iOS Education Deployment Overview

iPad brings an amazing set of tools to the classroom. Teachers can easily customise lessons using rich media and online courses. And students stay engaged and eager to learn using hands-on creative tools and apps on iPad.

This document offers guidance for how to deploy iOS devices in your school and how to get the most out your investment. It covers the following topics to help you create a deployment plan that best suits your environment:

- Deployment models
- Preparing your infrastructure
- Initial setup
- Configuring and managing devices
- Distributing apps
- Ongoing management
- Support options

Deployment Models

There are three models commonly used to deploy iOS devices in an education setting: institution-owned one-to-one deployment, student-owned device deployment and shared-use deployment. While most institutions have a preferred model, your institution may use multiple models.

The following are a few examples of how these models would be applied in an education institution:

- A high school may plan and deploy an institution-owned one-to-one model for all years.
- A system may first deploy an institution-owned one-to-one model at a single high school, then roll out identical models for the entire system.
- A K–6 school may deploy an institution-owned one-to-one model in the primary school, and a shared-use model for younger students.
- In higher education, a department may deploy an institution-owned one-to-one model, although it is also common to see the student-owned model deployed campus-wide or across multiple campuses.

Exploring these models in more detail will help you identify the best deployment model for your unique environment. Once you've identified the preferred deployment models for your institution, your team can explore Apple's deployment and management capabilities in detail. These programs and tools are covered at an overview level within this guide, and in greater detail in the iOS Deployment Reference.

Institution-owned one-to-one deployment

An institution-owned one-to-one deployment model creates the greatest opportunity for iOS devices to positively impact the learning process.

In a typical deployment, your institution purchases devices for all eligible students and instructors. This could be for a particular year level, a single department, or an entire school or university.

In this model, each user is assigned a device that's configured and managed by your institution. A Mobile Device Management (MDM) solution can simplify and automate this process. If the devices are purchased from Apple or participating Apple Authorised Resellers or carriers, your institution can use the Device Enrolment Program (DEP) to automate enrolment in MDM, so devices can be handed directly to users with customised settings and content pre-installed.

Users will also need an Apple ID. Once students have their Apple ID, they can get started using the built-in Setup Assistant to configure basic settings and have their devices automatically enrolled in MDM. They can then personalise their devices further or download their own content. You can send users invitations to download educational content, such as apps purchased through the Volume Purchase Program (VPP), or iTunes U courses. Your institution can deliver or update these resources over the air at any time during the academic year.

With Caching Server, most of these downloads can come from your local network. If your devices are supervised, apps will be installed automatically.

Learn more about Caching Server at www.apple.com/sg/osx/server/features/#caching-server.

The following table illustrates the administrator and user responsibilities for this deployment model.

Prepare	
Administrator: • Investigate, procure and deploy an MDM solution, such as Profile Manager or a third-party system. • Sign up for the DEP and VPP. • Unbox and (optionally) asset-tag the device.	**Users:** • Create an Apple ID, iTunes Store account and iCloud account.
Set up and configure	
Administrator: • Assign devices in the DEP for supervision and streamlined MDM enrolment, or use Apple Configurator to configure and supervise devices. • Configure and install accounts, settings and restrictions wirelessly, via MDM.	**Users:** • Receive the device. • Personalise the device using Setup Assistant and enter a personal Apple ID. • Enter institution credentials in Setup Assistant for the DEP (optional). • Device settings and configurations are automatically received via MDM.
Distribute apps and books	
Administrator: • Purchase apps through the VPP and assign them to users via MDM. • Send VPP invitations to users. • Install Caching Server to speed up content delivery over the local network.	**Users:** • Accept the VPP invitation. • Download and install apps assigned by the institution. • If the device is supervised, apps can be pushed to the device automatically.

Ongoing management	
Administrator: • Revoke and reassign apps to other users via MDM, as needed. • Using MDM, query managed devices to monitor compliance, or trigger alerts if users add unapproved apps. • Use MDM to lock devices, reset device passwords, remotely wipe any managed accounts or data, or wipe a device entirely. • Deploy Apple TV to support AirPlay.	**Users:** • Back up the device to iTunes or iCloud, to save documents and other personal content. • If the device is lost or stolen, use Find My iPhone to locate it.

Student-owned device deployment

In this model, students set up and configure their own devices. To enable access to institutional services such as Wi-Fi, mail and calendars, or to configure the device for specific classroom requirements, institutions commonly enrol student-owned devices in an MDM system. In K–12 environments, MDM can also play a roll in managing student-owned devices.

