



iOS Deployment Overview for Education

Contents

- Ownership models
- Deploying institution-owned devices
- Deploying student-owned devices
- Deployment steps
- Personalizing devices
- Support options

iPad and iOS 9 brings an amazing set of tools to the classroom. Teachers and staff can easily customize lessons with interactive textbooks, rich media, online courses, and the productivity features built into every device. And students can access the rich content ecosystem available only on iOS to make learning more relevant and personal.

Apple is committed to making it easier for schools and institutions of all sizes to deploy iPad. With iOS 9 we've enhanced deployment programs and mobile device management to simplify and streamline deployment in both one-to-one and shared environments. Now every student can get up and running quickly—opening up a world of new learning experiences. Apple has a complete set of tools to help you deploy iOS devices:

- Mobile device management (MDM) solutions streamline deployment and management.
- The Device Enrolment Program (DEP) automates enrolment of Apple devices into your MDM solution.
- The Volume Purchase Program (VPP) lets you purchase apps in bulk and distribute them to students.

Note: Not all programs are available in all countries or regions.

This document offers guidance on deploying iOS devices in your school or institution, and covers topics to help you create a deployment plan that best suits your environment.

Ownership models

The process for deploying devices depends primarily on whether your institution or your students own the devices. Your institution will first need to enrol in Apple Deployment Programs for either type of deployment; see the “Apple Deployment Programs” section of this guide.

Institution-owned devices

With an institution-owned device deployment, devices are purchased by your institution from Apple or a participating Apple Authorized Reseller or carrier. In this case, you can provide a device to each student, referred to as a *one-to-one* deployment. This type of deployment could be for a particular grade level; a department; or an entire school district, college, or university. You can also rotate devices among students, referred to as a *shared* deployment.

In general, an institution-owned deployment follows four steps: preparing your institution's infrastructure, setting up devices, deploying them, and ongoing management.

Student-owned devices

With a student-owned device deployment, devices are purchased, set up, and configured by the students or their parents. The general steps for a student-owned device deployment include preparing your institution's infrastructure and ongoing management.

Your institution might include a mix of scenarios. Here are some examples:

- A middle school might plan and deploy an institution-owned one-to-one model for all grade levels.
- A large district might 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 might deploy both an institution-owned one-to-one model for fifth through eighth grades, and a shared deployment for kindergarten through fourth grades.
- In higher education, a department might deploy an institution-owned one-to-one model.
- In higher education, the student-owned model is common at the campus or multicampus level.

Exploring these scenarios will help you identify the best choices for your unique environment. Deployment topics are covered at an overview level in this guide, and in greater detail in the online iOS Deployment Technical Reference: help.apple.com/deployment/ios.

Deploying institution-owned devices

With iOS 9 you can deploy all your institution-owned devices with a set of flexible tools for both one-to-one or shared devices.

One-to-one deployments

A one-to-one deployment 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 staff.

In the one-to-one model, each user is assigned a device that's configured and managed by your institution; an MDM solution simplifies and automates this process. DEP can automate enrolment in MDM, so devices can be handed directly to users—complete with custom settings and content.

One-to-one deployments are covered in more detail in the iPad One-to-One Deployment Planning Guide For Education: help.apple.com/deployment/edu/1-1

Shared

In a shared deployment, iOS devices are purchased for use in a classroom, a lab, a library, or any use case where students share devices throughout the day. Because personalization is limited on these devices, a shared deployment doesn't allow institutions to take full advantage of a personalized learning environment for each student.

