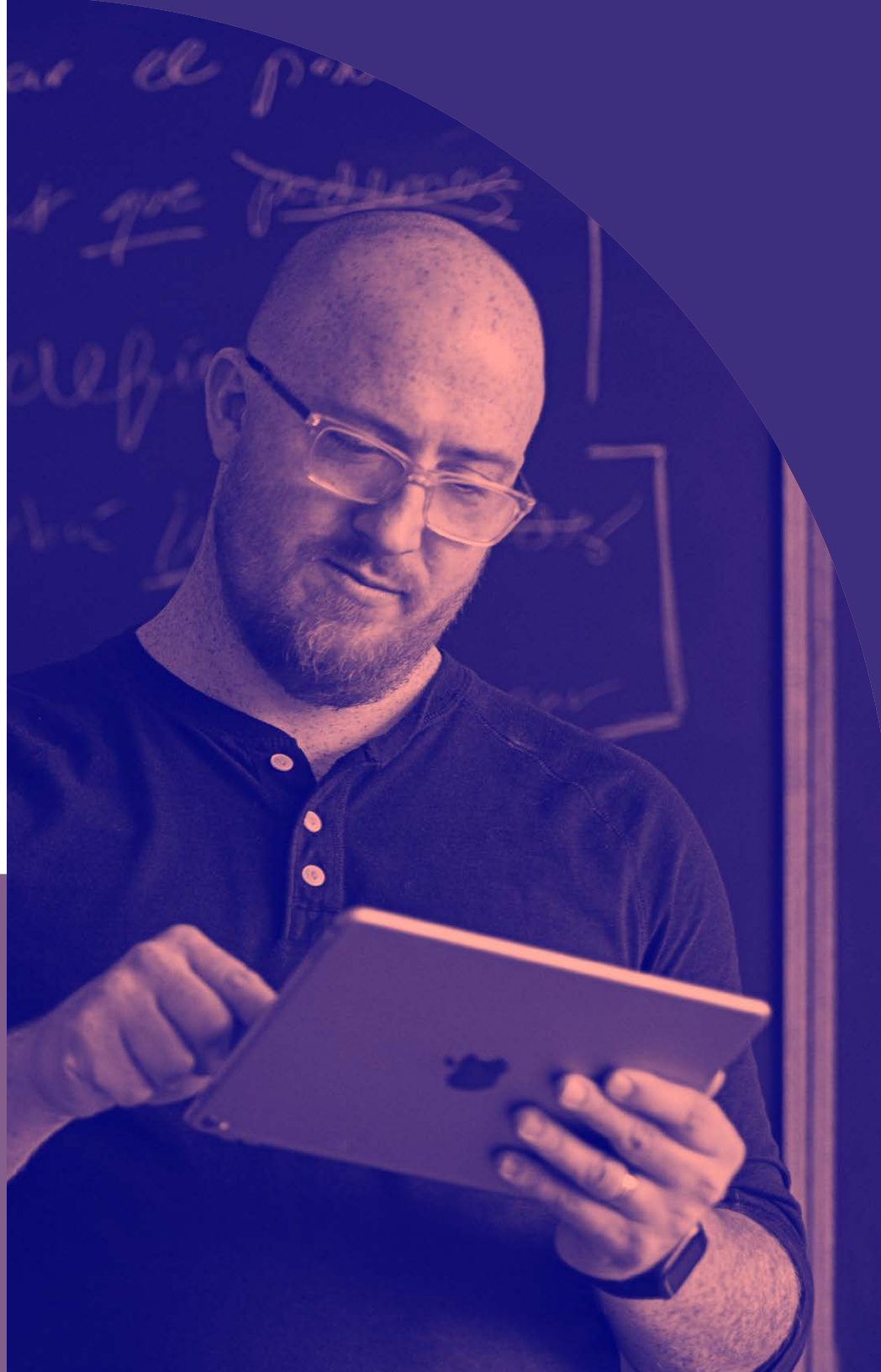
- Fastest and most efficient mobile hardware
- Native hardware-based encryption to keep data secure
- Touch and Face ID for biometric security
- Productivity apps to create documents, spreadsheets and presentations including Microsoft Office for iOS
- Split-screen multitasking for iPad
- Built-in support for modern, secure wireless networking, such as VPN and single sign-on
- Built-in Microsoft Exchange support for email, calendars and contacts

Who chooses iPad in higher education?