Having access to an institution's services acts as an incentive for users to enrol their devices in the institution's MDM server. Doing so ensures that all configuration settings, policies, restrictions, apps and other content are deployed automatically and unobtrusively, yet remain under the control of the institution. MDM enrolment is an 'opt in' process, so students can remove any content or services they don't need managed once they complete a course, graduate or leave the institution.

The following table illustrates the administrator and user responsibilities for this deployment model.

Prepare	
Administrator: • Investigate, procure and deploy an MDM solution, such as Profile Manager or a third-party system. • Sign up for the VPP.	**Users:** • Unbox and activate the device. • Create an Apple ID, iTunes Store account and iCloud account, if applicable.
Set up and configure	
Administrator: • Enrol devices using self-service setup, and configure accounts, settings and restrictions wirelessly using MDM, based on user or group policies defined by your institution.	**Users:** • Personalise the device using Setup Assistant and (optionally) enter a personal Apple ID. • Enrol in MDM.
Distribute apps	
Administrator: • Purchase apps through the VPP and assign them to users via MDM. • Send VPP invitations to users. • Install Caching Server to speed up content delivery over the local network.	**Users:** • Accept the VPP invitation. • Download and install apps assigned by the institution. • Update iOS and apps on the device.

Ongoing management	
Administrator:	**Users:**
• Revoke and reassign apps to other users via MDM, as needed. • Using MDM, query managed devices to monitor compliance, or trigger alerts if users add unapproved apps or content. • Use MDM to lock devices, reset device passwords, remotely wipe any managed accounts or data, or wipe a device entirely.	• Back up the device to iTunes or iCloud to save documents and other personal content. • If the device is lost or stolen, use Find My iPhone to locate it. • When the MDM relationship is removed, managed accounts and data are removed, but personal apps, data and content remain.

Shared-use deployment

In a shared-use model, the institution purchases iOS devices for use in a classroom or lab, and students share these devices throughout the day. Personalisation is limited on these devices, so this deployment model prevents institutions from taking full advantage of a personalised learning environment for every student. In addition to device rotation among older students, this approach can be used for one-to-one deployments in a highly controlled context, such as in lower grades. Device personalisation remains minimal in alternative deployment approaches.

Because institution staff members perform the setup, configuration and management, shared-use deployments are more tightly managed than one-to-one deployments. In a shared-use deployment, your institution takes responsibility for installing apps and other content necessary for learning.

The following table illustrates administrator and user responsibilities for this deployment model.

Prepare	
Administrator:	**Users:**
• Investigate, procure and deploy an MDM solution, such as Profile Manager. • Sign up for the VPP. • Unbox and (optionally) asset-tag the device. • Create institutional Apple ID(s) for each instance of Apple Configurator.	• No action necessary at this stage.

Set up and configure	
Administrator:	**Users:**
• Use Apple Configurator to configure and supervise devices. • Use Apple Configurator to enrol devices in MDM (optional). • Use Apple Configurator or MDM to install accounts, settings and restrictions.	• No action necessary at this stage.

Distribute apps	
Administrator:	**Users:**
• Purchase apps from the VPP and deploy them using redemption codes for installation and management with Apple Configurator.	• No action necessary at this stage.

Ongoing management	
Administrator: • Use Apple Configurator to update iOS on the devices. • Periodically reset devices to standard configuration using Apple Configurator. • Install and update apps on the devices using Apple Configurator. • Using MDM, query managed devices to monitor compliance, or trigger alerts if users add unapproved apps or content. • Use MDM to lock devices, reset device passwords, remotely wipe any managed accounts or data, or wipe a device entirely. • Regularly back up the Mac running Apple Configurator, as VPP purchases are managed locally.	**Users:** • No action necessary at this stage.

Preparing Your Infrastructure

After choosing the right deployment model(s), it's time to evaluate your existing network infrastructure to make sure your institution takes full advantage of everything that iOS offers.

Wi-Fi and networking

Consistent and dependable access to a strong network is critical to setting up and configuring iOS devices. As you plan your iOS device deployment, you'll need to make sure that your institution's Wi-Fi network and supporting infrastructure are robust and up to date. In addition, being able to support multiple devices with all your students and teachers connecting simultaneously is important to the success of your overall program.

iOS devices and your users must have access to your wireless network and Internet services for setup and configuration. You may need to configure your web proxy or firewall ports if devices are unable to access Apple's activation servers, iCloud or the iTunes Store.