The following chart illustrates the actions needed by administrators and users during each phase of institution-owned deployments. Unless otherwise indicated, actions serve both *one-to-one* and *shared* deployments.

| | Administrator | User |
|----------------|--|--------------------------|
| Prepare | Get infrastructure ready Investigate, procure, and deploy an MDM solution Sign up for DEP, VPP Purchase apps and with VPP Unbox and (optionally) asset tag devices | No user action necessary |

| | Administrator | User |
|---------------|---|--|
| Set up | Assign devices in DEP for supervision and streamlined enrolment in MDM Preinstall apps and settings with Apple Configurator 2 (optional) Configure and install accounts, settings, and restrictions wirelessly with MDM Assign apps directly to devices with MDM, assign books to users Install Caching Server to speed up content delivery over the local network | No user action necessary |
| Deploy | One-to-one only Hold deployment event and distribute devices to users | One-to-one only Sign in to school directory services for access to email, calendar, and other services (optional) |
| | Shared only Distribute devices to classroom carts | Shared only No user action necessary |
| Manage | Revoke and reassign apps to other devices with MDM, as needed Query managed devices to monitor compliance or trigger alerts if users add unapproved apps or content Use MDM to lock devices or reset device passcodes and wallpapers, remotely wipe any managed accounts or data, or wipe a device entirely, as needed Deploy Apple TV to support AirPlay Update apps and iOS remotely via MDM Periodically reset devices to standard configuration using Apple Configurator 2 | One-to-one only Set up personal Apple ID to personalize the device and access additional services such as iTunes U (if applicable) Back up the device to iTunes or iCloud to save documents and other personal content Locate lost or stolen devices with Find My iPhone Shared Only No user action necessary |

Deploying student-owned devices

Institutions that support a student-owned model will generally follow two main steps—prepare and manage—when deploying devices.

In this case, students set up and configure their own devices. In a typical higher-education environment, student-owned devices are usually enrolled in an institution’s MDM system to centrally manage institutional services, such as Wi-Fi, mail, and calendars. This case also occurs when devices need to be configured for specific classroom requirements. In K–12 environments, MDM can also play a role in managing student-owned devices.

Getting access to your institution’s services can be an incentive for students to enrol their devices in your MDM server. Doing so ensures that all configuration settings, policies, restrictions and apps are deployed automatically and unobtrusively, yet remain under your control. You’ll want to carefully select the appropriate management settings to make sure students are comfortable and motivated to keep their devices enrolled your institution’s MDM.

The following chart illustrates the actions required for a student-owned deployment.

| | Administrator | User |
|----------------|--|--------------------------------------|
| Prepare | <p>Select and configure an MDM solution, including device settings and policies, that best suits your educational institution</p> <p>Enrol in the Volume Purchase Program</p> <p>Determine the optimal infrastructure, including local and Wi-Fi networks, VPN and security configurations, services integration, caching of software on your local network, and filtering access to the Internet</p> <p>Using VPP, select and purchase apps for initial deployments</p> | Student sets up device |
| Manage | <p>Increase or decrease device management as MDM solutions add functionality</p> <p>Deploy additional VPP or in-house content</p> <p>Update certificates and tokens as necessary</p> | Student opts in to institution's MDM |

Deployment steps

This section provides a closer look at the general steps for deploying devices and apps including preparing infrastructure, setting up devices, deploying them, and managing them. The steps you use will depend on whether your institution or students own the devices.

1. Prepare

After identifying the right deployment for your institution, follow these steps to lay the groundwork. It's important to evaluate and prepare 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 deployments, you'll need to make sure 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.

For setup and configuration, iOS devices and your users need access to your wireless network and Internet services. You might need to configure your web proxy or firewall ports if devices can't access Apple's activation servers, iCloud, or the iTunes Store.

You'll also want to 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 such as 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, 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 Technical 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, the Mac App Store, the iTunes Store, iTunes U, and the 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 student, shares devices between multiple students, or relies on student-owned devices, proper management of the devices is essential. For all three scenarios, you can securely enrol all your devices with an MDM solution. MDM allows you to wirelessly configure and update settings, monitor compliance with your institution's policies, deploy apps and remotely wipe or lock managed devices.

MDM uses configuration profiles to distribute configuration information to iPad devices so you can automate the configuration of settings, accounts, restrictions, and credentials. Alternatively, configuration profiles can be sent as an email attachment, downloaded from a web page, or installed on devices through Apple Configurator 2.