In the recent **Vanson Bourne survey** on the importance of student device choice when preparing for the modern workforce:

94% of higher education institutions say they use iPad to enhance learning

Mobile device management overview

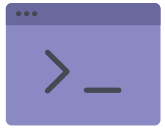


Why MDM is necessary

Mobile device management (MDM) is Apple's framework for managing iPadOS (operating system for iPad) and iOS (operating system for iPhone). To effectively manageApple devices and unleash their full potential, universities 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 deployments and ensure device security.

Deployment

Inventory



Configuration Profiles

Management Commands

App Deployment

Security and Privacy

The Architecture for MDM

Apple Push Notification service

When you send commands to Apple devices, your MDM server communicates with Apple's Push Notification service (APNs). APNs 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

Before you can use an MDM solution to manage your Apple 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 iPad, including enrollment via Apple Configurator, a user-based enrollment via a webpage, or automated zero-touch deployment with MDM and Apple School Manager.

Apple School Manager

Everything you need in one location

First introduced with iOS 9.3, Apple School Manager is a tool that allows IT administrators to more easily manage people, devices and content in a central, web-based portal. Apple School Manager simplifies higher education deployments by consolidating previous Apple deployment programs into one. Now with iOS 10.3 and higher, it is even easier to manage educational devices with Apple School Manager.

When schools pair iPad with education-supported mobile device management (MDM) solutions, they are able to:

- Automate device enrollment, setup and distribute apps and content
- Create Managed Apple IDs
- Utilize Shared iPad

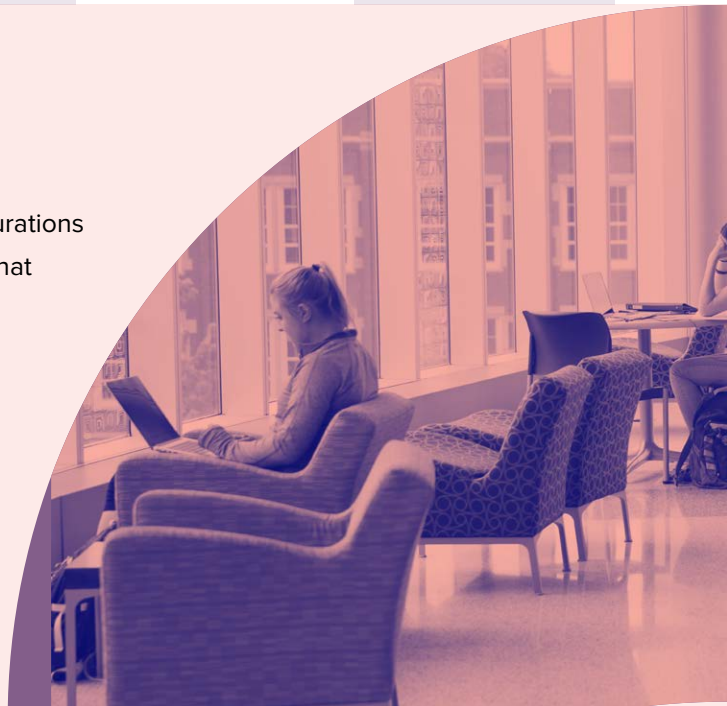
Deployment methods	Description	User experience	Supervision	Best for
Automated deployment with MDM and Apple School Manager	Automatic enrollment over the air (also referred to as zero-touch deployment)	User receives shrink-wrapped box, and the device is automatically configured when turned on	Yes, wirelessly	Everyone
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	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 iPadOS that enables deeper management by an MDM solution. 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...