You should also make sure your network infrastructure is set up to work correctly with Bonjour, Apple's standards-based, zero-configuration network protocol. Bonjour enables devices to automatically find services on a network. iOS devices like iPad use Bonjour to connect to AirPrint-compatible printers and AirPlay-compatible devices such as Apple TV. Some apps also use Bonjour to discover other devices for collaboration and sharing.

For more details on Wi-Fi and networking for education deployments, see the iOS Deployment Reference. Appendix B, 'Wi-Fi Infrastructure', explains the wireless technologies and standards iOS devices use, and provides information on designing wireless networks.

Learn more about Bonjour at www.apple.com/sg/support/bonjour.

Caching Server

Caching Server is an integrated feature of OS X Server that stores a local copy of frequently requested content from Apple servers, helping minimise the amount of bandwidth needed to download content. Caching Server speeds up the download and delivery of software through the App Store, the Mac App Store, the iTunes Store and iTunes U. It can also cache software updates for faster downloading to iOS devices.

Learn more about Caching Server at www.apple.com/sg/osx/server/features/#caching-server.

Mobile Device Management

Whether your institution offers an iPad for each user, shares devices among multiple users or relies on student-owned devices, it's essential to manage the devices properly. You can securely enrol — or register — your devices in an MDM solution. This allows you to wirelessly configure and update settings, monitor compliance with your institution's policies, deploy apps and remotely wipe or lock managed devices.

There are many MDM solutions available for iOS management. These third-party solutions support a variety of server platforms and can be accessed through off-premises cloud services. Each offers its own management consoles, features and pricing. Before choosing a solution, review the resources listed below to evaluate which management features are most relevant for your institution.

In addition to third-party MDM solutions, Apple offers Profile Manager, a feature of OS X Server. Profile Manager makes it easy to configure iOS devices so they're set up using your institution's specifications. Profile Manager has three components: a web-based administration tool, a self-service user portal for enrolling devices and downloading configuration profiles, and an MDM server.

Learn more about MDM at www.apple.com/sg/education/it/mdm.

Learn more about Profile Manager at www.apple.com/sg/osx/server/features/#profile-manager.

Initial Setup

After you've prepared your infrastructure, you'll want to set up Apple IDs, which you'll need to access key services from Apple such as iCloud. Understanding Apple IDs will help you inform your users about how to set up their own. An Apple ID is also required for users to configure their own devices through Setup Assistant — a feature of iOS that helps them get up and running quickly.

Apple ID

An Apple ID is an identity used to log in to Apple services such as the iTunes Store, the App Store and iCloud. These services give students access to a wide range of content to support creativity, collaboration, productivity and learning. With an Apple ID, students can store the content they create in their own accounts — so their work travels with them no matter which computer or device they use. Whether they're installing apps assigned in class or backing up homework to iCloud an Apple ID allows students to own their learning — and their content — even when they leave school.

For one-to-one and student-owned device deployments, each user should have their own Apple ID, so they can install apps provided by your institution; take notes in iBooks that they can access across multiple iOS devices; and enrol in iTunes U courses.

In a shared-use deployment, you can use an institution-owned Apple ID to deploy content on multiple devices via Apple Configurator.

Learn how to sign up for an Apple ID at appleid.apple.com/en_SG.

iCloud

iCloud lets users store personal content such as contacts, calendars, documents and photos, and keep them up to date on multiple devices.* Users can also share documents and projects with other iCloud users, anywhere and at any time. iOS devices use iCloud to automatically back up app data, photos and settings. And iCloud offers the ability to locate lost or stolen devices using a feature called Find My iPhone.

Some services — such as iCloud Photo Sharing, iCloud Keychain, iCloud Drive and iCloud Backup — can be disabled by using restrictions either entered manually on the device or set via configuration profiles.

Note: iCloud is not available in all areas, and features may vary by area.

Learn more about iCloud at www.apple.com/sg/icloud.

Setup Assistant

iOS includes Setup Assistant to help users activate the device, configure basic settings and personalise preferences such as language, location services, Siri, iCloud and Find My iPhone. Users can take iPad straight out of the box and use these features to get up and running, or your institution can perform these basic setup tasks before distributing the devices to students. When devices are configured for Apple's DEP, MDM enrolment is integrated into Setup Assistant.