With iOS 9, additional restrictions that prevent changes to pass codes, device names, and wallpapers make it easier for teachers and staff to manage devices in their classroom. iOS 9 also provides the option to turn off AirDrop on managed devices.

A broad range of MDM solutions for iOS management is available. These third-party solutions support a variety of cloud and on-premise server platforms. Each solution offers its own management consoles, features, and pricing. See the resources listed below before you choose a solution so you can evaluate which management features are most relevant for your institution.

In addition to third-party MDM solutions, a solution from Apple is available called Profile Manager, a feature of OS X Server. Profile Manager configures iOS devices and 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 MDM:

- IT in the Classroom: www.apple.com/ca/education/it/mdm
- Profile Manager: www.apple.com/ca/osx/server/features/#profile-manager

Apple Deployment Programs

Apple Deployment Programs are essential to an institution-owned one-to-one deployment.

- With the Device Enrolment Program (DEP), you can automate enrolment of Apple devices enrolled in MDM to streamline deployment.
- The Volume Purchase Program (VPP) allows you to purchase apps in volume and distribute them to users.

All institution-owned deployments take advantage of DEP and VPP. And one-to-one deployments can optionally take advantage of using Apple IDs to further personalize learning.

Sign up for Apple Deployment Programs early so you're prepared to complete the steps required for a successful deployment.

Note: Not all programs are available in all countries or regions.

For more information on program availability, see [What are Apple Deployment Programs?](#)

2. Setup

In this phase, you can leverage Apple Deployment Programs, an MDM solution, or optionally Apple Configurator 2 to configure your devices and assign content. You can approach your setup in several ways, depending on who owns the devices.

Configuring devices with mobile device management

With an MDM solution in place, you can configure and update settings, monitor compliance with institutional policies, and remotely wipe or lock managed devices. With iOS 9 and MDM, it's easy to distribute, manage, and configure apps purchased through VPP.

Device Enrolment Program

DEP provides a fast, streamlined way to deploy institutionally owned iOS devices so you can easily and wirelessly set up, configure, and supervise them. Once you link your MDM server to DEP, you can require all devices to be enrolled in MDM on initial setup.

Learn more about the Device Enrolment Program: www.apple.com/ca/education/it/dep

Supervised devices

To enable additional configuration options, settings, and restrictions, you can supervise iOS devices owned by your institution and remotely manage them using MDM. 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. To enable supervision of your institution-owned devices, use DEP or Apple Configurator 2.

Apple Configurator 2 for preparing devices

Accelerate initial deployments with the completely redesigned Apple Configurator 2. For one-to-one deployments, you can preinstall all your apps, saving time and network bandwidth. And for shared device deployments, you can fully set up iPad all the way to the Home screen. After initial setup, you can continue to manage everything over the air using MDM.

Apple Configurator 2 integrates seamlessly with the Device Enrolment Program to streamline device enrolment with MDM servers. You can also update devices to the latest version of iOS, configure device settings and restrictions, and install apps and other content. Apple Configurator 2 also works with device-based app assignment through VPP.

Apple Configurator 2 is available free on the Mac App Store and runs on OS X El Capitan.

Learn more about Apple Configurator 2: help.apple.com/configurator/mac

Distributing apps

The best way to purchase apps is through VPP. You can then assign them to devices or users using MDM. And with iOS 9 you can also preload apps for all your deployments using Apple Configurator 2, saving network bandwidth and time.

Volume Purchase Program

VPP gives institutions a simple way to purchase iOS apps in volume and distribute them using MDM or Apple Configurator 2 to students, teachers, administrators, and staff. Eligible institutions—including any K–12 institution or district or any accredited, degree-granting higher education institution—can purchase qualifying apps at a 50 percent discount on 20 units or more.

With iOS 9, you can install apps directly to devices without an Apple ID on the device—this capability dramatically simplifies deployment. You can also still distribute apps and book to users. iOS 9 makes it seamless to migrate apps from user-based to device-based distribution.