Zero-touch deployments with MDM and Apple School Manager in higher education

1

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

2

Purchase devices and link them to your Apple School Manager account. No need to unbox devices.

3

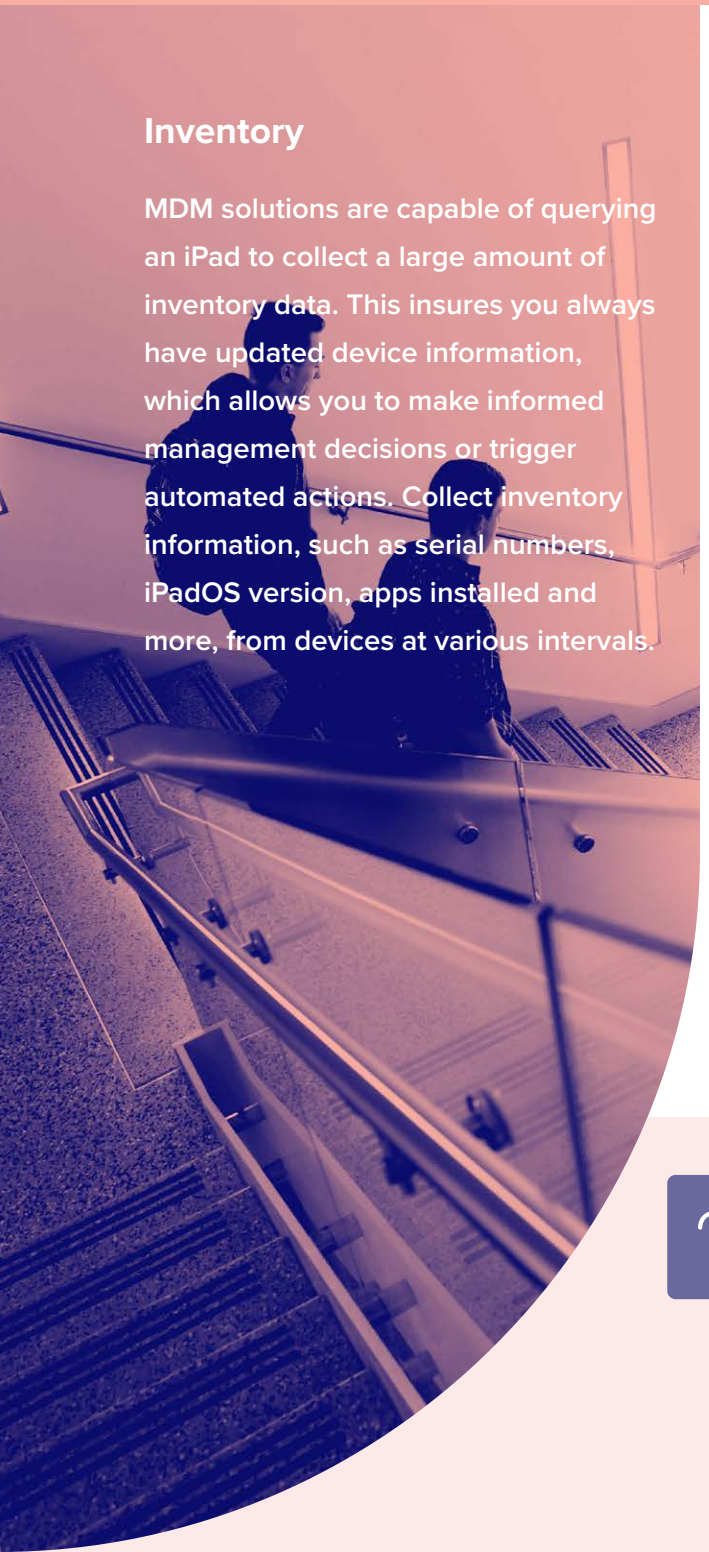
As a user turns their iPad on for the first time, the device will automatically be enrolled — no additional interaction is needed.