Configuring and Managing Devices

Before you deploy your iOS program, decide how you'll configure and manage the devices. IT teams and teachers can configure classroom devices using configuration profiles or over the air via MDM. Additional configuration options are available for supervised devices.

Configuration profiles

A configuration profile is an XML file that allows you to distribute configuration information to an iOS device. Configuration profiles automate the configuration of settings, accounts, restrictions and credentials. They can be installed through an email attachment, downloaded from a web page or installed on devices through Apple Configurator. If you need to configure a large number of devices or just prefer a low-touch, over-the-air deployment model, configuration profiles can be delivered through MDM.

Configuring devices via MDM

MDM enables schools and other institutions to enrol and manage devices securely, consistently and easily. With an MDM solution in place, IT teams or teachers can configure and update settings, monitor compliance with institutional policies, and remotely wipe or lock managed devices. MDM also makes it easy to distribute, manage, and configure apps purchased through the VPP.

Users enrol the device in an MDM server using an enrolment configuration profile or by following a URL. Individuals can complete this step themselves, or you can use the DEP to automate the enrolment process for institutionally owned devices (see below for details).

Supervised devices

To enable additional configuration options and restrictions, you may choose to supervise iOS devices owned by your institution. For example, supervision lets you silently push VPP apps, disallow the modification of account settings, and filter web connections via Global Proxy to make sure users' web traffic stays within the institution's network.

By default, all iOS devices are unsupervised. You can combine supervision with MDM remote management to manage additional settings and restrictions. To enable supervision of your institution's devices, use the DEP or Apple Configurator, and choose to supervise only devices that are owned by your institution.

Device Enrolment Program

The DEP provides a fast, streamlined way to deploy institutionally owned iOS devices purchased from Apple or participating Apple Authorised Resellers or carriers, allowing you to easily and wirelessly set up, configure and supervise devices.

After your institution enrols in the DEP, simply log in to the program website, link your MDM server to the program and assign the devices to users via MDM. Once a user has been assigned, any MDM-specified configurations are automatically installed using the Setup Assistant.

Learn more about the DEP at www.apple.com/sg/education/it/dep.

Apple Configurator

Apple Configurator — a free OS X application available from the Mac App Store — enables administrators to conveniently set up and configure multiple iOS devices at once via USB before deploying them to users. With this tool, your institution can quickly configure and update multiple devices to the latest version of iOS, configure device settings and restrictions, preconfigure MDM enrolment, and install apps and content.

Apple Configurator is ideal for scenarios where users share iOS devices that need to be quickly refreshed and kept up to date with the correct settings, policies, apps and data.

Learn more about Apple Configurator at help.apple.com/configurator/mac/1.4/#.

Distributing Apps

There are several ways to purchase and deliver apps and other content to your users. The most scalable method is to purchase apps through the VPP and assign them to users via MDM — a process called managed distribution. If multiple users are sharing devices, you can install apps and content locally using Apple Configurator.

Volume Purchase Program

The VPP gives educational institutions a simple way to purchase iOS apps in volume, and distribute them with MDM or Apple Configurator to students, teachers, administrators and employees.

The program also enables app developers to offer a 50 per cent discount on purchases of 20 units or more to eligible institutions, including any K–12 school, or any accredited, degree-granting higher education institution.

Distributing apps and books with managed distribution

iOS allows an institution to distribute free and paid apps over the air using MDM. With managed distribution, institutionally created books and EPUB books — as well as PDF documents — can be automatically pushed to devices and removed remotely.

MDM solutions integrate with the VPP, enabling your institution to purchase apps in volume, and automatically assign them to specific users or groups. Managed apps can be removed remotely by the MDM server or when the user removes their own device from MDM. When a user no longer needs an app, you can use MDM to revoke the app and reassign it to a different user. And you can use Caching Server to speed up the delivery of apps purchased through the VPP over your local network.

Learn more about the VPP at www.apple.com/sg/education/it/vpp.

Installing apps and content with Apple Configurator

In addition to its basic setup and configuration capabilities, you can use Apple Configurator to install apps and content. Apple Configurator is most helpful when it's used to supervise devices that won't be personalised by the user, such as shared iPad devices in a classroom. When you configure devices with Apple Configurator, you can install paid apps purchased through the VPP using redemption codes, as well as free apps.

Apple Configurator also allows you to install documents so they're available when your users start using the devices. Documents are available for apps that support iTunes file sharing. You can review or retrieve documents from iOS devices by connecting them to a Mac running Apple Configurator.

