iOS Education Deployment Overview

iPad brings an amazing set of tools to the classroom. Teachers can easily customize lessons with interactive apps, rich media, and online courses. And students stay engaged and eager to learn with 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. This overview covers the following topics to help you create a deployment plan that best suits your environment:

- Deployment models
- Preparing your infrastructure
- Initial setup
- Configure and manage devices
- Distribute apps
- Ongoing management
- Support options

Deployment Models

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

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

- A middle school may deploy an institution-owned one-to-one model for all grade levels.
- A large district may first deploy an institution-owned one-to-one model at a single high school, then roll out identical models for the entire district.
- A K–8 school may deploy both an institution-owned one-to-one model for fifth through eighth grades, and a shared-use model for kindergarten through fourth grades.
- In higher education, a department may deploy an institution-owned one-to-one.
- In higher education, it's common to see the student-owned model at the campus or multicampus level.

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 online iOS Deployment Technical Reference.

Institution-owned one-to-one

An institution-owned one-to-one deployment model provides 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 grade level, a department, or an entire school district, college, 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 Authorized 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 custom settings and content.

Users will also need an Apple ID. Once students have their Apple IDs, they can get started by using the built-in Setup Assistant to configure basic settings and have their devices automatically enrolled in MDM. They can then personalize their devices further or download their own content. You can send users invitations to download apps purchased through the Volume Purchase Program (VPP), or to enroll in iTunes U courses. Your institution can deliver or update these resources over the air anytime during the school 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: www.apple.com/osx/server/features/#caching-server

The following table illustrates the responsibilities of both the administrator and the user for this deployment model:

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

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

Student-owned

In this model, devices are set up and configured by the student. To use institutional services such as Wi-Fi, mail, and calendars, or to configure the device for specific classroom requirements, student-owned devices are commonly enrolled in an MDM system provided by the institution. In K–12 environments, MDM can also play a roll in managing student-owned devices.

Access to an institution's services acts as an incentive for users to enroll their devices in the institution's MDM server. This ensures that all configuration settings, policies, restrictions, apps, and 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 responsibilities of both the administrator and the user for this deployment model:

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

Ongoing management	
Administrator:	Users:
• Revoke and reassign apps to other users as needed with MDM. • With MDM, an administrator can query managed devices to monitor compliance, or trigger alerts if users add unapproved apps or content. • MDM can also lock devices or 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, the user can locate it with Find My iPhone. • When the MDM relationship is removed, managed accounts and data are removed, but the user's personal apps, data, and content are kept.

Shared use

In a shared-use model, iOS devices are purchased by the institution for use in a classroom or lab, and they are shared by students throughout the day. Personalization is limited on these devices and therefore institutions using this deployment model can't take full advantage of a personalized learning environment for every student. In addition to device rotation in a shared-use model, this approach could be used for a one-to-one deployment in a highly controlled context, such as in a lower-grade level deployment. Device personalization is minimal in this case as well.

Because the setup, configuration, and management are performed by your institution's staff, 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 the responsibilities of both the administrator and the user for this deployment model:

Prepare	
Administrator:	Users:
• Investigate, procure, and deploy an MDM solution, such as Profile Manager. • Sign up for 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 enroll 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 using VPP and deploy them using redemption codes for installation and management with Apple Configurator.	• No action necessary at this stage.

Ongoing management

Administrator:

- Update iOS on the device with Apple Configurator.
- Periodically reset devices to standard configuration using Apple Configurator.
- Install and update apps on the device with Apple Configurator.
- With MDM, you can query managed devices to monitor compliance, or trigger alerts if users add unapproved apps or content.
- MDM can also lock devices or reset device passwords, remotely wipe any managed accounts or data, or wipe a device entirely.
- Regular backup of the Mac running Apple Configurator is necessary, because VPP purchases are managed locally.

Users:

- No action necessary at this stage.

Preparing Your Infrastructure

After choosing the right deployment models, 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 simultaneous connections from all your students and teachers 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 iTunes Store.

You should also make sure that your network infrastructure is set up to work correctly with Bonjour, Apple's standards-based, zero-configuration network protocol. Bonjour enables devices to find services on a network automatically. 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 online iOS Deployment Technical Reference. Appendix A, "Wi-Fi Infrastructure," explains the wireless technologies and standards used by iOS devices and provides information on designing wireless networks.

iOS Deployment Reference: help.apple.com/deployment/ios

Learn more about Bonjour: www.apple.com/ca/support/bonjour

Caching Server

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

Learn more about Caching Server: www.apple.com/ca/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 enroll—or register—your devices with a mobile device management (MDM) solution. This allows you to wirelessly configure and update settings, monitor compliance with your institution policies, deploy apps and remotely wipe or lock managed devices.