4

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

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 iPad to collect a large amount of inventory data. This insures you always have updated device information, which allows you to make informed management decisions or trigger automated actions. Collect inventory information, such as serial numbers, iPadOS version, apps installed and more, from devices at various intervals.

Examples of data collected with MDM

Hardware Details

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

Software Details

- OS 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?

Use the inventory data from the MDM and empower yourself to answer common questions like: Are all my devices secure? How many apps do we have deployed? What version of iPadOS do we have deployed?

Configuration profiles

Configuration profiles give you the ability to tell your devices how 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. Configuration profiles also have the ability to restrict items in iPadOS, such as the Camera, Safari web browser or even the ability to rename 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

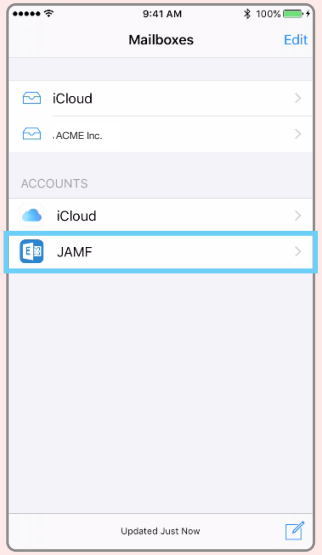
- Global HTTP Proxy
- Content Filter
- Domains
- Cellular
- Network Usage Rules
- Certificates

Other Settings

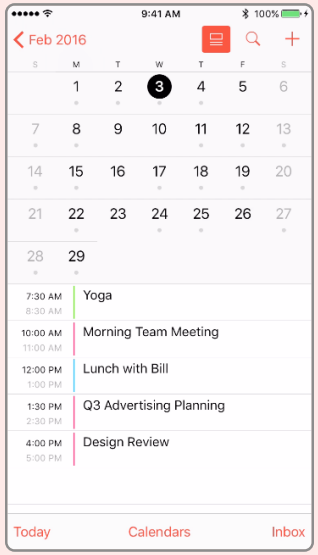
- AirPlay
- AirPlay Security
- Conference Room Display
- AirPrint
- Fonts
- SCEP
- Lock Screen Message
- Notifications
- Single Sign-on
- Access Point Name

Eliminate containers for iPadOS management

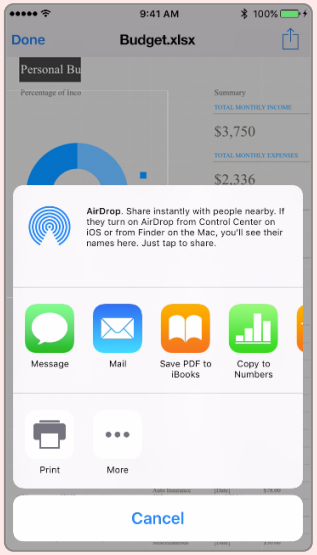
In the world of MDM, a container is an additional app designed to serve as a secure location for information such as email, calendars, contacts and even web browsing. Organizations are drawn to this concept, but it gets in the way of a good user experience. Containers became popular among some MDM solutions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



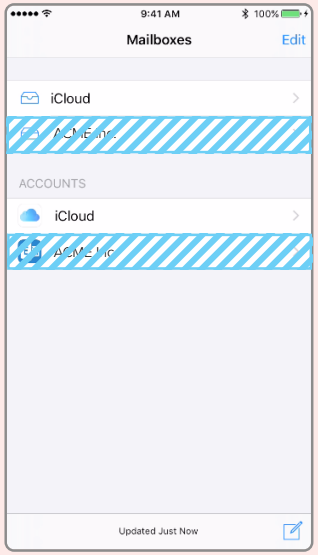
A configuration profile adds an Exchange account next to a user’s personal email account in the native Mail app.