Ongoing Management

With iOS 8, teachers can now manage devices and content in the classroom. After iOS devices are configured and enrolled in MDM, they can be managed wirelessly from anywhere. And MDM can help with remote management tasks like reassigning apps, querying devices and resetting device passwords.

Queries

An MDM server can query devices for a variety of information. This includes hardware information, such as serial number, device UDID or Wi-Fi MAC address, and software information, such as the iOS version and a detailed list of all apps installed on the device. This information can be used to help ensure users maintain the appropriate set of apps.

Commands

When a device is managed, the MDM server can perform a wide variety of administrative commands, including changing configuration settings automatically without user interaction, locking or wiping a device remotely or clearing a passcode lock so the user can reset their password. An MDM server can also request an iOS device to begin or end AirPlay Mirroring to a specific destination.

Single-app mode

This setting limits your device to a single app to help users stay focused on a task. For example, you can conduct single-app assessments on iPad. Single-app mode is enabled through managed apps on devices that are supervised via MDM.

App configuration

You can install new configuration settings before or after managed apps are installed. For example, an app could be configured to automatically open in a certain screen or section of a specified app.

AirPlay and Apple TV

Using AirPlay, teachers and students can wirelessly stream content from an iPad (or Mac) to a classroom projector or HDTV via Apple TV. Teachers can lead a class brainstorm or walk everyone through a presentation. And students can share projects and other work on the big screen.

iOS 8 supports the ability to stream content from an iOS device to Apple TV, even if the devices are on different networks or no network is available. Peer-to-peer AirPlay lets a user connect directly from a supported iOS device to an Apple TV without first connecting to your network. This eliminates the need to join the right network or disclose Wi-Fi passwords, and it avoids connection issues in complex network environments. Peer-to-peer AirPlay and Apple TV are enabled by default in iOS 8.

AirDrop

AirDrop allows wireless sharing among devices. The ability to share large files with ease can transform classroom workflows. Teachers can share and collect assignments via AirDrop, and students can share projects and documents.

Accessibility

iOS is the world's most advanced — and most accessible — mobile operating system. Innovative features like VoiceOver, Switch Control and Guided Access help those with special needs enjoy more of what iPad has to offer.

Learn more about iOS and accessibility at www.apple.com/sg/accessibility/ios.

Support Options

Apple provides a variety of programs and support options for iOS users. Before deploying devices, find out what's available for your institution and plan for any additional support you'll need.

AppleCare OS Support

AppleCare OS Support includes AppleCare Help Desk Support and incident support. This includes support for system components, network configuration and administration; integration into heterogeneous environments; professional software applications, web applications and services; and technical issues requiring the use of command-line tools for resolution.

AppleCare Help Desk Support

AppleCare Help Desk Support provides priority telephone access to Apple's senior technical support staff. It also includes a suite of tools for diagnosing and troubleshooting Apple hardware, which can help your institution manage resources more efficiently, while improving response time and reducing training costs. AppleCare Help Desk Support covers an unlimited number of support incidents for hardware and software diagnosis, and troubleshooting and issue isolation for iOS devices.

AppleCare for iOS device users

Every iOS device comes with a one-year limited warranty and complimentary telephone technical support for 90 days after the purchase date. This service coverage can be extended to two years from the original purchase date with AppleCare+ for iPhone, AppleCare+ for iPad or the AppleCare Protection Plan (APP) for iPod touch. You can call Apple's technical support experts as often as you like to get help with questions. Apple also provides convenient service options when devices need to be repaired. In addition, AppleCare+ covers up to two incidents of accidental damage, each subject to a service fee.

iOS Direct Service Program

As a benefit of AppleCare+ and the AppleCare Protection Plan, the iOS Direct Service Program enables your help desk to screen devices for issues without calling AppleCare or visiting an Apple Retail Store. If necessary, your institution can directly order a replacement iPhone, iPad, iPod touch or in-box accessories.

Learn more about AppleCare programs at www.apple.com/sg/support/products.

Summary

Whether your institution deploys iOS devices to a school, a university or a single classroom, there are many options for easy deployment and management. Choosing the right strategies for your organisation can help your team deliver devices and content that will open up a world of new learning opportunities in your institution.

Learn more about integrating iOS into institutions at www.apple.com/sg/education/it.

For more detailed technical information about deploying iOS, explore the iOS Deployment Reference at help.apple.com/deployment/ios.

*Some features require a Wi-Fi connection. Some features are not available in all countries. Access to some services is limited to 10 devices.