MDM solutions integrate with VPP, enabling your institution to purchase apps in volume and automatically assign them to specific users or groups. You can distribute free and paid apps over the air using 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 VPP: www.apple.com/ca/education/it/vpp

3. Deploy

Now that all your iPad devices are configured with settings, apps, you can start to distribute them. It's important to plan the logistics of handing out devices to students and staff, and some general recommendations are listed in the following section. In a one-to-one deployment, users will receive their own devices, while in shared deployments, devices will usually be placed in classroom carts.

Deployment events

Planning kickoff events to launch your deployment is critical. It is your institution's chance to reinforce the expectations of your community, including parents. These events can ensure the smooth handout of devices and help students get up and running before school begins.

The following considerations will help you plan deployment events for students, parents, and staff.

Plan deployment events and parent nights

One of the best ways to help get a large number of students and staff started with their devices is to hold kickoff events or parent nights. These events have multiple benefits:

- **Community education.** Deployment events can help your organization educate community members—including parents, guardians, and other stakeholders—on the vision and goals of the one-to-one initiative.
- **Parental consent.** Deployment events that involve parents are often referred to as parent nights, and they provide an efficient way to collect necessary parental consent. Your organization might also require additional consent and confirmation from parents, regardless of the age of the students.
- **Acceptable use policy.** Many school districts and universities have acceptable use policies for technology. Deployment events provide an opportunity to review such policies and to clearly communicate the responsibilities associated with your institution's initiative.
- **Distribution of devices.** A deployment event provides an efficient venue to distribute devices to students. It enables your organization to guide many users through the initial setup steps simultaneously and provide adequate support to ensure that users get up and running smoothly. If your organization will be holding parent nights, you might choose to distribute devices at those events, or you could hold separate deployment events to distribute devices directly to students. The benefit of distributing devices to students while parents are present is that you can communicate the importance of parental involvement in the initiative.
- **Configuration of devices.** Once your organization has MDM, VPP, and DEP in place, your iOS devices can be automatically configured when first used. A deployment event helps your organization confirm that all necessary user actions and all setup steps have taken place.

Determine deployment event participants

A deployment event is a great place for the community to come together. Invite all stakeholders to the event. Depending on your deployment, you might choose to invite students, parents, faculty, and/or staff to various events.

- **K–12 students.** Invite both parents and students to K–12 deployment events.
- **Higher education students.** If your organization is deploying devices to college or graduate students, the users themselves should be invited to deployment events.
- **Faculty and staff.** If your organization is deploying devices to faculty or staff, make sure they are invited to deployment events.

Scheduling deployment events

Depending on the number of users, you might need to schedule multiple events over a period of time. Many one-to-one deployments are initiated at the beginning of the school year in the fall. Parent nights and device distribution should occur before devices are required for learning. If students are expected to use devices for daily learning activities starting on the first day of school, then it is important to schedule deployment events over the summer break.

Deployment event staffing

To help both users and parents with any issues, plan to have sufficient staff on hand at the events. These individuals can be specialists, IT integrators, teachers, or others who are familiar with the deployment process and can provide hands-on assistance to students and parents.

Create a deployment event walk-through presentation

When distributing devices, it is beneficial to walk as many users as possible through the setup process to ensure that they can successfully complete each step. A great tool to facilitate this is a Keynote presentation that shows a screenshot for each step in the process, allowing users to follow along.

4. Manage

Teachers and admins can manage devices and content right in the classroom, and iOS devices that are configured and enrolled in MDM can be managed wirelessly from anywhere. In addition, remote management tasks such as reassigning apps, querying devices, and resetting device passwords are simplified with MDM.

Commands

An MDM server can perform a wide variety of administrative commands on devices that are managed, 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. Enhancements to the MDM protocol in iOS 9 provide new ways to secure and control devices in the classroom. For example, you can now install and manage apps even if student access to the App Store is restricted.