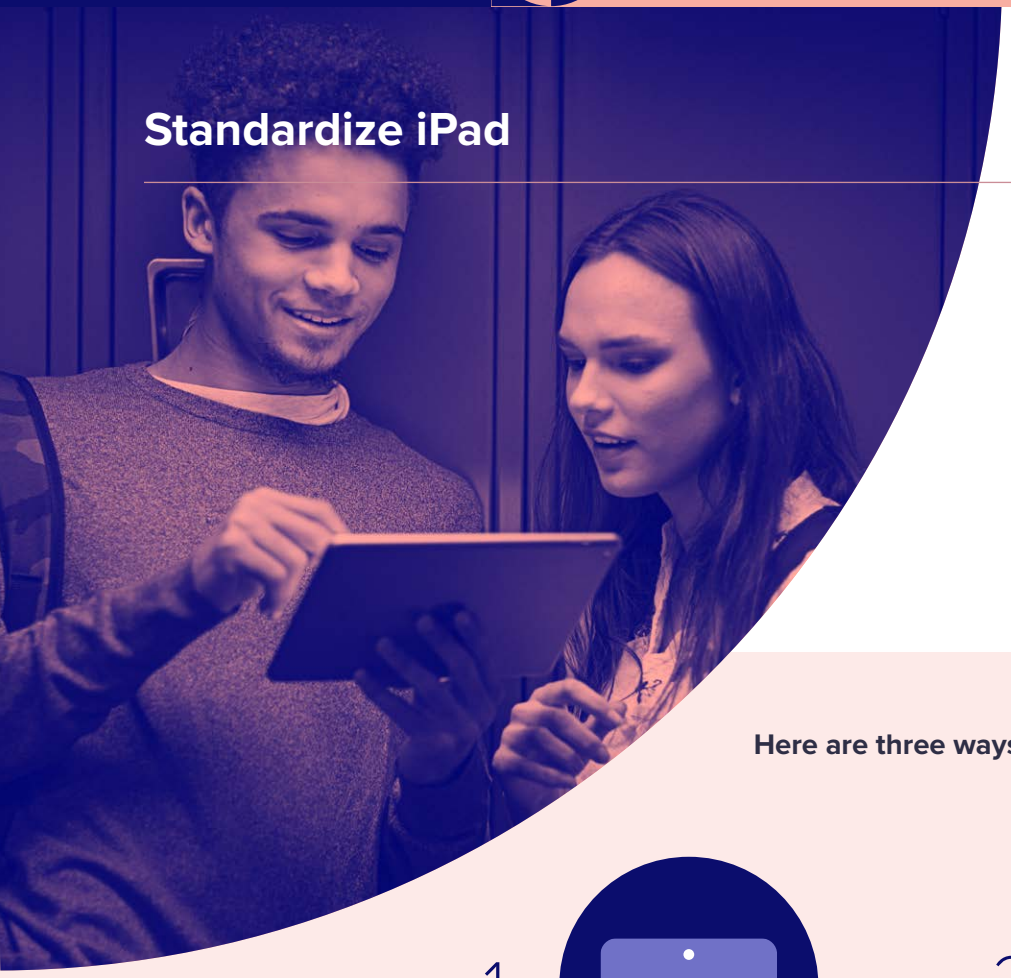
Corporate data now lives right next to personal data in the native apps, preserving user experience and security.



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.



Standardize iPad

Whether your iPad devices are used for students during lecture, or for staff and faculty as part of their job, help improve user productivity by offering a consistent experience on your institutionally owned devices. Standardizing Apple devices for your users 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 at your university:

1

Show/hide apps

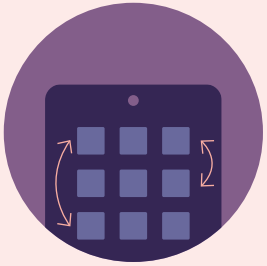
Display only the apps your staff and students need and hide the ones that are not necessary for their work.