A broad range of MDM solutions for iOS management are available. These third-party solutions support a variety of server platforms and can be accessed through off-premise cloud services. Each solution 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 a solution called 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 provides 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 mobile device management (MDM): www.apple.com/ca/education/it/mdm

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

Initial Setup

After you've prepared your infrastructure, you'll want to set up Apple IDs, which are required 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 Apple IDs. An Apple ID is also required for users to configure their own devices through Setup Assistant—a feature that lets them get up and running quickly.

Apple ID

An Apple ID is an identity used to log into 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 school work travels with them no matter which computer or device they use. Whether installing apps assigned by school 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 his or her own Apple ID. With an Apple ID, each student can install apps provided by the institution and enroll in iTunes U courses.

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

Learn how to sign up for an Apple ID: appleid.apple.com

iCloud

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

Some services, such as Photo Stream, iCloud Keychain, Documents in the Cloud, and Backup, can be disabled through the use of restrictions either entered manually on the device or set via configuration profiles.

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

Learn more about iCloud: www.apple.com/ca/icloud

Setup Assistant

iOS provides Setup Assistant to activate the device, configure basic settings, and personalize preferences such as language, location services, Siri, iCloud, and Find My iPhone. Users can take iPad right out of the box and use these features to get up and running, or your institution can perform these basic setup tasks. When devices are configured for Apple's Device Enrolment Program, MDM enrolment is integrated into the Setup Assistant.

Configure and Manage Devices

Before you deploy, decide how you'll configure and manage iOS devices. IT teams and teachers can configure classroom devices using either 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. Configuration profiles 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 mobile device management

MDM enables schools and other institutions to enroll 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 Volume Purchase Program (VPP).

Users enroll the device with an MDM server using an enrolment configuration profile or URL. This can be done directly by individuals or automated for institutionally owned devices via the Device Enrolment Program (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 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 remote management via MDM to manage additional settings and restrictions. To enable supervision of your institution's devices, use the Device Enrolment Program or Apple Configurator. You can supervise only devices that are owned by your institution.

Device Enrolment Program

The Device Enrolment Program (DEP) provides a fast, streamlined way to deploy institutionally owned iOS devices that are purchased from Apple or participating Apple Authorized Resellers or carriers, allowing you to easily and wirelessly set up, configure, and supervise devices.

After your institution enrolls in 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 during the Setup Assistant.

Learn more about the Device Enrolment Program: www.apple.com/ca/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 providing 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 in which 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: help.apple.com/configurator/mac/1.4/#

Distribute Apps

There are several ways to purchase and deliver apps and content to your users. The most scalable method is to purchase apps through the Volume Purchase Program and assign them to users with MDM. If you are sharing devices among multiple users, you can install apps and content locally with Apple Configurator.

Volume Purchase Program

The Volume Purchase Program (VPP) gives educational institutions a simple way to purchase 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 percent discount on purchases of 20 units or more to eligible institutions, including any K–12 institution or district, or any accredited, degree-granting higher education institution.

There are several ways to deploy apps and content throughout your institution. The most scalable method is to purchase apps through the Volume Purchase Program and assign them to users with MDM—a process called managed distribution. If you're using a shared-device deployment model, you can install apps and content locally using Apple Configurator.

Distributing apps with managed distribution

iOS allows an institution to distribute free and paid apps over the air using MDM.

MDM solutions integrate with 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 and reassign it to a different user. And you can use Caching Server to speed the delivery of apps purchased through VPP over your local network.

Learn more about the Volume Purchase Program: www.apple.com/ca/education/it/vpp

Installing apps and content with Apple Configurator

In addition to its basic setup and configuration capabilities, Apple Configurator can also be used to install apps and content. Apple Configurator is most helpful when it's used to supervise devices that won't be personalized by the user, such as with shared iPad devices in a classroom. When you configure devices with Apple Configurator, you can install paid apps purchased through VPP using redemption codes, and you can install 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 right 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, such as 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 that 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 users can reset passwords. 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 reachability issues in complex network environments. Peer-to-peer AirPlay and Apple TV are enabled by default in iOS 8.

AirDrop

AirDrop provides 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: www.apple.com/ca/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 to diagnose and troubleshoot Apple hardware, which can help your institution manage resources more efficiently; it also improves response time and reduces 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 with questions. Apple also provides convenient service options when devices need to be repaired. In addition, AppleCare+ for iPhone and AppleCare+ for iPad offer up to two incidents of accidental damage coverage, 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 Store. If necessary, your institution can directly order a replacement iPhone, iPad, iPod touch, or in-box accessories.

Learn more about AppleCare programs: www.apple.com/ca/support/products

Summary

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

Learn more about integrating iOS into institutions: www.apple.com/ca/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.