Queries

An MDM server can query devices for a variety of information, including hardware information, such as serial number, device UDID, or Wi-Fi MAC address; as well as 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.

Managing assessments

A device used for assessment should provide an easy way to limit a test taker to a single assessment app, and to disable hardware or software features that allow a test taker to circumvent the assessment and invalidate the results. iOS devices that are supervised and enrolled in MDM can use Single App Mode (SAM) or Autonomous Single App Mode (ASAM) to lock an iOS device to a single app. iOS includes a number of features—such as spell checking, auto-correction, grammar checking, and dictionary lookup—that can be temporarily disabled by MDM during an assessment. Your organization can configure your devices for these settings. Also, a number of MDM vendors offer teacher tools that allow teachers to send these commands right from their own iPad devices.

Learn more about about assessment with iPad: www.apple.com/education/ipad/resources/

Updating and deploying additional apps

After devices are deployed, you can install additional apps directly to them. If the App Store is disabled, you can still install apps using MDM, ensuring that your users get the appropriate apps.

AirPlay and Apple TV

Using AirPlay, teachers and students can wirelessly stream content from an iPad (or a Mac) to a classroom projector or an HDTV via Apple TV. MDM can prompt students to mirror their device on a specific Apple TV, so they can present to the entire class without complex configurations. 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 devices can stream content from an iOS device to Apple TV, even if the devices are on different networks. Peer-to-peer AirPlay lets a user connect directly from a supported iOS device to Apple TV without first connecting to your network. This capability eliminates the need to join the right network or disclose Wi-Fi passwords, and it prevents reachability issues in complex network environments.

Updating iOS remotely

Once devices are running iOS 9, you can use MDM to remotely update future versions of iOS.

Note: This capability is restricted to devices without pass codes.

Personalizing devices

After you've prepared your infrastructure and set up your iPad devices, you can prepare for device personalization. In one-to-one deployments, users can personalize their devices with their own Apple ID to access key Apple services, such as iCloud and iTunes U. Understanding Apple IDs will help you inform your users about how to set up their Apple ID.

Apple ID

An Apple ID is an identity used to log in to Apple services such as the iBooks Store, iTunes U, 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 schoolwork travels with them no matter which computer or device they use. Whether installing apps assigned by school, backing up homework to iCloud, or downloading a book, students can use their Apple ID to own their learning—and their content—even when they leave school.

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, which are 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

iTunes U

iTunes U makes the world's largest collection of free education content—including public courses and collections from leading schools, universities, museums, and cultural institutions—accessible to students.

With iTunes U, instructors can bring their classroom together on iPad. Instructors can build lessons with apps and their own materials, collect and grade assignments from students, hold one-on-one or group discussions, and annotate PDF assignments.

Learn more about iTunes U: www.apple.com/ca/education/ipad/itunes-u

Accessibility

iOS is the world's most advanced—and most accessible—mobile operating system. Students with special needs can use innovative features such as VoiceOver, Switch Control, and Guided Access to help them take advantage of what iPad has to offer.

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. It 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, as well as troubleshooting and issue isolation for iOS devices.

AppleCare for iOS devices

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

iOS 9 brings a new way to deploy iPad with one set of tools to streamline setup and content management. Whether your institution deploys iPad devices to an entire school district, a university, or a single classroom, you can deploy and manage them with the Apple Deployment Programs and MDM.

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

© 2015 Apple Inc. All rights reserved. Apple, the Apple logo, AirPlay, Apple TV, Bonjour, iBooks, iPad, iPhone, iPod touch, iTunes, iTunes U, Keychain, Keynote, Mac, the Mac logo, and OS X are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc. Apple Store, AppleCare, iCloud, and iTunes Store are service marks of Apple Inc., registered in the U.S. and other countries. App Store and iBooks Store are service marks of Apple Inc. Some products or promotions are not available outside the U.S. Product specifications are subject to change. Some features and applications are not available in all areas. Application availability and pricing are subject to change. September 2015