2

Set the Home screen wallpaper

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

3



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.

Management commands

Management commands (also known as MDM commands), are specifications 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 iPadOS to the latest version, and change the device name to make it easier for IT to manage their devices.

Available commands for MDM


Update Inventory


Lock Device


Clear Passcode


Clear Restrictions


Unmanage Device


Wipe Device


Send Blank Push


Set Wallpaper


Send Notification


Update iOS


Change Name


Lost Mode & Sound


Shutdown Device


Restart Device

Shared iPad Only


Logout User


Delete User

Manage Activation Lock with MDM

Activation Lock is designed to prevent the theft of iPhone and iPad devices. They both require an Apple ID and password, which means only those with that information can activate the devices. This feature is great for theft prevention, but can also cause problems for IT admins if they are not managing their students' Apple IDs. This, however, is easier to manage when pairing Activation Lock with an MDM. If a device is enrolled in an MDM, and it is supervised, an Activation Lock Bypass Code will allow the IT admin to unlock the device.

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. They retrieve the Bypass Code stored on the MDM server.

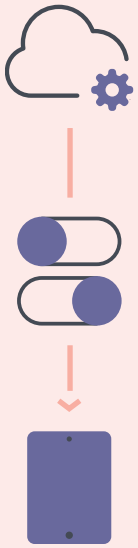
3

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

iPad serves as a great out-of-the-box communication tool on its own, but the rich library of personal and education apps in the App Store can enhance user can enhance a student's productivity and overall learning experience. Apps can transform 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?

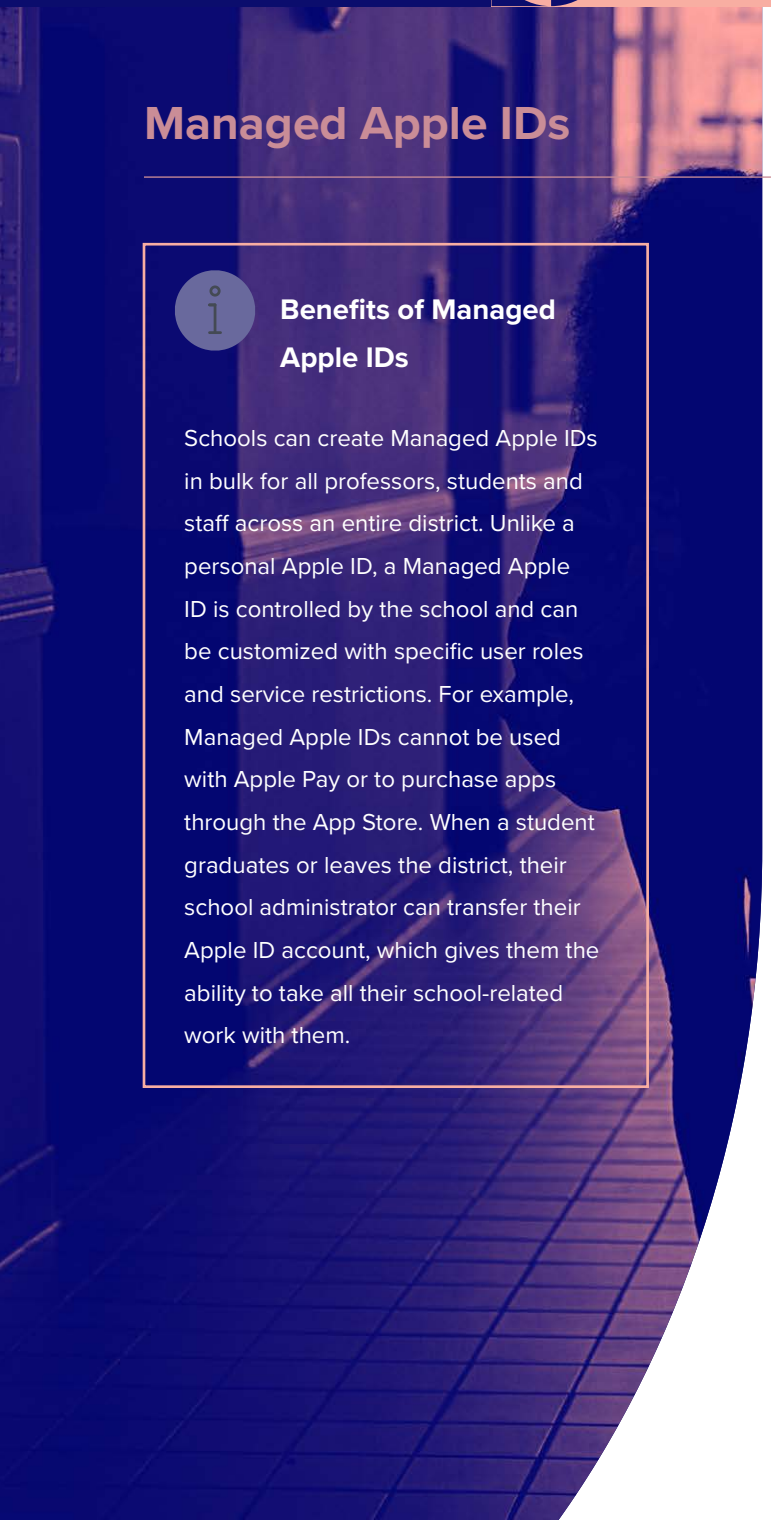
Introduced in iOS 5, managed apps differ from a standard app, because they are flagged as owned by an organization. Specifically, managed apps are distributed via an MDM solution and can be configured and reassigned by MDM.

Managed App Configuration

Sometimes deploying an app isn't enough. You'd like to pre-customize some of the settings. This is the premise for Managed App Configuration. App developers can customize what settings can be pre-configured by an MDM server for their app. For example, you could deploy the Box app with a pre-populated server URL. After entering a username and password, the app is operational.

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 iPadOS share sheet for opening documents. This allows for truly native data management without the need for a container.



Managed Apple IDs

Benefits of Managed Apple IDs

Schools can create Managed Apple IDs in bulk for all professors, 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, which gives them the ability to take all their school-related work with them.

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.

What about university owned apps?

Since the App 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.

Why are Apple IDs important for institutions?

An Apple ID allows students to take full advantage of iPadOS and the app ecosystem. For example, students can download educational apps, e-books and iTunes U content using their Apple ID.

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 as Apple IDs support two-step authentication.

Security and privacy

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

Lost Mode

With Lost Mode, schools 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 iPad receives a customized lock screen message, is disabled from use and sends its location to IT.

Encryption

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

Pre-app VPN

Virtual Private Networks (VPN) have long been implemented in higher education institutions 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 universities 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 and Face ID

A fingerprint sensor and facial recognition have been added to newer iPadOS devices, adding biometric security to the operating system. Touch ID and Face ID can be used to unlock a device and sign into certain apps. Fingerprint and facial data are stored locally on the device and is never shared with Apple.

Enforcing encryption on managed devices

To keep data private and protected, enforcing encryption on all managed devices is highly recommended. By applying a configuration profile to managed Apple devices that requires a passcode, data encryption is enabled.

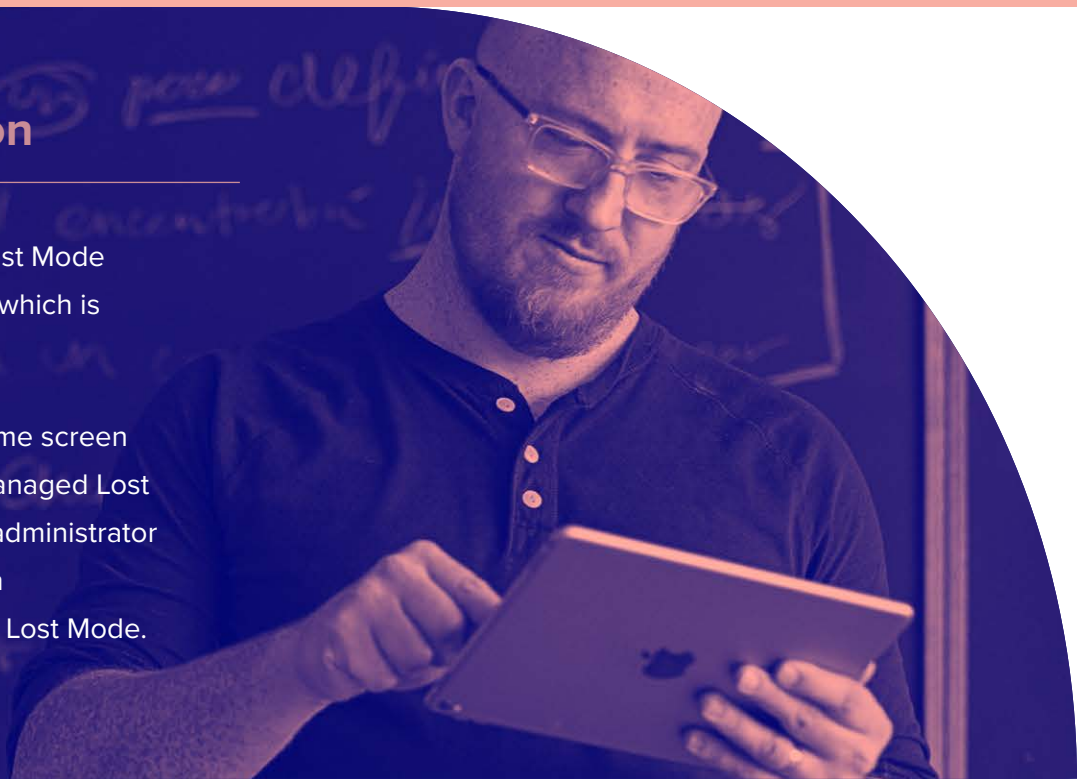
Within your configuration settings you can specify:

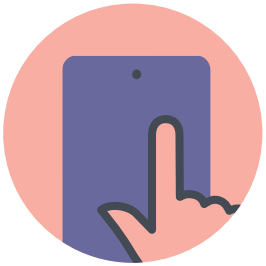
- Length of passcode
- Simple or complex passcodes
- Passcode rotation frequency
- Allow or deny previously used passcodes
- Auto lock time
- Maximum number of failed passcode attempts before wiping the device

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 feature. This setting can provide the device location, which is instrumental in finding lost or stolen devices.

Additionally, by requiring a passcode on the device, access to the Home screen is prevented, data privacy stays intact and the device is encrypted. 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.





Ensure devices are Supervised and disable the removal of the MDM profile using your MDM solution.

Set a lock screen message and apply physical asset tags that clearly show the device is owned by the institution. This will help deter theft.

Utilize Lost Mode if a device is missing. This disables the device, displays a custom message and reports the GPS coordinates.

Moving higher education forward with Apple TV

As mobile demands increase within higher education institutions, it's important that all of your technology can 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 wireless 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, schools 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 classrooms and offices.

jamf

MDM for higher education

Jamf is the leading mobile device management tool for Apple in higher education. Designed to automate common tasks around Apple deployment, inventory and security, Jamf makes device management easy, so you can better ensure a transformative learning experience while maintaining a secure environment.

Ready to get started?
Start unleashing the power of Apple and Jamf for your institution.

Request Trial